Μια Εισαγωγη στη Βασικη Αλγεβρα

Αποστολος Μπεληγιαννης

Απόστολος Μπεληγιάννης

Καθηγητής
Πανεπιστήμιο Ιωαννίνων

Μια Εισαγωγή στη Βασική Άλγεβρα

Ιωαννινα
Δεκεμβριος 2015

Μια Εισαγωγή στη Βασική Άλγεβρα

Συγγραφή

Απόστολος Μπεληγιάννης

Κριτικός αναγνώστης

Νικόλαος-Θεοδόσιος Μαρμαρίδης

Συντελεστές έκδοσης

Γλωσσική Επιμέλεια: Δημήτρης Κονάχος

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ

Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

http://www.kallipos.gr

ISBN: 978-960-603-262-2

Στη Χριστίνα και στον Δημήτρη

Περιεχόμενα

Πρόλογος

Το παρόν βιβλίο αποτελεί μια εισαγωγή στις έννοιες και μεθόδους της βασικής Άλγεβρας. Ειδικότερα, το κείμενο επικεντρώνεται στην μελέτη δύο εκ των θεμελιωδέστερων δομών στις οποίες βασίζεται η σύγχρονη Άλγεβρα: στη δομή της ομάδας και στη δομή του δακτυλίου. Το κείμενο χωρίζεται σε δύο θεματικά μέρη και σε 11 Κεφάλαια, εκτός της Εισαγωγής (Κεφάλαιο 0). Το πρώτο θεματικό μέρος είναι αφιερωμένο στη στοιχειώδη Θεωρία Ομάδων και αποτελείται από τα Κεφάλαια 1-6, και το δεύτερο θεματικό μέρος είναι αφιερωμένο στη στοιχειώδη Θεωρία Δακτυλίων και αποτελείται από τα Κεφάλαια 7-11.

Στο εισαγωγικό κεφάλαιο (Κεφάλαιο 0) του κειμένου υπενθυμίζουμε, ως επί το πλείστον χωρίς αποδείξεις, βασικές έννοιες και αποτελέσματα από τη θεωρία συνόλων και απεικονίσεων, της αριθμητικής των ακεραίων αριθμών, της Μαθηματικής Επαγωγής, και των μιγαδικών αριθμών. Επίσης δίνονται παραδείγματα και σταθεροποιούμε συμβολισμό ο οποίος θα είναι εν χρήσει καθ' όλη τη διάρκεια των σημειώσεων.

Το πρώτο μέρος του κειμένου, το οποίο είναι αφιερωμένο στη στοιχειώδη Θεωρία Ομάδων, ξεκινά με το πρώτο Κεφάλαιο στο οποίο αναπτύσσεται η βασική θεωρία σχέσεων ισοδυναμίας, συνόλων πηλίκο, (διμελών) πράξεων και μονοειδών. Οι έννοιες οι οποίες εισάγονται στο πρώτο Κεφάλαιο αποτελούν τη βάση για περισσότερο σύνθετες έννοιες οι οποίες είναι αντικείμενο των υπόλοιπων Κεφαλαίων. Έχει όμως καταβληθεί προσπάθεια η ανάπτυξη των επόμενων Κεφαλαίων να είναι ανεξάρτητη των περισσότερων εννοιών και αποτελεσμάτων του πρώτου Κεφαλαίου, κυρίως των αποτελεσμάτων τα οποία αφορούν τη θεωρία μονοειδών. Στο δεύτερο Κεφάλαιο εισάγεται η έννοια της ομάδας, μελετώνται οι κυριότερες ιδιότητες ομάδων, και δίνονται παραδείγματα. Αναλύεται η έννοια της υποομάδας, ο πίνακας Cayley μιας ομάδας, η έννοια της κανονικής υποομάδας, και επίσης εισάγονται διάφορες κατασκευές νέων ομάδων από παλαιές ομάδες (τομή, ευθύ γινόμενο, υποομάδα η οποία παράγεται από υποσύνολο κλπ.). Τέλος, εισάγεται η θεμελιώδης έννοια του ισομορφισμού ομάδων η οποία μας επιτρέπει την ταύτιση ομάδων με ταυτόσημες δομικές ιδιότητες. Το τρίτο Κεφάλαιο είναι αφιερωμένο στην έννοια της τάξης στοιχείου και ομάδας και στη θεωρία πλευρικών κλάσεων μιας υποομάδας σε μια ομάδα. Το κεντρικό αντικείμενο του τρίτου Κεφαλαίου αποτελεί το Θεώρημα του Lagrange και οι εφαρμογές του στη θεωρία πεπερασμένων ομάδων. Στο τέταρτο Κεφάλαιο αναλύεται η δομή των κυκλικών ομάδων. Οι κυκλικές ομάδες είναι η πλέον απλή μη τετριμμένη κλάση ομάδων και τα αποτελέσματα του τέταρτου Κεφαλαίου περιγράφουν πλήρως τη δομή τους. Στο πέμπτο Κεφάλαιο μελετάται η σημαντική κλάση των ομάδων μεταθέσεων επί ενός συνόλου και αναπτύσσεται η βασική τους θεωρία. Οι ομάδες μεταθέσεων αποτέλεσαν ιστορικά ένα από τα πρώτα παραδείγματα ομάδων, και έκτοτε η σπουδαιότητα τους οφείλεται στο ότι κάθε ομάδα μπορεί να υλοποιηθεί ως ομάδα μεταθέσεων κατάλληλου συνόλου, και επιπρόσθετα οι ομάδες μεταθέσεων ερμηνεύουν και περιγράφουν συμμετρίες οικείων γεωμετρικών σχημάτων. Στο έκτο και τελευταίο Κεφάλαιο του πρώτου μέρους του βιβλίου αναλύεται η έννοια της ομάδας πηλίκο ως προς μια κανονική υποομάδα. Το κεντρικό αντικείμενο του έκτου Κεφαλαίου αποτελούν τα Θεωρήματα Ισομορφισμών Ομάδων, και οι εφαρμογές τους στην μελέτη και ταξινόμηση ομάδων οι οποίες έχουν κοινές ή παρόμοιες δομικές ιδιότητες.

Το δεύτερο μέρος του κειμένου, το οποίο είναι αφιερωμένο στη στοιχειώδη Θεωρία Δακτυλίων, ξεκινά με το έβδομο Κεφάλαιο στο οποίο εισάγεται η έννοια του δακτυλίου και του υποδακτυλίου, αναπτύσσονται οι βασικές ιδιότητες δακτυλίων, αναλύονται διάφορες κατασκευές νέων δακτυλίων από παλαιούς (τομή υποδακτυλίων, ευθύ γινόμενο, υποδακτύλιος ο οποίος παράγεται από υποσύνολο, δακτύλιοι πολυωνύμων, δακτύλιοι πινάκων κλπ.), και δίνονται παραδείγματα επί των οποίων υλοποιούνται οι έννοιες οι οποίες εισάγονται στα επόμενα κεφάλαια. Το όγδοο Κεφάλαιο είναι αφιερωμένο στα ιδεώδη, στους δακτυλίους

πηλίκο, και στην ανάλυση των βασικών Θεωρημάτων Ισομορφισμών για δακτυλίους, και των εφαρμογών τους. Η έννοια του ιδεώδους είναι βασική στη μελέτη της δομής ενός δακτυλίου, καθώς η πολυπλοκότητα ενός δακτυλίου αντανακλάται στην πολυπλοκότητα της δομής των ιδεωδών του. Επιπρόσθετα, τα ιδεώδη μάς επιτρέπουν την κατασκευή του δακτυλίου πηλίκο ενός δακτυλίου ως προς ένα ιδεώδες, έννοιας η οποία είναι ανάλογη της έννοιας της ομάδας πηλίκο μιας ομάδας ως προς μια κανονική υποομάδα. Στο όγδοο Κεφάλαιο επίσης αναπτύσσουμε εφαρμογές των Θεωρημάτων Ισομορφισμών Δακτυλίων στη μελέτη και ταξινόμηση δακτυλίων οι οποίοι έχουν κοινές ή παρόμοιες δομικές ιδιότητες. Στο ένατο Κεφάλαιο αναπτύσσεται η βασική θεωρία της σημαντικής κλάσης των πολυωνυμικών δακτυλίων, η οποία, μεταξύ άλλων, μας επιτρέπει την παράσταση και κατασκευή νέων δακτυλίων από παλαιούς. Επίσης αναλύουμε την κατασκευή του σώματος κλασμάτων μιας ακέραιας περιοχής, και αναπτύσσουμε τις εφαρμογές του στην κατασκευή και μελέτη σωμάτων ρητών συναρτήσεων. Στο δέκατο Κεφάλαιο μελετώνται οι κύριες ιδιότητες πρώτων και μεγιστοτικών ιδεωδών ενός δακτυλίου. Τα πρώτα και μεγιστοτικά ιδεώδη αποτελούν τις σημαντικότερες κλάσεις ιδεωδών ενός δακτυλίου και έχουν εφαρμογές σε άλλα πεδία, όπως για παράδειγμα στη Γεωμετρία. Στο ενδέκατο και τελευταίο Κεφάλαιο του κειμένου αναπτύσσεται η βασική θεωρία δακτυλίων κυρίων ιδεωδών, Ευκλείδειων περιοχών, και περιοχών μονοσήμαντης ανάλυσης. Οι Ευκλείδειες περιοχές, οι περιοχές κυρίων ιδεωδών και οι περιοχές μονοσήμαντης ανάλυσης, με αύξουσα σειρά γενικότητας και πολυπλοκότητας, αποτελούν σημαντικές μη τετριμμένες κλάσεις μεταθετικών δακτυλίων με σχετικά ομαλή δομή οι οποίες τυποποιούν σε γενικότερα πλαίσια ιδιότητες, π.χ. διαιρετότητα, του δακτυλίου των ακεραίων αριθμών και του δακτυλίου πολυωνύμων με συντελεστές από ένα σώμα.

Το κείμενο συμπληρώνεται με δύο Παραρτήματα στα οποία αναλύονται εν συντομία περισσότερο σύνθετα θέματα. Στο Παράρτημα Α΄ προσδιορίζονται τα μεγιστοτικά ιδεώδη του δακτυλίου των συνεχών πραγματικών συναρτήσεων ορισμένων επί ενός κλειστού διαστήματος της πραγματικής ευθείας, και στο Παράρτημα Β΄ χαρακτηρίζονται οι μεταθετικοί δακτύλιοι οι οποίοι είναι περιοχές κυρίων ιδεωδών με βάση την ύπαρξη σταθμών ειδικού τύπου.

Στο κείμενο δίνεται έμφαση σε παραδείγματα, εφαρμογές και λυμένες ασκήσεις, οι οποίες βοηθούν στην πληρέστερη κατανόηση της εκτεθείσας θεωρίας, και επίσης στο τέλος κάθε κεφαλαίου παρατίθενται μια σειρά προτεινόμενων ασκήσεων προς λύση για τον αναγνώστη. Συνολικά περιέχονται στο κείμενο περίπου 490 άλυτες ασκήσεις. Στον αναγνώστη συστήνεται να κατανοήσει σε βάθος την απαιτούμενη θεωρία και, αφού μελετήσει τις μεθόδους οι οποίες χρησιμοποιούνται στην ανάλυση εφαρμογών και παραδειγμάτων του κειμένου, να προσπαθήσει να λύσει όσο το δυνατόν μεγαλύτερο αριθμό ασκήσεων από αυτές οι οποίες προτείνονται προς λύση στο τέλος κάθε κεφαλαίου. Στο τέλος του κειμένου παρατίθεται ενδεικτική βιβλιογραφία η οποία χρησιμοποιήθηκε στη συγγραφή των σημειώσεων και η οποία μπορεί να αποτελέσει βάση για μια περαιτέρω μελέτη των κύριων στοιχείων της Σύγχρονης Άλγεβρας από τον ενδιαφερόμενο αναγνώστη.

Στο κείμενο θεωρούμε γνωστές στοιχειώδεις έννοιες και αποτελέσματα, καθώς και συμβολισμούς από τα σύνολα και τη θεωρία διαιρετότητας ακεραίων, όπως αυτά υπενθυμίζονται στο εισαγωγικό κεφάλαιο 0. Επιπρόσθετα, υποθέτουμε ότι ο αναγνώστης έχει οικειότητα με τα συνήθη σύνολα αριθμών: το σύνολο $\mathbb{N}$ των φυσικών αριθμών, το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών, το σύνολο $\mathbb{Q}$ των ρητών αριθμών, το σύνολο $\mathbb{R}$ των πραγματικών αροθμών, και το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών.

Διδακτική Πορεία. Το βιβλίο περιέχει υλικό το οποίο υπερβαίνει κατά πολύ, ό,τι μπορεί να διδαχθεί σε ένα εισαγωγικό μάθημα βασικής Άλγεβρας σε ένα Τμήμα Μαθηματικών Ελληνικού Πανεπιστημίου. Για μια πρώτη αναγνωστική, αντίστοιχα διδακτική, προσέγγιση του αναγνώστη, αντίστοιχα του διδάσκοντα, στο υλικό το οποίο περιέχεται στο παρόν βιβλίο, συστήνεται η ακόλουθη διδακτική πορεία: Εξοικείωση με το συμβολισμό που ακολουθείται στο βιβλίο και με τις προκαταρκτικές έννοιες που περιλαμβάνονται στο εισαγωγικό Κεφάλαιο 0. Από το Κεφάλαιο 1, οι ενότητες 1.1, 1.2, και 1.3. Από το Κεφάλαιο 2, οι ενότητες 2.1, 2.2, 2.3, 2.4, και 2.6. Από το Κεφάλαιο 3, οι ενότητες 3.1, 3.2, 3.3, και 3.4. Από το Κεφάλαιο 4, η ενότητα 4.1, με πιθανή εξαίρεση την υποενότητα 4.1.3. Από το Κεφάλαιο 5, οι ενότητες 5.1, 5.2, και 5.3. Από το Κεφάλαιο 6, οι ενότητες 6.1, 6.2, 6.3, 6.4, και 6.5, με πιθανή εξαίρεση τις υποενότητες 6.1.2, 6.1.4, 6.3.5, 6.4.1, και 6.5.2. Από το Κεφάλαιο 7, οι ενότητες 7.1, 7.2, 7.3, 7.4, και 7.5. Από το Κεφάλαιο 8, οι ενότητες 8.1, 8.2, 8.3, και 8.4, με πιθανή εξαίρεση τις υποενότητες 8.1.3, 8.2.3, και 8.4.3. Από το Κεφάλαιο 9, οι ενότητες 9.1, 9.2, και 9.4. Από το Κεφάλαιο 10, οι ενότητες 10.1 και 10.2, με πιθανή εξαίρεση την υποενότητα 10.1.2. Τέλος από το Κεφάλαιο 11, η ενότητα 11.1. Από τις υπόλοιπες υποενότητες μπορούν να αντληθούν επιλεγμένα στοιχεία.

Ευχαριστώ θερμά τον κριτικό αναγνώστη Νικόλαο-Θεοδόσιο Μαρμαρίδη, Ομότιμο Καθηγητή του Πανεπιστημίου Ιωαννίνων, για τις ουσιαστικές παρατηρήσεις του οι οποίες συνέβαλαν αισθητά στην βελτίωση του βιβλίου, καθώς και τον Δημήτρη Κονάχο, ο οποίος είχε τη γλωσσική επιμέλεια, για την εξαιρετική συνεισφορά του στην αρτιότερη παρουσίαση του κειμένου.

Απόστολος Μπεληγιάννης
Ιωάννινα, Δεκέμβριος 2015

Κεφάλαιο 0

Προκαταρκτικές Έννοιες: Σύνολα και Αριθμοί

Στο παρόν εισαγωγικό Κεφάλαιο, υπενθυμίζουμε, κατά κύριο λόγο χωρίς αποδείξεις, βασικές γνώσεις από: τη στοιχειώδη θεωρία συνόλων και απεικονίσεων, την αριθμητική των φυσικών αριθμών, συμπεριλαμβανομένης της Αρχής Μαθηματικής Επαγωγής και των ισοδυνάμων της, την διαιρετότητα των ακεραίων αριθμών, και τις στοιχειώδεις ιδιότητες των μιγαδικών αριθμών. Επίσης εισάγουμε συμβολισμό ο οποίος θα είναι εν χρήσει καθ' όλη τη διάρκεια των σημειώσεων.

0.1 Σύνολα

Στη βάση των σύγχρονων Μαθηματικών βρίσκεται η έννοια του συνόλου. Στις παρούσες σημειώσεις δεν θα προσπαθήσουμε να ορίσουμε αυστηρά την έννοια του συνόλου, η οποία είναι πρωταρχική έννοια, αλλά θα ακολουθήσουμε τον μη αυστηρό ορισμό σύμφωνα με τον οποίο ένα **σύνολο** είναι μια συλλογή καλά ορισμένων και διακεκριμένων αντικειμένων, τα οποία μπορεί να σχετίζονται ή να μην σχετίζονται μεταξύ τους. Υποθέτουμε ότι ο αναγνώστης έχει μια στοιχειώδη οικειότητα με τα συνόλα και τις βασικές ιδιοτήτες τους, κάποιες από τις οποίες θα επαναλάβουμε εδώ χάριν ευκολίας του αναγνώστη και για να σταθεροποιήσουμε συμβολισμό ο οποίος θα είναι εν χρήσει καθ' όλη τη διάρκεια του κειμένου που ακολουθεί. Ιδιαίτερα θεωρούμε γνωστές τις έννοιες της συνεπαγωγής «$\Longrightarrow$» ή «$\Longleftarrow$», της έννοιας της ισοδυναμίας «$\Longleftrightarrow$», της έννοιας του ποσοδείκτη *για κάθε* «$\forall$», και της έννοιας του *υπάρχει* «$\exists$», μεταξύ μαθηματικών αντικειμένων ή μαθηματικών προτάσεων.

0.1.1 Σύνολα Αριθμών

Από τώρα και στο εξής θα χρησιμοποιούμε τα εξής οικεία σύμβολα:

$$\mathbb{N} = \{1, 2, \cdots, n, \cdots\}, \qquad \mathbb{N}_0 = \{0, 1, 2, \cdots, n, \cdots\}, \qquad \mathbb{N}_n = \{1, 2, \cdots, n\}$$

$$\mathbb{Z} = \{\cdots, -n, \cdots, -1, 0, 1, \cdots, n, \cdots, \}, \qquad \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$$

για τα σύνολα: $\mathbb{N}$ των φυσικών αριθμών, $\mathbb{N}_0$ των φυσικών αριθμών μαζί με το 0, $\mathbb{N}_n$ των n πρώτων φυσικών αριθμών, $\mathbb{Z}$ των ακεραίων αριθμών, και $\mathbb{Q}$ των ρητών αριθμών.

Επιπρόσθετα συμβολίζουμε με $\mathbb{R}$ το σύνολο των πραγματικών αριθμών και με $\mathbb{C}$ το σύνολο των μιγαδικών αριθμών, και θεωρούμε γνωστές τις βασικές στοιχειώδεις ιδιότητες των συνόλων αριθμών: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$.

0.1.2 Βασικές Έννοιες

Έστω X ένα σύνολο, το οποίο αποτελείται από αντικείμενα $a, b, c, \cdots$. Θα γράφουμε $a \in X$, υποδηλώνοντας ότι το αντικείμενο a είναι στοιχείο του συνόλου X ή ότι το αντικείμενο a ανήκει στο σύνολο X. Αν ένα

αντικείμενο a δεν ανήκει στο σύνολο X, θα γράφουμε $a \notin X$. Δύο σύνολα X και Y είναι ίσα, και τότε θα γράφουμε $X = Y$, αν κάθε στοιχείο του X είναι και στοιχείο του Y και κάθε στοιχείο του Y είναι και στοιχείο του X, δηλαδή αν: $\forall x \in X \Longrightarrow x \in Y$ και $\forall y \in Y \Longrightarrow y \in X$. Αν τα σύνολα X και Y δεν είναι ίσα, θα γράφουμε $X \neq Y$. Ένα σύνολο Y είναι **υποσύνολο** του συνόλου X, και τότε θα γράφουμε $Y \subseteq X$ ή $Y \subsetneqq X$ (σπανιότερα $X \supseteq Y$ ή $X \supsetneqq Y$), αν κάθε στοιχείο y του Y είναι και στοιχείο του X, δηλαδή αν: $y \in Y \Longrightarrow y \in X$. Αν το σύνολο Y είναι υποσύνολο του X και $Y \neq X$, θα λέμε ότι το Y είναι **γνήσιο υποσύνολο** του X και θα γράφουμε $Y \subset X$ ή $Y \subsetneq X$ ή $Y \subsetneqq X$. Σύμφωνα με αυτή την ορολογία, θα έχουμε: $X = Y$ αν και μόνο αν $Y \subseteq X$ και $X \subseteq Y$. Το **κενό σύνολο** είναι το σύνολο το οποίο δεν περιέχει κανένα στοιχείο, συμβολίζεται με $\emptyset$ και είναι υποσύνολο κάθε συνόλου. Ένα σύνολο X καλείται *μη κενό*, αν περιέχει τουλάχιστον ένα στοιχείο, και τότε θα γράφουμε $X \neq \emptyset$. Ένα σύνολο μπορεί να καθοριστεί με πολλούς τρόπους, για παράδειγμα με αναγραφή των στοιχείων του (συνήθως όταν περιέχει πεπερασμένο πλήθος στοιχείων) ή με χρήση κάποιας ιδιότητας (ή συνόλου ιδιοτήτων) την οποία ικανοποιούν τα στοιχεία του συνόλου. Έτσι, αν το σύνολο X αποτελείται από ένα πεπερασμένο πλήθος στοιχείων, έστω $x_1, x_2, \cdots, x_n$, τότε θα γράφουμε:

$$X = \{x_1, x_2, \cdots, x_n\}$$

Παρόμοια, αν P είναι μια ιδιότητα η οποία αφορά κάποια μαθηματικά ή μη αντικείμενα, τα οποία συνήθως είναι στοιχεία ενός συνόλου A, τότε το σύνολο όλων των αντικειμένων του συνόλου A, τα οποία ικανοποιούν την ιδιότητα P, θα συμβολίζεται με

$$X = \{x \in A \mid \text{το } x \text{ ικανοποιεί την ιδιότητα } P\}$$

Αν τα αντικείμενα τα οποία ικανοποιούν την ιδιότητα P δεν είναι στοιχεία κάποιου μεγαλύτερου συνόλου, τότε θα γράφουμε $X = \{x \mid \text{το } x \text{ ικανοποιεί την ιδιότητα } P\}$. Για παράδειγμα, αν $\mathbb{N} = \{1, 2, \cdots, n, n+1, \cdots\}$ είναι το σύνολο των θετικών ακεραίων ή φυσικών αριθμών, τότε το σύνολο το οποίο αποτελείται από όλους τους φυσικούς αριθμούς οι οποίοι είναι το πολύ ίσοι με 5 είναι $X = \{1, 2, 3, 4, 5\}$. Αν X είναι το σύνολο το οποίο αποτελείται από όλους τους θετικούς ακέραιους αριθμούς της μορφής $2n$, όπου n είναι τυχών θετικός αριθμός, τότε $X = \{a \in \mathbb{N} \mid \text{ο } a \text{ είναι άρτιος}\}$. Αν $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$ είναι το σύνολο των ακεραίων αριθμών, τότε το σύνολο των θετικών ακεραίων ή φυσικών αριθμών είναι: $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\} = \{1, 2, \cdots, n, \cdots\}$.

0.1.3 Πράξεις και Κατασκευές Συνόλων

Αν X είναι σύνολο, τότε το **δυναμοσύνολο** του συνόλου X ορίζεται να είναι το σύνολο όλων των υποσυνόλων του συνόλου X, και συμβολίζεται με $\mathscr{P}(X)$:

$$\mathscr{P}(X) = \{A \mid A \subseteq X\}$$

Το δυναμοσύνολο $\mathscr{P}(X)$ περιέχει πάντοτε ως στοιχεία του το κενό σύνολο $\emptyset$ και το σύνολο X.

Έστω ότι X είναι ένα σύνολο και ότι A και B είναι δύο υποσύνολα του X. Η **τομή** $A \cap B$ των υποσυνόλων A και B ορίζεται να είναι το σύνολο όλων των στοιχείων του X τα οποία ανήκουν στο A και στο B:

$$A \cap B = \{x \in X \mid x \in A \text{ και } x \in B\}$$

Τα υποσύνολα A και B καλούνται **ξένα** αν $A \cap B = \emptyset$. Η **ένωση** $A \cup B$ των υποσυνόλων A και B ορίζεται να είναι το σύνολο όλων των στοιχείων του X τα οποία ανήκουν είτε στο A είτε στο B:

$$A \cup B = \{x \in X \mid x \in A \text{ ή } x \in B\}$$

Η ένωση $A \cup B$ των υποσυνόλων A και B καλείται **ξένη ένωση**, αν: $A \cap B = \emptyset$.

Για την τομή και την ένωση υποσυνόλων ενός συνόλου ισχύουν οι εξής σχέσεις γνωστές ως Νόμοι του De Morgan.

Πρόταση 0.1.1 (Νόμοι του De Morgan). [1] *Αν A, B, και C είναι υποσύνολα ενός συνόλου X, τότε:*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{και} \quad A \cup (B \cap C) = A \cup B) \cap (A \cup C)$$

[1] Augustus De Morgan (27 Ιουνίου 1806 - 18 Μαρτίου 1871) [https://en.wikipedia.org/wiki/Augustus_De_Morgan]: Βρετανός μαθηματικός και θεωρητικός της Λογικής. Γνωστός για τους νόμους που φέρουν το όνομά του.

Έστω ότι A και B είναι δύο υποσύνολα ενός συνόλου X. Η **διαφορά** $A \setminus B$ **των συνόλων** A και B ορίζεται να είναι το σύνολο των στοιχείων του A τα οποία δεν ανήκουν στο B:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

Αν $B \subseteq A$, τότε η διαφορά $A \setminus B$ καλείται το **συμπλήρωμα** του B στο A.

Έστω I ένα σύνολο με στοιχεία $i, j, k, \cdots$. Έστω $\mathscr{A}$ μια συλλογή ή οικογένεια συνόλων, δηλαδή ένα σύνολο $\mathscr{A}$ τα στοιχεία του οποίου είναι επίσης σύνολα. Το σύνολο I καλείται **σύνολο δεικτών** για την οικογένεια συνόλων $\mathscr{A}$, αν για κάθε στοιχείο $i \in I$ υπάρχει ένα σύνολο A_i το οποίο ανήκει στην οικογένεια $\mathscr{A}$. Τότε θα γράφουμε $\mathscr{A} = \{A_i\}_{i \in I}$. Αν το σύνολο δεικτών I για την οικογένεια συνόλων $\mathscr{A}$ είναι πεπερασμένο, για παράδειγμα αν $I = \{1, 2, \cdots, n\}$, τότε $\mathscr{A} = \{A_i\}_{i \in I} = \{A_1, A_2, \cdots, A_n\}$. Για παράδειγμα, δύο σύνολα A_1 και A_2 αποτελούν τα στοιχεία μιας οικογένειας συνόλων $\{A_1, A_2\}$ όπου $I = \{1, 2\}$. Όπως και στην περίπτωση δύο υποσυνόλων ενός συνόλου, έτσι και στην περίπτωση μιας οικογένειας υποσυνόλων $\mathscr{A} = \{A_i\}_{i \in I}$ ενός συνόλου X, όπου I είναι ένα μη κενό σύνολο δεικτών, μπορούμε να ορίσουμε την έννοια της τομής και ένωσης των συνόλων της οικογένειας, ως εξής. Η **τομή** $\cap_{i \in I} A_i$ **της οικογένειας συνόλων** $\mathscr{A}$ ορίζεται να είναι το σύνολο

$$\bigcap_{i \in I} A_i = \{x \in X \mid x \in A_i,\ \forall i \in I\}$$

Η **ένωση** $\cup_{i \in I} A_i$ **της οικογένειας συνόλων** $\mathscr{A}$ ορίζεται να είναι το σύνολο

$$\bigcup_{i \in I} A_i = \{x \in X \mid \exists i \in I : x \in A_i\}$$

Η ένωση $\cup_{i \in I} A_i$ της οικογένειας υποσυνόλων $\mathscr{A} = \{A_i\}_{i \in I}$ ενός συνόλου X καλείται **ξένη ένωση**, αν για κάθε $i, j \in I$: $i \neq j \Longrightarrow A_i \cap A_j = \emptyset$.

Αν το σύνολο I είναι πεπερασμένο, έστω για παράδειγμα $I = \{1, 2, \cdots, n\}$, τότε θα γράφουμε:

$$\bigcap_{i \in I} A_i = \bigcap_{i=1}^{n} A_i = A_1 \bigcap A_2 \bigcap \cdots \bigcap A_n \quad \text{και} \quad \bigcup_{i \in I} A_i = \bigcup_{i=1}^{n} A_i = A_1 \bigcup A_2 \bigcup \cdots \bigcup A_n$$

Παρόμοια μπορουμε να ορίσουμε την τομή $\cap_{A \in \mathscr{K}} A$ και την ένωση $\cup_{A \in \mathscr{K}} A$ μιας οικογένειας υποσυνόλων $\mathscr{K} \subseteq \mathscr{P}(X)$ ενός συνόλου X ως εξής:

$$\bigcap_{A \in \mathscr{K}} A = \{x \in X \mid \forall A \in \mathscr{K} :\ x \in A\} \quad \text{και} \quad \bigcup_{A \in \mathscr{K}} A = \{x \in X \mid \exists A \in \mathscr{K} :\ x \in A\}$$

Έστω A και B δύο (μη κενά) σύνολα. Το (**καρτεσιανό**) **γινόμενο** $A \times B$ των συνόλων A και B ορίζεται να είναι το σύνολο όλων των διατεταγμένων ζευγών (a, b), όπου $a \in A$ και $b \in B$:

$$A \times B = \{(a, b) \mid a \in A \text{ και } b \in B\}$$

και όπου δύο διατεταγμένα ζεύγη $(a, b), (c, d) \in A \times B$ θεωρούνται ίσα, $(a, b) = (c, d)$, αν: $a = c$ και $b = d$.

Έτσι, για παράδειγμα, αν $A = \{1, 2, 3\}$ και $B = \{a, b\}$, τότε $A \times B = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.

Γενικεύοντας, αν $A_1, A_2, \cdots, A_n$ είναι n το πλήθος σύνολα, τότε το (**καρτεσιανό**) **γινόμενο** $\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n$ των συνόλων A_i, $1 \leq i \leq n$, ορίζεται να είναι το σύνολο όλων των διατεταγμένων n-άδων $(a_1, a_2, \cdots, a_n)$, όπου $a_i \in A_i$, $1 \leq i \leq n$:

$$\prod_{i=1}^{n} A_i = A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \cdots, a_n) \mid a_i \in A_i,\ 1 \leq i \leq n\}$$

και όπου δύο διατεταγμένες n-άδες $(a_1, a_2, \cdots, a_n)$, $(a'_1, a'_2, \cdots, a'_n) \in A \times B$ θεωρούνται ίσες, $(a_1, a_2, \cdots, a_n) = (a'_1, a'_2, \cdots, a'_n)$, αν: $a_i = a'_i$, $1 \leq i \leq n$.

0.2 Απεικονίσεις

Αν X είναι ένα μη κενό σύνολο, τότε μια **(διμελής) σχέση επί του** X είναι ένα υποσύνολο του καρτεσιανού γινομένου $X \times X$. Έστω X, Y δύο μη κενά σύνολα. Γενικεύοντας την έννοια της σχέσης επί ενός συνόλου, ορίζουμε μια **σχέση από το** X **στο** Y, ή μια *αντιστοιχία από το* X *στο* Y, να είναι ένα υποσύνολο του καρτεσιανού γινομένου $X \times Y$. Θα μας απασχολήσουν κυρίως οι ακόλουθες ειδικού τύπου σχέσεις από ένα σύνολο X σε ένα σύνολο Y:

Μια **απεικόνιση** $\mathscr{R}$ **από το** X **στο** Y είναι μια σχέση $\mathscr{R}$ από το X στο Y η οποία ικανοποιεί τις ακόλουθες ιδιότητες:

1. $\forall x \in X,\ \exists y \in Y\colon \quad (x,y) \in \mathscr{R}$.

2. $(x,y) \in \mathscr{R}$ και $(x,y') \in \mathscr{R} \implies y = y'$.

Δηλαδή, για κάθε $x \in X$ υπάρχει ακριβώς ένα στοιχείο $y \in Y$, έτσι ώστε $(x,y) \in \mathscr{R}$. Ισοδύναμα:

$$\forall x \in X,\ \exists y \in Y\colon\ (x,y) \in \mathscr{R} \quad \text{και} \quad (x,y_1),\ (x,y_2) \in \mathscr{R} \implies y_1 = y_2$$

Συνήθως μια απεικόνιση από το X στο σύνολο Y θα συμβολίζεται με ένα από τα παρακάτω σύμβολα:

$$f,\ g,\ h,\ \varphi,\ \psi,\ \cdots$$

Έστω $f \subseteq X \times Y$ μια απεικόνιση από το σύνολο X στο σύνολο Y. Τότε για κάθε $x \in X$, το μοναδικό, σύμφωνα με τον παραπάνω ορισμό, στοιχείο $y \in Y$, για το οποίο ισχύει $(x,y) \in f$, συμβολίζεται με $f(x) = y$, και η απεικόνιση f θα συμβολίζεται ως εξής:

$$f\colon X \longrightarrow Y,\quad x \longmapsto f(x)$$

Από τώρα και στο εξής θα χρησιμοποιούμε τον παραπάνω οικείο συμβολισμό για τις απεικονίσεις.

Έστω $f\colon X \longrightarrow Y$ μια απεικόνιση, και $A \subseteq X$ και $B \subseteq Y$ δύο υποσύνολα. Υπενθυμίζουμε ότι το υποσύνολο του Y

$$f(A) = \big\{y \in Y \mid \exists x \in A\colon y = f(x)\big\} = \big\{f(x) \in Y \mid x \in A\big\}$$

καλείται η **εικόνα** του A μέσω της f, και το υποσύνολο του X

$$f^{-1}(B) = \big\{x \in X \mid f(x) \in B\big\}$$

καλείται η **αντίστροφη εικόνα** του B μέσω της f. Ειδικότερα, θέτοντας $A = X$, έχουμε την **εικόνα** της f:

$$\mathsf{Im}(f) = f(X)$$

• ΠΟΤΕ ΔΥΟ ΑΠΕΙΚΟΝΙΣΕΙΣ ΕΙΝΑΙ ΙΣΕΣ; Επειδή ορίσαμε τις απεικονίσεις ως υποσύνολα καρτεσιανών γινομένων, δηλαδή ως τριάδες (X,Y,f), όπου $f \subseteq X \times Y$, διαπιστώνουμε ότι δύο απεικονίσεις (X,Y,f) και (X',Y',f'), δηλαδή $f\colon X \longrightarrow Y$ και $f'\colon X' \longrightarrow Y'$, είναι ίσες, και θα γράφουμε $f = f'$, αν και μόνο αν $(X,Y,f) = (X',Y',f')$, δηλαδή αν και μόνο αν $X = X', Y = Y'$ και τα υποσύνολα $f \subseteq X \times Y$ και $f' \subseteq X \times Y$ είναι ίσα. Το τελευταίο ιδιαίτερα σημαίνει ότι $f(x) = f'(x),\ \forall x \in X$. Επομένως, δύο απεικονίσεις $f, f'\colon X \longrightarrow Y$ είναι ίσες αν και μόνο αν $f(x) = f'(x),\ \forall x \in X$.

Τονίζουμε ιδιαίτερα ότι δύο απεικονίσεις $f\colon X \longrightarrow Y$ και $f'\colon Z \longrightarrow W$, όπου $X \neq Z$ ή $Y \neq W$, δεν είναι ποτέ ίσες. Για παράδειγμα, οι απεικονίσεις $f\colon \mathbb{N} \longrightarrow \mathbb{N},\ f(n) = 3n+5$, και $f'\colon \mathbb{N} \longrightarrow \mathbb{Z},\ f'(n) = 3n+5$ δεν είναι ίσες, μολονότι $f(n) = f'(n)$, για κάθε στοιχείο $n \in \mathbb{N}$.

Παράδειγμα 0.2.1. Για κάθε μη κενό σύνολο X, μπορούμε να θεωρήσουμε την **ταυτοτική** απεικόνιση

$$\mathsf{Id}_X\colon X \longrightarrow X,\ \ \mathsf{Id}_X(x) = x$$

η οποία ως υποσύνολο του $X \times X$ είναι η «διαγώνιος» $\mathsf{Id}_X = \big\{(x,x) \in X \times X \mid x \in X\big\}$. $\quad\surd$

Παράδειγμα 0.2.2. Έστω $S \subseteq X$ ένα υποσύνολο του συνόλου X. Τότε ορίζεται η **απεικόνιση έγκλεισης**

$$\iota_S \colon S \longrightarrow X, \quad \iota_S(s) = s$$

του υποσυνόλου S στο X. Παρατηρούμε ότι, αν και οι απεικονίσεις ι_S και Id_S ικανοποιούν τη σχέση $\iota_S(s) = s = \mathsf{Id}_S(s)$, $\forall s \in S$, δεν είναι ίσες. $\surd$

Παράδειγμα 0.2.3. Έστω X ένα μη κενό σύνολο, και $A \subseteq X$ ένα υποσύνολό του. Αν θέσουμε $\mathbf{2} = \{0,1\}$, τότε η **χαρακτηριστική συνάρτηση** του A ορίζεται να είναι η απεικόνιση

$$\chi_A \,:\, X \longrightarrow \mathbf{2}, \quad \chi_A(a) = \begin{cases} 1, & a \in A \\ 0, & a \notin A \end{cases} \quad \surd$$

Παράδειγμα 0.2.4. Έστω $f \colon X \longrightarrow Y$ μια απεικόνιση μεταξύ συνόλων. Αν $A \subseteq X$, είναι ένα μη κενό υποσύνολο του X, τότε ορίζεται η απεικόνιση

$$f|_A \colon A \longrightarrow Y, \quad f|_A(a) = f(a)$$

η οποία καλείται ο **περιορισμός της** f **στο υποσύνολο** A. Προφανώς $f|_A = f \circ \iota_A$. $\surd$

Κλείνουμε την παρούσα υποενότητα με παραδείγματα απεικονίσεων οι οποίες προκύπτουν με χρήση καρτεσιανών γινομένων συνόλων. Οι απεικονίσεις οι οποίες ορίζονται παρακάτω χαρακτηρίζονται μοναδικά από μια ιδιότητα.

Παράδειγμα 0.2.5. Έστω $\prod_{k=1}^{n} X_k := X_1 \times X_2 \times \cdots \times X_n$ το καρτεσιανό γινόμενο μιας πεπερασμένης οικογένειας $\{X_k\}_{k=1}^{n}$ μη κενών συνόλων. Τότε, για κάθε δείκτη $k = 1,2,\cdots,n$, ορίζεται η k-**οστή απεικόνιση-προβολής**

$$\pi_k \,:\, \prod_{k=1}^{n} X_k \;\longrightarrow\; X_k, \quad \pi_k(x_1, x_2, \cdots, x_n) = x_k$$

Η οικογένεια $\{\pi_k\}_{k=1}^{n}$ των απεικονίσεων-προβολών, ικανοποιεί την ακόλουθη ιδιότητα: *Αν A είναι ένα μη κενό σύνολο και $f_k \colon A \longrightarrow X_k$ είναι απεικονίσεις, $1 \le k \le n$, τότε υπάρχει μοναδική απεικόνιση $f \colon A \longrightarrow \prod_{k=1}^{n} X_k$, έτσι ώστε: $\pi_k \circ f = f_k$, $1 \le k \le n$.* Πράγματι οριζουμε μια απεικόνιση

$$f \colon A \longrightarrow \prod_{k=1}^{n} X_k, \quad f(a) = \big(f_1(a), f_2(a), \cdots, f_n(a)\big)$$

και τότε, $\forall k = 1,2,\cdots,n$:

$$\forall a \in A: \qquad (\pi_k \circ f)(a) = \pi_k(f(a)) = \pi_k\big(f_1(a), f_2(a), \cdots, f_n(a)\big) = f_k(a)$$

Άρα πράγματι $\pi_k \circ f = f_k$, $1 \le k \le n$. Έστω ότι $g \colon A \longrightarrow \prod_{k=1}^{n} X_k$ είναι μια άλλη απεικόνιση για την οποία ισχύει ότι $\pi_k \circ g = f_k$, $1 \le k \le n$. Για κάθε στοιχείο $a \in A$, θέτοντας $g(a) = (x_1, x_2, \cdots, x_n)$, θα έχουμε:

$$\pi_k(g(a)) = \pi_k(x_1, x_2, \cdots, x_n) \quad \Longrightarrow \quad f_k(a) = x_k, \quad 1 \le k \le n \quad \Longrightarrow \quad g(a) = \big(f_1(a), f_2(a), \cdots, f_n(a)\big), \quad \forall a \in A$$

Επομένως $g = f$. $\surd$

Παράδειγμα 0.2.6. Έστω $f_k \colon X_k \longrightarrow Y_k$, $1 \le k \le n$, μια οικογένεια απεικονίσεων. Τότε ορίζεται η **απεικόνιση-γινόμενο** $\prod_{k=1}^{n} f_k := f_1 \times f_2 \times \cdots \times f_k \colon \prod_{k=1}^{n} X_k \;\longrightarrow\; \prod_{k=1}^{n} Y_k$, ως εξής:

$$\prod_{k=1}^{n} f_k \,:\, \prod_{k=1}^{n} X_k \;\longrightarrow\; \prod_{k=1}^{n} Y_k, \quad \big(\prod_{k=1}^{n} f_k\big)(x_1, x_2, \cdots, x_n) = (f_1(x_1), f_2(x_2), \cdots, f_n(x_n))$$

Η απεικόνιση $\prod_{k=1}^n \colon \prod_{k=1}^n X_k \longrightarrow \prod_{k=1}^n Y_k$ ικανοποιεί τις σχέσεις $\pi_k^Y \circ \prod_{k=1}^n f_k = f_k \circ \pi_k^X$, $1 \le k \le n$, όπου $\pi_k^X \colon \prod_{k=1}^n X_k \longrightarrow X_k$ και $\pi_k^Y \colon \prod_{k=1}^n Y_k \longrightarrow U_k$ είναι οι αντίστοιχες απεικονίσεις προβολές, όπως στο Παράδειγμα 0.2.5. Πράγματι, για κάθε στοιχείο $x = (x_1, \cdots, x_n) \in \prod_{k=1}^n X_k$, και για κάθε $k = 1, 2, \cdots, n$, θα έχουμε:

$$(\pi_k^Y \circ \prod_{k=1}^n f_k)(x) = \pi_k^Y\big((\prod_{k=1}^n f_k)(x_1, \cdots, x_n)\big) = \pi_k^Y(f_1(x_1), \cdots, f_n(x_n)) = f_k(x_k) = f_k(\pi_k^X(x_1, \cdots, x_n) = (f_k \circ \pi_k^X)(x)$$

από όπου έπεται ότι: $\pi_k^Y \circ \prod_{k=1}^n f_k = f_k \circ \pi_k^X$, $1 \le k \le n$. Η απεικόνιση-γινόμενο $\prod_{k=1}^n f_k$ είναι η μοναδική η οποία ικανοποιεί τις παραπάνω σχέσεις διότι, αν $g \colon \prod_{k=1}^n X_k \longrightarrow \prod_{k=1}^n Y_k$ είναι μια άλλη απεικόνιση για την οποία ισχύει ότι: $\pi_k^Y \circ g = f_k \circ \pi_k^X$, $1 \le k \le n$, τότε για κάθε στοιχείο $x = (x_1, \cdots, x_n \in \prod_{k=1}^n X_k$ θα έχουμε:

αν $g(x) = (y_1, \cdots, y_n)$, τότε $\pi_k(g(x)) = \pi_k(y_1, \cdots, y_n) \implies f_k \pi_k^X(x) = y_k, \implies f_k(x_k) = y_k, \quad 1 \le k \le n$

δηλαδή $g(x_1, \cdots, x_n = (f_1(x_1, \cdots, f_n(x_n))$, και άρα $g = \prod_{k=1}^n f_k$. $\quad \surd$

Έστω $\mathscr{A} = \{A_i\}_{i \in I}$ μια οικογένεια συνόλων, όπου I είναι ένα σύνολο δεικτών. Μια I-**άδα στοιχείων** των συνόλων A_i, $i \in I$, είναι μια απεικόνιση $f \colon I \longrightarrow \cup_{i \in I} A_i$, έτσι ώστε $f(i) \in A_i$. Συνήθως μια I-άδα στοιχείων f συμβολίζεται με αναγραφή των τιμών της $f(i) := a_i \in A_i$ ως στοιχείων μιας ακολουθίας $(a_i)_{i \in I}$, όπου $a_i \in A_i$, $\forall i \in I$. Για παράδειγμα, αν $I = \{1, 2, 3\}$, και $f \colon I \longrightarrow A_1 \cup A_2 \cup A_3$ είναι μια I-άδα στοιχείων, τότε, θέτοντας $f(1) = a_1$, $f(2) = a_2$, και $f(3) = a_3$, μπορούμε να γράψουμε ισοδύναμα την f ως (a_1, a_2, a_3), δηλαδή ως μια τριάδα στοιχείων. Αν $I = \{1, 2, \cdots, n\}$, τότε μια I-άδα στοιχείων είναι απλώς μια n-άδα στοιχείων.

Το (**καρτεσιανό**) **γινόμενο** $\prod_{i \in I} A_i$ της οικογένειας συνόλων $\mathscr{A} = \{A_i\}_{i \in I}$, όπου I είναι ένα σύνολο δεικτών, ορίζεται να είναι το σύνολο όλων των I-άδων στοιχείων των συνόλων A_i, $i \in I$:

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} \mid a_i \in A_i, \ \forall i \in I\}$$

0.2.1 Η Άλγεβρα των Απεικονίσεων

Υπενθυμίζουμε ότι, αν $f \colon X \longrightarrow Y$ και $g \colon W \longrightarrow Z$ είναι απεικονίσεις και $Y = W$, τότε (και μόνο τότε) ορίζεται η «*σύνθεση*» των απεικονίσεων f και g ως το ακόλουθο υποσύνολο του $X \times Z$:

$$g \circ f = \{(x, z) \in X \times Z \mid (f(x), z) \in g \subseteq Y \times Z\}$$

Με άλλα λόγια $g \circ f$ είναι η απεικόνιση

$$g \circ f \colon X \longrightarrow Z, \quad (g \circ f)(x) = g(f(x))$$

Υπενθυμίζουμε επίσης ότι, αν $f \colon X \longrightarrow Y$, $g \colon Y \longrightarrow Z$, και $h \colon Z \longrightarrow W$ είναι απεικονίσεις, τότε ορίζονται οι συνθέσεις $h \circ (g \circ f)$ και $(h \circ g) \circ f$ και ισχύει

$$\text{Αν} \quad X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W \quad \text{τότε} \quad h \circ (g \circ f) = (h \circ g) \circ f \qquad \text{(προσεταιριστική ιδιότητα σύνθεσης)}$$

Πράγματι οι συνθέσεις $g \circ f$, $h \circ (g \circ f)$, και $h \circ g$, $(h \circ g) \circ f$ ορίζονται και $\forall x \in X$:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x)) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$$

Παρατηρούμε ότι:

$$\text{για κάθε απεικόνιση} \quad f \colon X \longrightarrow Y \quad \text{ισχύει ότι:} \quad \mathsf{Id}_Y \circ f = f \quad \& \quad f \circ \mathsf{Id}_X = f$$

Παρατήρηση 0.2.7. Αν $f,g\colon X\longrightarrow X$ είναι απεικονίσεις επί ενός συνόλου X, έτσι ώστε οι συνθέσεις $f\circ g$ και $g\circ f$ ορίζονται, γενικά οι απεικονίσεις $f\circ g$ και $g\circ f$ δεν είναι ίσες. Το μικρότερο σύνολο X στο οποίο μπορούμε να δούμε ότι $f\circ g\neq g\circ f$, είναι να θεωρήσουμε ένα σύνολο X με δύο στοιχεία: $X=\{a,b\}$. Τότε ορίζουμε απεικόνιση $f\colon X\longrightarrow X$, ως εξής: $f(a)=b$, $f(b)=b$, και απεικόνιση $g\colon X\longrightarrow X$, ως εξής: $g(a)=a$, $g(b)=a$. Θα έχουμε $(f\circ g)(a)=f(g(a))=f(a)=b$ και $(g\circ f)(a)=g(f(a))=g(b)=a$. Επομένως $(f\circ g)(a)\neq(g\circ f)(a)$, και άρα $f\circ g\neq g\circ f$.

Αν το σύνολο $X=\{a,b,\cdots\}$ έχει παραπάνω από δύο στοιχεία, τότε, ορίζοντας απεικονίσεις $f,g\colon X\longrightarrow X$ να έχουν τιμές στα στοιχεία a και b όπως παραπάνω, και θέτοντας $f(x)=x=g(x)$, $\forall x\in X\setminus\{a,b\}$, αποκτούμε απεικονίσεις f, g επί του X έτσι ώστε $f\circ g\neq g\circ f$. Προφανώς, αν το σύνολο X έχει ένα στοιχείο $X=\{a\}$, τότε $f\circ g=g\circ f$ διότι η μοναδική απεικόνιση $f\colon X\longrightarrow X$ είναι η ταυτοτική $f=\mathsf{Id}_X$. ▲

Έστω $f\colon X\longrightarrow Y$ μια απεικόνιση. Παραπάνω ορίσαμε την αντίστροφη εικόνα $f^{-1}(B)$ κάθε υποσυνόλου του X να είναι το υποσύνολο $\{x\in X\mid f(x)\in B\}$. Ιδιαίτερα έχουμε το υποσύνολο $f^{-1}(Y)=\{x\in X\mid f(x)\in Y\}$. Παρατηρούμε ότι υπάρχουν τουλάχιστον δύο προβλήματα αν προσπαθήσουμε να ορίσουμε «απεικόνιση» $f^{-1}\colon Y\longrightarrow X$ ως εξής: $f^{-1}(y)=x$, όπου $f(x)=y$. Πράγματι: (α) για δεδομένο στοιχείο $y\in Y$, μπορεί να μην υπάρχει στοιχείο $x\in X$ έτσι ώστε $f(x)=y$, δηλαδή μπορεί $f^{-1}(\{y\})=\emptyset$, και (β) αν για δεδομένο $y\in Y$, έχουμε $f^{-1}(y)\neq\emptyset$, μπορεί να υπάρχουν διακεκριμένα στοιχεία $x_1,x_2\in f^{-1}(\{y\})$, και τότε θα είχαμε $f^{-1}(y)=x_1\neq x_2=f^{-1}(y)$. Τα προβλήματα αυτά παύουν να υπάρχουν αν η απεικόνιση f είναι (α) «επί» και (β) η απεικόνιση f είναι «1-1», με τις ακόλουθες έννοιες:

1. Η f καλείται «**απεικόνιση 1-1**» αν: $\forall x,y\in X$, $f(x)=f(y)\Longrightarrow x=y$.
2. Η f καλείται «**απεικόνιση επί**», αν: $\mathsf{Im}(f)=Y$, δηλαδή: $\forall y\in Y$, $\exists x\in X$: $f(x)=y$.
3. Η f καλείται «**αντιστρέψιμη απεικόνιση**», αν υπάρχει απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε:

$$g\circ f=\mathsf{Id}_X\qquad\&\qquad f\circ g=\mathsf{Id}_Y \tag{†}$$

Πρόταση 0.2.8. *Μια απεικόνιση $f\colon X\longrightarrow Y$ είναι «1-1» και «επί» αν και μόνο αν η f είναι αντιστρέψιμη.*
Αν $g,h\colon Y\longrightarrow X$ είναι δύο απεικόνισεις έτσι ώστε: $g\circ f=\mathsf{Id}_X=h\circ f$ και $f\circ g=\mathsf{Id}_Y=f\circ h$, τότε $g=h$.

Απόδειξη. «$\Longrightarrow$» Έστω ότι η $f\colon X\longrightarrow Y$ είναι «1-1» και «επί». Ορίζουμε μια απεικόνιση $g\colon Y\longrightarrow X$, ως εξής. Για κάθε $y\in Y$, επειδή η f είναι «επί», υπάρχει ένα στοιχείο $x\in X$ έτσι ώστε $f(x)=y$. Το στοιχείο αυτό x είνα μοναδικό διότι αν $f(x)=y$ και $f(x')=y$, τότε $f(x)=f(x')$ και επομένως $x=x'$ διότι η f είναι «1-1». Ορίζουμε $g(y)=x$, όπου x είναι το μοναδικό στοιχείο $x\in X$ έτσι ώστε $f(x)=y$. Δείχνουμε ότι: $(g\circ f)(x)=x$, $\forall x\in X$ και $(f\circ g)(y)=y$, $\forall y\in Y$. Πράγματι $(g\circ f)(x)=g(f(x))$ είναι το μοναδικό στοιχείο x' του X έτσι ώστε $f(x')=f(x)$, από όπου $x'=x$ διότι η f είναι «1-1». Άρα $g(f(x))=x$. Από την άλλη πλευρά, επειδή $g(y)$ είναι το μοναδικό στοιχείο του X έτσι ώστε $f(x)=y$, θα έχουμε $f(g(y))=f(x)=y$. Επομένως $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$, και άρα η f είναι αντιστρέψιμη.

«$\Longleftarrow$» Έστω οτι η απεικόνιση f είναι αντιστρέψιμη, και άρα υπάρχει απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$. Έστω $f(x)=f(x')$. Τότε $g(f(x))=g(f(x'))\Longrightarrow(g\circ f)(x)=(g\circ f)(x')\Longrightarrow\mathsf{Id}_X(x)=\mathsf{Id}_X(x')\Longrightarrow x=x'$ και άρα η f είναι «1-1». Από τη σχέση $g\circ f=\mathsf{Id}_X$ βλέπουμε ότι για κάθε $x\in X$ έχουμε $g(f(x))=x$, το οποίο σημαίνει ότι η g είναι «επί».

Τέλος, έστω $h\colon Y\longrightarrow X$ μια άλλη απεικόνιση έτσι ώστε $h\circ f=\mathsf{Id}_X$ και $f\circ h=\mathsf{Id}_Y$. Τότε:

$$h\circ f=\mathsf{Id}_X\implies(h\circ f)\circ g=\mathsf{Id}_X\circ g\implies h\circ(f\circ g)=g\implies h\circ\mathsf{Id}_Y=g\implies h=g$$ ■

Παρατήρηση 0.2.9. Αν $f\colon X\longrightarrow Y$ και $g\colon Y\longrightarrow X$ είναι απεικονίσεις και ισχύει ότι $g\circ f=\mathsf{Id}_X$, τότε από την απόδειξη της Πρότασης 0.2.8 έπεται ότι η f είναι «1-1» και η g είναι «επί». ▲

Αν η απεικόνιση $f\colon X\longrightarrow Y$ είναι «1-1» και «επί», ισοδύναμα η f είναι αντιστρέψιμη, σύμφωνα με την Πρόταση 0.2.8 υπάρχει μοναδική απεικόνιση $g\colon Y\longrightarrow X$ έτσι ώστε $g\circ f=\mathsf{Id}_X$ και $f\circ g=\mathsf{Id}_Y$. Η απεικόνιση g καλείται η **αντίστροφη απεικόνιση** της f και συμβολίζεται με $g=f^{-1}$.

Πόρισμα 0.2.10. *Έστω ότι $f\colon X \longrightarrow Y$ είναι μια αντιστρέψιμη απεικόνιση. Τότε η αντίστροφη απεικόνιση $f^{-1}\colon Y \longrightarrow X$ είναι επίσης αντιστρέψιμη αεπικόνιση και ισχύει: $(f^{-1})^{-1} = f$.*

Απόδειξη. Επειδή η f είναι αντιστρέψιμη, έπεται ότι υπάρχει η αντίστροφή της $f^{-1}\colon Y \longrightarrow X$ και ισχύει:

$$f^{-1} \circ f = \mathsf{Id}_X \quad \& \quad f \circ f^{-1} = \mathsf{Id}_Y$$

Οι παραπάνω σχέσεις δείχνουν ότι η f^{-1} είναι αντιστρέψιμη και η αντίστροφή της είναι η $(f^{-1})^{-1} = f$. ■

Παράδειγμα 0.2.11. Έστω ότι $X = \{x, y, z\}$ είναι ένα σύνολο με τρία στοιχεία, και έστω $Y = \{1, 2, 3\}$. Θεωρούμε την απεικόνιση $f\colon X \longrightarrow Y$ ως εξής: $f(x) = 2$, $f(y) = 3$ και $f(z) = 1$. Τότε προφανώς η f είναι «1-1» και «επί» και άρα η f είναι αντιστρέψιμη. Η αντίστροφή της είναι η απεικόνιση $f^{-1}\colon X \longrightarrow Y$, η οποία ορίζεται ως εξής: $f^{-1}(1) = z$, $f^{-1}(2) = x$, και $f^{-1}(3) = y$. √

Πρόταση 0.2.12. *Έστω ότι $f\colon X \longrightarrow Y$ και $g\colon Y \longrightarrow Z$ είναι απεικονίσεις.*

1. *Αν οι απεικονίσεις f, g είναι «1-1», τότε η απεικόνιση $g \circ f$ είναι «1-1». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «1-1», τότε η απεικόνιση f είναι «1-1».*

2. *Αν οι απεικονίσεις f, g είναι «επί», τότε η απεικόνιση $g \circ f$ είναι «επί». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «επί», τότε η απεικόνιση g είναι «επί».*

3. *Αν οι απεικονίσεις f, g είναι αντιστρέψιμες, τότε η απεικόνιση $g \circ f$ είναι αντιστρέψιμη και ισχύει ότι:*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι αντιστρέψιμη. τότε η f είναι «1-1» και η g είναι «επί».

Απόδειξη. 1. Έστω ότι οι απεικονίσεις f, g είναι «1-1», και έστω $x, y \in X$ έτσι ώστε: $(g \circ f)(x) = (g \circ f)(y)$. Τότε $g(f(x)) = g(f(y))$, και επομένως $f(x) = f(y)$ διότι η g είναι «1-1». Επειδή η f είναι επίσης «1-1», θα έχουμε $x = y$, και άρα η $g \circ f$ είναι «1-1». Αντίστροφα, αν τα στοιχεία $x, y \in X$ είναι τέτοια ώστε $f(x) = f(y)$, τότε θα έχουμε $g(f(x)) = g(f(y))$, δηλαδή $(g \circ f)(x) = (g \circ f)(y)$. Επομένως, αν η απεικόνιση $g \circ f$ είναι «1-1», τότε θα έχουμε $x = y$, και άρα η f είναι «1-1».

2. Έστω ότι οι απεικονίσεις f, g είναι «επί», και έστω ένα στοιχείο $z \in Z$. Επειδή η g είναι «επί», έπεται ότι υπάρχει στοιχείο $y \in Y$ έτσι ώστε $g(y) = z$, και επειδή η f είναι «επί», έπεται ότι υπάρχει στοιχείο $x \in Y$ έτσι ώστε $f(x) = y$. Τότε $(g \circ f)(x) = g(f(x)) = g(y) = z$ και άρα η $g \circ f$ είναι «επί». Αντίστροφα, αν η απεικόνιση $g \circ f$ είναι «επί», και $z \in Z$, τότε υπάρχει $x \in X$ έτσι ώστε $(g \circ f)(x) = g(f(x)) = y$, και επομένως η g είναι «επί».

3. Έστω ότι οι απεικονίσεις f, g είναι αντιστρέψιμες. Τότε από την Πρόταση 0.2.8 έπεται ότι οι f, g είναι απεικονίσεις «1-1» και «επί». Από τα μέρη 1. και 2. έπεται τότε ότι η σύνθεση $g \circ f$ είναι «1-1» και «επί», και επομένως πάλι από την Πρόταση 0.2.8 η απεικόνιση $g \circ f$ είναι αντιστρέψιμη, και άρα υπάρχει η αντίστροφή της $(g \circ f)^{-1}$. Επιπλέον, χρησιμοποιώντας την προσεταιριστική ιδιότητα της σύνθεσης απεικονίσεων, θα έχουμε:

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = ((g \circ f^{-1}) \circ f) \circ g^{-1} = (g \circ (f^{-1} \circ f)) \circ g^{-1} = (g \circ \mathsf{Id}_X) \circ g^{-1} = g \circ g^{-1} = \mathsf{Id}_Y$$

$$(f^{-1} \circ g^{-1}) \circ (g \circ f) = ((f^{-1} \circ g^{-1}) \circ g) \circ f = (f^{-1} \circ (g^{-1} \circ g)) \circ f = (f^{-1} \circ \mathsf{Id}_X) \circ f = f^{-1} \circ f = \mathsf{Id}_X$$

Λόγω της μοναδικότητας της αντίστροφης απεικόνισης, βλέπε την Πρόταση 0.2.8, θα έχουμε: $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Τέλος αν η απεικόνιση $g \circ f$ είναι αντιστρέψιμη, τότε όπως παραπάνω η $g \circ f$ είναι «1-1» και «επί» και τότε από τα μέρη 1. και 2. έπεται ότι η f είναι «1-1» και η g είναι επί. ■

Παρατήρηση 0.2.13. Παρατηρούμε ότι η σύνθεση απεικονίσεων $f, g, h, \cdots : X \longrightarrow X$, όπου X είναι ένα μη κενό σύνολο, ορίζεται πάντα. Ιδιαίτερα, για κάθε απεικόνιση $f : X \longrightarrow X$, και για κάθε θετικό ακέραιο n, ορίζεται επαγωγικά η απεικόνιση

$$f^n := \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ φορές}} : X \longrightarrow X, \quad x \longmapsto f^n(x)$$

ως εξής. Αν $n = 1$, τότε $f^1 = f$. Αν $n = 2$, τότε $f^2 = f \circ f$. Αν $n \geq 3$ και έχει οριστεί επαγωγικά η απεικόνιση f^{n-1}, τότε ορίζουμε $f^n = f^{n-1} \circ f$.

Από την άλλη πλευρά, ορίζουμε $f^0 = \mathrm{Id}_X$. Αν επιπλέον *η απεικόνιση f είναι αντιστρέψιμη*, οπότε ορίζεται η αντίστροφή της $f^{-1} : X \longrightarrow X$, τότε μπορούμε να ορίσουμε αρνητικές ακέραιες δυνάμεις f^{-n}, όπου $n \geq 1$, της f, ως εξής:

$$f^{-n} : X \longrightarrow X, \quad f^{-n} = (f^{-1})^n \quad \blacktriangle$$

Άσκηση 0.2.14. *Έστω $f_k : X_k \longrightarrow Y_k$, $1 \leq k \leq n$, μια οικογένεια απεικονίσεων μεταξύ μη-κενών συνόλων, και έστω η απεικόνιση-γινόμενο*

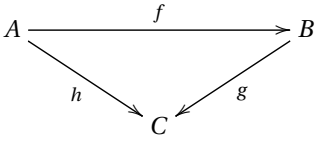
$$\prod_{k=1}^{n} f_k : \prod_{k=1}^{n} X_k \longrightarrow \prod_{k=1}^{n} Y_k, \quad (\prod_{k=1}^{n} f_k)(x_1, x_2, \cdots, x_n) = (f_1(x_1), f_2(x_2), \cdots, f_n(x_n))$$

όπως στο παράδειγμα 0.2.6. Να δειχθεί ότι η απεικόνιση $\prod_{k=1}^{n} f_k$ είναι «1-1», αντίστοιχα «επί», αν και μόνο αν οι απεικονίσεις f_k, $1 \leq k \leq n$ είναι «1-1», αντίστοιχα «επί». Αν οι απεικονίσεις f_k, $1 \leq k \leq n$ είναι «1-1» και «επί», να βρεθεί η αντίστροφη $(\prod_{k=1}^{n} f_k)^{-1}$ της απεικόνισης-γινόμενο $\prod_{k=1}^{n} f_k$.

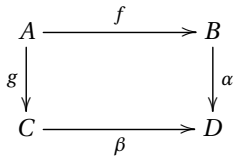
Συμβολισμός 0.2.15 (Ειδικού Τύπου Απεικονίσεις και Μεταθετικά Διαγράμματα)**.** Αν μια απεικόνιση $f : A \longrightarrow B$ είναι «1-1», «επί», ή «1-1» και «επί», τότε συχνά θα συμβολίζουμε αντίστοιχα

$$A \overset{f}{\rightarrowtail} B, \qquad A \overset{f}{\twoheadrightarrow} B, \qquad f : A \overset{\cong}{\longrightarrow} B$$

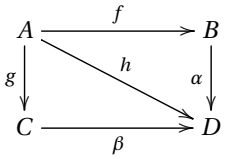
Συχνά η ισότητα μεταξύ (συνθέσεων) απεικονίσεων παριστάται μέσω μεταθετικών διαγραμμάτων. Ένα **μεταθετικό διάγραμμα** *συνόλων και απεικονίσεων* είναι ένα διάγραμμα το οποίο αποτελείται από κορυφές, οι οποίες αντιστοιχούν σε σύνολα και προσανατολισμένες ακμές μεταξύ των κορυφών, οι οποίες αντιστοιχούν σε απεικονίσεις μεταξύ συνόλων, έτσι ώστε όλες οι τεθλασμένες γραμμές οι οποίες σχηματίζονται από τις ακμές του διαγράμματος και οι οποίες έχουν την ίδια αρχή και το ίδιο τέλος δίνουν, μέσω της σύνθεσης, την ίδια απεικόνιση. Για παράδειγμα, αν $f : A \longrightarrow B$ και $g : B \longrightarrow C$ και $h : A \longrightarrow C$ είναι απεικονίσεις μεταξύ συνόλων, τότε ισχύει ότι: $h = g \circ f$ αν και μόνο αν το ακόλουθο διάγραμμα είναι μεταθετικό.



Παρόμοια, αν $f : A \longrightarrow B$ και $\alpha : B \longrightarrow D$ και $g : A \longrightarrow C$, και $\beta : C \longrightarrow D$ είναι απεικονίσεις μεταξύ συνόλων, τότε ισχύει ότι: $\alpha \circ f = \beta \circ g$ αν και μόνο αν το ακόλουθο διάγραμμα είναι μεταθετικό:



Για παράδειγμα, το διάγραμμα απεικονίσεων μεταξύ συνόλων



είναι μεταθετικό αν: $\alpha \circ f = h$ και $\beta \circ g = h$ (και τότε προφανως θα έχουμε και $\alpha \circ f = \beta \circ g$). ▲

0.2.2 Πεπερασμένα και Άπειρα Σύνολα

Υπενθυμίζουμε κάποια βασικά στοιχεία που αφορούν πεπερασμένα και άπειρα σύνολα.

Για κάθε φυσικό αριθμό n, θεωρούμε το σύνολο

$$\mathbb{N}_n = \{1, 2, \cdots, n\}$$

Ένα σύνολο X **έχει πλήθος στοιχείων ίσο με** n, αν υπάρχει μια «1-1» και «επί» απεικόνιση $f: X \longrightarrow \mathbb{N}_n$. Τότε θα γράφουμε

$$|X| = \#X = \mathsf{card}(X) = n$$

Ένα μη κενό σύνολο X καλείται **πεπερασμένο**, και τότε θα γράφουμε $|X| < \infty$, αν, με την παραπάνω έννοια, έχει πλήθος στοιχείων ίσο με n, για κάποιον φυσικό αριθμό n. Το μη-κενό σύνολο X καλείται **άπειρο** αν δεν είναι πεπερασμένο, και τότε θα γράφουμε $|X| = \infty$. Τέλος, ορίζουμε το πλήθος των στοιχείων του κενού συνόλου $\emptyset$ να είναι ίσο με 0. Η επόμενη Παρατήρηση δείχνει ότι οι παραπάνω ορισμοί ειναι «καλοί», δηλαδή δεν περιέχουν αντιφάσεις.

Παρατήρηση 0.2.16. Αν $f: X \longrightarrow \mathbb{N}_n$ και $g: X \longrightarrow \mathbb{N}_m$ είναι «1-1» και «επί» απεικονίσεις, τότε $n = m$.

Πράγματι τότε οι απεικονίσεις f, g είναι αντιστρέψιμες και άρα ορίζεται η απεικόνιση $h = g \circ f^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ η οποία, σύμφωνα με την Πρόταση 0.2.12 και το Πόρισμα 0.2.10, είναι «1-1» και «επί» και άρα είναι αντιστρέψιμη. Επειδή η h είναι «1-1», έπεται ότι τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι διαφορετικά στοιχεία του $\mathbb{N}_m$ και επομένως $n \leq m$. Παρόμοια, επειδή η h^{-1} είναι «1-1», έπεται ότι τα στοιχεία $h^{-1}(1), h^{-1}(2), \cdots, h^{-1}(m)$ είναι διαφορετικά στοιχεία του $\mathbb{N}_n$ και επομένως $m \leq n$. Άρα $n = m$. ▲

Έστω ότι X και Y είναι δύο μη-κενά σύνολα.

1. Το σύνολο X **έχει το πολύ τόσα στοιχεία όσα έχει το σύνολο** Y, και τότε γράφουμε: $|X| \leq |Y|$, αν υπάρχει μια «1-1» απεικόνιση $f: X \longrightarrow Y$.

2. Το σύνολο X **έχει τουλάχιστον όσα στοιχεία έχει το σύνολο** Y, και τότε γράφουμε: $|X| \geq |Y|$, αν υπάρχει μια απεικόνιση «επί» $f: X \longrightarrow Y$.

3. Τα σύνολα X και Y **έχουν το ίδιο πλήθος στοιχείων**, και τότε γράφουμε: $|X| = |Y|$, αν υπάρχει μια «1-1» και «επί» απεικόνιση $f: X \longrightarrow Y$. Διαφορετικά θα γράφουμε $|X| \neq |Y|$.

4. Θα γράφουμε $|X| < |Y|$, αν $|X| \leq |Y|$ και $|X| \neq |Y|$, και θα λέμε ότι το X έχει λιγότερα στοιχεία από όσα έχει το Y. Ισοδύναμα αυτό ισχύει αν υπάρχει «1-1» απεικόνιση $X \longrightarrow Y$ αλλά δεν υπάρχει «επί» απεικόνιση $X \longrightarrow Y$. Παρόμοια θα γράφουμε $|X| > |Y|$, αν $|X| \geq |Y|$ και $|X| \neq |Y|$, και θα λέμε ότι το X έχει περισσότερα στοιχεία από όσα έχει το Y. Ισοδύναμα αυτό ισχύει αν υπάρχει «επί» απεικόνιση $X \longrightarrow Y$, αλλά δεν υπάρχει «1-1» απεικόνιση $X \longrightarrow Y$.

5. Το σύνολο X καλείται **αριθμήσιμο** αν έχει το ίδιο πλήθος στοιχείων με το σύνολο $\mathbb{N}$ των θετικών ακεραίων. Διαφορετικά το σύνολο X καλείται **μη αριθμήσιμο**.

Επισημαίνουμε ότι γράφοντας $|X| \leq |Y|$ δεν συμβολίζουμε μια σχέση ανισότητας μεταξύ αριθμών αλλά το γεγονός ότι υπάρχει «1-1» απεικόνιση από το σύνολο X στο σύνολο Y. Παρόμοια για τους συμβολισμούς $|X| \geq |Y|$ και $|X| = |Y|$.

Πρόταση 0.2.17. *Έστω ότι X και Y είναι δύο πεπερασμένα σύνολα, και έστω ότι $|X| = n$ και $|Y| = m$.*

1. *Υπάρχει «1-1» απεικόνιση $f: X \longrightarrow Y \iff n \leq m$.*
2. *Υπάρχει «επί» απεικόνιση $f: X \longrightarrow Y \iff n \geq m$.*
3. *Αν $|X| = |Y|$, τότε μια απεικόνιση $f: X \longrightarrow Y$ είναι αντιστρέψιμη αν και μόνο αν είτε η f είναι «1-1» είτε η f είναι «επί».*
4. *Αν $|X| \neq |Y|$, τότε για κάθε «επί» απεικόνιση $f: X \longrightarrow Y$ υπάρχει τουλάχιστον ένα ζεύγος (x_1, x_2) στοιχείων του X έτσι ώστε $x_1 \neq x_2$ και $f(x_1) = f(x_2)$*[2].

Απόδειξη. Επειδή $|X| = n$, έπεται ότι υπάρχει «1-1» και «επί» απεικόνιση $\alpha: X \longrightarrow \mathbb{N}_n$, και επειδή $|Y| = m$, έπεται ότι υπάρχει «1-1» και «επί» απεικόνιση $\beta: X \longrightarrow \mathbb{N}_m$. Ιδιαίτερα τότε υπάρχουν οι απεικονίσεις α^{-1} και β^{-1} οι οποίες είναι επίσης «1-1» και «επί».

1. Αν υπάρχει «1-1» απεικόνιση $f: X \longrightarrow Y$, τότε η σύνθεση $h := \beta \circ f \circ \alpha^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ είναι προφανώς μια «1-1» απεικόνιση, και τότε τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι ανά δύο διαφορετικά στοιχεία του συνόλου $\mathbb{N}_m$. Επομένως $n \leq m$. Αντίστροφα, αν $n \leq m$, τότε $\mathbb{N}_m = \mathbb{N}_n \cup \{n+1, \cdots, m\}$ και προφανώς η απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_m$, $h(k) = k$, $\forall k = 1, \cdots, n$, είναι «1-1». Η σύνθεση $\beta^{-1} \circ h \circ \alpha: X \longrightarrow Y$ είναι, σύμφωνα με την Πρόταση 0.2.12, μια απεικόνιση «1-1».

2. Έστω ότι υπάρχει μια «επί» απεικόνιση $f: X \longrightarrow Y$. Τότε σύμφωνα με την Πρόταση 0.2.12, η απεικόνιση $h := \beta \circ f \circ \alpha^{-1}: \mathbb{N}_n \longrightarrow \mathbb{N}_m$ είναι «επί». Επομένως, για κάθε $k \in \mathbb{N}_m$, υπάρχει τουλάχιστον ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Τότε όμως $m \leq n$. Αντίστροφα, αν $m \leq n$, τότε $\mathbb{N}_n = \mathbb{N}_m \cup \{m+1, \cdots, n\}$ και προφανώς η απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_m$, $h(k) = k$, αν $1 \leq k \leq m$ και $h(k) = 1$, αν $m+1 \leq k \leq n$, είναι «επί». Τότε, σύμφωνα με την Πρόταση 0.2.12, η απεικόνιση $f := \beta^{-1} \circ h \circ \alpha: X \longrightarrow Y$ είναι «επί».

3. Υποθέτουμε ότι $n = m$, και έστω $f: X \longrightarrow Y$ μια απεικόνιση. Αν η f είναι «1-1», τότε όπως στο μέρος 1. υπάρχει μια «1-1» απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_n$ και επομένως τα στοιχεία $h(1), h(2), \cdots, h(n)$ είναι ανά δύο διαφορετικά. Τότε, $\mathbb{N}_n = \{h(1), \cdots, h(n)\}$ και άρα η h είναι «επί». Αν η f είναι «επί», τότε όπως στο μέρος 2. υπάρχει μια «επί» απεικόνιση $h: \mathbb{N}_n \longrightarrow \mathbb{N}_n$ και άρα για κάθε $k \in \mathbb{N}_n$ υπάρχει τουλάχιστον ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Αν για δεδομένο k έχουμε $h(l_1) = k = h(l_2)$, τότε αναγκαστικά $l_1 = l_2$ διότι διαφορετικά το σύνολο $\mathbb{N}_n$ θα περιείχε τουλάχιστον $n+1$ στοιχεία. Άρα, για κάθε $k \in \mathbb{N}_n$, υπάρχει ακριβώς ένα $l \in \mathbb{N}_n$ έτσι ώστε $h(l) = k$. Τότε προφανώς η h είναι «1-1».

4. Προκύπτει άμεσα από το μέρος 3. ∎

Παράδειγμα 0.2.18. Έστω X ένα μη-κενό σύνολο. Θεωρούμε το σύνολο $\mathbf{2} = \{0, 1\}$, και έστω

$$\mathbf{2}^X := \{f: X \longrightarrow \mathbf{2} \mid f : \text{απεικόνιση}\}$$

Επίσης θεωρούμε το *δυναμοσύνολο* $\mathscr{P}(X)$ του X, δηλαδή το σύνολο όλων των υποσυνόλων του X. Θα δείξουμε ότι:

$$|X| \ < \ |\mathbf{2}^X| \ = \ |\mathscr{P}(X)|$$

(α) Ορίζουμε απεικόνιση

$$\Omega: X \longrightarrow \mathbf{2}^X, \quad \Omega(a) = \chi_{\{a\}}$$

όπου $\chi_{\{a\}}$ είναι η χαρακτηριστική συνάρτηση του μονοσυνόλου $\{a\}$, βλέπε Παράδειγμα 0.2.3. Αν $\Omega(a) = \Omega(b)$, τότε $\chi_{\{a\}} = \chi_{\{b\}}$ και επομένως $\chi_{\{a\}}(a) = \chi_{\{b\}}(a)$, από όπου έπεται ότι $1 = \begin{cases} 1, \text{ αν } b = a \\ 0, \text{ αν } b \neq a \end{cases}$. Άρα θα έχουμε $a = b$, και επομένως η απεικόνιση Ω είναι «1-1». Η απεικόνιση Ω δεν είναι «επί» διότι, επειδή $X \neq \emptyset$, έπεται ότι το X

[2] Αυτός ο ισχυρισμός είναι η μαθηματική διατύπωση της θεμελιώδους αρχής απαρίθμησης γνωστής ως «*Αρχή του Περιστερώνα*»: Αν $n = |X|$ περιστέρια τοποθετηθούν σε $m = |Y| < n$ φωλιές, τότε σε τουλάχιστον μία φωλιά υπάρχουν τουλάχιστον δύο περιστέρια. Η αυστηρή διατύπωση αυτής της αρχής είναι η εξής: *Έστω X και Y δύο πεπερασμένα σύνολα, και $f: X \longrightarrow Y$ μια απεικόνιση. Τότε: (α) αν $|X| > |Y|$, τότε η f δεν είναι «1-1», και (β) αν $|X| < |Y|$, τότε η f δεν είναι «επί».*

περιέχει τουλάχιστον ένα στοιχείο, έστω το a. Τότε ορίζονται οι απεικονίσεις $f\colon X \longrightarrow \mathbf{2}$, $f(a)=0$, και $f(x)=1$, $\forall x \neq a$, και $g\colon X \longrightarrow \mathbf{2}$, $g(a)=0$, και $g(x)=1$, $\forall x \neq a$. Αν η απεικόνιση Ω είναι «επί», τότε υπάρχει στοιχείο $b \in X$ έτσι ώστε $\Omega(b) = \chi_{\{b\}} = f$, και επομένως $\chi_{\{b\}}(a) = f(a)$, δηλαδή: $\begin{cases} 1, \text{ αν } b=a \\ 0, \text{ αν } b \neq a \end{cases} = \begin{cases} 0, \text{ αν } b=a \\ 1, \text{ αν } b \neq a \end{cases}$, το οποίο είναι άτοπο. Άρα η Ω δεν είναι «επί» και επομένως: $|X| < |\mathbf{2}^X|$.

(β) Γενικότερα θα δείξουμε ότι δεν υπάρχει «1-1» και «επί» απεικόνιση $f\colon X \longrightarrow \mathscr{P}(X)$. Πράγματι, αν υπάρχει μια τέτοια απεικόνιση, τότε για κάθε στοιχείο $x \in X$, το $f(x)$ είναι ένα υποσύνολο του X και επομένως είτε $x \in f(x)$ ή $x \notin f(x)$. Θεωρούμε το υποσύνολο $S = \{x \in X \mid x \notin f(x)\}$. Επειδή η f είναι «επί», έπεται ότι υπάρχει $y \in X$ έτσι ώστε $f(y) = S$. Τότε είτε $y \in S$ ή $y \notin S$. Όμως $y \in S = f(y)$ σημαίνει ότι $y \notin f(y)$ και $y \notin S = f(y)$ σημαίνει ότι $y \in f(y)$. Και οι δύο περιπτώσεις μάς οδηγούν σε άτοπο και επομένως δεν υπάρχει «1-1» και «επί» απεικόνιση $: X \longrightarrow \mathscr{P}(X)$.

(γ) Θεωρούμε απεικονίσεις

$$\Phi\colon \mathscr{P}(X) \longrightarrow \mathbf{2}^X, \quad \Phi(A) = \chi_A \qquad \text{και} \qquad \Psi\colon \mathbf{2}^X \longrightarrow \mathscr{P}(X), \quad \Psi(f) = f^{-1}(\{1\})$$

Θα δείξουμε ότι η Φ είναι αντιστρέψιμη με αντίστροφη την Ψ. Για κάθε υποσύνολο $A \subseteq X$, έχουμε:

$$\Psi\Phi(A) = \Psi(\chi_A) = \chi_A^{-1}(\{1\}) = \left\{x \in X \mid x \in \chi_A^{-1}(x)\right\} = \left\{x \in X \mid \chi_A(x) = 1\right\} = \left\{x \in X \mid x \in A\right\} = A$$

Δηλαδή $\Psi\Phi = \mathsf{Id}_{\mathscr{P}(X)}$. Για κάθε απεικόνιση $f\colon X \longrightarrow \mathbf{2}$, έχουμε:

$$\Phi\Psi(f) = \Phi(f^{-1}(\{1\})) = \chi_{f^{-1}(\{1\})} \quad \text{και} \quad \forall x \in X\colon \ \chi_{f^{-1}(\{1\})}(x) = \begin{cases} 1, \text{ αν } x \in f^{-1}(\{1\}) \\ 0, \text{ αν } x \notin f^{-1}(\{1\}) \end{cases} = \begin{cases} 1, \text{ αν } f(x) = 1 \\ 0, \text{ αν } f(x) = 0 \end{cases} = f(x)$$

Επομένως $\chi_{f^{-1}(\{1\})}(x) = f(x)$, $\forall x \in X$, και άρα $\chi_{f^{-1}(\{1\})} = f$, δηλαδή $\Phi\Psi(f) = f$. Επειδή η απεικόνιση f ήταν τυχαία, έπεται ότι $\Phi\Psi = \mathsf{Id}_{\mathbf{2}^X}$. Έτσι η απεικόνιση Φ είναι αντιστρέψιμη με αντίστροφη την απεικόνιση Ψ, και επομένως $|\mathbf{2}^X| = |\mathscr{P}(X)|$. $\surd$

Ο συμβολισμός $\mathbf{2}^X$ για ένα σύνολο X προέρχεται από το Παράδειγμα 0.2.18 σε συνδυασμό με την ακόλουθη παρατήρηση.

Παρατήρηση 0.2.19. Για κάθε σύνολο X ισχύει ότι:

$$|X| < \infty \quad \Longrightarrow \quad |\mathscr{P}(X)| = 2^{|X|}$$

Αν $X = \emptyset$, τότε $|X| = 0$ και το $\mathscr{P}(X)$ περιέχει μόνο το στοιχείο $\emptyset$. Άρα $|\mathscr{P}(\emptyset)| = 1 = 2^0 = 2^{|\emptyset|}$. Αν $|X| = 1$, τότε $X = \{a\}$ και $\mathscr{P}(X) = \{\emptyset, \{a\}\}$ και επομένως $|\mathscr{P}(X)| = 2 = 2^1 = 2^{|X|}$. Υποθέτουμε ότι $|\mathscr{P}(X)| = 2^{|X|}$, για κάθε σύνολο με $|X| = n$, όπου $n \geq 2$. Έστω $|X| = n+1$, και έστω $a \in X$. Θεωρούμε το σύνολο $Y = X \setminus \{a\}$ για το οποίο έχουμε $|Y| = n$. Αν S είναι ένα υποσύνολο του X, τότε είτε $a \in S$ ή $a \notin S$. Στην τελευταία περίπτωση, θα έχουμε προφανώς ότι $S \subseteq Y$. Επομένως τα υποσύνολα του X συμπίπτουν με τα υποσύνολα S του Y, τα οποία από την Επαγωγική Υπόθεση σε πλήθος είναι $|\mathscr{P}(Y)| = 2^{|Y|} = 2^n$, μαζί με τα υποσύνολα $S \cup \{a\}$ του X, για κάθε υποσύνολο S του Y, και τα οποία σε πλήθος είναι όσα και τα υποσύνολα του Y, δηλαδή είναι 2^n. Έτσι το πλήθος των υποσυνόλων του $\mathscr{P}(X)$ είναι $2^n + 2^n = 2 \cdot 2^n = 2^{n+1} = 2^{|X|}$. Από την Αρχή Μαθηματικής Επαγωγής, έπεται ότι $|\mathscr{P}(X)| = 2^{|X|}$, για κάθε πεπερασμένο σύνολο X. ▲

Παράδειγμα 0.2.20.

1. $|\mathbb{N}| = |\mathbb{Z}|$, διότι, όπως μπορεί να δειχθεί εύκολα, η απεικόνιση

$$f\colon \mathbb{N} \longrightarrow \mathbb{Z}, \quad f(n) = (-1)^n \left[\frac{n}{2}\right]$$

είναι «1-1» και «επί», όπου $\left[\frac{n}{2}\right]$ συμβολίζει τον μεγαλύτερο ακέραιο ο οποίος δεν υπερβαίνει τον $\frac{n}{2}$.

2. $|\mathbb{Z}| = |2\mathbb{Z}|$, όπου $2\mathbb{Z} = \{2n \in \mathbb{Z} \mid n \in \mathbb{Z}\}$ είναι το σύνολο των αρτίων ακεραίων, διότι όπως μπορεί να δειχθεί εύκολα η απεικόνιση

$$f\colon \mathbb{Z} \longrightarrow 2\mathbb{Z}, \quad f(n) = 2n$$

είναι «1-1» και «επί».

3. $|\mathbb{N}\times\mathbb{N}| = |\mathbb{N}|$, διότι όπως μπορεί να δειχθεί εύκολα η απεικόνιση

$$f:\mathbb{N}\times\mathbb{N}\longrightarrow\mathbb{N},\quad f(n,m)=\frac{(m+n-2)(m+n-1)}{2}+n$$

είναι «1-1» και «επί».

4. Αποδεικνύεται παρόμοια ότι $|\mathbb{N}| = |\mathbb{Q}|$, και άρα το σύνολο $\mathbb{Q}$ είναι αριθμήσιμο. Όμως τα σύνολα $\mathbb{R}$ και $\mathbb{C}$ είναι άπειρα μη αριθμήσιμα και έχουν το ίδιο πλήθος στοιχείων. $\surd$

Υποθέτουμε ότι X και Y είναι δύο σύνολα, όχι απαραίτητα πεπερασμένα. Αν $|X| \le |Y|$, δηλαδή αν υπάρχει «1-1» απεικόνιση $: X \longrightarrow Y$, και αν $|Y| \le |X|$, δηλαδή αν υπάρχει «1-1» απεικόνιση $: Y \longrightarrow X$, τότε το ακόλουθο αποτέλεσμα το οποίο οφείλεται στους Schröder-Bernstein πιστοποιεί ότι τα σύνολα X και Y έχουν το ίδιο πλήθος στοιχείων, δηλαδή υπάρχει «1-1» και «επί» απεικόνιση $X \longrightarrow Y$.

Πρόταση 0.2.21 (Schröder-Bernstein)**.** [3] [4] *Αν X και Y είναι δύο σύνολα, τότε:*

$$|X| \le |Y| \quad \textit{και} \quad |Y| \le |X| \qquad \Longleftrightarrow \qquad |X| = |Y|$$

0.3 Ακέραιοι Αριθμοί

Στην παρούσα ενότητα, θα υπενθυμίσουμε βασικές έννοιες από την αριθμητική και τη διαιρετότητα των ακεραίων αριθμών. Επίσης θα αναλύσουμε εν συντομία την Αρχή της Μαθηματικής Επαγωγής, καθώς και διάφορες αποδεικτικές μεθόδους, οι οποίες θα χρησιμοποιηθούν στη συνέχεια του κειμένου.

0.3.1 Το σύνολο των Φυσικών Αριθμών και η Αρχή Μαθηματικής Επαγωγής

Θεωρούμε γνωστές τις στοιχειώδεις ιδιότητες του συνόλου[5] των θετικών ακεραίων ή φυσικών αριθμών

$$\mathbb{N} = \{1, 2, \cdots, n, \cdots\}$$

καθώς και του συνόλου $\mathbb{N}_0 = \mathbb{N}\cup\{0\} = \{0, 1, 2, \cdots, n, \cdots\}$ των μη αρνητικών ακεραίων. Το σύνολο $\mathbb{N}_0$ προκύπτει ως επέκταση του συνόλου $\mathbb{N}$ έτσι ώστε, για κάθε $n \in \mathbb{N}$, η εξίσωση $n + x = n$ να έχει λύση.

Στη μελέτη της δομής και των βασικών ιδιοτήτων του συνόλου $\mathbb{N}$ των φυσικών αριθμών, αλλά και σε σημαντικές αποδεικτικές μεθόδους, θεμελιώδη ρόλο διαδραματίζουν διάφορες αρχές αξιωματικού χαρακτήρα. Οι σημαντικότερες από αυτές τις αρχές είναι οι εξής. Πριν περάσουμε στην διατύπωσή τους, υπενθυμίζουμε ότι, αν S είναι ένα μη κενό υποσύνολο του συνόλου $\mathbb{N}$ των φυσικών αριθμών, τότε ένα *ελάχιστο*, αντίστοιχα *μέγιστο*, στοιχείο του S είναι ένα στοιχείο $x \in S$, έτσι ώστε, για κάθε $s \in S$: $x \le s$, αντίστοιχα $s \le x$. Ένα ελάχιστο, αντίστοιχα μέγιστο, στοιχείο του S συμβολίζεται με $\min S$, αντίστοιχα $\max S$.

---

[3] Felix Bernstein (24 Φεβρουαρίου 1878 - 3 Δεκεμβρίου 1956) [https://en.wikipedia.org/wiki/Felix_Bernstein_(mathematician)]: Γερμανός μαθηματικός, γνωστός για την απόδειξη του Θεωρήματος Schröder-Bernstein.

[4] Friedrich Wilhelm Karl Ernst Schröder (25 Νοεμβρίου 1841 - 16 Ιουνίου 1902) [https://en.wikipedia.org/wiki/Felix_Bernstein_(mathematician)]: Γερμανός μαθηματικός με συμβολή στην Μαθηματική Λογική.

[5] Το σύνολο των φυσικών αριθμών μπορεί να οριστεί αξιωματικά, ξεκινώντας από ένα μη κενό σύνολο $\mathbb{N}$, ένα διακεκριμένο στοιχείο $1 \in \mathbb{N}$, και μια απεικόνιση

$$\mathsf{s}:\mathbb{N}\longrightarrow\mathbb{N},\quad n\longmapsto \mathsf{s}(n)$$

η οποία ικανοποιεί τα **αξιώματα του Peano**:

1. $\forall n \in \mathbb{N}$: $1 \neq \mathsf{s}(n)$.
2. Η απεικόνιση s είναι «1-1».
3. Αν $A \subseteq \mathbb{N}$ είναι ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:

   (α') $1 \in A$.

   (β') $n \in A \Longrightarrow \mathsf{s}(n) \in A$.

   τότε $A = \mathbb{N}$.

(ΑΚΔ) Αρχη Καλης Διαταξης: Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.

(ΑΜΕ)$_1$ Αρχη Μαθηματικης Επαγωγης$_1$: Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:

(α) $1 \in S$.

(β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.

Τότε: $S = \mathbb{N}$.

(ΑΜΕ)$_2$ Αρχη Μαθηματικης Επαγωγης$_2$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(1)$ είναι αληθής.

(β) $\forall k \in \mathbb{N}$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

(ΑΜ) Αρχη Μεγιστου: Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.

Θα δείξουμε ότι οι παραπάνω αρχές είναι μεταξύ τους ισοδύναμες.

Θεώρημα 0.3.1. *Οι ακόλουθες προτάσεις είναι ισοδύναμες:*

1. *(ΑΚΔ): Κάθε μη κενό υποσύνολο του συνόλου $\mathbb{N}$ έχει ελάχιστο στοιχείο.*
2. *(ΑΜΕ)$_1$: Έστω S ένα υποσύνολο του συνόλου $\mathbb{N}$ για το οποίο ισχύουν τα εξής:*

   (α) $1 \in S$.

   (β) $\forall k \in \mathbb{N}$: $k \in S \implies k+1 \in S$.

   Τότε: $S = \mathbb{N}$.
3. *(ΑΜΕ)$_2$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:*

   (α) *Η πρόταση $P(1)$ είναι αληθής.*

   (β) $\forall k \in \mathbb{N}$: *η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.*

   Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.
4. *(ΑΜ): Κάθε μη κενό άνω φραγμένο υποσύνολο του συνόλου $\mathbb{N}$ έχει μέγιστο στοιχείο.*

Απόδειξη. • (ΑΚΔ) $\implies$ (ΑΜΕ)$_1$ Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω S ένα υποσύνολο του $\mathbb{N}$ έτσι ώστε $1 \in S$, και $k \in S \implies k+1 \in S$.

Υποθέτουμε ότι $S \neq \mathbb{N}$. Τότε το σύνολο $\mathbb{N} \setminus S$ είναι μη κενό. Επόμενως από την αρχή καλής διάταξης έπεται ότι το $\mathbb{N} \setminus S$ έχει ελάχιστο στοιχείο:

$$\ell = \min(\mathbb{N} \setminus S), \quad \text{δηλαδή} \quad \ell \in \mathbb{N} \setminus S \quad \text{και} \quad \ell \leq x, \ \ \forall x \in \mathbb{N} \setminus S$$

Αν $\ell = 1$, τότε $1 \in \mathbb{N} \setminus S$ το οποίο είναι άτοπο, διότι από την υπόθεση έχουμε $1 \in S$. Άρα $\ell > 1$ και επομένως $1 \leq \ell - 1 < \ell$.

Τότε το στοιχείο $\ell - 1$ θα ανήκει στο S, διότι διαφορετικά $\ell - 1 \in \mathbb{N} \setminus S$, κάτι το οποίο είναι άτοπο διότι $\ell - 1 < \ell$ και το ℓ είναι το ελάχιστο στοιχείο του $\mathbb{N} \setminus S$. Απο την ιδιότητα (β) του συνόλου S θα έχουμε τότε: $1 \in S$, και $\ell - 1 \in S \implies \ell \in S$. Αυτό όμως είναι άτοπο διότι εκ κατασκευής $\ell \in \mathbb{N} \setminus S$, δηλαδή $\ell \notin S$.

Στο άτοπο καταλήξαμε υποθέτοντας ότι $S \neq \mathbb{N}$. Επομένως θα έχουμε $S = \mathbb{N}$, και άρα ισχύει η πρώτη εκδοχή της Αρχής Μαθηματικής Επαγωγής.

• $(\text{ΑΜΕ})_1 \implies (\text{ΑΜΕ})_2$ Υποθέτουμε ότι ισχύει η πρώτη εκδοχή της Αρχής Μαθηματικής Επαγωγής και έστω η πρόταση $P(n)$, $n \in \mathbb{N}$, για την οποία ικανοποιούνται οι συνθήκες του μέρους **3**. Θεωρούμε το ακόλουθο σύνολο

$$S = \{n \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής}\}$$

Προφανώς τότε για το υποσύνολο S ικανοποιούνται οι συνθήκες (α) και (β) του μέρους **2**. Επομένως θα έχουμε ότι $S = \mathbb{N}$, το οποίο σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$. Άρα ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής.

• $(\text{ΑΜΕ})_2 \implies (\text{ΑΚΔ})$ Υποθέτουμε ότι ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής και έστω $S \subseteq \mathbb{N}$ ένα μη κενό υποσύνολο του $\mathbb{N}$.

Υποθέτουμε ότι το S δεν έχει ελάχιστο στοιχείο. Για κάθε $n \in \mathbb{N}$, θεωρούμε την πρόταση

$$P(n): \text{ για κάθε } k \in \mathbb{N} \text{ έτσι ώστε } 1 \le k \le n, \text{ ισχύει ότι: } k \notin S$$

Η πρόταση $P(1)$, δηλαδή ο ισχυρισμός ότι $1 \notin S$, είναι αληθής. Πράγματι, αν $1 \in S$, τότε προφανώς το 1 είναι ελάχιστο στοιχείο του S, κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο.

Υποθέτουμε ότι η πρόταση $P(n)$ είναι αληθής, δηλαδή κανένας από τους αριθμούς $1, 2, \cdots, n$ δεν ανήκει στο S. Αν το $n+1$ ανήκει στο S, τότε επειδή $k \notin S$, όπου $1 \le k \le n$, έπεται άμεσα ότι το $n+1$ είναι ελάχιστο στοιχείο του S, κάτι το οποίο είναι άτοπο διότι το S δεν έχει ελάχιστο στοιχείο. Άρα θα έχουμε ότι $n+1 \notin S$. Αυτό όμως σημαίνει ότι η πρόταση $P(n+1)$ είναι αληθής.

Από την δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής έπεται τότε ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$, και επομένως $\forall n \in \mathbb{N}$, $1 \le k \le n \implies k \notin S$. Με άλλα λόγια, $\forall n \in \mathbb{N}$, $n \notin S$. Αυτό όμως, επειδή $S \subseteq \mathbb{N}$, σημαίνει ότι $S = \emptyset$, κάτι το οποίο είναι άτοπο από την αρχική μας υπόθεση.

Στο άτοπο καταλήξαμε υποθέτοντας ότι το μη κενό υποσύνολο S του $\mathbb{N}$ δεν έχει ελάχιστο στοιχείο. Άρα το S έχει ελάχιστο στοιχείο και επομένως ισχύει η Αρχή Καλής Διάταξης.

– Έτσι έχουμε δείξει ότι οι τρεις πρώτες αρχές (ΑΚΔ), $(\text{ΑΜΕ})_1$, $(\text{ΑΜΕ})_2$ είναι ισοδύναμες. Ολοκληρώνουμε την απόδειξη δείχνοντας ότι: $(\text{ΑΚΔ}) \implies (\text{ΑΜ}) \implies (\text{ΑΜΕ})_2$.

• $(\text{ΑΚΔ}) \implies (\text{ΑΜ})$ Υποθέτουμε ότι ισχύει η Αρχή Καλής Διάταξης, και έστω $T \subseteq \mathbb{N}$ ένα μη-κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Έστω $b \in \mathbb{N}$ ένα άνω φράγμα του T, δηλαδή:

$$b \in \mathbb{N} \text{ και } t \le b, \ \forall t \in T$$

Ορίζουμε ένα νέο σύνολο, το σύνολο όλων των άνω φραγμάτων του T στο $\mathbb{N}$:

$$S = \{s \in \mathbb{N} \mid t < s, \ \forall t \in T\}$$

Το σύνολο S είναι μη κενό διότι $\forall t \in T$: $t \le b < b+1$, και άρα $b+1 \in S$.

Από την Αρχή Καλής Διάταξης, έπεται ότι το σύνολο S έχει ελάχιστο στοιχείο, έστω ότι αυτό είναι το s_0:

$$s_0 = \min S, \quad \text{δηλαδή } s_0 \in S \text{ και } s_0 \le s, \ \forall s \in S$$

Από τον ορισμό του συνόλου S, έπεται ότι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \le t_0$. Πράγματι, αν $s_0 - 1 > t$, $\forall t \in T$, τότε θα είχαμε ότι $s_0 - 1 \in S$, κάτι το οποίο είναι άτοπο διότι $s_0 - 1 < s_0$ και το s_0 είναι ένα ελάχιστο στοιχείο του S.

Άρα πράγματι υπάρχει ένα στοιχείο $t_0 \in T$ έτσι ώστε: $s_0 - 1 \le t_0$. Επειδή όμως έχουμε και $t_0 < s_0$, έπεται ότι θα έχουμε $s_0 - 1 = t_0 \in T$. Ισχυριζόμαστε ότι:

$$t_0 = \max T, \quad \text{δηλαδή το } t_0 \text{ είναι μέγιστο στοιχείο του } T$$

Πράγματι, το t_0 ανήκει εκ κατασκευής στο T και επιπλέον επειδή από τον ορισμό του συνόλου S έχουμε $t < s_0$, $\forall t \in T$, έπεται ότι $t \le s_0 - 1 = t_0$, $\forall t \in T$. Δηλαδή $t_0 = \max T$.

• $(\text{ΑΜ}) \implies (\text{ΑΜΕ})_2$ Υποθέτουμε ότι ισχύει η Αρχή Μεγίστου, και έστω $P(n)$ μια πρόταση η οποία εξαρτάται από το $n \in \mathbb{N}$, για την οποία ισχύει ότι η $P(1)$ είναι αληθής, και για κάθε φυσικό αριθμό n: $P(n)$ είναι αληθής $\implies$ $P(n+1)$ είναι αληθής.

Έστω ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Ορίζουμε τότε ένα σύνολο T ως εξής:

$$T = \{t \in \mathbb{N} \mid \text{η πρόταση } P(n) \text{ είναι αληθής } \forall n \in \mathbb{N}: \ 1 \leq n \leq t\}$$

Επειδή η πρόταση $P(1)$ είναι αληθής, έπεται ότι $1 \in T$ και άρα $T \neq \emptyset$. Επιπρόσθετα, ο φυσικός αριθμός m είναι προφανώς ένα άνω φράγμα για το σύνολο T. Πράγματι αν $k \in \mathbb{N}$ και $m \leq k$, τότε $k \notin T$, διότι διαφορετικά, αν $k \in T$, τότε θα είχαμε ότι η $P(m)$ είναι αληθής, κάτι το οποίο δεν ισχύει.

Έτσι το T είναι ένα μη κενό και άνω φραγμένο υποσύνολο του $\mathbb{N}$. Επομένως από την Αρχή Μεγίστου, το σύνολο T έχει ένα μέγιστο στοιχείο, έστω ότι αυτό είναι το t_0:

$$t_0 = \max T, \ \text{δηλαδή} \ \ t_0 \in T \ \ \text{και} \ \ t \leq t_0, \ \forall t \in T$$

Από τον ορισμό του συνόλου T θα έχουμε ότι η πρόταση $P(t_0)$ είναι αληθής. Τότε από την υπόθεση θα έχουμε ότι και η πρόταση $P(t_0+1)$ είναι αληθής. Αυτό όμως σημαίνει ότι η πρόταση $P(n)$ είναι αληθής για κάθε $n \in \mathbb{N}$ έτσι ώστε: $1 \leq n \leq t_0+1$, και επομένως ο αριθμός t_0+1 ανήκει στο σύνολο T. Αυτό όμως είναι άτοπο διότι $t_0 < t_0+1$ και το t_0 είναι μέγιστο στοιχείο του T.

Στο άτοπο καταλήξαμε υποθέτοντας ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε η πρόταση $P(m)$ δεν είναι αληθής. Άρα η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$, και επομένως ισχύει η δεύτερη εκδοχή της Αρχής Μαθηματικής Επαγωγής. ■

Σχόλιο 0.3.2. Από τώρα και στο εξής θα υποθέτουμε ότι ισχύει μια και επομένως και οποιαδήποτε από τις υπόλοιπες, από τις αρχές του παραπάνω Θεωρήματος. Κάθεμια από τις παραπάνω αρχές είναι ισοδύναμη με την αξιωματική θεμελίωση του συνόλου $\mathbb{N}$ των φυσικών αριθμών, η οποία πιστοποιεί την ύπαρξη ενός συνόλου $\mathbb{N}$ το οποίο ικανοποιεί την Αρχή Μαθηματικής Επαγωγής. √

Εναλλακτικές Μορφές Μαθηματικής Επαγωγής. Είδαμε μέχρι τώρα δύο (ισοδύναμες) μορφές της Αρχής Μαθηματικής Επαγωγής, τις $(\text{ΑΜΕ})_1$ και $(\text{ΑΜΕ})_2$. Θα δούμε κάποιες ακόμα χρήσιμες μορφές της Αρχής Μαθηματικής Επαγωγής.

$(\text{ΑΜΕ})_3$ Αρχη Μαθηματικης Επαγωγης$_3$: Έστω $P(n)$ μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(1)$ είναι αληθής.

(β) $\forall k \in \mathbb{N}$, $1 \leq k < n$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(n)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \in \mathbb{N}$.

$(\text{ΑΜΕ})_4$ Αρχη Μαθηματικης Επαγωγης$_4$: Έστω ότι n_0 είναι ένας φυσικός αριθμός, και $P(n)$ είναι μια πρόταση η οποία εξαρτάται από τον φυσικό αριθμό $n \in \mathbb{N}$, όπου $n \geq n_0$, για την οποία ισχύουν τα εξής:

(α) Η πρόταση $P(n_0)$ είναι αληθής.

(β) Είτε $\forall k \in \mathbb{N}$, $n_0 \leq k < n$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(n)$ είναι αληθής, είτε $\forall k \in \mathbb{N}$, $k \geq n_0$: η πρόταση $P(k)$ είναι αληθής $\implies$ η πρόταση $P(k+1)$ είναι αληθής.

Τότε: η πρόταση $P(n)$ είναι αληθής, $\forall n \geq n_0$.

Υπενθυμίζουμε ότι στο σύνολο $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ των μη αρνητικών ακεραίων ορίζονται οι συνήθεις πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» φυσικών αριθμών, οι οποίες ικανοποιούν τις ακόλουθες ιδιότητες, $\forall x, y, z \in \mathbb{N}$:

1. $(x+y)+z = x+(y+z)$ (Προσεταιριστικότητα της πρόσθεσης)
2. $x+y = y+x$ (Μεταθετικότητα της πρόσθεσης)
3. $x+0 = x = 0+x$ (Ύπαρξη ουδετέρου στοιχείου ως προς την πρόσθεση)

4. $x+y=x+z \implies y=z$ (Νόμος διαγραφής ως προς την πρόσθεση)
5. $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ (Προσεταιριστικότητα του πολλαπλασιασμού)
6. $x\cdot y = y\cdot x$ (Μεταθετικότητα του πολλαπλασιασμού)
7. $x\cdot 1 = x = 1\cdot x$ (Ύπαρξη ουδετέρου στοιχείου ως προς τον πολλαπλασιασμό)
8. $x\cdot y = x\cdot z$ και $x\neq 0 \implies y=z$ (Νόμος διαγραφής ως προς τον πολλαπλασιασμό)
9. $x\cdot(y+z) = x\cdot y + x\cdot z$ και $(x+y)\cdot z = x\cdot z + y\cdot z$ (Επιμεριστικότητα του πολλαπλασιασμού ως προς την πρόσθεση)

Το σύνολο $\mathbb{N}_0$ των μη αρνητικών ακεραίων είναι εφοδιασμένο με τη συνήθη σχέση διάταξης «≤»:

$$b\leq a \iff \text{υπάρχει } c\in\mathbb{N}_0 : \ a=b+c$$

δηλαδή ο μη αρνητικός ακέραιος a είναι *μεγαλύτερος ή ίσος* από τον μη αρνητικό ακέραιο b, ισοδύναμα ο b είναι *μικρότερος ή ίσος* από τον a, αν η εξίσωση $a=b+x$ έχει λύση στο σύνολο $\mathbb{N}_0$. Θα γράφουμε επίσης $a\geq b$, και αν $b\leq a$ και $a\neq b$ θα γράφουμε $b<a$ ή $a>b$.

Για την σχέση διάταξης ≤ στο σύνολο $\mathbb{N}_0$ ισχύουν οι ακόλουθες οικείες ιδιότητες, $\forall x,y,z\in\mathbb{N}_0$:

1. $y\leq x$ και $x\leq y \implies x=y$ (Αντισυμμετρία)
2. $x\leq y$ και $y\leq z \implies x\leq z$ (Μεταβατικότητα)
3. Είτε $x\leq y$ είτε $y\leq x$ (Διχοτομία)
4. $y\leq x \implies y+z\leq x+z$ (Συμβατότητα ως προς την πρόσθεση)
5. $y\leq x \implies y\cdot z\leq x\cdot z$ (Συμβατότητα ως προς τον πολλαπλασιασμό)
6. $y\leq x$ και $z\leq w \implies y+z\leq x+w$ και $y\cdot z\leq x\cdot w$.

0.3.2 Διαιρετότητα Ακεραίων

Συμβολίζουμε με $\mathbb{Z}$ το σύνολο των ακεραίων αριθμών:

$$\mathbb{Z}=\{\cdots,-2,-1,0,1,2,\cdots\}$$

το οποίο είναι ξένη ένωση $-\mathbb{N}\cup\{0\}\cup\mathbb{N}$ του συνόλου $-\mathbb{N}=\{\cdots,-3,-2,-1\}$ των αρνητικών ακεραίων αριθμών, του μηδενός 0, και του συνόλου $\mathbb{N}$ των θετικών ακεραίων αριθμών. Το σύνολο $\mathbb{Z}$ προκύπτει ως επέκταση του συνόλου $\mathbb{N}_0$ έτσι ώστε, $\forall n\in\mathbb{N}_0$, η εξίσωση $n+x=0$ να έχει λύση.

Ένας ακέραιος b **διαιρεί** τον ακέραιο a ή ο ακέραιος a είναι **πολλαπλάσιο** του ακεραίου b, αν υπάρχει ακέραιος c έτσι ώστε $a=bc$. Αν $b\mid a$, τότε ο ακέραιος b καλείται **διαιρέτης** του a και θα γράφουμε $b\mid a$. Ο ακέραιος b καλείται γνήσιος διαιρέτης του a αν $b\neq\pm a$ και $b\neq\pm 1$. Αν ο ακέραιος b δεν διαιρεί τον ακέραιο a θα γράφουμε $b\nmid a$. Οι βασικές ιδιότητες διαιρετότητας ακεραίων περιγράφονται στην ακόλουθη Πρόταση.

Πρόταση 0.3.3. *Έστω $a,b,c\in\mathbb{Z}$.*

1. *(i) $a\mid a$, (ii) $1\mid a$, (iii) $a\mid 0$, και (iv) $0\mid b \iff b=0$.*
2. *$a\mid b \iff -a\mid b \iff a\mid -b \iff -a\mid -b \iff |a|\mid|b|$.*
3. *$a\mid b$ και $b\mid c \implies a\mid c$.*
4. *$a\mid b$ και $c\mid d \implies ac\mid bd$.*
5. *$a\mid b$ και $a\mid c \implies a\mid bx+cy$, $\forall x,y\in\mathbb{Z}$.*

6. $a \mid b$ *και* $b \neq 0 \implies |a| \leq |b|$.

7. $a \mid b$ *και* $b \mid a \implies |a| = |b|$.

Θεώρημα 0.3.4 (Ευκλείδεια Διαίρεση)**.** *Αν a, b είναι ακέραιοι, και $b \neq 0$, τότε υπάρχει μοναδικό ζεύγος ακεραίων q, r έτσι ώστε:*

$$a = bq + r, \qquad 0 \leq r < |b|$$

Υπενθυμίζουμε ότι ο θετικός ακέραιος $p > 1$ καλείται **πρώτος** αν ο p δεν έχει γνήσιους θετικούς διαιρέτες. Ο θετικός ακέραιος a καλείται **σύνθετος** αν $a = bc$, για κάποιους θετικούς ακέραιους b, c, όπου $1 < b, c < a$. Οι πρώτοι αριθμοί αποτελούν θεμελιώδη έννοια στα Μαθηματικά και ικανοποιούν σημαντικές ιδιότητες

Πρόταση 0.3.5. *Έστω $a, b \in \mathbb{Z}$ και p είναι ένας πρώτος αριθμός έτσι ώστε: $p \mid ab$. Τότε είτε $p \mid a$ είτε $p \mid b$.*

Θεώρημα 0.3.6 (Θεμελιώδες Θεώρημα της Αριθμητικής)**.** *Κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί ως γινόμενο $a = p_1 p_2 \cdots p_n$ πρώτων αριθμών $p_1, p_2, \cdots, p_n$ με μοναδικό τρόπο: αν $a = q_1 q_2 \cdots q_m$, όπου οι θετικοί ακέραιοι $q_1, q_2, \cdots, q_m$ είναι πρώτοι, τότε $n = m$ και υπάρχει μια αναδιάταξη των πρώτων p_i και q_j, όπου $1 \leq i, j \leq n$, έτσι ώστε: $p_i = q_i$, $1 \leq i \leq n$.*

Σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής, κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί με μοναδικό τρόπο ως γινόμενο

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \tag{1}$$

όπου οι $p_1, p_2, \cdots, p_k$ είναι διακεκριμμένοι πρώτοι αριθμοί με $p_1 < p_2 < \cdots < p_k$, και $a_i \geq 1$, $1 \leq i \leq k$. Η παράσταση (1) καλείται η **πρωτογενής ανάλυση** του a. Η πρωτογενής ανάλυσης ενός θετικού ακεραίου $a > 1$ μπορεί να επεκταθεί στην πρωτογενή ανάλυση κάθε ακεραίου $a \neq 0, \pm 1$: $a = \pm p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$.

Όπως προκύπτει εύκολα από την πρωτογενή ανάλυση (1) ενός θετικού ακεραίου $a > 1$, ένας θετικός ακέραιος d είναι διαιρέτης του a αν και μόνο αν μπορεί να γραφεί στην μορφή $d = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, όπου $0 \leq b_i \leq a_i$, $1 \leq i \leq k$.

Αν $n_1, n_2, \cdots, n_k$ είναι θετικοί ακέραιοι, τότε ένας **μέγιστος κοινός διαιρέτης** των $n_1, n_2, \cdots, n_k$ είναι ένας θετικός ακέραιος d ο οποίος ικανοποιεί τις ακόλουθες ιδιότητες:

1. $d \mid n_i$, $1 \leq i \leq k$.

2. Αν $\delta \in \mathbb{N}$ και $\delta \mid n_i$, $1 \leq i \leq k$, τότε $\delta \leq d$.

Παρόμοια ένα **ελάχιστο κοινό πολλαπλάσιο** των θετικών ακεραίων $n_1, n_2, \cdots, n_k$ είναι ένας θετικός ακέραιος e ο οποίος ικανοποιεί τις ακόλουθες ιδιότητες:

1. $n_i \mid e$, $1 \leq i \leq k$.

2. Αν $\epsilon \in \mathbb{N}$ και $n_i \mid \epsilon$, $1 \leq i \leq k$, τότε $e \leq \epsilon$.

Ο μέγιστος κοινός διαιρέτης, αντίστοιχα το ελάχιστο κοινό πολλαπλάσιο, θετικών ακεραίων a_i, $1 \leq i \leq k$, υπάρχει πάντα, είναι μοναδικός, αντίστοιχα μοναδικό, και συμβολίζεται με $(a_1, a_2, \cdots, a_k)$ ή $\text{ΜΚΔ}(a_1, a_2, \cdots, a_k)$, αντίστοιχα $[a_1, a_2, \cdots, a_k]$ ή $\text{ΕΚΠ}(a_1, a_2, \cdots, a_k)$. Οι θετικοί ακέραιοι $a_1, a_2, \cdots, a_k$ καλούνται **πρώτοι μεταξύ τους**, αντίστοιχα **πρώτοι μεταξύ τους ανά δύο**, αν $(a_1, a_2, \cdots, a_k) = 1$, αντίστοιχα αν $(a_i, a_j) = 1$, $1 \leq i \neq j \leq n$.

Πρόταση 0.3.7. *Έστω $a, b \in \mathbb{N}$.*

1. *Αν $\delta \in \mathbb{N}$ και $\delta \mid a$ και $\delta \mid b$, τότε $\delta \mid (a, b)$.*

2. *Αν $\epsilon \in \mathbb{N}$ και $a \mid \epsilon$ και $b \mid \epsilon$, τότε $[a, b] \mid \epsilon$.*

3. *Υπάρχουν ακέραιοι x και y έτσι ώστε: $(a, b) = ax + by$. Αντίστροφα, αν $ax + by = 1$, τότε $(a, b) = 1$.*

4. *Αν* $a \mid bc$ *και* $(a,b) = 1$, *τότε* $a \mid c$.

5. $$(a,b)[a,b] = ab$$

6. *Οι θετικοί ακέραιοι* a *και* b *μπορούν να γραφούν ως γινόμενο μη-αρνητικών δυνάμεων των ίδιων διακεκριμένων πρώτων αριθμών* $p_1, p_2, \cdots, p_k$*:*

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{και} \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}, \quad \text{όπου} \quad a_i, b_i \geq 0, \quad 1 \leq i \leq k$$

και τότε:

$$(a,b) = p_1^{\min\{a_1,b_1\}} p_2^{\min\{a_2,b_2\}} \cdots p_k^{\min\{a_k,b_k\}}$$
$$[a,b] = p_1^{\max\{a_1,b_1\}} p_2^{\max\{a_2,b_2\}} \cdots p_k^{\max\{a_k,b_k\}}$$

Οι ισχυρισμοί της παραπάνω Πρότασης γενικεύονται εύκολα για πεπερασμένο πλήθος θετικών ακεραίων $a_1, a_2, \cdots, a_k$.

0.4 Μιγαδικοί Αριθμοί

Επεκτάσεις του συνόλου των ακεραίων αριθμών αποτελούν με σειρά γενικότητας:

1. Το σύνολο $\mathbb{Q}$ των ρητών αριθμών:
$$\mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \neq 0 \right\}$$
όπου μπορούμε να υποθέσουμε ότι $(a,b) = 1$. Το σύνολο $\mathbb{Q}$ προκύπτει ως επέκταση του συνόλου $\mathbb{Z}$ των ακεραίων, έτσι ώστε εξισώσεις της μορφής $bx = a$, $a, b \in \mathbb{Z}$, $b \neq 0$, να έχουν λύση.

2. Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών το οποίο προκύπτει ως επέκταση του συνόλου $\mathbb{Q}$ των ρητών αριθμών, έτσι ώστε εξισώσεις της μορφής $x^2 = 2$ να έχουν λύση.

3. Το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών το οποίο προκύπτει ως επέκταση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών, έτσι ώστε εξισώσεις της μορφής $x^2 + 1 = 0$ να έχουν λύση.

Θεωρούμε γνωστή τη θεμελίωση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών. Το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών μπορεί να οριστεί κατά πολλούς (ισοδύναμους) τρόπους, κάποιους από αυτούς θα δούμε και σε επόμενα κεφάλαια. Άτυπα μπορούμε να πούμε ότι ένας μιγαδικός αριθμός είναι της μορφής $a + bi$, όπου οι a, b είναι πραγματικοί αριθμοί, και ικανοποιούνται οι εξής κανόνες ισότητας, πρόσθεσης «+» και πολλαπλασιασμού «·»:

(i) $a + bi = c + di$, όπου $a, b, c, d \in \mathbb{R}$, αν και μόνο αν $a = c$ και $b = d$.

(ii) $(a + bi) + (c + di) = (a + c) + (b + d)i$ και $(a + bi) - (c + di) = (a + c) - (b + d)i$.

(iii) $(a + bi) \cdot (c + di) = (ac - bd) + (bc + ad)i$.

Αυστηρότερα, θεωρούμε το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$ του συνόλου $\mathbb{R}$ των πραγματικών αριθμών με τον εαυτό του, στο οποίο ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·», ως εξής:

$$(a,b) + (c,d) = (a + c, b + d) \quad \text{και} \quad (a,b) \cdot (c,d) = (ac - bd, ad + bc)$$

Θέτοντας $1 = (1,0)$ και $i = (0,1)$, και ορίζοντας $r(a,b) = (ra, rb)$, $\forall r \in \mathbb{R}$, θα έχουμε:

$$i^2 = -1 \quad \text{και} \quad (a,b) = a(1,0) + b(0,1) = a1 + bi \quad \text{και} \quad 1 \cdot (a,b) = (a,b) = (a,b) \cdot 1$$

Συνήθως παραλείπουμε το σύμβολο $1 = (1,0)$ στην γραφή $(a,b) = a1 + bi$. Έτσι το ζεύγος $(a,b) \in \mathbb{R} \times \mathbb{R}$ μπορεί να γραφεί ως $z = a + bi$ και καλείται **μιγαδικός αριθμός** με *πραγματικό μέρος* τον πραγματικό αριθμό a και *φανταστικό μέρος* τον πραγματικό αριθμό b. Ο μιγαδικός αριθμός i καλείται **φανταστική μονάδα**. Το σύνολο όλων των μιγαδικών αριθμών συμβολίζεται με $\mathbb{C}$, και ως σύνολο ταυτίζεται με το καρτεσιανό γινόμενο $\mathbb{R} \times \mathbb{R}$, το οποίο θεωρούμε πάντα εφοδιασμένο με τις πράξεις πρόσθεσης και πολλαπλασιασμού, όπως αυτές περιγράφονται με βάση τους παραπάνω συμβολισμούς, από τις σχέσεις (i), (ii), και (iii). Χάριν ευκολίας στον συμβολισμό, ακολουθούμε τις εξής συμβάσεις: $0 + 0i = 0$ και $a + 0i = a$.

Για τις παραπάνω πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» μιγαδικών αριθμών ικανοποιούνται οι ακόλουθες ιδιότητες, $\forall x, y, z \in \mathbb{C}$:

1. $(x + y) + z = x + (y + z)$ (Προσεταιριστικότητα της πρόσθεσης)
2. $x + y = y + x$ (Μεταθετικότητα της πρόσθεσης)
3. $x + 0 = x = 0 + x$ (Ύπαρξη ουδετέρου στοιχείου ως προς την πρόσθεση)
4. Για κάθε $x \in \mathbb{Z}$, $x + (-x) = 0 = (-x) + x$ (Ύπαρξη αντιθέτου στοιχείου ως προς την πρόσθεση)
5. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Προσεταιριστικότητα του πολλαπλασιασμού)
6. $x \cdot y = y \cdot x$ (Μεταθετικότητα του πολλαπλασιασμού)
7. $x \cdot (y + z) = x \cdot y + x \cdot z$ και $(x + y) \cdot z = x \cdot z + y \cdot z$ (Επιμεριστικότητα του πολλαπλασιασμού ως προς την πρόσθεση)
8. $x \cdot 1 = x = 1 \cdot x$ (Ύπαρξη ουδετέρου στοιχείου ως προς τον πολλαπλασιασμό)

Από τις παραπάνω ιδιότητες έπονται άμεσα οι εξής νόμοι διαγραφής:

$$x + y = x + z \implies y = z \qquad \text{(Νόμος διαγραφής ως προς την πρόσθεση)}$$

$$x \cdot y = x \cdot z \text{ και } x \neq 0 \implies y = z \quad \text{(Νόμος διαγραφής ως προς τον πολλαπλασιασμό)}$$

Αν $z = a + bi$ είναι ένας μιγαδικός αριθμός, τότε ο *συζυγής* του z είναι ο μιγαδικός αριθμός $\overline{z} = a - bi$, και έτσι ορίζεται η απεικόνιση συζυγίας

$$\bar{}: \mathbb{C} \longrightarrow \mathbb{C}, \quad z = a + bi \longmapsto \overline{z} = a - bi$$

η οποία ικανοποιεί τις ακόλουθες ιδιότητες, $\forall z, w \in \mathbb{C}$:

(α) $\overline{\overline{z}} = z$.

(β) $\overline{z \pm w} = \overline{z} \pm \overline{w}$.

(γ) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.

(δ) $z \cdot \overline{z} \in \mathbb{R}$. Επιπλέον $z \cdot \overline{z} \geq 0$ και $z \cdot \overline{z} = 0$ αν και μόνο αν $z = 0$.

Το *μέτρο* του μιγαδικού αριθμού $z = a + bi$ ορίζεται να είναι ο μη-αρνητικός πραγματικός αριθμός

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}$$

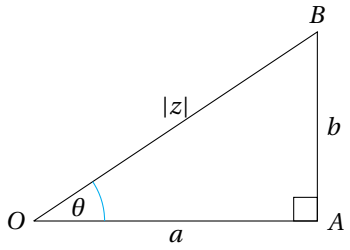
Τότε εύκολα βλέπουμε ότι $\forall z, w \in \mathbb{C}$:

$$|z| \in \mathbb{R}, \quad |z| \geq 0 \quad \text{και} \quad |z| = 0 \iff z = 0, \qquad |z \cdot w| = |z| \cdot |w|$$

Παρατηρούμε ότι, αν z είναι ένας μη-μηδενικός μιγαδικός αριθμός, τότε ορίζεται ο μιγαδικός αριθμός $\frac{\overline{z}}{|z|^2}$ και ισχύει ότι $z \cdot \frac{\overline{z}}{|z|^2} = \frac{|z|}{|z|^2} = 1$. Επομένως:

9. Για κάθε $0 \neq x \in \mathbb{C}$, υπάρχει μιγαδικός αριθμός y έτσι ώστε $x \cdot y = 1 = y \cdot x$ (Ύπαρξη αντιστρόφου στοιχείου ως προς τον πολλαπλασιασμό)

Επιστρέφοντας προσωρινά στην μορφή ενός μιγαδικού αριθμού $z = a + bi$ ως ζεύγους $z = (a, b)$ και άρα ως σημείου του επιπέδου $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$, ο μη αρνητικός αριθμός $|z| = \sqrt{a^2 + b^2}$ είναι η απόσταση του σημείου του επιπέδου με συντεταγμένες (a, b) από την αρχή των αξόνων με συντεταγμένες $(0, 0)$. Στο ορθογώνιο τρίγωνο OBA το οποίο σχηματίζεται στο επίπεδο $\mathbb{R}^2$ από την αρχή των αξόνων $O = (0, 0)$, από το σημείο $B = (a, b)$, και το σημείο $A = (a, 0)$, έστω θ η γωνία την οποία σχηματίζουν οι πλευρές OB και OA:



Τότε θα έχουμε την *πολική μορφή* του μιγαδικού αριθμού $z = a + bi$:

$$a = |z| \cos\theta, \qquad b = |z| \sin\theta, \quad \text{και} \quad z = |z|\big(\cos\theta + i \sin\theta\big)$$

Η πολική μορφή ενός μιγαδικού αριθμού είναι χρήσιμη στον προσδιορισμό της n-οστής δύναμης ενός μιγαδικού αριθμού, όπως πιστοποιεί το ακόλουθο Θεώρημα.

Θεώρημα 0.4.1 (Θεώρημα De Moivre). [6] *Αν $z = a + bi = r(\cos\theta + i \sin\theta)$, όπου $r = |z|$, τότε, $\forall n \geq 1$:*

$$z^n = (a + bi)^n = [r(\cos\theta + i \sin\theta)]^n = r^n(\cos n\theta + i \sin n\theta)$$

Χρησιμοποιώντας τον τύπο του Euler $e^{ix} = \cos x + i \sin x$, $\forall x \in \mathbb{R}$, μπορούμε επίσης να γράψουμε:

$$z = re^{i\theta} = r(\cos\theta + i \sin\theta)$$

Ένας μιγαδικός αριθμός z καλείται **n-οστή ρίζα της μονάδας** αν $z^n = 1$. Το σύνολο όλων των n-οστών ριζών της μονάδας συμβολίζεται με

$$\mathsf{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

Αν $z = r(\cos\theta + i \sin\theta) \in \mathsf{U}_n$ είναι μια n-οστή ρίζα της μονάδας, όπου $r = |z|$, τότε $|z^n| = |z|^n = 1$ και άρα επειδή ο πραγματικός αριθμός $|z|$ είναι μη αρνητικός θα έχουμε $r = |z| = 1$. Επιπλέον

$$z^n = 1 \implies \cos n\theta + i \sin n\theta = 1 \implies \cos n\theta = 1 \text{ και } \sin n\theta = 0 \implies \theta = \frac{2k\pi}{n}, \quad k \in \mathbb{Z}$$

Ιδιαίτερα έπεται ότι

$$\text{αν} \qquad \omega_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}, \qquad \text{τότε} \qquad \omega_n^n = 1$$

Μια n-οστή ρίζα της μονάδας z καλείται **πρωταρχική n-οστή ρίζα της μονάδας**, αν $z^k \neq 1$ για κάθε θετικό ακέραιο $k < n$.

Ισχυρισμός: Ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας και, αν ω είναι μια πρωταρχική n-οστή ρίζα της μονάδας, τότε υπάρχει μια ισότητα συνόλων:

$$\mathsf{U}_n = \{\omega^k \in \mathbb{C} \mid k \in \mathbb{Z}\} = \{1, \omega, \omega^2, \cdots, \omega^{n-1}\}$$

[6] Abraham de Moivre (26 Μαίου 1667 - 27 Νοεμβρίου 1754) [https://en.wikipedia.org/wiki/Abraham_de_Moivre]: Γάλλος μαθηματικός με συμβολή στην τριγωνομετρία, στους μιγαδικούς αριθμούς, και στη Θεωρία Πιθανοτήτων. Γνωστός κυρίως για το παρόν Θεώρημα που φέρει το όνομά του.

Πράγματι από την Ευκλείδεια Διαίρεση του ακεραίου k με το n: $k = nq + r$, $0 \leq r < n$, έπεται ότι

$$\omega^k = \omega^{nq+r} = (\omega^n)^q \cdot \omega^r = \omega^r$$

Επιπλέον τα στοιχεία $1, \omega, \omega^2, \cdots, \omega^{n-1}$ είναι ανά δύο διαφορετικά διότι αν $\omega^k = \omega^l$, όπου $0 \leq k, l \leq n-1$ και όπου χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $l \leq k$, τότε $\omega^{k-l} = 1$ και αυτό είναι άτοπο διότι $k - l < n$ και ο αριθμός ω είναι μια n-στή ρίζα της μονάδας.

Ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μοναδας διότι, αν $\omega_n^k = 1$, όπου $k < n$, τότε όπως παραπάνω θα έχουμε $\frac{2\pi}{n} = \frac{2l\pi}{n}$, για κάποιον ακέραιο l και επομένως $k = nl$, δηλαδή $n \mid k$ και άρα $n \leq k$ το οποίο είναι άτοπο. Επομένως ο μιγαδικός αριθμός ω_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας.

Επομένως κάθε άλλη n-οστή ρίζα της μονάδας είναι ένας εκ των μιγαδικών αριθμών

$$\mathsf{U}_n = \{\omega_n^0 = 1, \omega_n, \omega_n^2, \cdots, \omega_n^{n-1}\}$$

Μέρος Ι

Θεωρία Ομάδων

Κεφάλαιο 1

Σχέσεις Ισοδυναμίας και Πράξεις

Στο παρόν Κεφάλαιο θα αναπτύξουμε τα βασικά στοιχεία από τη θεωρία σχέσεων μερικής διάταξης, σχέσεων ισοδυναμίας και διαμερίσεων οι οποίες ορίζονται επί ενός συνόλου. Στη συνέχεια θα μελετήσουμε βασικές ιδιότητες αλγεβρικών δομών, δηλαδή συνόλων τα οποία είναι εφοδιασμένα με μια ή περισσότερες διμελείς πράξεις οι οποίες ικανοποιούν συγκεκριμένα αξιώματα τα οποία γενικεύουν γνωστές ιδιότητες της πρόσθεσης και του πολλαπλασιασμού σε οικεία σύνολα αριθμών. Τέλος, θα αναλύσουμε τις στοιχειώδεις ιδιότητες μονοειδών, μιας εκ των κυριότερων αλγεβρικών δομών η οποία αποτελεί τη βάση για τις πλέον σημαντικές αλγεβρικές δομές τις οποίες θα μελετήσουμε αργότερα: τη δομή της ομάδας και τη δομή του δακτυλίου.

1.1 Σχέσεις Μερικής Διάταξης και Διαγράμματα Hasse

Στην παρούσα ενότητα θα μελετήσουμε εν συντομία την έννοια του μερικώς διατεταγμένου συνόλου και της γεωμετρικής παράστασής του μέσω του αντίστοιχου διαγράμματος Hasse.

1.1.1 Σχέσεις μερικής διάταξης

Θα ξεκινήσουμε υπενθυμίζοντας κάποιες βασικές έννοιες γύρω από διάφορους τύπους σχέσεων οι οποίες ορίζονται επί συνόλων.

Έστω ότι X και Y είναι δύο μη κενά σύνολα. Υπενθυμίζουμε από το Κεφάλαιο 0 ότι μια (διμελής) **σχέση $\mathscr{R}$ από το σύνολο X στο σύνολο Y** είναι ένα υποσύνολο $\mathscr{R}$ του καρτεσιανού γινομένου $X \times Y$, δηλαδή $\mathscr{R} \subseteq X \times Y$. Μια σχέση $\mathscr{R}$ από το σύνολο X στον εαυτό του καλείται **σχέση επί του X**.

Συμβολισμός: Αν $\mathscr{R}$ είναι μια σχέση από το σύνολο X στο σύνολο Y, και $(x, y) \in \mathscr{R} \subseteq X \times Y$, τότε θα γράφουμε:

$$x \mathscr{R} y \qquad \text{ή} \qquad x \sim_{\mathscr{R}} y \qquad \text{ή} \qquad x \equiv y (\mathscr{R})$$

Υπό προϋποθέσεις μπορούν να οριστούν διάφορες «πράξεις» σε σχέσεις επί συνόλων. Θεωρούμε μη-κενά σύνολα X, Y, Z, και W. Έστω $\mathscr{R} \subseteq X \times Y$, $\mathscr{T} \subseteq Y \times Z$, και $\mathscr{S} \subseteq Z \times W$, σχέσεις από το X και Y, από το Y στο Z, και από το Z στο W αντίστοιχα. Η *σύνθεση* $\mathscr{R} \circ \mathscr{T}$ των σχέσεων $\mathscr{R}$ και $\mathscr{T}$ ορίζεται ως η ακόλουθη σχέση από το X στο Z:

$$\mathscr{T} \circ \mathscr{R} = \left\{(x, z) \in X \times Z \mid \text{υπάρχει } y \in Y : (x, y) \in \mathscr{R} \text{ και } (y, z) \in \mathscr{T}\right\}$$

Επίσης η *αντίστροφη* της σχέσης $\mathscr{R}$ από το X στο Y ορίζεται ως η ακόλουθη σχέση από το Y στο X:

$$\mathscr{R}^{-1} = \left\{(y, x) \in Y \times X \mid (x, y) \in \mathscr{R}\right\}$$

Συμβολίζουμε με I_X την ακόλουθη «διαγώνια» ή ταυτοτική σχέση επί ενός συνόλου X:

$$I_X = \left\{(x, x) \in X \times X \mid x \in X\right\}$$

Στη συνέχεια θα μας απασχολήσουν κυρίως τρεις κατηγορίες σχέσεων επί ενός συνόλου: οι σχέσεις μερικής διάταξης, οι απεικονίσεις και οι σχέσεις ισοδυναμίας. Γενικά οι κυριότερες ιδιότητες τις οποίες μπορεί να ικανοποιεί ή να μην ικανοποιεί μία σχέση $\mathscr{R}$ επί ενός μη-κενού συνόλου X είναι οι ακόλουθες:

Κυριότερες Ιδιότητες Σχέσεων $\mathscr{R}$ επί Συνόλων X

1.
$$\forall x \in X: \quad (x,x) \in \mathscr{R} \qquad \text{(ανακλαστική ιδιότητα)}$$

2.
$$\forall x,y \in X: \quad (x,y) \in \mathscr{R} \implies (y,x) \in \mathscr{R} \qquad \text{(συμμετρική ιδιότητα)}$$

3.
$$\forall x,y \in X: \quad (x,y) \in \mathscr{R} \text{ και } (y,x) \in \mathscr{R} \implies x = y \qquad \text{(αντισυμμετρική ιδιότητα)}$$

4.
$$\forall x,y,z \in X: \quad (x,y) \in \mathscr{R} \text{ και } (y,z) \in \mathscr{R} \implies (x,z) \in \mathscr{R} \qquad \text{(μεταβατική ιδιότητα)}$$

Η επόμενη παρατήρηση περιγράφει τις παραπάνω ιδιότητες με βάση τις πράξεις μεταξύ σχέσεων που έχουμε ορίσει.

Παρατήρηση 1.1.1. Έστω $\mathscr{R}$ μια σχέση επί του μη κενού συνόλου X. Τότε:

1. *Η σχέση $\mathscr{R}$ είναι ανακλαστική αν και μόνο αν $I_X \subseteq \mathscr{R}$.*

   Πράγματι: αν η σχέση $\mathscr{R}$ είναι ανακλαστική, τότε για κάθε στοιχείο $x \in X$, έχουμε $(x,x) \in \mathscr{R}$ και επομένως $I_X \subseteq \mathscr{R}$. Αντίστροφα, αν $I_X \subseteq \mathscr{R}$, τότε επειδή εξ ορισμού για κάθε στοιχείο $x \in X$, έχουμε $(x,x) \in I_X$, έπεται ότι $\forall x \in X$: $(x,x) \in \mathscr{R}$ και άρα η σχέση R είναι ανακλαστική.

2. *Η σχέση $\mathscr{R}$ είναι συμμετρική αν και μόνο αν $\mathscr{R}^{-1} = \mathscr{R}$.*

   Πράγματι: έστω ότι η σχέση $\mathscr{R}$ είναι συμμετρική, και έστω $(x,y) \in \mathscr{R}^{-1}$. Τότε εξ ορισμού έχουμε $(y,x) \in \mathscr{R}$ και, επειδή η $\mathscr{R}$ είναι συμμετρική, έπεται ότι $(x,y) \in \mathscr{R}$ και επομένως $\mathscr{R}^{-1} \subseteq \mathscr{R}$. Παρόμοια, αν $(x,y) \in \mathscr{R}$, τότε λόγω συμμετρικότητας έπεται ότι $(y,x) \in \mathscr{R}$ και επομένως εξ ορισμού θα έχουμε $(x,y) \in \mathscr{R}^{-1}$. Άρα $\mathscr{R} \subseteq \mathscr{R}^{-1}$ και επομένως $\mathscr{R} = \mathscr{R}^{-1}$. Αντίστροφα αν $\mathscr{R} = \mathscr{R}^{-1}$, τότε προφανώς για τυχόντα στοιχεία $x,y \in X$, αν $(x,y) \in \mathscr{R}$, τότε $(x,y) \in \mathscr{R}^{-1}$ το οποίο σημαίνει ότι $(y,x) \in \mathscr{R}$, δηλαδή η $\mathscr{R}$ είναι συμμετρική.

3. *Η σχέση $\mathscr{R}$ είναι αντισυμμετρική αν και μόνο αν $\mathscr{R} \cap \mathscr{R}^{-1} \subseteq I_X$.*

   Πράγματι: Έστω ότι η σχέση $\mathscr{R}$ είναι αντισυμμετρική, και έστω $(x,y) \in \mathscr{R} \cap \mathscr{R}^{-1}$, δηλαδή $(x,y) \in \mathscr{R}$ και $(x,y) \in \mathscr{R}^{-1}$. Η τελευταία σχέση εξ ορισμού δίνει ότι $(y,x) \in \mathscr{R}$ και τότε λόγω αντισυμμετρικότητας έπεται ότι $x = y$ και άρα $(x,y) = (x,x) \in I_X$. Επομένως $\mathscr{R} \cap \mathscr{R}^{-1} \subseteq I_X$. Αντίστροφα, αν ισχύει $\mathscr{R} \cap \mathscr{R}^{-1} \subseteq I_X$ και αν $(x,y) \in \mathscr{R}$ και $(y,x) \in \mathscr{R}$, τότε $(x,y) \in \mathscr{R}$ και $(x,y) \in \mathscr{R}^{-1}$, δηλαδή $(x,y) \in \mathscr{R} \cap \mathscr{R}^{-1} \subseteq I_X$, και επομένως $x = y$, δηλαδή η $\mathscr{R}$ είναι αντισυμμετρική.

4. *Η σχέση $\mathscr{R}$ είναι μεταβατική αν και μόνο αν $\mathscr{R} \circ \mathscr{R} \subseteq \mathscr{R}$.*

   Πράγματι: Έστω ότι η σχέση $\mathscr{R}$ είναι μεταβατική και έστω $(x,y) \in \mathscr{R} \circ \mathscr{R}$, δηλαδή υπάρχει $z \in X$ έτσι ώστε $(x,z) \in \mathscr{R}$ και $(z,y) \in \mathscr{R}$. Τότε λόγω μεταβατικότητας θα έχουμε ότι $(x,y) \in \mathscr{R}$ και επομένως $\mathscr{R} \circ \mathscr{R} \subseteq \mathscr{R}$. Αντίτσροφα, αν $\mathscr{R} \circ \mathscr{R} \subseteq \mathscr{R}$, και $x,y,z \in X$ έτσι ώστε $(x,y) \in \mathscr{R}$ και $(y,z) \in \mathscr{R}$, τότε εξ ορισμού $(x,z) \in \mathscr{R} \circ \mathscr{R} \subseteq \mathscr{R}$ και επομένως η $\mathscr{R}$ είναι μεταβατική. ▲

Ορισμός 1.1.2. *Μια σχέση $\mathscr{R} \subseteq X \times X$ επί του συνόλου X καλείται* **σχέση μερικής διάταξης** *αν η $\mathscr{R}$ ικανοποιεί (α) την ανακλαστική ιδιότητα, (β) την αντισυμμετρική ιδιότητα, και (γ) την μεταβατική ιδιότητα.*

Όπως θα δούμε αργότερα και σε συγκεκριμένα παραδείγματα, μια σχέση μερικής διάταξης επί ενός συνόλου «συγκρίνει» στοιχεία του συνόλου ως προς μια έννοια μεγέθους. Έτσι συνήθως μια σχέση μερικής διάταξης $\mathscr{R}$ επί ενός συνόλου X συμβολίζεται με ένα από τα παρακάτω σύμβολα

$$\leq, \quad \preccurlyeq, \quad \lesssim, \quad \eqslantless, \quad \subseteq, \quad \trianglelefteq, \quad \leqslant, \quad \precsim, \quad \cdots$$

Στο παρόν κείμενο θα γράφουμε $x \preccurlyeq_{\mathscr{R}} y$ αντί $(x,y) \in \mathscr{R}$ αν η $\mathscr{R}$ είναι μια σχέση μερικής διάταξης επί του συνόλου X. Αν είναι μάλιστα σαφές για ποια σχέση μερικής διάταξης $\mathscr{R}$ πρόκειται, τότε γράφουμε απλώς $x \preccurlyeq y$. Γενικά, αν $x, y \in X$, τότε γράφουμε:

$$x \prec_{\mathscr{R}} y, \qquad \text{αν} \qquad x \preccurlyeq_{\mathscr{R}} y \quad \text{και} \quad x \neq y$$

Μια σχέση μερικής διάταξης «$\preccurlyeq$» επί του X καλείται σχέση **ολικής διάταξης** αν ικανοποιείται η ακόλουθη ιδιότητα:

$$\forall x, y \in X: \quad \text{είτε} \quad x \preccurlyeq y \quad \text{ή} \quad y \preccurlyeq x$$

Ένα **μερικώς διατεταγμένο σύνολο** είναι ένα ζεύγος $(X, \preccurlyeq)$ όπου το X είναι ένα μη-κενό σύνολο και «$\preccurlyeq$» είναι μια σχέση μερικής διάταξης επί του X. Σημειώνουμε ότι, αν $Y \subseteq X$ είναι ένα μη-κενό υποσύνολο του X, τότε το ζεύγος $(Y, \preccurlyeq')$ είναι ένα μερικώς διατεταγμένο σύνολο, όπου «$\preccurlyeq'$» συμβολίζει τον περιορισμό στο Y της σχέσης μερικής διάταξης «$\preccurlyeq$» επί του X. Με άλλα λόγια, η σχέση «$\preccurlyeq'$» ορίζεται, $\forall y_1, y_2 \in Y$, ως εξής: $y_1 \preccurlyeq' y_2$ αν και μόνο αν $y_1 \preccurlyeq y_2$.

Ένα **ολικώς διατεταγμένο σύνολο** είναι ένα ζεύγος $(X, \preccurlyeq)$ όπου το X είναι ένα μη-κενό σύνολο και «$\preccurlyeq$» είναι μια σχέση ολικής διάταξης επί του X.

Γενικά, ένα σύνολο X μπορεί να είναι εφοδιασμένο με πολλές σχέσεις μερικής διάταξης. Έτσι, όπως θα δούμε στο Παράδειγμα 1.1.3, στο σύνολο $\mathbb{N}_n = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$ ορίζονται δύο σχέσεις μερικής διάταξης εκ των οποίων η μία είναι σχέση ολικής διάταξης και η άλλη όχι. Αν η σχέση μερικής διάταξης «$\preccurlyeq$» επί του X είναι σαφής από το πλαίσιο στο οποίο εργαζόμαστε και δεν υπάρχει κίνδυνος σύγχισης, θα καλούμε το X μερικώς διατεταγμένο σύνολο και η σχέση μερικής διάταξης «$\preccurlyeq$» θα υπονοείται.

Παράδειγμα 1.1.3 (Παραδείγματα μερικώς ή ολικώς διατεταγμένων συνόλων)**.**

1. Θεωρούμε το σύνολο των φυσικών αριθμών $\mathbb{N}$ και για κάθε φυσικό αριθμό n, το υποσύνολο

   $$\mathbb{N}_n = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$$

   Τα σύνολα $(\mathbb{N}, \leq)$ και $(\mathbb{N}_n, \leq)$ είναι ολικώς διατεταγμένα σύνολα, όπου «$\leq$» είναι η γνωστή σχέση διάταξης στο $\mathbb{N}$. Δηλαδή $a \leq b$, αν η διαφορά $b - a$ ανήκει στο σύνολο $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

   Παρόμοια, με την συνηθισμένη έννοια του συμβόλου «$\leq$», τα σύνολα $(\mathbb{Q}, \leq)$ και $(\mathbb{R}, \leq)$ είναι μερικώς διατεταγμένα σύνολα.

2. Έστω X ένα μη κενό σύνολο και $\mathscr{P}(X)$ το δυναμοσύνολο του X, δηλαδή το σύνολο των υποσυνόλων του X. Τότε το ζεύγος $(\mathscr{P}(X), \subseteq)$ είναι ένα μερικώς διατεταγμένο σύνολο, όπου «$\subseteq$» συμβολίζει την σχέση υποσυνόλου. Το μερικώς διατεταγμένο σύνολο $\mathscr{P}(X)$ γενικά δεν είναι ολικά διατεταγμένο. Για παράδειγμα, αν $X = \{a, b, c\}$, τότε $\{a, b\} \nsubseteq \{b, c\}$ και $\{a, c\} \nsubseteq \{a, b\}$.

   Θεωρούμε το ακόλουθο υποσύνολο $\mathscr{S} = \{\mathbb{N}_n \subseteq \mathbb{N} \mid n \in \mathbb{N}\}$ του $\mathscr{P}(\mathbb{N})$, όπου, όπως παραπάνω, $\mathbb{N}_n = \{k \in \mathbb{N} \mid 1 \leq k \leq n\}$, $\forall n \geq 1$. Τότε το ζεύγος $(\mathscr{S}, \subseteq)$ είναι ένα ολικώς διατεταγμένο σύνολο.

3. Έστω $\mathscr{C}([0,1])$ το σύνολο των συνεχών πραγματικών συναρτήσεων $f: [0,1] \longrightarrow \mathbb{R}$ επί του κλειστού διαστήματος $[0,1] \subseteq \mathbb{R}$. Ορίζοντας στο σύνολο $\mathscr{C}([0,1])$ την ακόλουθη σχέση: $\forall f, g \in \mathscr{C}([0,1])$, $f \preccurlyeq g$ αν και μόνο αν $f(x) \leq g(x)$, $\forall x \in \mathbb{R}$. Χρησιμοποιώντας ότι η σχέση «$\leq$» είναι μια σχέση μερικής διάταξης επί του $\mathbb{R}$, βλέπουμε εύκολα ότι η σχέση «$\preccurlyeq$» είναι σχέση μερικής διάταξης επί του $\mathscr{C}([0,1])$.

4. Έστω $\mathscr{V}$ ένας διανυσματικός χώρος υπεράνω του $\mathbb{R}$. Αν $\mathscr{S}$ συμβολίζει το σύνολο των υπόχωρων του $\mathscr{V}$, τότε το ζεύγος $(\mathscr{S}, \subseteq)$, όπου «$\subseteq$» είναι η σχέση του υποσυνόλου, είναι ένα μερικώς διατεταγμένο σύνολο.

5. Επί του συνόλου $\mathbb{N}$ των φυσικών αριθμών ορίζουμε μια σχέση (την *σχέση διαιρετότητας* θετικών ακεραίων) ως εξής:

$$\forall n, m \in \mathbb{N}: \quad n \preccurlyeq m \iff n \mid m, \quad \text{δηλαδή αν υπάρχει } k \in \mathbb{N}: \quad m = nk$$

Προφανώς $n \mid n$, $\forall n \in \mathbb{N}$. Αν για δύο φυσικούς αριθμούς n, m ισχύει ότι $n \mid m$ και $m \mid k$, τότε θα έχουμε $m = nr$ και $k = ms$ για κάποιους φυσικούς αριθμούς r, s. Έτσι $k = nrs$ και επομένως $n \mid k$. Τέλος, αν για δύο φυσικούς αριθμούς n, m ισχύει ότι $n \mid m$ και $m \mid n$, τότε θα έχουμε $m = nr$ και $n = mk$ για κάποιους φυσικούς αριθμούς r, k, από όπου έπεται ότι $n = nrk$. Τότε $rk = 1$ και επομένως $r = k = 1$. Άρα $n = m$. Συνοψίζοντας, βλέπουμε ότι η σχέση «$\preccurlyeq$» είναι μια σχέση μερικής διάταξης επί του $\mathbb{N}$. Η σχέση «$\preccurlyeq$» δεν είναι σχέση ολικής διάταξης, διότι για παράδειγμα $3 \not\preccurlyeq 5$ και $5 \not\preccurlyeq 3$, καθώς $3 \nmid 5$ και $5 \nmid 3$.

Παρόμοια, $\forall n \in \mathbb{N}$, η σχέση «$\preccurlyeq$» είναι μια σχέση μερικής διάταξης επί του $\mathbb{N}_n$ η οποία δεν είναι σχέση ολικής διάταξης. Τέλος, αν Δ_n συμβολίζει το σύνολο διαιρετών του φυσικού αριθμού n, τότε η σχέση «$\preccurlyeq$» είναι μια σχέση μερικής διάταξης επί του Δ_n η οποία δεν είναι σχέση ολικής διάταξης.

6. Θεωρούμε το σύνολο X των μη αρνητικών δυνάμεων του 2:

$$X = \{2^k \in \mathbb{N} \mid k \in \mathbb{N}_0\}$$

εφοδιασμένο με την σχέση διαιρετότητας: $\forall x, y \in X$: $x \preccurlyeq y$ αν και μόνο αν $x \mid y$. Τότε το ζεύγος $(X, \preccurlyeq)$ είναι ένα ολικώς διατεταγμένο σύνολο. Πράγματι η σχέση «$\preccurlyeq$» είναι προφανώς μια σχέση μερικής διάταξης επί του X. Αν $x, y \in X$, τότε $x = 2^n$ και $y = 2^m$, όπου $n, m \geq 0$. Τότε είτε $n \leq m$ ή $m \leq n$. Αυτό αντίστοιχα σημαίνει ότι είτε $2^n \leq 2^m$ ή $2^m \leq 2^n$. Τότε θα έχουμε ότι είτε $y = 2^m = 2^n 2^{n-m} = x2^{n-m}$ ή $x = 2^n = 2^m 2^{m-n} = y2^{m-n}$, και επομένως είτε $x \mid y$ ή $y \mid x$, δηλαδή $x \preccurlyeq y$ ή $y \preccurlyeq x$. Έτσι πράγματι η σχέση «$\preccurlyeq$» είναι μια σχέση ολικής διάταξης επί του X. $\surd$

Έστω $(X, \preccurlyeq)$ ένα μερικώς διατεταγμένο σύνολο. Θεωρούμε ένα μη κενό υποσύνολο $S \subseteq X$ του X.

(α) Ένα **άνω φράγμα** για το S είναι ένα στοιχείο $x \in X$, έτσι ώστε: $s \preccurlyeq x$, $\forall s \in S$. Ένα **ελάχιστο άνω φράγμα** για το S είναι ένα άνω φράγμα $z \in X$ για το S έτσι ώστε $z \preccurlyeq y$ για κάθε άλλο άνω φράγμα y για το S. Προφανώς ένα ελάχιστο άνω φράγμα για το υποσύνολο S, αν υπάρχει, είναι μοναδικό, διότι, αν z_1 και z_2 είναι ελάχιστα άνω φράγματα για το S, τότε θα έχουμε $z_1 \preccurlyeq z_2$ και $z_2 \preccurlyeq z_1$, και επομένως $z_1 = z_2$. Το ελάχιστοι άνω φράγμα του συνόλου S συμβολίζεται με $\bigvee S$, και αν $S = \{a, b\}$, τότε θα γράφουμε: $\bigvee S = a \vee b$.

Για παράδειγμα, έστω $S = \{a_1, a_2, \cdots, a_n\} \subseteq \mathbb{N}$ ένα πεπερασμένο μη κενό σύνολο θετικών ακεραίων, και θεωρούμε το μερικώς διατεταγμένο σύνολο $(\mathbb{N}, |)$, όπου «$|$» είναι η σχέση διαιρετότητας, όπως στο μέρος 5, του Παραδείγματος 1.1.3. Τότε το ελάχιστο άνω φράγμα του συνόλου S υπάρχει και είναι το ελάχιστο κοινό πολλαπλάσιο $[a_1, a_2, \cdots, a_n]$ των αριθμών $a_1, a_2, \cdots, a_n$.

(β) Ένα **κάτω φράγμα** για το S είναι ένα στοιχείο $x \in X$ έτσι ώστε: $x \preccurlyeq s$, $\forall s \in S$. Ένα **μέγιστο κάτω φράγμα** για το S είναι ένα κάτω φράγμα $w \in X$ για το S έτσι ώστε $y \preccurlyeq w$ για κάθε άλλο κάτω φράγμα y για το S. Προφανώς ένα μέγιστο κάτω φράγμα για το υποσύνολο S, αν υπάρχει, είναι μοναδικό, διότι αν w_1 και w_2 είναι μέγιστα κάτω φράγματα για το S, τότε θα έχουμε $w_1 \preccurlyeq w_2$ και $w_2 \preccurlyeq w_1$, και επομένως $w_1 = w_2$. Το μέγιστο κάτω φράγμα του συνόλου S συμβολίζεται με $\bigwedge S$, και αν $S = \{a, b\}$, τότε θα γράφουμε: $\bigwedge S = a \wedge b$.

Για παράδειγμα, έστω $S = \{a_1, a_2, \cdots, a_n\} \subseteq \mathbb{N}$ ένα πεπερασμένο μη-κενό σύνολο θετικών ακεραίων, και θεωρούμε το μερικώς διατεταγμένο σύνολο $(\mathbb{N}, |$, όπου «$|$» είναι η σχέση διαιρετότητας, όπως στο μέρος 5, του Παραδείγματος 1.1.3. Τότε το μέγιστο κάτω φράγμα του συνόλου S υπάρχει και είναι ο μέγιστος κοινός διαιρέτης $(a_1, a_2, \cdots, a_n)$ των αριθμών $a_1, a_2, \cdots, a_n$.

Για μελλοντική χρήση, σημειώνουμε τον ακόλουθο ορισμό ο οποίος περιγράφει μια σημαντική κλάση μερικώς διατεταγμένων συνόλων.

Ορισμός 1.1.4. *Ένα μερικώς διατεταγμένο σύνολο $(X,\preccurlyeq)$ καλείται* **σύνδεσμος**,[1] *αν κάθε ζεύγος στοιχείων του $a,b\in X$, υπάρχει το μέγιστο κάτω φράγμα $a\bigwedge b$ στο X, και το ελάχιστο άνω φράγμα $a\bigvee b$ στο X.*

Ένας σύνδεσμος $(X,\preccurlyeq)$ καλείται **πλήρης σύνδεσμος**, *αν κάθε μη κενό υποσύνολο $S\subseteq X$ έχει μέγιστο κάτω φράγμα $\bigwedge S$ στο X και ελάχιστο άνω φράγμα $\bigvee S$ στο X.*

Για παράδειγμα, το μερικώς διατεταγμένο σύνολο $(\mathbb{N},|)$ των θετικών ακεραίων εφοδιασμένο με τη σχέση διαιρετότητας «$|$» αποτελεί σύνδεσμο. Το μερικώς διατεταγμένο σύνολο $(\mathscr{P}(X),\subseteq)$, όπου «$\subseteq$» είναι η σχέση έγκλεισης και $\mathscr{P}(X)$ είναι το δυναμοσύνολο ενός μη-κενού συνόλου X είναι ένας πλήρης σύνδεσμος. Προφανώς κάθε σύνδεσμος $(X,\preccurlyeq)$, όπου το σύνολο X είναι πεπερασμένο, είναι πλήρης.

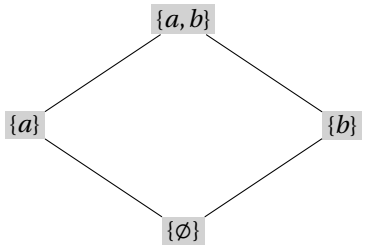
1.1.2 Το Διάγραμμα Hasse ενός Μερικώς Διατεταγμένου Συνόλου

Ένα μερικώς διατεταγμένο σύνολο $(X,\preccurlyeq)$ μπορεί να περιγραφεί από ένα διάγραμμα, το διάγραμμα Hasse του $(X,\preccurlyeq)$, αποτελούμενο από κορυφές και ακμές, και το οποίο περιέχει όλες τις ουσιώδεις πληροφορίες σχετικά με το X ως μερικώς διατεταγμένο σύνολο. Η αναπαράσταση του $(X,\preccurlyeq)$ μέσω του διαγράμματος Hasse είναι πολύ χρήσιμη, κυρίως όταν το σύνολο X είναι πεπερασμένο.

Για να ορίσουμε το διάγραμμα Hasse χρειαζόμαστε την έννοια της κάλυψης στοιχείων του X. Έστω x,y δύο στοιχεία του μερικώς διατεταγμένου συνόλου $(X,\preccurlyeq)$. Το στοιχείο y καλείται **κάλυψη** του x αν $x\prec y$ και δεν υπάρχει στοιχείο $z\in X$ έτσι ώστε $x\prec z\prec y$. Το **διάγραμμα Hasse**[2] του $(X,\preccurlyeq)$ έχει ως κορυφές σημεία τα οποία είναι σε «1-1» και «επί» αντιστοιχία με τα στοιχεία του X. Δύο κορυφές του διαγράμματος οι οποίες αναπαριστούν τα στοιχεία x,y του X, ενώνονται με μια ακμή, αν το y είναι κάλυψη του x, και τότε τοποθετούμε την κορυφή y υπεράνω της κορυφής x. Γενικά οι κορυφές του διαγράμματος Hasse οι οποίες αντιστοιχούν στα στοιχεία τού X τοποθετούνται στο διάγραμμα κατά τέτοιον τρόπο, ώστε, αν τα x,y είναι στοιχεία του X με $x\prec y$, τότε η κορυφή η οποία αντιστοιχεί στο x να κείται χαμηλότερα από την κορυφή που αντιστοιχεί στο y. Χάριν ευκολίας, από τώρα και στο εξής ταυτίζουμε τις κορυφές του διαγράμματος Hasse του μερικώς διατεταγμένου συνόλου $(X,\preccurlyeq)$ με τα στοιχεία του X.

Έστω $(X,\preccurlyeq)$ ένα μερικώς διατεταγμένο σύνολο και υποθέτουμε ότι το σύνολο X είναι πεπερασμένο. Αν x,y είναι δύο στοιχεία του X, τότε προφανώς θα έχουμε ότι $x\prec y$ αν και μόνο αν υπάρχει μια ακολουθία $z_1,z_2,\cdots,z_k$ στοιχείων του X, όπου $x=z_1$ και $z_k=y$, έτσι ώστε το στοιχείο z_{l+1} είναι κάλυψη του z_l, για κάθε $l=1,2,\cdots,k-1$. Αν $x\neq y$ και δεν υπάρχει ακολουθία ακμών η οποία ενώνει τα x και y, τότε τα στοιχεία x και y δεν είναι συγκρίσιμα.

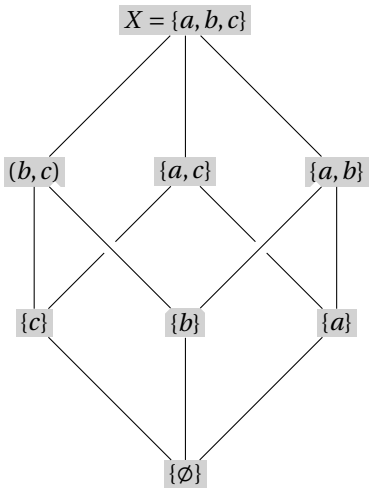
Παράδειγμα 1.1.5. 1. Έστω $X=\{a,b\}$ ένα σύνολο με δύο στοιχεία. Τότε $\mathscr{P}(X)=\big\{\emptyset,\{a\},\{b\},X\big\}$. Το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\mathscr{P}(X),\subseteq)$ είναι το εξής (παρατηρούμε ότι τα στοιχεία $\{a\}$ και $\{b\}$ δεν είναι συγκρίσιμα):



2. Έστω $X=\{a,b,c\}$ ένα σύνολο με τρία στοιχεία. Τότε $\mathscr{P}(X)=\big\{\emptyset,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},X\big\}$. Το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\mathscr{P}(X),\subseteq)$ είναι το εξής:

[1] Σύνδεσμος: ελληνική απόδοση του όρου "lattice".

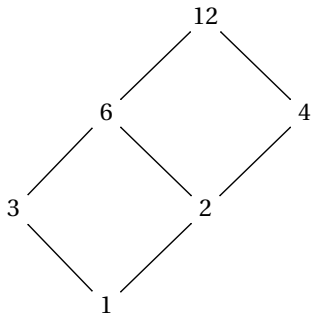
[2] Helmut Hasse (25 Αυγούστου 1898 - 26 Δεκεμβρίου 1979) [https://en.wikipedia.org/wiki/Helmut_Hasse]: Σημαντικός Γερμανός μαθηματικός, με θεμελιώδη συμβολή στη Θεωρία Αριθμών και στην Άλγεβρα, ιδιαίτερα στη Θεωρία Κλάσεων Σωμάτων, στη Διοφαντική Γεωμετρία και στη Θεωρία Συναρτήσεων ζ.



3. Έστω το μερικώς διατεταγμένο σύνολο $(\Delta_8, \preccurlyeq)$, όπου Δ_8 είναι το σύνολο των θετικών διαιρετών του 8, δηλαδή το σύνολο $\{1,2,4,8\}$, και «$\preccurlyeq$» η σχέση διαιρετότητας: $n \preccurlyeq m$ αν και μόνο αν $n \mid m$, όπως στο μέρος 5 του Παραδείγματος 1.1.3. Το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\Delta_8, \preccurlyeq)$ είναι το εξής:

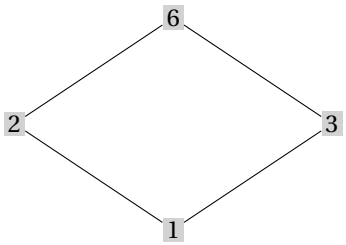
Παρατηρούμε ότι το μερικώς διατεταγμένο σύνολο $(\Delta_8, \preccurlyeq)$ είναι ολικώς διατεταγμένο, διότι δύο οποιαδήποτε στοιχεία του είναι συγκρίσιμα.

4. Έστω το μερικώς διατεταγμένο σύνολο $(\Delta_{12}, \preccurlyeq)$, όπου Δ_{12} είναι το σύνολο των θετικών διαιρετών του 12, δηλαδή το σύνολο $\{1,2,3,4,6,12\}$, και «$\preccurlyeq$» η σχέση διαιρετότητας: $n \preccurlyeq m$ αν και μόνο αν $n \mid m$, όπως στο μέρος 5 του Παραδείγματος 1.1.3. Το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\Delta_{12}, \preccurlyeq)$ είναι το εξής:



Παράδειγμα 1.1.6. Θεωρούμε το μερικώς διατεταγμένο σύνολο $(\Delta_k, \preccurlyeq)$, όπου Δ_k είναι το σύνολο των θετικών διαιρετών του φυσικού αριθμού k, και «$\preccurlyeq$» η σχέση διαιρετότητας: $n \preccurlyeq m$ αν και μόνο αν $n \mid m$, όπως στο μέρος 5 του Παραδείγματος 1.1.3.

1. Αν $k=6$, τότε θα έχουμε $\Delta_6=\{1,2,3,6\}$, και το διάγραμμα Hasse του μερικώς διατεταγμένου σύνολου $(\Delta_6,\preccurlyeq)$ είναι:

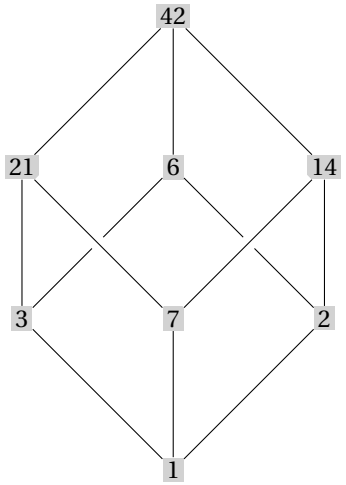


Παρατηρούμε ότι το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\Delta_6,\preccurlyeq)$ συμπίπτει με το διάγραμμα Hasse του μερικώς διατεταγμένου σύνολου $(\mathscr{P}(X),\subseteq)$, όπου $X=\{a,b\}$ είναι ένα σύνολο με δύο στοιχεία. Τα σύνολα Δ_6 και $\mathscr{P}(X)$ είναι σε «1-1» και «επί» αντιστοιχία f:

$$1\longleftrightarrow\{\emptyset\},\ \ 2\longleftrightarrow\{a\},\ \ 3\longleftrightarrow\{b\},\ \ 6\longleftrightarrow\{a,b\}$$

η οποία διατηρεί τις σχέσεις μερικής διάταξης, με την έννοια ότι $x\preccurlyeq y$ στο Δ_6 αν και μόνο αν $f(x)\subseteq f(y)$, $\forall x,y\in\Delta_6$.

2. Αν $k=42$, τότε θα έχουμε $\Delta_{42}=\{1,2,3,6,7,14,21,42\}$, και το διάγραμμα Hasse του μερικώς διατεταγμένου σύνολου $(\Delta_{42},\preccurlyeq)$ είναι:



Παρατηρούμε ότι το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου $(\Delta_{42},\preccurlyeq)$ συμπίπτει με το διάγραμμα Hasse του μερικώς διατεταγμένου σύνολου $(\mathscr{P}(X),\subseteq)$, όπου $X=\{a,b,c\}$ είναι ένα σύνολο με τρία στοιχεία. Τα σύνολα Δ_{42} και $\mathscr{P}(X)$ είναι σε «1-1» και «επί» αντιστοιχία f:

$$1\longleftrightarrow\{\emptyset\},\ \ 2\longleftrightarrow\{a\},\ \ 3\longleftrightarrow\{c\},\ \ 7\longleftrightarrow\{b\},\ \ 21\longleftrightarrow\{b,c\},\ \ 6\longleftrightarrow\{a,c\},\ \ 14\longleftrightarrow\{a,b\},\ \ 42\longleftrightarrow\{a,b,c\}$$

η οποία διατηρεί τις σχέσεις μερικής διάταξης, με την έννοια ότι $x\preccurlyeq y$ στο Δ_{42} αν και μόνο αν $f(x)\subseteq f(y)$ στο $\mathscr{P}(X)$, $\forall x,y\in\Delta_{42}$. $\surd$

1.2 Σχέσεις Ισοδυναμίας και Διαμερίσεις

1.2.1 Σχέσεις Ισοδυναμίας

Προχωρούμε ορίζοντας τη βασική έννοια της παρούσας παραγράφου.

Ορισμός 1.2.1. *Μια* **σχέση ισοδυναμίας** *επί του X είναι μια σχέση $\mathscr{R} \subseteq X \times X$ επί του X, η οποία ικανοποιεί τις ακόλουθες τρεις ιδιότητες:* (α) *την ανακλαστική ιδιότητα,* (β) *την συμμετρική ιδιότητα, και* (γ) *την μεταβατική ιδιότητα. Υπενθυμίζουμε (βλέπε 1.1.1):*

1.

$$\forall x \in X: \quad (x,x) \in \mathscr{R} \qquad \text{(ανακλαστική ιδιότητα)}$$

2.

$$\forall x,y \in X: \quad (x,y) \in \mathscr{R} \implies (y,x) \in \mathscr{R} \qquad \text{(συμμετρική ιδιότητα)}$$

3.

$$\forall x,y,z \in X: \quad (x,y) \in \mathscr{R} \quad \text{και} \quad (y,z) \in \mathscr{R} \implies (x,z) \in \mathscr{R} \qquad \text{(μεταβατική ιδιότητα)}$$

Όπως και στο εδάφιο των σχέσεων, αντί $(x,y) \in \mathscr{R}$, συχνά θα θα χρησιμοποιούμε έναν εκ των παρακάτω συμβολισμών:

$$x \mathscr{R} y \qquad \text{ή} \qquad x \sim_{\mathscr{R}} y \qquad \text{ή} \qquad x \equiv y (\mathscr{R})$$

Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί του συνόλου X. Αν $x \in X$, η **κλάση ισοδυναμίας** του x ως προς την $\mathscr{R}$ ορίζεται να είναι το ακόλουθο σύνολο:

$$[x]_{\mathscr{R}} = \{ y \in X \mid y \sim_{\mathscr{R}} x \} \subseteq X$$

Επειδή $x \sim_{\mathscr{R}} x$, έπεται ότι $x \in [x]_{\mathscr{R}}$ και άρα η κλάση ισοδυναμίας κάθε στοιχείου $x \in X$ είναι πάντοτε διάφορη του κενού συνόλου.

Το σύνολο $X/\mathscr{R}$ όλων των κλάσεων ισοδυναμίας των στοιχείων του X

$$X/\mathscr{R} = \{ [x]_{\mathscr{R}} \subseteq X \mid x \in X \}$$

ως προς τη σχέση ισοδυναμίας $\mathscr{R}$, καλείται το **σύνολο-πηλίκο** του X ως προς την $\mathscr{R}$. Σημειώνουμε ότι κάθε στοιχείο του $X/\mathscr{R}$ είναι ένα υποσύνολο του X, και επομένως το σύνολο πηλίκο είναι μια συλλογή υποσυνόλων του X.

Η απεικόνιση **κανονικής προβολής** του X επί του συνόλου πηλίκο $X/\mathscr{R}$ του X ως προς τη σχέση ισοδυναμίας $\mathscr{R}$ ορίζεται να είναι η απεικόνιση

$$\pi_{\mathscr{R}}: X \longrightarrow X/\mathscr{R}, \quad \pi_{\mathscr{R}}(x) = [x]_{\mathscr{R}}$$

η οποία είναι προφανώς απεικόνιση «επί».

Παράδειγμα 1.2.2. Για κάθε μη-κενό σύνολο X, η σχέση I_X η οποία ορίζεται ως εξής

$$\forall x,y \in X: \quad x \sim_{I_X} y \iff x = y$$

είναι προφανώς μια σχέση ισοδυναμίας επί του X, η οποία καλείται *ταυτοτική σχέση ισοδυναμίας*. Ως υποσύνολο του $X \times X$ έχουμε ότι $I_X = \{(x,x) \in X \times X \mid x \in X\}$.

Προφανώς η I_X είναι η μικρότερη σχέση ισοδυναμίας η οποία μπορεί να οριστεί επί του X, με την έννοια ότι, αν $\mathscr{R} \subseteq X \times X$ είναι μια άλλη σχέση ισοδυναμίας επί του X, τότε $I_X \subseteq \mathscr{R}$.

Η σχέση M_X επί του X, η οποία ορίζεται ως εξής: $\forall x,y \in X: \quad x \sim_{M_X} y$, είναι προφανώς μια σχέση ισοδυναμίας επί του X. Ως υποσύνολο του $X \times X$ έχουμε ότι $M_X = \{(x,y) \in X \times X \mid x,y \in X\} = X \times X$.

Προφανώς η M_X είναι η μεγαλύτερη σχέση ισοδυναμίας, η οποία μπορεί να οριστεί επί του X, με την έννοια ότι αν $\mathscr{R} \subseteq X \times X$ είναι μια τυχούσα σχέση ισοδυναμίας επί του X, τότε $I_X \subseteq \mathscr{R} \subseteq M_X$. $\surd$

Παρατήρηση 1.2.3. Το σύνολο $\mathsf{EqRel}(X)$ όλων των σχέσεων ισοδυναμίας επί ενός μη-κενού συνόλου X αποτελεί ένα μερικώς διατεταγμένο σύνολο $(\mathsf{EqRel}(X), \preccurlyeq)$, αν ορίσουμε:

$$\forall \mathscr{R}, \mathscr{T} \in \mathsf{EqRel}(X): \quad \mathscr{R} \preccurlyeq \mathscr{T} \iff \mathscr{R} \subseteq \mathscr{T} \ \text{(ως υποσύνολα του } X \times X)$$

Ισοδύναμα: $\mathscr{R} \preccurlyeq \mathscr{T}$ αν και μόνο αν $\forall x, y \in X$: $x \sim_{\mathscr{R}} y \Longrightarrow x \sim_{\mathscr{T}} y$.

Στο μερικώς διατεταγμένο σύνολο $(\mathsf{EqRel}(X), \preccurlyeq)$ η ταυτοτική σχέση ισοδυναμίας I_X είναι το μικρότερο στοιχείο, και η σχέση ισοδυναμίας M_X είναι το μεγαλύτερο στοιχείο. ▲

Παράδειγμα 1.2.4. Αν $\mathscr{F}$ είναι μια συλλογή συνόλων, θεωρούμε την ακόλουθη σχέση $\mathscr{R}$ επί του $\mathscr{F}$:

$$\forall A, B \in \mathscr{F}: \quad A \sim_{\mathscr{R}} B \iff |A| = |B|$$

Τότε η $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του $\mathscr{F}$. Πράγματι, για κάθε σύνολο $A \in \mathscr{F}$ έχουμε $|A| = |A|$ διότι υπάρχει η «1-1» και «επί» απεικόνιση $\mathsf{Id}_A: A \longrightarrow A$, και άρα $A \sim_{\mathscr{R}} A$. Αν $A, B \in \mathscr{F}$ και $A \sim_{\mathscr{R}} B$, έστω μια «1-1» και «επί» απεικόνιση $f: A \longrightarrow B$. Τότε θα έχουμε και $B \sim_{\mathscr{R}} A$, δηλαδή $|B| = |A|$ διότι υπάρχει η «1-1» και «επί» απεικόνιση $f^{-1}: B \longrightarrow A$. Τέλος, αν $A, B, C \in \mathscr{F}$ και ισχύει ότι $A \sim_{\mathscr{R}} B$ και $B \sim_{\mathscr{R}} C$, τότε θα έχουμε $|A| = |B|$ και $|B| = |C|$. Ισοδύναμα υπάρχουν «1-1» και «επί» απεικονίσεις $f: A \longrightarrow B$ και $g: B \longrightarrow C$. Τότε η απεικόνιση $g \circ f: A \longrightarrow C$ είναι «1-1» και «επί» και άρα $|A| = |C|$, δηλαδή $A \sim_{\mathscr{R}} C$. Συνοψίζοντας, δείξαμε ότι η σχέση «$\sim_{\mathscr{R}}$» είναι μια σχέση ισοδυναμίας επί της συλλογής συνόλων $\mathscr{F}$. $\surd$

Παράδειγμα 1.2.5. Για κάθε θετικό ακέραιο αριθμό n, θεωρούμε την ακόλουθη σχέση $\mathscr{R}_n$ επί του συνόλου των ακεραίων αριθμών:

$$\forall x, y \in \mathbb{Z}: \quad x \sim_{\mathscr{R}_n} y \iff n \mid x - y$$

Τότε η $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του $\mathbb{Z}$. Πράγματι, επειδή $n \mid 0$, για κάθε ακέραιο x, έχουμε ότι $n \mid x - x$, και άρα $x \sim_{\mathscr{R}_n} x$. Αν $x, y \in \mathbb{Z}$ και $x \sim_{\mathscr{R}_n} y$, τότε $n \mid x - y$ και προφανώς θα έχουμε και $n \mid y - x$, δηλαδή $y \sim_{\mathscr{R}_n} x$. Τέλος, αν $x, y, z \in \mathbb{Z}$ και $x \sim_{\mathscr{R}_n} y$ και $y \sim_{\mathscr{R}_n} z$, θα έχουμε $n \mid x - y$ και $n \mid y - z$. Έτσι, υπάρχουν ακέραιοι k, l έτσι ώστε: $x - y = kn$ και $y - z = ln$. Προσθέτοντας κατά μέλη, θα έχουμε $x - z = (k + l)n$, και άρα $n \mid x - z$, δηλαδή $x \sim_{\mathscr{R}_n} z$. Συνοψίζοντας, δείξαμε ότι η σχέση «$\sim_{\mathscr{R}_n}$» είναι μια σχέση ισοδυναμίας επί του $\mathbb{Z}$. $\surd$

Παράδειγμα 1.2.6. Επί του συνόλου $\mathbb{N}_0 \times \mathbb{N}_0$ ορίζουμε την ακόλουθη σχέση:

$$\forall (m, n), (m', n') \in \mathbb{N}_0 \times \mathbb{N}_0: \quad (m, n) \sim_{\mathscr{R}} (m', n') \iff m + n' = n + m'$$

Τότε η $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του $\mathbb{N}_0 \times \mathbb{N}_0$. Πράγματι, επειδή $m + n = n + m$ για τυχόντα $n, m \in \mathbb{N}_0$, έπεται ότι $(m, n) \sim_{\mathscr{R}} (m, n)$. Αν $(m, n), (m', n') \in \mathbb{N}_0 \times \mathbb{N}_0$ και ισχύει ότι: $(m, n) \sim_{\mathscr{R}} (m', n')$, τότε θα έχουμε $m + n' = n + m'$. Προφανώς τότε ισχύει ότι $m' + n = n' + m$ και άρα $(m', n') \sim_{\mathscr{R}} (m, n)$. Τέλος, έστω $(m, n), (m', n'), (m'', n'') \in \mathbb{N}_0 \times \mathbb{N}_0$ και υποθέτουμε ότι ισχύει: $(m, n) \sim_{\mathscr{R}} (m', n')$ και $(m', n') \sim_{\mathscr{R}} (m'', n'')$. Τότε θα έχουμε $m + n' = n + m'$ και $m' + n'' = n' + m''$, και επομένως: $m + n' + n'' = n + m' + n''$ από όπου έπεται ότι $m + n' + n'' = n + m' + m''$ και άρα $m + n'' = n + m''$. Η τελευταία σχέση δείχνει ότι $(m, n) \sim_{\mathscr{R}} (m'', n'')$. Συνοψίζοντας, δείξαμε ότι η σχέση «$\sim_{\mathscr{R}}$» είναι μια σχέση ισοδυναμίας επί του $\mathbb{N}_0 \times \mathbb{N}_0$. $\surd$

Παράδειγμα 1.2.7. Επί του συνόλου $\mathbb{Z} \times \mathbb{Z}^*$, όπου $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, θεωρούμε την ακόλουθη σχέση:

$$\forall (m, n), (r, s) \in \mathbb{Z} \times \mathbb{Z}^*: \quad (m, n) \sim_{\mathscr{T}} (r, s) \iff m \cdot s = n \cdot r$$

Τότε η $\mathscr{T}$ είναι μια σχέση ισοδυναμίας επί του $\mathbb{Z} \times \mathbb{Z}^*$. Πράγματι, επειδή $m \cdot n = n \cdot m$ για τυχόντα $n, m \in \mathbb{Z}$, όπου $n \neq 0$, έπεται ότι $(m, n) \sim_{\mathscr{T}} (m, n)$. Αν $(m, n), (r, s) \in \mathbb{Z} \times \mathbb{Z}^*$ και ισχύει ότι: $(m, n) \sim_{\mathscr{T}} (r, s)$, τότε θα έχουμε $m \cdot s = n \cdot r$. Προφανώς τότε ισχύει ότι $r \cdot n = s \cdot m$ και άρα $(r, s) \sim_{\mathscr{T}} (m, n)$. Τέλος, έστω $(m, n), (r, s), (x, y) \in \mathbb{Z} \times \mathbb{Z}^*$ και υποθέτουμε ότι ισχύει: $(m, n) \sim_{\mathscr{T}} (r, s)$ και $(r, s) \sim_{\mathscr{T}} (x, y)$. Τότε θα έχουμε $m \cdot s = n \cdot r$ και $r \cdot y = s \cdot x$, και επομένως: $m \cdot s \cdot y = n \cdot r \cdot y$ από όπου έπεται ότι $m \cdot s \cdot y = n \cdot s \cdot x$ και άρα $m \cdot y = n \cdot x$, διότι $s \neq 0$. Η τελευταία σχέση δείχνει ότι $(m, n) \sim_{\mathscr{T}} (x, y)$. Συνοψίζοντας, δείξαμε ότι η σχέση «$\sim_{\mathscr{T}}$» είναι μια σχέση ισοδυναμίας επί του $\mathbb{Z} \times \mathbb{Z}^*$. $\surd$

Στα παραδείγματα 1.2.6 και 1.2.7 παρατηρούμε ότι το σύνολο των ακεραίων $\mathbb{Z}$ προκύπτει, μέσω μιας «1-1» και «επί» απεικόνισης, ως σύνολο πηλίκο μιας κατάλληλης σχέσης ισοδυναμίας $\mathscr{R}$ επί του συνόλου $\mathbb{N}_0 \times \mathbb{N}_0$, και το σύνολο των ρητών $\mathbb{Q}$ προκύπτει, μέσω μιας «1-1» και «επί» απεικόνισης, ως σύνολο πηλίκο μιας κατάλληλης σχέσης ισοδυναμίας $\mathscr{T}$ επί του συνόλου $\mathbb{Z} \times \mathbb{Z}^*$. Σε αυτό το πλαίσιο, αν γνωρίζουμε το σύνολο $\mathbb{N}_0$, μπορούμε να *ορίσουμε* το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών να είναι το σύνολο πηλίκο $(\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R}$, και ακολούθως να *ορίσουμε* το σύνολο $\mathbb{Q}$ των ρητών αριθμών να είναι το σύνολο πηλίκο $(\mathbb{Z} \times \mathbb{Z}^*)/\mathscr{T}$. Στην Άσκηση 1.5.10 του παρόντος Κεφαλαίου περιγράφεται το σύνολο $\mathbb{R}$ των πραγματικών αριθμών ως σύνολο πηλίκο μιας κατάλληλης σχέσης ισοδυναμίας επί του συνόλου ακολουθιών ρητών αριθμών, και στην Άσκηση 1.5.11 περιγράφεται το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών ως σύνολο πηλίκο μιας κατάλληλης σχέσης ισοδυναμίας επι του συνόλου των πολυωνύμων με πραγματικούς συντελεστές.

Παράδειγμα 1.2.8. [Ισοδυναμία Πινάκων] Έστω $\mathsf{M}_{m\times n}(\mathbb{K})$, όπου $\mathbb{K} = \mathbb{Q}, \mathbb{R}$, ή $\mathbb{C}$, το σύνολο των $m \times n$ πινάκων υπεράνω του $\mathbb{K}$. Ορίζουμε μια σχέση $\mathscr{R}$ επί του $\mathsf{M}_{m\times n}(\mathbb{K})$ ως εξής:

$$\forall A, B \in \mathsf{M}_{m\times n}(\mathbb{K}): \quad A \sim_{\mathscr{R}} B \quad \Longleftrightarrow \quad \text{υπάρχουν αντιστρέψιμοι πίνακες } P \in \mathsf{M}_{m\times m}(\mathbb{K}) \text{ και } Q \in \mathsf{M}_{n\times n}(\mathbb{K})$$
$$\text{έτσι ώστε: } P^{-1} \cdot A \cdot Q = B$$

Χρησιμοποιώντας στοιχειώδεις ιδιότητες πινάκων, έπεται εύκολα ότι η σχέση $\mathscr{R}$ είνναι μια σχέση ισοδυναμίας επί του συνόλου $\mathsf{M}_{m\times n}(\mathbb{K})$. Πράγματι $A \sim_{\mathscr{R}} A$, διότι μπορούμε να διαλέξουμε τους (αντιστρέψιμους) μοναδιαίους πίνακες $P = I_m$ και $Q = I_n$ και τότε $I_m^{-1} \cdot A \cdot I_n = A$. Αν $A, B \in \mathsf{M}_{m\times n}(\mathbb{K})$ και ισχύει: $A \sim_{\mathscr{R}} B$, τότε θα έχουμε $P^{-1} \cdot A \cdot Q = B$ για κάποιους αντιστρέψιμους πίνακες $P \in \mathsf{M}_{m\times m}(\mathbb{K})$ και $Q \in \mathsf{M}_{n\times n}(\mathbb{K})$. Τότε, πολλαπλασιάζοντας την τελευταία σχέση από τα αριστερά με τον πίνακα P και από τα δεξιά με τον πίνακα Q^{-1}, θα έχουμε: $A = P \cdot B \cdot Q^{-1} = P_1^{-1} \cdot B \cdot Q_1$, όπου $P_1 = P^{-1}$ και $Q_1 = Q^{-1}$. Άρα $B \sim_{\mathscr{R}} A$. Τέλος, αν $A, B, C \in \mathsf{M}_{m\times n}(\mathbb{K})$ και ισχύει: $A \sim_{\mathscr{R}} B$ και $B \sim_{\mathscr{R}} C$, τότε θα έχουμε $P^{-1} \cdot A \cdot Q = B$ και $R^{-1} \cdot B \cdot T = C$ για κάποιους αντιστρέψιμους πίνακες $P, R \in \mathsf{M}_{m\times m}(\mathbb{K})$ και $Q, T \in \mathsf{M}_{n\times n}(\mathbb{K})$. Τότε θα έχουμε:

$$R^{-1} \cdot B \cdot T = C \implies R^{-1} \cdot (P^{-1} \cdot A \cdot Q) \cdot T = C \implies (R^{-1} \cdot P^{-1}) \cdot A \cdot (Q \cdot T) = C \implies (P \cdot R)^{-1} \cdot A \cdot (Q \cdot T) = C$$

Επειδή οι πίνακες $P \cdot R$ και $Q \cdot T$ είναι αντιστρέψιμοι, ως γινόμενα αντιστρέψιμων πινάκων, έπεται ότι θα έχουμε $A \sim_{\mathscr{R}} C$. Άρα η σχέση $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του συνόλου $\mathsf{M}_{m\times n}(\mathbb{K})$, η οποία καλείται *ισοδυναμία πινάκων*, και οι πίνακες $A, B \in \mathsf{M}_{m\times n}(\mathbb{K})$ καλούνται *ισοδύναμοι* αν: $A \sim_{\mathscr{R}} B$. $\surd$

Παράδειγμα 1.2.9 (Ομοιότητα Τετραγωνικών Πινάκων)**.** Έστω $\mathsf{M}_n(\mathbb{K}) := \mathsf{M}_{n\times n}(\mathbb{K})$, όπου $\mathbb{K} = \mathbb{Q}, \mathbb{R}$, ή $\mathbb{C}$, το σύνολο των τετραγωνικών $n \times n$ πινάκων υπεράνω του $\mathbb{K}$. Ορίζουμε μια σχέση $\mathscr{T}$ επί του $\mathsf{M}_n(\mathbb{K})$ ως εξής:

$$\forall A, B \in \mathsf{M}_n(\mathbb{K}): \quad A \sim_{\mathscr{T}} B \quad \Longleftrightarrow \quad \text{υπάρχει αντιστρέψιμος πίνακας } P \in \mathsf{M}_n(\mathbb{K}) \text{ έτσι ώστε: } P^{-1} \cdot A \cdot P = B$$

Εργαζόμενοι όπως στο Παράδειγμα 1.2.8, βλέπουμε ότι η παραπάνω σχέση $\mathscr{T}$ επί του συνόλου $\mathsf{M}_n(\mathbb{K})$ είναι μια σχέση ισοδυναμίας, η οποία καλείται *ομοιότητα (τετραγωνικών) πινάκων*, και οι $A, B \in \mathsf{M}_n(\mathbb{K})$ καλούνται *όμοιοι* αν: $A \sim_{\mathscr{R}} B$. $\surd$

Αν $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί ενός συνόλου X, τότε ένα φυσιολογικό ερώτημα το οποίο προκύπτει είναι ποια είναι η σχέση μεταξύ δύο κλάσεων ισοδυναμίας στοιχείων του X.

Λήμμα 1.2.10. *Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί του συνόλου X, και $x, y \in X$. Τότε:*

1. *Τα ακόλουθα είναι ισοδύναμα:*

(α΄) $x \sim_{\mathscr{R}} y$.

(β΄) $x \in [y]_{\mathscr{R}}$.

(γ΄) $y \in [x]_{\mathscr{R}}$.

(δ΄) $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$.

2. *Δύο κλάσεις ισοδυναμίας είτε ταυτίζονται είτε είναι ξένες:*

$$\textit{Είτε} \quad [x]_{\mathscr{R}} = [y]_{\mathscr{R}} \qquad \textit{είτε} \qquad [x]_{\mathscr{R}} \cap [y]_{\mathscr{R}} = \emptyset$$

Απόδειξη. **1.** (α′) $\Longrightarrow$ (β′) Έστω ότι $x \sim_{\mathscr{R}} y$. Τότε από τη συμμετρική ιδιότητα θα έχουμε $y \sim_{\mathscr{R}} x$, το οποίο σημαίνει ότι $x \in [y]_{\mathscr{R}}$.

(β′) $\Longrightarrow$ (γ′) Έστω ότι $x \in [y]_{\mathscr{R}}$. Τότε $y \sim_{\mathscr{R}} x$ και επομένως από την συμμετρική ιδιότητα θα έχουμε ότι $x \sim_{\mathscr{R}} y$, δηλαδή $y \in [x]_{\mathscr{R}}$.

(γ′) $\Longrightarrow$ (δ′) Έστω ότι $y \in [x]_{\mathscr{R}}$, δηλαδή ισχύει ότι $x \sim_{\mathscr{R}} y$. Έστω $z \in [x]_{\mathscr{R}}$. Τότε $z \sim_{\mathscr{R}} x$ και άρα από την μεταβατική ιδιότητα θα έχουμε $z \sim_{\mathscr{R}} y$. Επομένως $z \in [y]_{\mathscr{R}}$ και επομένως $[x]_{\mathscr{R}} \subseteq [y]_{\mathscr{R}}$. Αντίστροφα, αν $z \in [y]_{\mathscr{R}}$, τότε $z \sim_{\mathscr{R}} y$ και άρα $y \sim_{\mathscr{R}} z$. Από την μεταβατική ιδιότητα θα έχουμε $x \sim_{\mathscr{R}} z$ ή ισοδύναμα $z \sim_{\mathscr{R}} x$. Επομένως $z \in [x]_{\mathscr{R}}$ και άρα $[y]_{\mathscr{R}} \subseteq [x]_{\mathscr{R}}$. Έτσι δείξαμε ότι: $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$.

(δ′) $\Longrightarrow$ (α′) Έστω ότι $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$. Επειδή $x \in [x]_{\mathscr{R}}$, θα έχουμε $x \in [y]_{\mathscr{R}}$ και άρα $y \sim_{\mathscr{R}} x$ ή ισοδύναμα $x \sim_{\mathscr{R}} y$.

2. Αρκεί να δείξουμε ότι, αν $[x]_{\mathscr{R}} \cap [y]_{\mathscr{R}} \neq \emptyset$, τότε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$. Έστω $z \in [x]_{\mathscr{R}} \cap [y]_{\mathscr{R}}$. Τότε $z \in [x]_{\mathscr{R}}$ και $z \in [y]_{\mathscr{R}}$. Αυτό σημαίνει ότι: $z \sim_{\mathscr{R}} x$ και $z \sim_{\mathscr{R}} y$. Ισοδύναμα, επειδή η σχέση «$\sim_{\mathscr{R}}$» είναι σχέση ισοδυναμίας, έπεται ότι $x \sim_{\mathscr{R}} z$ και $z \sim_{\mathscr{R}} y$. Από την μεταβατική ιδιότητα τότε θα έχουμε $x \sim_{\mathscr{R}} y$ και άρα από το **1.** θα έχουμε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$. ■

Σύμφωνα με το Λήμμα 1.2.10, αν $y \in [x]_{\mathscr{R}}$, τότε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$ και γι' αυτό κάθε στοιχείο $y \in [x]_{\mathscr{R}}$, καλείται **αντιπρόσωπος** της κλάσης ισοδυναμίας $[x]_{\mathscr{R}}$. Προφανώς, αφού $x \sim_{\mathscr{R}} x$, το x είναι ένας αντιπρόσωπος της κλάσης ισοδυναμίας του $[x]_{\mathscr{R}}$. Θα δούμε αργότερα σε συγκεκριμένα παραδείγματα ότι πολλές φορές υπάρχει μια «φυσιολογική επιλογή» τού αντιπροσώπου μιας κλάσης ισοδυναμίας.

Στο ακόλουθο παράδειγμα θα προσδιορίσουμε τα σύνολα πηλίκα των σχέσεων ισοδυναμίας των παραδειγμάτων 1.2.5, 1.2.6, και 1.2.7.

Παράδειγμα 1.2.11. **1.** Θεωρούμε τη σχέση ισοδυναμίας «$\mathscr{R}_n$» επί του $\mathbb{Z}$ η οποία περιγράφεται στο Παράδειγμα 1.2.5. Αν $x \in \mathbb{Z}$, τότε θα γράφουμε $[x]_n$ για την κλάση ισοδυναμίας του x ως προς τη σχέση ισοδυναμίας $\mathscr{R}_n$. Θα έχουμε:

$$[x]_n = \{y \in \mathbb{Z} \mid x \sim_{\mathscr{R}_n} y\} = \{y \in \mathbb{Z} \mid n \mid y-x\} = \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z}:\ y-x = k\cdot n\} = \{y \in \mathbb{Z} \mid \exists k \in \mathbb{Z}:\ y = x+k\cdot n\}$$

Επομένως

$$[x]_n = \{x+k\cdot n \in \mathbb{Z} \mid k \in \mathbb{Z}\} = \{\cdots,\ x-2n,\ x-n,\ x,\ x+n,\ x+2n,\ \cdots\}$$

Θα προσδιορίσουμε το σύνολο πηλίκο

$$\mathbb{Z}/\sim_{\mathscr{R}_n} = \{[x]_n \subseteq \mathbb{Z} \mid x \in \mathbb{Z}\}$$

Έστω $x \in \mathbb{Z}$. Από την Ευκλείδεια Διαίρεση του ακέραιου x με τον θετικό ακέραιο n, θα έχουμε:

$$x = q\cdot n + r, \qquad r, q \in \mathbb{Z} \quad \& \quad 0 \leq r < n$$

Τότε $x - r = q\cdot n$, και άρα $n \mid x-r$, δηλαδή: $x \sim_{\mathscr{R}_n} r$. Από το Λήμμα 1.2.10 έπεται ότι $[x]_n = [r]_n$, και άρα $\{[x]_n \subseteq \mathbb{Z} \mid x \in \mathbb{Z}\} \subseteq \{[r]_n \subseteq \mathbb{Z} \mid 0 \leq r \leq n-1\}$. Επειδή προφανώς ισχύει και η αντίστροφη έγκλειση, έπεται ότι:

$$\mathbb{Z}/\sim_{\mathscr{R}_n} = \{[r]_n \subseteq \mathbb{Z} \mid\ 0 \leq r \leq n-1\}$$

Σημειώνουμε ότι, αν $0 \leq r_1, r_2 \leq n-1$ και $[r_1]_n = [r_2]_n$, τότε από το Λήμμα 1.2.10 έπεται ότι $r_1 \sim_{\mathscr{R}_n} r_2$, δηλαδή $n \mid r_1 - r_2$ και τότε θα έχουμε $n \leq r_1 - r_2$ το οποίο, επειδή $r_1, r_2 < n$, μπορεί να συμβαίνει μόνο όταν $r_1 - r_2 = 0$, δηλαδή $r_1 = r_2$. Επομένως, αν $0 \leq r_1 \neq r_2 \leq n-1$, τότε $[r_1]_n \neq [r_2]_n$, και επομένως το σύνολο πηλίκο $\mathbb{Z}/\sim_{\mathscr{R}_n}$, το οποίο από τώρα και στο εξής θα το συμβολίζουμε με $\mathbb{Z}_n$, έχει ακριβώς n το πλήθος στοιχεία:

$$\mathbb{Z}_n := \mathbb{Z}/\sim_{\mathscr{R}_n} = \{[r]_n \subseteq \mathbb{Z} \mid\ 0 \leq r \leq n-1\} = \{[0]_n,\ [1]_n,\ \cdots,\ [n-1]_n\}$$

Το σύνολο πηλίκο $\mathbb{Z}_n$ καλείται το *σύνολο των κλάσεων υπολοίπων ακεραίων* mod n, τα δε στοιχεία του *κλάσεις υπολοίπων* mod n, και η απεικόνιση κανονικής προβολής $\pi_{\mathscr{R}_n}\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\pi_{\mathscr{R}_n}(x) = [x]_n$, συμβολίζεται με

$$\pi_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \quad \pi(x) = [x]_n$$

Σημειώνουμε ότι: *δύο ακέραιοι x, y είναι ισοδύναμοι ως προς τη σχέση $\mathscr{R}_n$, δηλαδή $x \sim_{\mathscr{R}_n} y$ αν και μόνο αν έχουν το ίδιο υπόλοιπο όταν διαιρεθούν με το n.* Πράγματι, αν $x \sim_{\mathscr{R}_n} y$, τότε $[x]_n = [y]_n$ και αν r_1, r_2 είναι τα υπόλοιπα των διαιρέσεων των x, y με το n, τότε όπως παραπάνω θα έχουμε $[x]_n = [r_1]_n$ και $[y]_n = [r_2]_n$. Επομένως $[r_1]_n = [r_2]_n$, και άρα όπως παραπάνω θα έχουμε $r_1 = r_2$. Αντίστροφα, αν οι ακέραιοι x και y έχουν το ίδιο υπόλοιπο r όταν διαιρεθούν με το n, τότε θα έχουμε $x = q_1 \cdot n + r$ και $y = q_2 \cdot n + r$, και τότε $x - y = (q_1 - q_2) \cdot n$, δηλαδή $n \mid x - y$. Έτσι $x \sim_{\mathscr{R}_n} y$.

2. Θεωρούμε τη σχέση ισοδυναμίας «$\mathscr{R}$» επί του $\mathbb{N}_0 \times \mathbb{N}_0$ η οποία περιγράφεται στο Παράδειγμα 1.2.6. Θα προσδιορίσουμε το σύνολο πηλίκο $(\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R}$. Για κάθε στοιχείο $(m, n) \in \mathbb{N}_0 \times \mathbb{N}_0$, θα έχουμε:

$$[(m,n)]_{\mathscr{R}} = \{(x,y) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid (x,y) \sim_{\mathscr{R}} (m,n)\} = \{(x,y) \in \mathbb{N}_0 \times \mathbb{N}_0 \mid x + n = y + m\}$$

Παρατηρούμε ότι αν $(x, y) \sim_{\mathscr{R}} (m, n)$, τότε $x + n = y + m$ και άρα $m - n = x - y$. Θεωρούμε την απεικόνιση $\Phi'\colon \mathbb{N}_0 \times \mathbb{N}_0 \longrightarrow \mathbb{Z}$, $\Phi'(m, n) = m - n$. Αν $(m, n) \sim_{\mathscr{R}} (k, l)$, τότε θα έχουμε $m + l = n + k$ και άρα $m - n = k - l$. Επομένως $\Phi'(m, n) = \Phi'(k, l)$, και τότε ορίζοντας

$$\Phi : (\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R} \longrightarrow \mathbb{Z}, \quad \Phi([(m,n)]_{\mathscr{R}}) = m - n$$

δηλαδή $\Phi([(m, n)]_{\mathscr{R}}) = \Phi'(m, n)$, έπεται εύκολα ότι αποκτούμε μια καλά ορισμένη απεικόνιση $\Phi\colon (\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R} \longrightarrow \mathbb{Z}$, βλέπε και την Πρόταση 1.2.13. Πράγματι, αν $[(m, n)]_{\mathscr{R}} = [(k, l)]_{\mathscr{R}}$, τότε από το Λήμμα 1.2.10 έπεται ότι $(m, n) \sim_{\mathscr{R}} (k, l)$ και άρα $\Phi([(m, n)]_{\mathscr{R}}) = \Phi'(m, n) = m - n = k - l = \Phi'(k, l) = \Phi([(k, l)]_{\mathscr{R}})$. Έτσι η απεικόνιση Φ είναι καλά ορισμένη, δηλαδή είναι ανεξάρτητη της επιλογής αντιπροσώπου (m, n) της κλάσης ισοδυναμίας $[(m, n)]_{\mathscr{R}}$.

Θα δείξουμε ότι η απεικόνιση Φ είναι «1-1» και «επί».

Αν $[(m, n)]_{\mathscr{R}}, [(m', n')]_{\mathscr{R}} \in (\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R}$ και ισχύει ότι $\Phi([(m, n)]_{\mathscr{R}}) = \Phi([(m', n')]_{\mathscr{R}})$, τότε θα έχουμε $m - n = m' - n'$ και άρα $m + n' = m' + n$. Αυτό σημαίνει ότι $(m, n) \sim_{\mathscr{R}} (m', n')$ και τότε από το Λήμμα 1.2.10 θα έχουμε ότι $[(m, n)]_{\mathscr{R}} = [(m', n')]_{\mathscr{R}}$. Επομένως η Φ είναι «1-1». Τέλος η Φ είναι «επί» διότι για κάθε ακέραιο $z \in \mathbb{Z}$, έχουμε $\Phi([(z, 0)]_{\mathscr{R}}) = z - 0 = z$, αν $z \in \mathbb{N}_0$, και $\Phi([(0, -z)]_{\mathscr{R}}) = 0 - (-z) = z$, αν $z < 0$. Συνοψίζοντας, δείξαμε ότι το σύνολο πηλίκο $(\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R}$ είναι σε «1-1» και «επί» αντιστοιχία με το σύνολο των ακεραίων αριθμών.

3. Θεωρούμε τη σχέση ισοδυναμίας «$\mathscr{R}$» επί του $\mathbb{Z} \times \mathbb{Z}^*$ η οποία περιγράφεται στο Παράδειγμα 1.2.7. Θα προσδιορίσουμε το σύνολο πηλίκο $(\mathbb{Z} \times \mathbb{Z}^*)/\mathscr{R}$. Για κάθε στοιχείο $(m, n) \in \mathbb{Z} \times \mathbb{Z}^*$, θα έχουμε:

$$[(m,n)]_{\mathscr{R}} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid (x,y) \sim_{\mathscr{R}} (m,n)\} = \{(x,y) \in \mathbb{Z} \times \mathbb{Z}^* \mid x \cdot n = y \cdot m\}$$

Θεωρούμε την απεικόνιση $\Psi'\colon Z \times \mathbb{Z}^* \longrightarrow \mathbb{Q}$, $\Psi'(m, n) = \frac{m}{n}$. Αν $(m, n), (r, s) \in \mathbb{Z} \times \mathbb{Z}^*$ και ισχύει $(m, n) \sim_{\mathscr{R}} (r, s)$, τότε θα έχουμε $m \cdot s = n \cdot r$ και άρα, επειδή $n, s \neq 0$, έπεται ότι: $\frac{m}{n} = \frac{r}{s}$. Επομένως $\Psi'(m, n) = \Psi'(r, s)$, και τότε ορίζοντας

$$\Psi : (\mathbb{Z} \times \mathbb{Z}^*)/\mathscr{R} \longrightarrow \mathbb{Q}, \quad \Psi([(m,n)]_{\mathscr{R}}) = \frac{m}{n}$$

δηλαδή $\Psi([(m, n)]_{\mathscr{R}}) = \Psi'(m, n)$, έπεται εύκολα ότι αποκτούμε μια καλά ορισμένη απεικόνιση $\Psi\colon (\mathbb{N}_0 \times \mathbb{N}_0)/\mathscr{R} \longrightarrow \mathbb{Z}$, βλέπε και την Πρόταση 1.2.13. Πράγματι, αν $[(m, n)]_{\mathscr{R}} = [(k, l)]_{\mathscr{R}}$, τότε από το Λήμμα 1.2.10 έπεται ότι $(m, n) \sim_{\mathscr{R}} (k, l)$ και άρα $\Psi([(m, n)]_{\mathscr{R}}) = \Psi'(m, n) = \frac{m}{n} = \frac{k}{l} = \Psi'(k, l) = \Psi([(k, l)]_{\mathscr{R}})$. Έτσι η απεικόνιση Ψ είναι καλά ορισμένη, δηλαδή είναι ανεξάρτητη της επιλογής αντιπροσώπου (m, n) της κλάσης ισοδυναμίας $[(m, n)]_{\mathscr{R}}$.

Θα δείξουμε ότι η απεικόνιση Ψ είναι «1-1» και «επί».

Αν $[(m,n)]_{\mathscr{R}}, [(r,s)]_{\mathscr{R}} \in (\mathbb{Z}\times\mathbb{Z}^*)/\mathscr{R}$ και ισχύει ότι $\Psi([(m,n)]_{\mathscr{R}}) = \Psi([(r,s)]_{\mathscr{R}})$, τότε θα έχουμε $\frac{m}{n} = \frac{r}{s}$ και επομένως $m\cdot s = n\cdot r$. Αυτό σημαίνει ότι $(m,n) \sim_{\mathscr{R}} (r,s)$ και τότε από το Λήμμα 1.2.10 θα έχουμε ότι $[(m,n)]_{\mathscr{R}} = [(r,s)]_{\mathscr{R}}$. Επομένως η Ψ είναι «1-1». Τέλος, η Ψ είναι «επί» διότι για κάθε ρητό αριθμό $\frac{m}{n} \in \mathbb{Q}$, έχουμε $\Phi([(m,n)]_{\mathscr{R}}) = \frac{m}{n}$. Συνοψίζοντας, δείξαμε ότι το σύνολο πηλίκο $(\mathbb{Z}\times\mathbb{Z}^*)/\mathscr{R}$ είναι σε «1-1» και «επί» αντιστοιχία με το σύνολο των ρητών αριθμών. ✓

Το επόμενο Πόρισμα συνοψίζει κάποιες βασικές ιδιότητες τις οποίες έχει το σύνολο πηλίκο των κλάσεων ισοδυναμίας.

Πόρισμα 1.2.12. *Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί του μη-κενού συνόλου X.*

1. $\forall x \in X:\ [x]_{\mathscr{R}} \neq \emptyset$.
2. *Είτε* $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$ *είτε* $[x]_{\mathscr{R}} \cap [y]_{\mathscr{R}} = \emptyset$.
3. $X = \bigcup_{x\in X} [x]_{\mathscr{R}}$.

Απόδειξη. **1.** Έστω $x \in X$. Επειδή $x \in [x]_{\mathscr{R}}$, έπεται ότι $[x]_{\mathscr{R}} \neq \emptyset$.
2. Το ζητούμενο προκύπτει από το μέρος **2.** του Λήμματος 1.2.10.
3. Επειδή $\forall x \in X$, ισχύει ότι $x \in [x]_{\mathscr{R}}$, θα έχουμε $X = \bigcup_{x\in X}\{x\} \subseteq \bigcup_{x\in X}[x]_{\mathscr{R}}$ και άρα $X = \bigcup_{x\in X}[x]_{\mathscr{R}}$. ■

Από το Πόρισμα 1.2.12 βλέπουμε ότι το σύνολο-πηλίκο $X/\mathscr{R}$ είναι ένα σύνολο υποσυνόλων του X, των κλάσεων ισοδυναμίας των στοιχείων του X ως προς τη σχέση ισοδυναμίας $\mathscr{R}$, το οποίο ικανοποιεί την ακόλουθη ιδιότητα: κάθε στοιχείο του συνόλου X ανήκει σε μία και μόνο μία κλάση ισοδυναμίας. Αυτή η ιδιότητα μας οδηγεί στην έννοια της διαμέρισης ενός συνόλου την οποία θα μελετήσουμε στην υποενότητα 1.2.3.

1.2.2 «Καλά Ορισμένες» Απεικονίσεις και Σχέσεις Ισοδυναμίας

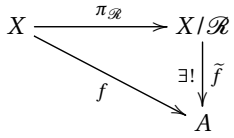
Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί του συνόλου X. Αν $f\colon X \longrightarrow Y$ είναι μια απεικόνιση, συχνά θέλουμε να ορίσουμε μια «*επαγόμενη*» απεικόνιση $\widetilde{f}\colon X/\mathscr{R} \longrightarrow Y$, έτσι ώστε $f = \widetilde{f}\circ\pi_{\mathscr{R}}$, και άρα να έχουμε $f(x) = (\widetilde{f}\circ\pi_{\mathscr{R}})(x) = \widetilde{f}([x]_{\mathscr{R}})$, $\forall x \in X$. Έτσι είναι φυσιολογικό να προσπαθήσουμε να το κάνουμε θέτοντας $\widetilde{f}([x]_{\mathscr{R}}) = f(x)$. Όμως αυτή η διαδικασία, αν και ορίζει μια σχέση $\widetilde{f}$, δεν ορίζει πάντα απεικόνιση, διότι ο ορισμός της τιμής $\widetilde{f}([x]_{\mathscr{R}}) = f(x)$ της $\widetilde{f}$ εξαρτάται από την τιμή της f στον αντιπρόσωπο x της κλάσης ισοδυναμίας $[x]_{\mathscr{R}}$. Με άλλα λόγια, αν y είναι ένας άλλος αντιπρόσωπος της κλάσης ισοδυναμίας $[x]_{\mathscr{R}}$, οπότε θα έχουμε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$, δεν είναι απαραίτητο να ισχύει ότι $f(x) = f(y)$, και κατ' επέκταση δεν είναι απαραίτητο να ισχύει ότι $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$, δηλαδή δεν είναι απαραίτητο η σχέση $\widetilde{f}$ να είναι απεικόνιση. Για παράδειγμα, θεωρούμε την απεικόνιση $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}_4$, $f(x) = [2x]_4$, και έστω η σχέση ισοδυναμίας $\mathscr{R}_7$ επί του $\mathbb{Z}$ όπως στο παράδειγμα 1.2.5, δηλαδή $x \sim_{\mathscr{R}_7} y \iff 7 \mid x-y$, και τότε $\mathbb{Z}/_{\mathscr{R}_7} = \mathbb{Z}_7$. Αν υπήρχε απεικόνιση $\widetilde{f}\colon \mathbb{Z}_7 \longrightarrow \mathbb{Z}_4$ έτσι ώστε $f = \widetilde{f}\circ\varpi_7$, τότε θα είχαμε $f(x) = \widetilde{f}([x]_7) = [2x]_4$, $\forall x \in \mathbb{Z}$. Όμως στο σύνολο πηλίκο $\mathbb{Z}_7$ έχουμε $[0]_7 = [7]_7$ και άρα, επειδή υποθέσαμε ότι η $\widetilde{f}$ είναι απεικόνιση, θα έχουμε $\widetilde{f}([0]_7) = \widetilde{f}([7]_7)$, δηλαδή $[2\cdot 0]_4 = [2\cdot 7]_4$. Τότε $[0]_4 = [14]_4$ ή ισοδύναμα $0 \sim_{\mathscr{R}_4} 14$, δηλαδή $4 \mid 14-0$, το οποίο είναι άτοπο. Άρα δεν υπάρχει απεικόνιση $\widetilde{f}\colon \mathbb{Z}_7 \longrightarrow \mathbb{Z}_4$ έτσι ώστε $\varpi_7 \circ \widetilde{f} = f$ ή ισοδύναμα, θέτοντας $\widetilde{f}([x]_7) = f(x)$, δεν ορίζεται απεικόνιση $\mathbb{Z}_7 \longrightarrow \mathbb{Z}_4$.

Πρακτικά, όπως δείχνει η παρακάτω Πρόταση 1.2.13, για να εξετάσουμε αν η σχέση $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση εξετάζουμε αν ο ορισμός της είναι ανεξάρτητος της επιλογής αντιπροσώπου, με την ακόλουθη έννοια: $\forall x, y \in X:\ x \sim_{\mathscr{R}} y \implies f(x) = f(y)$.

Πρόταση 1.2.13. *Έστω $f\colon X \longrightarrow A$ μια απεικόνιση μεταξύ συνόλων και $\mathscr{R}$ μια σχέση ισοδυναμίας επί του συνόλου X. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η αντιστοιχία*
$$\widetilde{f}\colon X/\mathscr{R} \longrightarrow A, \quad \widetilde{f}([x]_{\mathscr{R}}) = f(x)$$
είναι μια καλά ορισμένη απεικόνιση.

2. *Υπάρχει μοναδική απεικόνιση* $\widetilde{f}\colon X/\mathscr{R} \longrightarrow A$ *έτσι ώστε:* $\widetilde{f}\circ\pi_{\mathscr{R}} = f$*, δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:*



3. $\forall x, y \in X\colon\ x \sim_{\mathscr{R}} y \implies f(x) = f(y)$.

Αν ισχύει μια από τις παραπάνω ισοδύναμες συνθήκες, τότε: (α) *η απεικόνιση* $\widetilde{f}$ *είναι «επί» αν και μόνο αν η απεικόνιση* f *είναι «επί», και* (β) *η απεικόνιση* $\widetilde{f}$ *είναι «1-1» αν και μόνο αν* $\forall x, y \in X\colon\ f(x) = f(y) \implies x \sim_{\mathscr{R}} y$.

Απόδειξη. (α) **1.** $\implies$ **2.** Παρατηρούμε ότι για κάθε στοιχείο $x \in X$ έχουμε: $(\widetilde{f}\circ\pi_{\mathscr{R}})(x) = \widetilde{f}(\pi_{\mathscr{R}}(x)) = \widetilde{f}([x]_{\mathscr{R}}) = f(x)$. Επομένως $\widetilde{f}\circ\pi_{\mathscr{R}} = f$. Αν $g\colon X/\mathscr{R} \longrightarrow A$ είναι μια άλλη απεικόνιση έτσι ώστε $g\circ\pi_{\mathscr{R}} = f$, τότε για κάθε κλάση ισοδυναμίας $[x]_{\mathscr{R}} \in X/\mathscr{R}$ θα έχουμε: $g([x]_{\mathscr{R}}) = g(\pi_{\mathscr{R}}(x)) = (g\circ\pi_{\mathscr{R}})(x) = f(x) = \widetilde{f}([x]_{\mathscr{R}})$. Επομένως θα έχουμε $g = \widetilde{f}$.

2. $\implies$ **1.** Επειδή από την υπόθεση είναι $\widetilde{f}\circ\pi_{\mathscr{R}} = f$, όπως παραπάνω για κάθε $[x]_{\mathscr{R}} \in X/\mathscr{R}$, θα έχουμε: $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}(\pi_{\mathscr{R}}(x)) = (\widetilde{f}\circ\pi_{\mathscr{R}})(x) = f(x)$. Άρα, θέτοντας $\widetilde{f}([x]_{\mathscr{R}}) = f(x)$, αποκτούμε μια καλά ορισμένη απεικόνιση $\widetilde{f}\colon X/\mathscr{R} \longrightarrow A$.

1. $\implies$ **3.** Αν η $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση, και $x \sim_{\mathscr{R}} y$, τότε από το Λήμμα 1.2.10 θα έχουμε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$. Τότε προφανώς θα έχουμε $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$ και επομένως $f(x) = f(y)$.

3. $\implies$ **1.** Αν ισχύει το 3., τότε για να ορίζει η αντιστοιχία $\widetilde{f}$ μια απεικόνιση θα πρέπει $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$, για τυχόντα στοιχεία $[x]_{\mathscr{R}}, [y]_{\mathscr{R}} \in X/\mathscr{R}$ έτσι ώστε $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$. Η τελευταία ισότητα με χρήση του Λήμματος 1.2.10 δίνει $x \sim_{\mathscr{R}} y$ και άρα από το 3. έχουμε $f(x) = f(y)$, δηλαδή $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$.

(β) Υποθέτουμε τώρα ότι ισχύει μια από τις παραπάνω ισοδύναμες συνθήκες.

(i) Αν η απεικόνιση f είναι «επί», τότε για κάθε $a \in A$ υπάρχει $x \in X$ έτσι ώστε $f(x) = x$. Τότε θα έχουμε $\widetilde{f}([x]_{\mathscr{R}}) = f(x) = a$, και άρα η απεικόνιση $\widetilde{f}$ είναι «επί». Αντίστροφα, αν η $\widetilde{f}$ είναι «επί», τότε, επειδή $\widetilde{f}\circ\pi_{\mathscr{R}} = f$ και επειδή η απεικόνιση $\pi_{\mathscr{R}}$ είναι «επί», έπεται ότι η f είναι απεικόνιση «επί» ως σύνθεση απεικονίσεων «επί».

(ii) Αν η απεικόνιση $\widetilde{f}$ είναι «1-1», έστω $x, y \in X$ έτσι ώστε $f(x) = f(y)$. Τότε θα έχουμε $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$ και επομένως $[x]_{\mathscr{R}} = [y]_{\mathscr{R}}$, διότι η $\widetilde{f}$ είναι «1-1». Από το Λήμμα 1.2.10 έπεται τότε ότι $x \sim_{\mathscr{R}} y$. Αντίστροφα, υποθέτουμε ότι $\forall x, y \in X\colon\ f(x) = f(y) \implies x \sim_{\mathscr{R}} y$, και έστω ότι $\widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$, δηλαδή $f(x) = f(y)$. Τότε από την υπόθεση έπεται ότι $x \sim_{\mathscr{R}} y$. ∎

Θα δούμε μια εφαρμογή της Πρότασης 1.2.13. Έστω X και Y δύο μη-κενά σύνολα και $\mathscr{R}$ και $\mathscr{T}$ σχέσεις ιδοσυναμίας επί των X και Y αντίστοιχα. Αν $f\colon X \longrightarrow Y$ είναι μια απεικόνιση, τότε θα λέμε ότι η f **διατηρεί τις σχέσεις ισοδυναμίας** $\mathscr{R}$ και $\mathscr{T}$, και θα γράφουμε $f(\mathscr{R}) \subseteq \mathscr{T}$, αν:

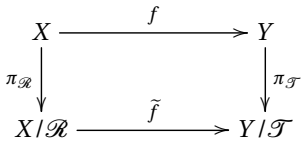
$$\forall x_1, x_2 \in X\colon\ x_1 \sim_{\mathscr{R}} x_2 \quad\implies\quad f(x_1) \sim_{\mathscr{T}} f(x_2)$$

δηλαδή, αν: $(x_1, x_2) \in \mathscr{R} \implies (f(x_1), f(x_2)) \in \mathscr{T}$.

Πόρισμα 1.2.14. *Έστω ότι* $f\colon X \longrightarrow Y$ *είναι μια απεικόνιση μεταξύ συνόλων και υποθέτουμε ότι* $\mathscr{R}$*, αντίστοιχα* $\mathscr{T}$*, είναι μια σχέση ισοδυναμίας επί του* X*, αντίστοιχα του* Y*. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. $f(\mathscr{R}) \subseteq \mathscr{T}$*, δηλαδή η* f *διατηρεί τις σχέσεις ισοδυναμίας* $\mathscr{R}$ *και* $\mathscr{T}$*.*

2. *Υπάρχει μοναδική απεικόνιση* $\widetilde{f}\colon X/\mathscr{R} \longrightarrow Y/\mathscr{T}$ *έτσι ώστε* $\pi_{\mathscr{T}}\circ f = \widetilde{f}\circ\pi_{\mathscr{R}}$*, δηλαδή το ακόλουθο τετράγωνο είνα μεταθετικό:*



και τότε η $\widetilde{f}$ ορίζεται ως εξής: $\widetilde{f}([x]_{\mathscr{R}}) = [f(x)]_{\mathscr{T}}$.

3. *Θέτοντας* $\widetilde{f}\colon X/\mathscr{R} \longrightarrow X/\mathscr{T}$, $\widetilde{f}([x]_{\mathscr{R}}) = [f(x)]_{\mathscr{T}}$, *αποκτούμε μια καλά ορισμένη απεικόνιση.*

Αν ισχύει μια από τις παραπάνω ισοδύναμες συνθήκες, τότε: (α) *η απεικόνιση $\widetilde{f}$ είναι «επί» αν και μόνο αν η απεικόνιση f είναι «επί», και* (β) *η απεικόνιση $\widetilde{f}$ είναι «1-1» αν και μόνο αν* $\forall x, y \in X\colon\ f(x) = f(y) \implies x \sim_{\mathscr{R}} y$.

Απόδειξη. Θεωρούμε την σύνθεση απεικονίσεων

$$\pi_{\mathscr{T}} \circ f\colon\ X \longrightarrow Y/\mathscr{T}, \quad (\pi_{\mathscr{T}} \circ f)(x) = [f(x)]_{\mathscr{T}}$$

Παρατηρούμε ότι η f διατηρεί τις σχέσεις ισοδυναμίας $\mathscr{R}$ και $\mathscr{T}$, δηλαδή $\forall x_1, x_2 \in X\colon\ x_1 \sim_{\mathscr{R}} x_2 \implies f(x_1) \sim_{\mathscr{T}} f(x_2)$, αν και μόνο αν, $\forall x_1, x_2 \in X\colon\ x_1 \sim_{\mathscr{R}} x_2 \implies (\pi_{\mathscr{T}} \circ f)(x_1) = [f(x_1)]_{\mathscr{T}} = [f(x_2)]_{\mathscr{T}} = (\pi_{\mathscr{T}} \circ f)(x_2)$.

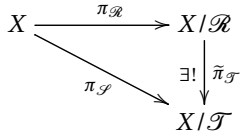
Επομένως από την Πρόταση 1.2.13, εφαρμοσμένη στην απεικόνιση $\pi_{\mathscr{T}} \circ f$, έπεται ότι η f διατηρεί τις σχέσεις ισοδυναμίας $\mathscr{R}$ και $\mathscr{S}$ αν και μόνο αν υπάρχει μοναδική απεικόνιση $\widetilde{f}\colon X/\mathscr{R} \longrightarrow Y/\mathscr{T}$ έτσι ώστε $\pi_{\mathscr{T}} \circ f = \widetilde{f} \circ \pi_{\mathscr{R}}$, αν και μόνο αν, θέτοντας $\widetilde{f}([x]_{\mathscr{R}}) = [f(x)]_{\mathscr{T}}$, $\forall x \in X$, αποκτούμε μια καλά ορισμένη απεικόνιση $\widetilde{f}\colon X/\mathscr{R} \longrightarrow Y/\mathscr{T}$.

Αν ισχύει μια από τις παραπάνω ισοδύναμες συνθήκες, τότε οι ισχυρισμοί (α) και (β) προκύπτουν άμεσα από την Πρόταση 1.2.13. ■

Πόρισμα 1.2.15. *Αν $\mathscr{R}$ και $\mathscr{T}$ είναι δύο σχέσεις ισοδυναμίας επί ενός συνόλου X, τότε τα ακόλουθα είναι ισοδύναμα:*

1. $\mathscr{R} \subseteq \mathscr{T}$.

2. *Υπάρχει μοναδική απεικόνιση $\widetilde{\pi}_{\mathscr{T}}\colon X/\mathscr{R} \longrightarrow X/\mathscr{T}$ έτσι ώστε:* $\widetilde{\pi}_{\mathscr{T}} \circ \pi_{\mathscr{R}} = \pi_{\mathscr{T}}$, *δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:*



3. *Θέτοντας* $\widetilde{\pi}_{\mathscr{T}}\colon X/\mathscr{R} \longrightarrow X/\mathscr{T}$, $\widetilde{\pi}_{\mathscr{S}}([x]_{\mathscr{R}}) = [(x)]_{\mathscr{T}}$, *αποκτούμε μια καλά ορισμένη απεικόνιση.*

Αν $\mathscr{R} \subseteq \mathscr{T}$, τότε η απεικόνιση $\widetilde{\pi}_{\mathscr{T}}$ είναι «επί», και η $\widetilde{\pi}_{\mathscr{T}}$ είναι απεικόνιση «1-1» αν και μόνο αν $\mathscr{R} = \mathscr{T}$.

Απόδειξη. Η απόδειξη προκύπτει άμεσα, εφαρμόζοντας την Πρόταση 1.2.13 στην απεικόνιση κανονικής προβολής $\pi_{\mathscr{T}}\colon X \longrightarrow X/\mathscr{T}$ ή εφαρμόζοντας το Πόρισμα 1.2.14 στην ταυτοτική απεικόνιση $\mathsf{Id}_X\colon X \longrightarrow X$. ■

Παράδειγμα 1.2.16. Θεωρούμε τις σχέσεις διαιρετότητας $\mathscr{R}_6$ και $\mathscr{R}_3$ επί του συνόλου $\mathbb{Z}$ των ακεραίων, και τότε $\mathbb{Z}/\mathscr{R}_6 = \mathbb{Z}_6$ και $\mathbb{Z}/\mathscr{R}_3 = \mathbb{Z}_3$, βλέπε Παράδειγμα 1.2.11. Επειδή, $\forall x, y \in \mathbb{Z}$, προφανώς έχουμε $6 \mid x - y \implies 3 \mid x - y$, έπεται ότι $\mathscr{R}_6 \subseteq \mathscr{R}_3$. Τότε από το Πόρισμα 1.2.15 έπεται ότι, θέτοντας $f([x]_6) = [x]_3$, αποκτούμε μια καλά ορισμένη απεικόνιση $f\colon \mathbb{Z}_6 \longrightarrow \mathbb{Z}_3$, η οποία είναι και η μοναδική απεικόνιση έτσι ώστε $f \circ \pi_6 = \pi_3$. √

Σχόλιο 1.2.17. Υπάρχουν περιπτώσεις κατά τις οποίες, δοθείσης μιας σχέσης ισοδυναμίας $\mathscr{R}$ επί ενός συνόλου X και ενός συνόλου A, θέλουμε να ορίσουμε με φυσιολογικό τρόπο απεικόνιση $\widetilde{f}\colon X/\mathscr{R} \longrightarrow A$, χωρίς να υπάρχει εκ των προτέρων απεικόνιση $f\colon X \longrightarrow A$, όπως στην Πρόταση 1.2.13. Σε αυτήν την περίπτωση θα πρέπει πάντα να εξετάζουμε αν ο ορισμός του στοιχείου $\widetilde{f}([x]_{\mathscr{R}}) \in A$ είναι ανεξάρτητος της επιλογής αντιπροσώπου της κλάσης ισοδυναμίας $[x]_{\mathscr{R}}$, με άλλα λόγια θα πρέπει να εξετάζουμε αν: $\forall x, y \in X\colon\ x \sim_{\mathscr{R}} y \implies \widetilde{f}([x]_{\mathscr{R}}) = \widetilde{f}([y]_{\mathscr{R}})$. ▲

1.2.3 Διαμερίσεις και Σχέσεις Ισοδυναμίας

Στην παρούσα υποενότητα θα αναλύσουμε την έννοια της διαμέρισης ενός συνόλου, καθώς και τη σχέση μεταξύ διαμερίσεων και σχέσεων ισοδυναμίας.

Έστω X ένα μη κενό σύνολο.

Ορισμός 1.2.18. *Μια* **διαμέριση** *του X είναι μια συλλογή υποσυνόλων $\Delta = \{A_i \mid A_i \subseteq X\}_{i\in I}$ του X, όπου I είναι ένα σύνολο δεικτών, έτσι ώστε να ικανοποιούνται οι ακόλουθες ιδιότητες:*

1. $\forall i \in I\colon\ A_i \neq \emptyset$.
2. $\forall i, j \in I\colon\ \ i \neq j \implies A_i \cap A_j = \emptyset$.
3. $X = \bigcup_{i\in I} A_i$.

Αν $\Delta = \{A_i \mid i \in I\}$ είναι μια διαμέριση του X, τότε συχνά αυτό θα το υποδηλώνουμε γράφοντας:

$$X = \sum_{i\in I} A_i$$

Με άλλα λόγια, μια διαμέριση του μη κενού συνόλου X είναι μια συλλογή Δ μη κενών υποσυνόλων του X με την ιδιότητα κάθε στοιχείο του συνόλου X να ανήκει σε ένα και μόνο ένα σύνολο της συλλογής Δ.

Υπενθυμίζουμε ότι, αν X είναι ένα σύνολο, τότε

$$|X| \qquad \text{ή} \qquad \#(X)$$

συμβολίζει το πλήθος των στοιχείων του X.

Παρατήρηση 1.2.19. Έστω X ένα πεπερασμένο σύνολο και $\Delta = \{A_i \mid A_i \subseteq X\}_{i\in I}$ μια διαμέριση του συνόλου X. Τότε προφανώς το σύνολο δεικτών I και κάθε υποσύνολο A_i της διαμέρισης είναι πεπερασμένα σύνολα και επομένως, επειδή το X είναι ξένη ένωση των A_i, δηλαδή

$$X = \bigcup_{i\in I} A_i, \qquad \text{και} \qquad A_i \bigcap A_j = \emptyset, \qquad \forall i \neq j$$

θα έχουμε:

$$|X| = \sum_{i\in I} |A_i| \quad \blacktriangle$$

Η επόμενη Πρόταση εξασφαλίζει ότι κάθε διαμέριση Δ του συνόλου X ορίζει μια σχέση ισοδυναμίας $\mathscr{R}$ επί του X, έτσι ώστε οι κλάσεις ισοδυναμίας των στοιχείων του X ως προς την $\mathscr{R}$ να συμπίπτουν με τα υποσύνολα της διαμέρισης Δ.

Πρόταση 1.2.20. *Έστω $\Delta = \{A_i \mid A_i \subseteq X\}_{i\in I}$ μια διαμέριση του μη-κενού συνόλου X. Τότε, ορίζοντας*

$$\mathscr{R}_\Delta := \{(x, y) \in X \times X \mid \exists\, i \in I\colon\ x, y \in A_i\}$$

αποκτούμε μια σχέση ισοδυναμίας $\mathscr{R}_\Delta$ επί του X. Επιπλέον:

1. *$\forall x \in X\colon\ [x]_{\mathscr{R}_\Delta} = A_i$, για κάποιο $i \in I$ (το i είναι ο μοναδικός δείκτης $i \in I$ έτσι ώστε $x \in A_i$).*

2. *$X/\mathscr{R}_\Delta = \Delta$ ως συλλογές υποσυνόλων του X.*

Απόδειξη. Δείχνουμε πρώτα ότι η σχέση $\mathscr{R}_\Delta$ είναι σχέση ισοδυναμίας επί του X.

- Έστω $x \in X$. Επειδή η συλλογή υποσυνόλων Δ είναι μια διαμέριση του X, έπεται ότι $x \in X = \bigcup_{i\in I} A_i$ και άρα υπάρχει δείκτης $i \in I$ έτσι ώστε: $x \in A_i$. Τότε προφανώς $(x, x) \in \mathscr{R}_\Delta$, δηλαδή $x \sim_{\mathscr{R}_\Delta} x$, και άρα για τη σχέση $\mathscr{R}_\Delta$ ισχύει η ανακλαστική ιδιότητα.
- Έστω $x, y \in X$ και υποθέτουμε ότι $(x, y) \in \mathscr{R}_\Delta$, δηλαδή $x \sim_{\mathscr{R}_\Delta} y$. Τότε εξ ορισμού υπάρχει δείκτης $i \in I$ έτσι ώστε $x, y \in A_i$ και προφανώς τότε $y, x \in A_i$. Άρα $(y, x) \in \mathscr{R}_\Delta$ δηλαδή $y \sim_{\mathscr{R}_\Delta} x$ και άρα για τη σχέση $\mathscr{R}_\Delta$ ισχύει η συμμετρική ιδιότητα.

• Έστω ότι $(x,y) \in \mathscr{R}_\Delta$ και $(y,z) \in \mathscr{R}_\Delta$, δηλαδή $x \sim_{\mathscr{R}_\Delta} y$ και $y \sim_{\mathscr{R}_\Delta} z$. Τότε υπάρχουν δείκτες $i, j \in I$ έτσι ώστε: $x, y \in A_i$ και $y, z \in A_j$. Τότε όμως $y \in A_i \cap A_j$. Επειδή από τον ορισμό της διαμέρισης έχουμε $A_i \cap A_j = \emptyset$ αν $i \neq j$, έπεται ότι αναγκαστικά θα έχουμε $i = j$ και άρα $A_i = A_j$. Επομένως $x, y, z \in A_i$, το οποίο σημαίνει ότι $(x,z) \in \mathscr{R}_\Delta$, δηλαδή $x \sim_{\mathscr{R}_\Delta} z$, και άρα για τη σχέση $\mathscr{R}_\Delta$ ισχύει η μεταβατική ιδιότητα.

1. Έστω $x \in X$. Τότε υπάρχει μοναδικός δείκτης $i \in I$ έτσι ώστε: $x \in A_i$. Θα έχουμε:

$$[x]_{\mathscr{R}_\Delta} = \{y \in X \mid y \sim_{\mathscr{R}_\Delta} x\} = \{y \in X \mid \exists j \in I : \ x, y \in A_j\}$$

Επειδή $x \in A_i$ και $A_i \cap A_j = \emptyset$ αν $i \neq j$, θα έχουμε αναγκαστικά $i = j$ και άρα:

$$[x]_{\mathscr{R}_\Delta} = \{y \in X \mid \exists j \in I : \ x, y \in A_j\} = \{y \in X \mid y \in A_i\} = A_i$$

2. Επειδή $X/\mathscr{R}_\Delta = \{[x]_{\mathscr{R}_\Delta} \mid x \in X\}$ και $[x]_{\mathscr{R}_\Delta} = A_i$, όπου $i \in I$ είναι ο μοναδικός δείκτης για τον οποίο ισχύει $x \in A_i$, θα έχουμε ότι:

$$X/\mathscr{R}_\Delta = \{[x]_{\mathscr{R}_\Delta} \mid x \in X\} = \{A_i \mid i \in I\} = \Delta$$ ■

Παράδειγμα 1.2.21. Θα περιγράψουμε όλες τις δυνατές διαμερίσεις επί συνόλων X με 1, 2, ή 3 στοιχεία, καθώς και τις επαγόμενες σχέσεις ισοδυναμίας επί του X, όπως αυτές προκύπτουν από την Πρόταση 1.2.20.

1. Αν $X = \{x\}$, τότε η μοναδική διαμέριση του X είναι προφανώς η $\Delta = \{X = \{x\}\}$. Η μοναδική σχέση ισοδυναμίας επί του X είναι τότε η σχέση $\mathscr{R}_\Delta$ κατά την οποία, για το μοναδικό στοιχείο $x \in X$, ισχύει ότι: $x \sim_{\mathscr{R}_\Delta} x$. Ως υποσύνολο του $X \times X$ η $\mathscr{R}_\Delta$ είναι το υποσύνολο $\mathscr{R}_\Delta = \{(x,x) \in X \times X \mid x \in X\} = X \times X$.

2. Αν $X = \{x, y\}$, τότε θα έχουμε τις διαμερίσεις του X:

$$\Delta_1 = \{X = \{x, y\}\} \qquad \text{και} \qquad \Delta_2 = \{\{x\}, \ \{y\}\}$$

   Για τη διαμέριση Δ_1, η επαγόμενη σχέση ισοδυναμίας οριζεται από τις σχέσεις: $x \sim_{\mathscr{R}_{\Delta_1}} x$, $x \sim_{\mathscr{R}_{\Delta_1}} y$, $y \sim_{\mathscr{R}_{\Delta_1}} x$, και $y \sim_{\mathscr{R}_{\Delta_1}} y$. Ως υποσύνολο του $X \times X$ έχουμε ότι: $\mathscr{R}_{\Delta_1} = \{(x,x), (x,y), (y,x), (y,y)\} = X \times X$.
   Για την διαμέριση Δ_2, η επαγόμενη σχέση ισοδυναμίας οριζεται από τις σχέσεις: $x \sim_{\mathscr{R}_{\Delta_2}} x$, και $y \sim_{\mathscr{R}_{\Delta_2}} y$. Ως υποσύνολο του $X \times X$ έχουμε ότι: $\mathscr{R}_{\Delta_1} = \{(x,x), (y,y)\} = I_X$.

3. Αν $X = \{x, y, z\}$, τότε θα έχουμε τις ακόλουθες διαμερίσεις του X:

$$\Delta_1 = \{X = \{x, y, z\}\}, \quad \Delta_2 = \{\{x, y\}, \ \{z\}\}, \quad \Delta_3 = \{\{x, z\}, \ \{y\}\}, \quad \Delta_4 = \{\{y, z\}, \ \{x\}\}, \quad \Delta_5 = \{\{x\}, \ \{z\}, \ \{y\}\}$$

   (α′) Η σχέση ισοδυναμίας επί του X την οποία ορίζει η διαμέριση Δ_1, ως υποσύνολο του $X \times X$, είναι η εξής:
   $$\mathscr{R}_{\Delta_1} = X \times X$$

   (β′) Η σχέση ισοδυναμίας επί του X την οποία ορίζει η διαμέριση Δ_2, ως υποσύνολο του $X \times X$, είναι η εξής:
   $$\mathscr{R}_{\Delta_2} = \{(x,x), (y,y), (x,y), (y,x), (z,z)\}$$

   (γ′) Η σχέση ισοδυναμίας επί του X την οποία ορίζει η διαμέριση Δ_3, ως υποσύνολο του $X \times X$, είναι η εξής:
   $$\mathscr{R}_{\Delta_3} = \{(x,x), (z,z), (x,z), (z,x), (y,y)\}$$

   (δ′) Η σχέση ισοδυναμίας επί του X την οποία ορίζει η διαμέριση Δ_4, ως υποσύνολο του $X \times X$, είναι η εξής:
   $$\mathscr{R}_{\Delta_4} = \{(y,y), (z,z), (y,z), (z,y), (x,x)\}$$

   (ε′) Η σχέση ισοδυναμίας επί του X την οποία ορίζει η διαμέριση Δ_5, ως υποσύνολο του $X \times X$, είναι η εξής:
   $$\mathscr{R}_{\Delta_5} = \{(x,x), (y,y), (z,z)\}$$ ✓

Συνδυάζοντας το Πόρισμα 1.2.12 και την Πρόταση 1.2.20, έχουμε το ακόλουθο βασικό Θεώρημα το οποίο επιτρέπει την μετάβαση από σχέσεις ισοδυναμίας σε διαμερίσεις και αντιστρόφως χωρίς να χάνεται πληροφορία. Συμβολίζουμε με $\mathscr{D}$ τη συλλογή όλων των διαμερίσεων του συνόλου X και με $\mathscr{S}$ τη συλλογή όλων των σχέσεων ισοδυναμίας επί του X.

Θεώρημα 1.2.22. *Έστω X ένα μη-κενό σύνολο. Τότε οι απεικονίσεις*

$$\Phi : \mathscr{D} = \{\text{Διαμερίσεις } \Delta \text{ του } X\} \longrightarrow \mathscr{S} = \{\text{Σχέσεις ισοδυναμίας } \mathscr{R} \text{ επί του } X\}, \qquad \Phi(\Delta) = \mathscr{R}_\Delta$$

$$\Psi : \mathscr{S} = \{\text{Σχέσεις ισοδυναμίας } \mathscr{R} \text{ επί του } X\} \longrightarrow \mathscr{D} = \{\text{Διαμερίσεις } \Delta \text{ του } X\}, \qquad \Psi(\mathscr{R}) = \Delta_{\mathscr{R}} := X/\mathscr{R}$$

ορίζουν μια «1-1» και «επί» αντιστοιχία μεταξύ του συνόλου $\mathscr{D}$ των διαμερίσεων του X και του συνόλου $\mathscr{S}$ των κλασεων ισοδυναμίας επί του X, και άρα για κάθε $\mathscr{R} \in \mathscr{S}$ και για κάθε $\Delta \in \mathscr{D}$:

$$\mathscr{R}_{\Delta_{\mathscr{R}}} = \mathscr{R} \quad \text{και} \quad \Delta_{\mathscr{R}_\Delta} = \Delta$$

Απόδειξη. Από το Πόρισμα 1.2.12 και την Πρόταση 1.2.20 έπεται ότι οι αντιστοιχίες Φ και Ψ ορίζουν απεικονίσεις $\Phi\colon \mathscr{D} \longrightarrow \mathscr{S}$, $\Phi(\Delta) = \mathscr{R}_\Delta$ και $\Psi\colon \mathscr{S} \longrightarrow \mathscr{D}$, $\Psi(\mathscr{R}) = \Delta_{\mathscr{R}} := X/\mathscr{R}$.

Για την ολοκλήρωση της απόδειξης, αρκεί να δείξουμε ότι οι απεικονίσεις Φ και Ψ είναι η μία αντίστροφη της άλλης. Με άλλα λόγια, αρκεί να δείξουμε ότι:

$$\forall \Delta \in \mathscr{D}: \ \Psi\Phi(\Delta) = \Delta \quad \text{και} \quad \forall \mathscr{R} \in \mathscr{S}: \ \Phi\Psi(\mathscr{R}) = \mathscr{R}$$

ή ισοδύναμα:

$$\forall \Delta \in \mathscr{D}: \ \Delta_{\mathscr{R}_\Delta} = \Delta \quad \text{και} \quad \forall \mathscr{R} \in \mathscr{S}: \ \mathscr{R}_{\Delta_{\mathscr{R}}} = \mathscr{R}$$

Από την Πρόταση 1.2.20 έπεται ότι για κάθε διαμέριση Δ του X έχουμε $X/\mathscr{R}_\Delta = \Delta$ ως συλλογές υποσυνόλων του X. Έτσι

$$\Psi\Phi(\Delta) = \Psi(\mathscr{R}_\Delta) = X/\mathscr{R}_\Delta = \Delta$$

Για να δείξουμε τώρα ότι $\forall \mathscr{R} \in \mathscr{S}: \ \Phi\Psi(\mathscr{R}) = \mathscr{R}$, αρκεί να δείξουμε ότι $\mathscr{R}_{\Delta_{\mathscr{R}}} = \mathscr{R}$. Υπενθυμίζουμε ότι η διαμέριση $\Delta_{\mathscr{R}}$, την οποία ορίζει επί του X η σχέση ισοδυναμίας $\mathscr{R}$, αποτελείται από την συλλογή των (διακεκριμένων) κλάσεων ισοδυναμίας $[x]_{\mathscr{R}}$ των στοιχείων του X. Έτσι εξ ορισμού για την επαγόμενη σχέση ισοδυναμίας $\mathscr{R}_{\Delta_{\mathscr{R}}}$ την οποία ορίζει η $\Delta_{\mathscr{R}}$ θα έχουμε: $\forall x, y \in X$: $(x, y) \in \mathscr{R}_{\Delta_{\mathscr{R}}}$ αν και μόνο αν τα στοιχεία x και y ανήκουν στο ίδιο σύνολο της διαμέρισης $\Delta_{\mathscr{R}}$, δηλαδή αν και μόνο αν υπάρχει $z \in X$ έτσι ώστε $x, y \in [z]_{\mathscr{R}}$. Αυτό όμως συμβαίνει αν και μόνο αν $z \sim_{\mathscr{R}} x$ και $z \sim_{\mathscr{R}} y$ και επομένως αν και μόνο αν $x \sim_{\mathscr{R}} y$ αν και μόνο αν $(x, y) \in \mathscr{R}$. Συνοψίζοντας, δείξαμε ότι:

$$\forall x, y \in X: \ (x, y) \in \mathscr{R}_{\Delta_{\mathscr{R}}} \iff (x, y) \in \mathscr{R}$$

Επομένως, $\mathscr{R}_{\Delta_{\mathscr{R}}} = \mathscr{R}$ και άρα $\forall \mathscr{R} \in \mathscr{S}: \ \Phi\Psi(\mathscr{R}) = \mathscr{R}$. Έτσι δείξαμε ότι οι απεικονίσεις Φ και Ψ είναι «1-1» και «επί» και επιπλέον: $\Psi = \Phi^{-1}$. ■

Παρατήρηση 1.2.23. Έστω X ένα σύνολο το οποίο έχει n στοιχεία: $|X| = n$. Πόσες διαφορετικές σχέσεις ισοδυναμίας υπάρχουν ορισμένες επί του X;

Έστω

$$B_n = \text{πλήθος σχέσεων ισοδυναμίας επί ενός συνόλου } X \text{ με } n \text{ στοιχεία}$$

Χρησιμοποιώντας ότι οι σχέσεις ισοδυναμίας του συνόλου X είναι σε «1-1» και «επί» αντιστοιχία με τις διαμερίσεις του X, αποδεικνύεται ότι ο αριθμός B_n, ο οποίος καλείται **ο n-οστός αριθμός του Bell**,[3] δίνεται από την αναδρομική σχέση

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k$$

[3] E.T. Bell (1883-1960) [http://en.wikipedia.org/wiki/Eric_Temple_Bell], Σκωτσέζος μαθηματικός (και συγγραφέας, μεταξύ άλλων, και διηγημάτων επιστημονικής φαντασίας), ο οποίος εργάστηκε στις ΗΠΑ. Ο E.T. Bell μελέτησε τους αριθμούς που φέρουν το όνομά του σε εργασία του το 1934, αν και μια συστηματική θεωρία για τους αριθμούς αυτούς είχε αναπτυχθεί 25-30 χρόνια πριν από τον σπουδαίο Ινδό μαθηματικό Srinivasa Ramanujan (1887-1920) [http://en.wikipedia.org/wiki/Srinivasa_Ramanujan], ο οποίος, αν και αυτοδίδακτος, είχε σημαντική συνεισφορά στη Θεωρία Αριθμών και στη Μαθηματική Ανάλυση.

Για παράδειγμα οι πρώτοι 10 αριθμοί του Bell είναι οι εξής:

$$B_0 = 1, \quad B_1 = 1, \quad B_2 = 2, \quad B_3 = 5, \quad B_4 = 15, \quad B_5 = 52, \quad B_6 = 203$$

$$B_7 = 877, \quad B_8 = 4140, \quad B_9 = 21147, \quad B_{10} = 115975 \quad \blacktriangle$$

1.2.4 Απεικονίσεις και Σχέσεις Ισοδυναμίας

Έστω $f\colon X \longrightarrow Y$ μια απεικόνιση μεταξύ των μη-κενών συνόλων X, Y. Ορίζουμε μια σχέση $\mathscr{R}_f$ επί του συνόλου X ως εξής:

$$\mathscr{R}_f = \big\{(x,y) \in X \times X \mid f(x) = f(y)\big\}$$

Η επόμενη πρόταση δείχνει ότι η σχέση $\mathscr{R}_f$ είναι μια σχέση ισοδυναμίας επί του X και περιγράφει το σύνολο πηλίκο $X/\mathscr{R}_f$.

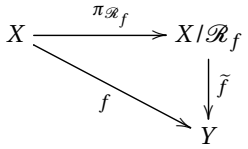
Πρόταση 1.2.24. **1.** *Η σχέση $\mathscr{R}_f$ είναι μια σχέση ισοδυναμίας επί του X. Επιπλέον, $\forall\, x \in X$:*

$$[x]_{\mathscr{R}_f} = f^{-1}\big\{f(x)\big\} = \big\{x' \in X \mid f(x) = f(x')\big\}$$

και η απεικόνιση f επάγει μια «1-1» απεικόνιση

$$\widetilde{f}\ :\ X/\mathscr{R}_f \longrightarrow Y, \quad \overline{f}([x]_{\mathscr{R}_f}) = f(x)$$

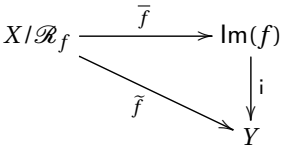
έτσι ώστε $\widetilde{f} \circ \pi_{\mathscr{R}_f} = f$, δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:



2. *Η απεικόνιση $\widetilde{f}$ επάγει μια «1-1» και «επί» απεικόνιση*

$$\overline{f}\ :\ X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f), \quad \overline{f}([x]_{\mathscr{R}_f}) = f(x)$$

όπου $\mathsf{i}\colon \mathsf{Im}(f) \longrightarrow Y$, $\mathsf{i}(y) = y$, είναι η κανονική έγκλειση, και ισχύει ότι $\overline{f} \circ \mathsf{i} = \widetilde{f}$, δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:

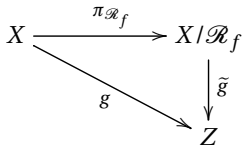


Ιδιαίτερα η απεικόνιση f είναι «επί» αν και μόνο αν η απεικόνιση $\widetilde{f}$ είναι «1-1» και «επί».

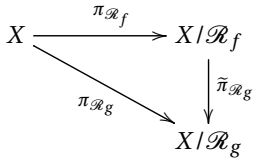
3. *Αν $g\colon X \longrightarrow Z$ είναι μια απεικόνιση έτσι ώστε να ικανοποιείται η ακόλουθη συνθήκη:*

$$\forall\, x, y \in X\colon \quad f(x) = f(y) \quad \Longrightarrow \quad g(x) = g(y) \tag{†}$$

τότε υπάρχει μοναδική απεικόνιση $\widetilde{g}\colon X/\mathscr{R}_f \longrightarrow Z$, έτσι ώστε: $\widetilde{g} \circ \pi_{\mathscr{R}_f} = g$, δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:



Ιδιαίτερα, υπάρχει μοναδική απεικόνιση $\tilde{\pi}_{\mathscr{R}_g} : X/\mathscr{R}_f \longrightarrow X/\mathscr{R}_g$, η οποία είναι «επί», έτσι ώστε $\tilde{\pi}_{\mathscr{R}_g} \circ \pi_{\mathscr{R}_f} = \pi_{\mathscr{R}_g}$, δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό:



Απόδειξη. Θα έχουμε:

1. Δείχνουμε πρώτα ότι η σχέση $\mathscr{R}_f$ είναι σχέση ισοδυναμίας επί του X:

- Έστω $x \in X$. Τότε $x \sim_{\mathscr{R}_f} x$ διότι $f(x) = f(x)$. Άρα η σχέση $\mathscr{R}_f$ είναι ανακλαστική.
- Έστω $x, y \in X$, και υποθέτουμε ότι $x \sim_{\mathscr{R}_f} y$. Τότε $f(x) = f(y)$. Άρα $f(y) = f(x)$ και επομένως $y \sim_{\mathscr{R}_f} x$, δηλαδή η σχέση $\mathscr{R}_f$ είναι συμμετρική.
- Έστω $x, y, z \in X$ και υποθέτουμε ότι $x \sim_{\mathscr{R}_f} y$ και $y \sim_{\mathscr{R}_f} z$. Τότε $f(x) = f(y)$ και $f(y) = f(z)$. Προφανώς τότε $f(x) = f(z)$ και επομένως $x \sim_{\mathscr{R}_f} z$, δηλαδή η σχέση $\mathscr{R}_f$ είναι μεταβατική.

Έστω $x \in X$. Τότε:

$$[x]_{\mathscr{R}_f} = \{y \in X \mid y \sim_{\mathscr{R}_f} x\} = \{y \in X \mid f(y) = f(x)\} = \{y \in X \mid y \in f^{-1}(\{f(x)\})\} = f^{-1}(\{f(x)\})$$

Από την Πρόταση 1.2.13 έπεται ότι υπάρχει μοναδική απεικόνιση

$$\tilde{f} : X/\mathscr{R}_f \longrightarrow Y, \quad \text{έτσι ώστε:} \quad \tilde{f} \circ \pi_{\mathscr{R}_f} = f$$

και τότε ισχύει, $\forall x \in X$: $\tilde{f}([x]_{\mathscr{R}_f}) = f(x)$. Δείχνουμε ότι η $\tilde{f}$ είναι «1-1». Έστω ότι $\tilde{f}([x]_{\mathscr{R}_f}) = \tilde{f}([y]_{\mathscr{R}_f})$ και επομένως $f(x) = f(y)$. Εξ ορισμού θα έχουμε τότε $x \sim_{\mathscr{R}_f} y$, και από το Λήμμα 1.2.10 έπεται ότι $[x]_{\mathscr{R}_f} = [y]_{\mathscr{R}_f}$. Αυτό δείχνει ότι η $\tilde{f}$ είναι «1-1».

2. Θέτοντας $\overline{f}([x]_{\mathscr{R}_f}) = f(x)$, αποκτούμε μια απεικόνιση $\overline{f} : X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f)$, για την οποία ισχύει ότι $\mathsf{i} \circ \overline{f} = \tilde{f}$. Προφανώς η $\overline{f}$ είναι «επί», διότι αν $y \in \mathsf{Im}(f)$, τότε $y = f(x)$ για κάποιο $x \in X$, και επομένως $\overline{f}([x]_{\mathscr{R}_f}) = f(x) = y$. Επιπλέον η απεικόνιση $\overline{f}$ είναι «1-1» διότι η $\tilde{f}$ είναι «1-1». Άρα η απεικόνιση $\overline{f}$ είναι «1-1» και «επί».

Επειδή η f είναι «επί» αν και μόνο αν η «1-1» απεικόνιση i είναι «επί», από τη σχέση $\mathsf{i} \circ \overline{f} = \tilde{f}$ έπεται ότι η f είναι «επί» αν και μόνο αν η «1-1» απεικόνιση $\tilde{f}$ είναι «1-1» και «επί».

3. Τέλος, έστω $g : X \longrightarrow Z$ μια απεικόνιση για την οποία ισχύει η σχέση (†). Τότε θα έχουμε, $\forall x, y \in X$: $x \sim_{\mathscr{R}_f} y \implies g(x) = g(y)$. Από την Πρόταση 1.2.13 έπεται τότε ότι υπάρχει μοναδική απεικόνιση $\tilde{g} : X/\mathscr{R}_f \longrightarrow Z$, έτσι ώστε: $\tilde{g} \circ \pi_f = g$, από όπου βλέπουμε ότι, $\forall x \in X$: $\tilde{g}([x]_{\mathscr{R}_f}) = g(x)$. Ο τελευταίος ισχυρισμός προκύπτει από το Πόρισμα 1.2.15, διότι η σχέση (†) συνεπάγει την έγκλειση $\mathscr{R}_f \subseteq \mathscr{R}_g$ ως υποσύνολα του $X \times X$. ■

Ορισμός 1.2.25. *Η σχέση ισοδυναμίας $\mathscr{R}_f$ η οποία ορίζεται στο σύνολο X μέσω μιας απεικόνισης $f : X \longrightarrow Y$ καλείται η* **επαγόμενη από την f σχέση ισοδυναμίας** *στο σύνολο X.*

Παράδειγμα 1.2.26. Έστω $f : X \longrightarrow Y$ μια απεικόνιση και $\mathscr{R}_f$ η επαγόμενη σχέση ισοδυναμίας επι του X. Αν η f είναι «1-1», τότε όπως προκύπτει από την Πρόταση 1.2.24, θα έχουμε

$$\forall x \in X : \quad [x]_{\mathscr{R}_f} = \{x\}$$

και τότε η απεικόνιση κανονικής προβολής $\pi_{\mathscr{R}_f} : X \longrightarrow X/\mathscr{R}_f$ είναι «1-1» και «επί». ✓

Παράδειγμα 1.2.27. Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί του συνόλου X. Τότε η απεικόνιση κανονικής προβολής

$$\pi_{\mathscr{R}} : X \longrightarrow X/\mathscr{R}, \qquad \pi_{\mathscr{R}}(x) = [x]_{\mathscr{R}}$$

επάγει στο X την ίδια σχέση ισοδυναμίας: $\mathscr{R} = \mathscr{R}_{\pi_{\mathscr{R}}}$. Πραγματικά, χρησιμοποιώντας το Λήμμα 1.2.10, έχουμε:

$$x \sim_{\mathscr{R}_{\pi_{\mathscr{R}}}} y \iff \pi_{\mathscr{R}}(x) = \pi_{\mathscr{R}}(y) \iff [x]_{\mathscr{R}} = [y]_{\mathscr{R}} \iff x \sim_{\mathscr{R}} y \quad \checkmark$$

Παράδειγμα 1.2.28. Έστω $X = \{1,2,3,4,5\}$ και $U = \{2,4,5,6\}$. Θεωρούμε την απεικόνιση $f: X \longrightarrow Y$ η οποία ορίζεται από τις σχέσεις: $f(1) = f(5) = 2$, $f(2) = 2$, και $f(3) = f(4) = 5$. Αν $\mathscr{R}_f$ είναι η επαγόμενη από την f σχέση ισοδυναμίας επί του X, τότε ως υποσύνολο του $X \times X$ θα έχουμε

$$\mathscr{R}_f = \{(1,1),\ (2,2),\ (3,3),\ (4,4),\ (5,5), (1,5),\ (5,1), (3,4),\ (4,3)\}$$

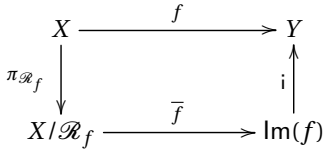
Επιπρόσθετα θα έχουμε $[1]_{\mathscr{R}_f} = \{1,5\}$, $[2]_{\mathscr{R}_f} = \{2\}$, και $[3]_{\mathscr{R}_f} = \{3,4\}$, και $X/\mathscr{R}_f = \{[1]_{\mathscr{R}_f}, [2]_{\mathscr{R}_f}, [3]_{\mathscr{R}_f}\}$. Η «1-1» και «επί» απεικόνιση $\overline{f}: X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f)$ της Πρότασης 1.2.24 είναι η απεικόνιση η οποία ορίζεται από τις σχέσεις: $\overline{f}([1]_{\mathscr{R}_f}) = 2$, $\overline{f}([2]_{\mathscr{R}_f}) = 4$, $\overline{f}([3]_{\mathscr{R}_f}) = 5$. $\checkmark$

Από την Πρόταση 1.2.24 έπεται ότι κάθε απεικόνιση $f: X \longrightarrow Y$ μπορεί να γραφεί ως σύνθεση

$$f = \mathsf{i} \circ \overline{f} \circ \pi_{\mathscr{R}_f}$$

1. μιας απεικόνισης «επί»
$$\pi_{\mathscr{R}_f} : X \longrightarrow X/\mathscr{R}_f, \qquad \pi_{\mathscr{R}_f}(x) = [x]_{\mathscr{R}_f}$$
2. μιας απεικόνισης «1-1» και «επί»
$$\overline{f} : X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f), \qquad \overline{f}([x]_{\mathscr{R}_f}) = f(x)$$
3. μιας απεικόνισης «1-1»
$$\mathsf{i} : \mathsf{Im}(f) \longrightarrow Y, \qquad \mathsf{i}(y) = y$$

Σχηματικά:



Παρατηρούμε ότι, αν η f είναι απεικόνιση «επί», τότε η επαγόμενη απεικόνιση $\overline{f}: X/\mathscr{R}_f \longrightarrow Y$ συμπίπτει με την $\widetilde{f}: X/\mathscr{R}_f \longrightarrow Y$ και είναι «1-1» και «επί». Συμπερασματικά:

1. Κάθε σχέση ισοδυναμίας $\mathscr{R}$ σε ένα σύνολο X ορίζει μια απεικόνιση «επί», την $\pi_{\mathscr{R}}: X \longrightarrow X/\mathscr{R}$, της οποίας η επαγόμενη σχέση ισοδυναμίας $\mathscr{R}_{\pi_{\mathscr{R}}}$ επί του X συμπίπτει με την $\mathscr{R}$: $\mathscr{R}_{\pi_{\mathscr{R}}} = \mathscr{R}$.

2. Κάθε απεικόνιση «επί» $f: X \longrightarrow Y$ ορίζει μια σχέση ισοδυναμίας επί του X, την $\mathscr{R}_f$, η οποία επάγει μια απεικόνιση «επί» $\pi_{\mathscr{R}_f}: X \longrightarrow X/\mathscr{R}_f$ και υπάρχει μια «1-1» και «επί» απεικόνιση $\overline{f}: X/\mathscr{R}_f \longrightarrow Y$. Ταυτίζοντας το σύνολο Y με το σύνολο πηλίκο $X/\mathscr{R}_f$ μέσω της απεικόνισης $\overline{f}$ και χρησιμοποιώντας ότι $f = \overline{f} \circ \pi_{\mathscr{R}}$, βλέπουμε ότι η απεικόνιση $f: X \longrightarrow Y$ ταυτίζεται με την απεικόνιση κανονικής προβολής $\pi_{\mathscr{R}}: X \longrightarrow X/\mathscr{R} = Y$.

Έτσι, ταυτίζοντας σύνολα τα οποία βρίσκονται σε «1-1» και «επί» αντιστοιχία μεταξύ τους, βλέπουμε ότι:
«για κάθε μη κενό σύνολο X, υπάρχει μια «1-1» και «επί» αντιστοιχία μεταξύ σχέσεων ισοδυναμίας $\mathscr{R}$ επί του X και απεικονίσεων «επί» οι οποίες έχουν πεδίο ορισμού το σύνολο X».

Κλείνουμε την παρούσα ενότητα με την ακόλουθη Πρόταση η οποία θα μας είναι χρήσιμη στα επόμενα κεφάλαια.

Πρόταση 1.2.29. *Έστω $\mathcal{S}$ και $\mathcal{R}$ δύο σχέσεις ισοδυναμίας επί ενός μη-κενού συνόλου X έτσι ώστε, ως υποσύνολα του $X \times X$, να ισχύει ότι: $\mathcal{S} \subseteq \mathcal{R}$. Τότε, ορίζοντας μια σχέση $\mathcal{R}/\mathcal{S}$ επί του $X/\mathcal{S}$ ως εξής*

$$\forall [x]_{\mathcal{S}}, [y]_{\mathcal{S}} \in X/\mathcal{S}: \quad [x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}} \iff x \sim_{\mathcal{R}} y,$$

αποκτούμε μια σχέση ισοδυναμίας επί του συνόλου πηλίκου $X/\mathcal{S}$. Δηλαδή η σχέση $\mathcal{R}/\mathcal{S}$ ως υποσύνολο του καρτεσιανού γινομένου $X/\mathcal{S} \times X/\mathcal{S}$ ορίζεται ώς εξής:

$$\mathcal{R}/\mathcal{S} = \left\{([x]_{\mathcal{S}}, [y]_{\mathcal{S}}) \in X/\mathcal{S} \times X/\mathcal{S} \mid (x, y) \in \mathcal{R}\right\}$$

Επιπλέον η απεικόνιση

$$F: X/\mathcal{S}\big/\mathcal{R}/\mathcal{S} \longrightarrow X/\mathcal{R}, \quad F\left([[x]_{\mathcal{S}}]_{\mathcal{R}/\mathcal{S}}\right) = [x]_{\mathcal{R}}$$

είναι «1-1» και «επί».

Απόδειξη. **1.** Παρατηρούμε ότι, αν $[x]_{\mathcal{S}} = [x']_{\mathcal{S}}$ και $[y]_{\mathcal{S}} = [y']_{\mathcal{S}}$, τότε $x \sim_{\mathcal{S}} x'$ και $y \sim_{\mathcal{S}} y'$, και άρα, επειδή $\mathcal{S} \subseteq \mathcal{R}$, θα έχουμε $x \sim_{\mathcal{R}} x'$ και $y \sim_{\mathcal{R}} y'$. Επομένως, αν επιπλέον έχουμε $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}}$, δηλαδή $x \sim_{\mathcal{R}} y$, τότε, επειδή η $\mathcal{R}$ είναι σχέση ισοδυναμίας επί του X, θα έχουμε $x \sim_{\mathcal{R}} y'$ και $x' \sim_{\mathcal{R}} x$ και άρα $x' \sim_{\mathcal{R}} y'$. Επομένως $[x']_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y']_{\mathcal{S}}$.

Δείχνουμε ότι η σχέση $\mathcal{R}/\mathcal{S}$ είναι μια σχέση ισοδυναμίας επί του συνόλου πηλίκου $X/\mathcal{S}$.

(α') Για κάθε στοιχείο $[x]_{\mathcal{S}} \in X/\mathcal{S}$, έχουμε: $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [x]_{\mathcal{S}}$ διότι $x \sim_{\mathcal{R}} x$. Άρα η σχέση $\mathcal{R}/\mathcal{S}$ είναι ανακλαστική.

(β') Έστω $[x]_{\mathcal{S}}, [y]_{\mathcal{S}} \in X/\mathcal{S}$ έτσι ώστε $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}}$. Τότε εξ ορισμού θα έχουμε $x \sim_{\mathcal{R}} y$ και επομένως $y \sim_{\mathcal{R}} x$, διότι η $\mathcal{R}$ είναι συμμετρική. Έτσι θα έχουμε $[y]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [x]_{\mathcal{S}}$ και επομένως η σχέση $\mathcal{R}/\mathcal{S}$ είναι συμμετρική.

(γ') Έστω $[x]_{\mathcal{S}}, [y]_{\mathcal{S}}, [z]_{\mathcal{S}} \in X/\mathcal{S}$ έτσι ώστε $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}}$ και $[y]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [z]_{\mathcal{S}}$. Τότε εξ ορισμού θα έχουμε $x \sim_{\mathcal{R}} y$ και $y \sim_{\mathcal{R}} z$, και επομένως θα έχουμε και $x \sim_{\mathcal{R}} z$ διότι η $\mathcal{R}$ είναι μεταβατική. Έτσι προκύπτει ότι $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [z]_{\mathcal{S}}$ και επομένως η σχέση $\mathcal{R}/\mathcal{S}$ είναι μεταβατική.

2. Δείχνουμε το ζητούμενο με βάση τα ακόλουθα βήματα: (α') η αντιστοιχία

$$f: X/\mathcal{S} \longrightarrow X/\mathcal{R}, \quad f([x]_{\mathcal{S}}) = [x]_{\mathcal{R}}$$

είναι μια απεικόνιση «επί», και (β') η σχέση ισοδυναμίας $\mathcal{R}_f$ την οποία ορίζει η f επί του συνόλου $X/\mathcal{S}$ συμπίπτει με την σχέση ισοδυναμίας $\mathcal{R}/\mathcal{S}$.

(α') *Η f είναι μια απεικόνιση «επί»*

$$f: X/\mathcal{S} \longrightarrow X/\mathcal{R}, \quad f([x]_{\mathcal{S}}) = [x]_{\mathcal{R}}$$

Πράγματι, έστω $[x]_{\mathcal{S}}, [y]_{\mathcal{S}} \in X/\mathcal{S}$ έτσι ώστε: $[x]_{\mathcal{S}} = [y]_{\mathcal{S}} \in X/\mathcal{S}$. Τότε, ως γνωστόν, θα έχουμε $x \sim_{\mathcal{S}} y$, δηλαδή $(x, y) \in \mathcal{S}$. Επειδή $\mathcal{S} \subseteq \mathcal{R}$, θα έχουμε $(x, y) \in \mathcal{R}$ και επομένως $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$. Δηλαδή θα έχουμε $f([x]_{\mathcal{S}}) = f([y]_{\mathcal{S}})$. Επομένως η f είναι καλά ορισμένη.
Η f είναι προφανώς «επί», διότι, αν $[x]_{\mathcal{R}} \in X/\mathcal{R}$, τότε $[x]_{\mathcal{S}} \in X/\mathcal{S}$ και $f([x]_{\mathcal{S}}) = [x]_{\mathcal{R}}$.

(β') *Η σχέση ισοδυναμίας $\mathcal{R}_f$ την οποία ορίζει η f επί του συνόλου $X/\mathcal{S}$ συμπίπτει με την σχέση ισοδυναμίας $\mathcal{R}/\mathcal{S}$.*
Πράγματι, έστω $[x]_{\mathcal{S}}, [y]_{\mathcal{S}} \in X/\mathcal{S}$ έτσι ώστε: $f([x]_{\mathcal{S}}) = f([y]_{\mathcal{S}})$ και άρα $[x]_{\mathcal{R}} = [y]_{\mathcal{R}}$. ή ισοδύναμα $x \sim_{\mathcal{R}} y$. Έτσι από τον ορισμό θα έχουμε ισοδύναμα $[x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}}$. Συνοψίζουμε:

$$[x]_{\mathcal{S}} \sim_{\mathcal{R}_f} [y]_{\mathcal{S}} \iff f([x]_{\mathcal{S}}) = f)([y]_{\mathcal{S}}) \iff [x]_{\mathcal{S}} \sim_{\mathcal{R}/\mathcal{S}} [y]_{\mathcal{S}}$$

(γ') Από τα βήματα (α') και (β') και την Πρόταση 1.2.24, βλέπουμε ότι η απεικόνιση

$$F: X/\mathcal{S}\big/\mathcal{R}/\mathcal{S} \longrightarrow X/\mathcal{R}, \quad F\left([[x]_{\mathcal{S}}]_{\mathcal{R}/\mathcal{S}}\right) = f([x]_{\mathcal{S}}) = [x]_{\mathcal{R}}$$

είναι «1-1» και «επί». ■

Η σχέση $\mathcal{R}/\mathcal{S}$ της Πρότασης 1.2.29 καλείται *σχέση ισοδυναμίας πηλίκο* της $\mathcal{R}$ ως προς την $\mathcal{S}$, επί του συνόλου πηλίκου $X/\mathcal{S}$.

1.2.5 Σχέσεις Ισοδυναμίας Παραγόμενες από Υποσύνολα

Αν X είναι ένα σύνολο και $\mathscr{R}$ είναι μια σχέση επί του X, δηλαδή ένα υποσύνολο του $X \times X$, τότε ένα φυσικό ερώτημα είναι αν υπάρχει σχέση ισοδυναμίας $\langle \mathscr{R} \rangle$ επί του X η οποία περιέχει την $\mathscr{R}$ και είναι η μικρότερη σχέση ισοδυναμίας επί του X η οποία περιέχει τη σχέση $\mathscr{R}$.

Πρόταση 1.2.30. *Έστω X ένα σύνολο και $\{\mathscr{R}_i\}_{i\in I}$ μια οικογένεια σχέσεων ισοδυναμίας επί του X. Τότε η τομή*

$$\bigcap_{i\in I} \mathscr{R}_i \subseteq X \times X$$

είναι μια σχέση ισοδυναμίας επί του συνόλου X.

Απόδειξη. Επειδή, για κάθε $i \in I$, η σχέση $\mathscr{R}_i$ είναι σχέση ισοδυναμίας επί του X, έπεται ότι $(x,x) \in \mathscr{R}_i$, $\forall x \in X$. Τότε προφανώς $(x,x) \in \bigcap_{i\in I} \mathscr{R}_i$, και άρα η σχέση $\bigcap_{i\in I}$ είναι ανακλαστική. Αν $x, y \in X$ και ισχύει ότι $(x,y) \in \bigcap_{i\in I} \mathscr{R}_i$, τότε $(x,y) \in \mathscr{R}_i$ για κάθε $i \in I$. Επειδή η σχέση $\mathscr{R}_i$ είναι σχέση ισοδυναμίας, θα έχουμε $(y,x) \in \mathscr{R}_i$ για κάθε $i \in I$ και τότε $(y,x) \in \bigcap_{i\in I} \mathscr{R}_i$, δηλαδή η σχέση $\bigcap_{i\in I} \mathscr{R}_i$ είναι συμμετρική. Τέλος, αν $x, y, z \in X$ και ισχύει ότι $(x,y) \in \bigcap_{i\in I} \mathscr{R}_i$ και $(y,z) \in \bigcap_{i\in I} \mathscr{R}_i$, τότε για κάθε δείκτη $i \in I$ θα έχουμε $(x,y), (y,z) \in \mathscr{R}_i$. Επειδή, για κάθε $i \in I$, η σχέση $\mathscr{R}_i$ είναι σχέση ισοδυναμίας, έπεται ότι $(x,z) \in \mathscr{R}_i$ και άρα $(x,z) \in \bigcap_{i\in I} \mathscr{R}_i$, δηλαδή η σχέση $\bigcap_{i\in I} \mathscr{R}_i$ είναι μεταβατική. ■

Η ακόλουθη συνέπεια της Πρότασης 1.2.30 δείχνει ότι κάθε σχέση $\mathscr{R}$, η οποία δεν είναι απαραίτητα σχέση ισοδυναμίας, επί ενός συνόλου X περιέχεται σε μια ελάχιστη σχέση ισοδυναμίας $\langle \mathscr{R} \rangle$ η οποία ορίζεται επί του X.

Πόρισμα 1.2.31. *Έστω X ένα σύνολο και $\mathscr{R}$ μια σχέση επί του X. Τότε η σχέση*

$$\langle \mathscr{R} \rangle := \bigcap \{ \mathscr{T} \subseteq X \times X \mid \mathscr{T} : \textit{σχέση ισοδυναμίας επί του } X \textit{ και } \mathscr{R} \subseteq \mathscr{T} \}$$

είναι η μικρότερη σχέση ισοδυναμίας επί του X η οποία περιέχει τη σχέση $\mathscr{R}$.

Απόδειξη. Έστω S η οικογένεια υποσυνόλων $\{ \mathscr{T} \subseteq X \times X \mid \mathscr{T} : \textit{σχέση ισοδυναμίας επί του } X \textit{ και } \mathscr{R} \subseteq \mathscr{T} \}$ του $X \times X$. Η οικογένεια S δεν είναι κενή διότι περιέχει τη μεγαλύτερη σχέση ισοδυναμίας M_X επί του X η οποία ως υποσύνολο του $X \times X$ συμπίπτει με το $X \times X$, βλέπε το Παράδειγμα 1.2.2. Από την Πρόταση 1.2.30 έπεται ότι η τομή $\langle \mathscr{R} \rangle = \bigcap_{\mathscr{T}\in\mathsf{S}} \mathscr{T}$ είναι μια σχέση ισοδυναμίας επί του X, και προφανώς $\mathscr{R} \subseteq \langle \mathscr{R} \rangle$ διότι $\mathscr{R} \subseteq \mathscr{T}$, $\forall \mathscr{T} \in \mathsf{S}$. Αν $\mathscr{U}$ είναι μια σχέση ισοδυναμίας επί του X έτσι ώστε $\mathscr{R} \subseteq \mathscr{U}$, τότε $\mathscr{U} \in \mathsf{S}$ και άρα $\langle \mathscr{R} \rangle = \bigcap_{\mathscr{T}\in\mathsf{S}} \mathscr{T} \subseteq \mathscr{U}$. Επομένως η $\langle \mathscr{R} \rangle$ είναι η μικρότερη σχέση ισοδυναμίας επί του X η οποία περιέχει τη σχέση $\mathscr{R}$. ■

Έστω X ένα σύνολο και $\mathscr{R}$ μια σχέση επί του X. Η σχέση ισοδυναμίας $\langle \mathscr{R} \rangle$ η οποία κατασκευάστηκε στο Πόρισμα 1.2.31 καλείται η **σχέση ισοδυναμίας επί του X η οποία παράγεται από τη σχέση $\mathscr{R}$**.

Η τελευταία Πρόταση της παρούσας ενότητας δίνει μια περιγραφή των στοιχείων της σχέσης ισοδυναμίας η οποία παράγεται από μια σχέση επί ενός συνόλου.

Πρόταση 1.2.32. *Έστω X ένα σύνολο και $\mathscr{R}$ μια σχέση επί του X. Η σχέση ισοδυναμίας $\langle \mathscr{R} \rangle$ επί του X η οποία παράγεται από τη σχέση $\mathscr{R}$ έχει την ακόλουθη περιγραφή:*

$$\langle \mathscr{R} \rangle = \big\{ (a,b) \in X \times X \mid a = b \quad \acute{\eta} \quad \exists n \geq 0 \quad \textit{και} \quad x_0, \cdots, x_n \in X : \quad x_1 = a, \quad x_n = b, \quad \textit{και:}$$

$$(x_k, x_{k+1}) \in \mathscr{R} \quad \acute{\eta} \quad (x_{k+1}, x_k) \in \mathscr{R}, \quad 1 \leq k \leq n \big\}$$

Απόδειξη. Συμβολίζοντας με $\mathscr{T}$ το υποσύνολο του $X \times X$ το οποίο περιγράφεται στο δεύτερο μέλος της ζητούμενης ισότητας, θα δείξουμε ότι: (α) η σχέση $\mathscr{T}$ είναι μια σχέση ισοδυναμίας επί του X και ισχύει $\mathscr{R} \subseteq \mathscr{T}$, και ($\beta$) αν $\mathscr{S}$ είναι μια σχέση ισοδυναμίας επί του X έτσι ώστε $\mathscr{R} \subseteq \mathscr{S}$, τότε $\mathscr{T} \subseteq \mathscr{S}$.

(α) Δείχνουμε πρώτα ότι η σχέση $\mathscr{T}$ είναι σχέση ισοδυναμίας.

(α') *Η σχέση $\mathscr{T}$ είναι ανακλαστική:* Πράγματι από τον ορισμό της $\mathscr{T}$ έπεται ότι για κάθε $a \in X$, έχουμε $(a,a) \in \mathscr{T}$.

(β') *Η σχέση $\mathscr{T}$ είναι συμμετρική:* Πράγματι, έστω ότι $(a,b) \in \mathscr{T}$. Αν $a = b$, τότε προφανώς θα έχουμε $(b,a) \in \mathscr{T}$. Υποθέτουμε ότι $a \neq b$, και τότε υπάρχουν στοιχεία $x_1, \cdots, x_{n+1} \in X$, έτσι ώστε $x_1 = a$, $x_{n+1} = b$, και είτε $(x_k, x_{k+1}) \in \mathscr{R}$ ή $(x_{k+1}, x_k) \in \mathscr{R}$, όπου $1 \leq k \leq n$. Θέτοντας $y_1 := b = x_{n+1}$, $y_2 := x_n$, $\cdots$, $y_{n+1} := x_1 = a$, έπεται ότι $(y_k, y_{k+1}) \in \mathscr{R}$ ή $(y_{k+1}, y_k) \in \mathscr{R}$, όπου $1 \leq k \leq n$, και άρα θα έχουμε $(b,a) \in \mathscr{T}$. Επομένως η σχέση $\mathscr{T}$ είναι συμμετρική.

(γ') *Η σχέση $\mathscr{T}$ είναι μεταβατική:* Υποθέτουμε ότι $(a,b) \in \mathscr{T}$ και $(b,c) \in \mathscr{T}$. Αν $a = b$ ή $b = c$, τότε προφανώς $(a,c) \in \mathscr{T}$. Αν $a \neq b$ και $b \neq c$, από τον ορισμό της $\mathscr{T}$ έπεται ότι

i. υπάρχουν στοιχεία $x_1, \cdots, x_{n+1} \in X$, έτσι ώστε $x_1 = a$, $x_{n+1} = b$, και είτε $(x_k, x_{k+1}) \in \mathscr{R}$ ή $(x_{k+1}, x_k) \in \mathscr{R}$, όπου $1 \leq k \leq n$,

ii. υπάρχουν στοιχεία $y_1, \cdots, y_{m+1} \in X$, έτσι ώστε $y_1 = b$, $y_{m+1} = c$, και είτε $(y_l, y_{l+1}) \in \mathscr{R}$ ή $(y_{l+1}, y_l) \in \mathscr{R}$, όπου $1 \leq l \leq m$.

Θεωρούμε τα $n+m+1$ στοιχεία του X:

$$a = x_1,\ x_2,\ \cdots,\ x_n,\ x_{n+1} = b = y_1,\ y_2,\ \cdots,\ y_n,\ y_{n+1} = c$$

για τα οποία, με χρήση των σχέσεων (α') και (β') θα έχουμε:

$$(x_1, x_2) \in \mathscr{R} \text{ ή } (x_2, x_1) \in \mathscr{R}, \quad \cdots, \quad (x_n, x_{n+1}) \in \mathscr{R} \text{ ή } (x_{n+1}, x_n) \in \mathscr{R}$$

$$(x_{n+1}, y_2) \in \mathscr{R} \text{ ή } (y_2, x_{n+1}) \in \mathscr{R}, \ (y_2, y_3) \in \mathscr{R} \text{ ή } (y_3, y_2) \in \mathscr{R}, \ \cdots, \ (y_m, y_{m+1}) \in \mathscr{R} \text{ ή } (y_{m+1}, y_m) \in \mathscr{R}$$

Επειδή $a = x_1$, $b = x_{n+1} = y_1$, και $c = y_{m+1}$, οι παραπάνω σχέσεις δείχνουν ότι $(a,c) \in \mathscr{T}$, και επομένως η σχέση $\mathscr{T}$ είναι μεταβατική.

Συνοψίζοντας, δείξαμε ότι η σχέση $\mathscr{T}$ είναι μια σχέση ισοδυναμίας επί του X.

Τέλος, ισχύει $\mathscr{R} \subseteq \mathscr{T}$, διότι, αν $(a,b) \in \mathscr{R}$, τότε από τον ορισμό της $\mathscr{T}$ έπεται ότι $(a,b) \in \mathscr{T}$.

(β) Έστω $\mathscr{S}$ μια σχέση ισοδυναμίας επί του X, για την οποία ισχύει ότι $\mathscr{R} \subseteq \mathscr{S}$. Θα δείξουμε ότι $\mathscr{T} \subseteq \mathscr{S}$. Έστω $(a,b) \in \mathscr{T}$. Αν $a = b$, τότε $(a,b) \in \mathscr{S}$ διότι η $\mathscr{S}$ είναι ανακλαστική ως σχέση ισοδυναμίας επί του X. Αν $a \neq b$, τότε υπάρχουν στοιχεία $x_1, \cdots, x_{n+1} \in X$, έτσι ώστε $x_1 = a$, $x_{n+1} = b$, και είτε $(x_k, x_{k+1}) \in \mathscr{R}$ είτε $(x_{k+1}, x_k) \in \mathscr{R}$, όπου $1 \leq k \leq n$. Επειδή $\mathscr{R} \subseteq \mathscr{S}$, θα έχουμε είτε $(x_k, x_{k+1}) \in \mathscr{S}$ είτε $(x_{k+1}, x_k) \in \mathscr{S}$, όπου $1 \leq k \leq n$. Επειδή η $\mathscr{S}$ είναι συμμετρική και μεταβατική ως σχέση ισοδυναμίας επί του X, οι παραπάνω σχέσεις δίνουν ότι $(a,b) \in \mathscr{S}$. Επομένως $\mathscr{T} \subseteq \mathscr{T}$. ■

Παράδειγμα 1.2.33. Έστω $X = \{1,2,3,4,5,6,7\}$ και έστω η ακόλουθη σχέση επί του X:

$$\mathscr{R} = \{(2,2),\ (1,3),\ (5,7),\ (3,4),\ (6,4)\}$$

Επειδή η σχέση $\langle\mathscr{R}\rangle$ περιέχει την $\mathscr{R}$, έπεται ότι τα στοιχεία $(2,2), (1,3), (5,7), (3,4), (6,4)$ ανήκουν στην $\langle\mathscr{R}\rangle$. Επειδή η $\langle\mathscr{R}\rangle$ είναι ανακλαστική, έπεται ότι η σχέση $\langle\mathscr{R}\rangle$ περιέχει τα στοιχεία $(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7)$. Προφανώς η σχέση $\mathscr{R}_1 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (1,3), (5,7), (3,4), (6,4)\}$ είναι η μικρότερη ανακλαστική σχέση επί του X η οποία περιέχει την $\mathscr{R}$. Όμως η σχέση $\mathscr{R}_1$ δεν είναι συμμετρική διότι, αν και περιέχει το στοιχείο $(1,3)$, δεν περιέχει το στοιχείο $(3,1)$. Επειδή η $\mathscr{R}$, άρα και η $\langle\mathscr{R}\rangle$, περιέχει τα στοιχεία $(1,3), (5,7), (3,4), (6,4)$, και επειδή η $\langle\mathscr{R}\rangle$ είναι συμμετρική, έπεται ότι η $\langle\mathscr{R}\rangle$ περιέχει και τα στοιχεία $(3,1), (7,5), (4,3), (4,6)$. Επομένως η $\langle\mathscr{R}\rangle$ περιέχει τα στοιχεία του συνόλου $\mathscr{R}_2 = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (1,3), (5,7), (3,4), (6,4), (3,1), (4,3), (7,5), (4,6)\}$. Το παραπάνω υποσύνολο περιγράφει την μικρότερη ανακλαστική και συμμετρική σχέση επί του X η οποία περιέχει την $\mathscr{R}$. Όμως η σχέση $\mathscr{R}_2$ δεν είναι μεταβατική διότι, για παράδειγμα, αν και περιέχει τα στοιχεία $(1,3)$ και $(3,4)$, δεν περιέχει το στοιχείο $(1,4)$. Έτσι, επειδή η $\langle\mathscr{R}\rangle$ είναι μεταβατική και περιέχει τα στοιχεία του παραπάνω συνόλου $\mathscr{R}_2$, θα περιέχει και τα στοιχεία $(1,4), (4,1), (3,6), (6,3), (1,6), (6,1)$. Επομένως θα έχουμε:

$$\langle\mathscr{R}\rangle = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7), (1,3), (5,7), (3,4), (6,4), (3,1), (4,3), (7,5), (1,4), (4,6),$$
$$(1,4), (4,1), (1,6), (6,1), (3,6), (6,3)\} \quad \surd$$

1.3 Πράξεις

Στην παρούσα ενότητα θα μελετήσουμε την έννοια της (διμελούς) πράξης επί ενός συνόλου, καθώς και τις βασικές ιδιότητες πράξεων οι οποίες ικανοποιούν συγκεκριμένα αξιώματα τα οποία γενικεύουν γνωστές ιδιότητες της πρόσθεσης και πολλαπλασιασμού σε οικεία σύνολα αριθμών.

1.3.1 Η έννοια της πράξης: βασικές ιδιότητες και παραδείγματα

(Διμελείς) Πράξεις επί συνόλων είναι ειδικού τύπου απεικονίσεις οι οποίες αντιστοιχούν σε κάθε ζεύγος στοιχείων ενός συνόλου ένα νέο στοιχείο του:

Ορισμός 1.3.1. *Μια (διμελής)* **πράξη** *επί ενός συνόλου X είναι μια απεικόνιση*

$$\mu : X \times X \longrightarrow X, \quad (x, y) \longmapsto \mu(x, y)$$

Παρατήρηση 1.3.2. Γενικότερα, αν $n \geq 1$, μια *n-μελής πράξη* είναι μια απεικόνιση

$$\mu : X^n = \underbrace{X \times X \times \cdots \times X}_{n-\text{παράγοντες}} \longrightarrow X, \quad (x_1, x_2, \cdots, x_n) \longmapsto \mu(x_1, x_2, \cdots, x_n)$$

Έτσι μια 1-μελής πράξη επί του X είναι μια απεικόνιση $X \longrightarrow X$. Για παράδειγμα, οι απεικονίσεις $\mu\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, $\mu(z) = -z$ και $\nu\colon \mathbb{R}^* \longrightarrow \mathbb{R}^*$, $\mu(x) = x^{-1}$ είναι 1-μελείς πράξεις επί των $\mathbb{Z}$ και $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ αντίστοιχα, και η απεικόνιση $\mu\colon \mathbb{R} \times \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$, $\mu(x, y, z) = xy + xz$ είναι μια 3-μελής πράξη επί του $\mathbb{R}$. Επίσης, αν $n = 0$, τότε κατά σύμβαση ορίζεται το σύνολο X^0 να είναι ένα μονοσύνολο, έστω $\{\omega\}$, και μια 0-μελής πράξη μ είναι απλώς μια σταθερή απεικόνιση $\mu\colon X^0 = \{\omega\} \longrightarrow X$ η οποία ορίζει ένα συγκεκριμμένο στοιχείο e του X: $\mu(\omega) = e$.

Μια *Αλγεβρική Δομή* επί του X είναι ένα ζεύγος (X, S), όπου X είναι ένα σύνολο και $S = \{\mu, \pi, \nu, \cdots\}$ είναι μια (συνήθως πεπερασμένη) συλλογή n-μελών πράξεων (για διάφορες τιμές του $n \in \mathbb{N}_0$) επί του X, οι οποίες ικανοποιούν έναν πεπερασμένο αριθμό αξιωμάτων.[4] Θα ασχοληθούμε σχεδόν αποκλειστικά με αλγεβρικές δομές του εξής τύπου

$$(X, \mu), \quad \text{όπου } \mu\colon X \times X \longrightarrow X \text{ είναι μια διμελής πράξη επί του } X$$

$$(X, \mu, \nu), \quad \text{όπου } \mu, \nu\colon X \times X \longrightarrow X \text{ είναι δύο διμελείς πράξεις επί του } X$$

όπου οι εμπλεκόμενες πράξεις ικανοποιούν συγκεκριμένα αξιώματα τα οποία αφορούν ιδιότητες οι οποίες γενικεύουν ιδιότητες γνωστών μας πράξεων, όπως για παράδειγμα η πρόσθεση και ο πολλαπλασιασμός αριθμών (φυσικών, ακεραίων, ρητών, πραγματικών, μιγαδικών αριθμών). Έτσι το ζεύγος $(\mathbb{Z}, +)$ και η τριάδα $(\mathbb{Z}, +, \cdot)$, όπου «+» και «·» συμβολίζουν τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού ακεραίων, αποτελούν παραδείγματα αλγεβρικών δομών.

Από την άλλη πλευρά μια *(διμελής) εξωτερική πράξη* ή *(αριστερή) δράση* ενός συνόλου S επί ενός συνόλου X, ορίζεται να είναι μια απεικόνιση $\pi\colon S \times X \longrightarrow X$, $(s, x) \longmapsto \pi(s, x)$, η οποία συνήθως ικανοποιεί συγκεκριμένες ιδιότητες. Σε διαφορετικό πλαίσιο, ενδιαφέρον παρουσιάζουν δομές του τύπου (X, S, π), όπου $\pi\colon S \times X \longrightarrow X$ είναι μια εξωτερική πράξη επί του X ή του τύπου $(X, \mu; S, \pi)$, όπου $\mu\colon X \times X \longrightarrow X$ είναι μια εσωτερική πράξη επί του X και $\pi\colon S \times X \longrightarrow X$ είναι μια εξωτερική πράξη επί του X. Δομές του τελευταίου τύπου συναντώνται στην Γραμμική Άλγεβρα (διανυσματικοί χώροι) και θα μας απασχολήσουν μόνο περιστασιακά ως πηγή παραδειγμάτων. ▲

Συμβολισμός: Παραδοσιακά και χάριν απλότητας μια πράξη μ επί ενός συνόλου X παριστάται με ένα εκ των συμβόλων:

$$\mu = *, \quad \circ, \quad \bullet, \quad \#, \quad \star, \quad +, \quad -, \quad \cdot, \quad \ldots$$

[4] Η μελέτη ιδιοτήτων αλγεβρικών δομών ειδικού τύπου είναι βασικό αντικείμενο της *Αφηρημένης Άλγεβρας*, και η γενική θεωρία αλγεβρικών δομών διάφορων τύπων αποτελεί αντικείμενο της *Καθολικής Άλγεβρας*.

Αντίστοιχα, το αποτέλεσμα $\mu(x,y)$ της πράξης μ στο ζεύγος στοιχείων (x,y) του X, συμβολίζεται ως εξής:

$$\mu(x,y) \;=\; x*y, \quad x\circ y, \quad x\bullet y, \quad x\#y, \quad x\star y, \quad x+y, \quad x-y, \quad x\cdot y, \quad xy, \quad \ldots$$

Ακολουθώντας την παραπάνω παράδοση, από τώρα και στο εξής θα συμβολίζουμε μια πράξη μ επί του X με το σύμβολο «$\star$», και επομένως το αποτέλεσμα $\mu(x,y)$ της πράξης μ επί του ζεύγους στοιχείων $(x,y)\in X\times X$, θα συμβολίζεται με $x\star y$. Αργότερα θα απλοποιήσουμε περαιτέρω τον συμβολισμό μας.

Ορισμός 1.3.3. *Έστω «$\star$» μια πράξη επί ενός συνόλου X.*

1. *Η πράξη «$\star$» καλείται* **προσεταιριστική** *αν ισχύει:*

$$\forall x,y,z\in X: \qquad x\star(y\star z)=(x\star y)\star z$$

2. *Η πράξη «$\star$» καλείται* **μεταθετική** *αν ισχύει:*

$$\forall x,y\in X: \qquad x\star y=y\star x$$

Για την οικεία πράξη πρόσθεσης «$+$» ή πολλαπλασιασμού «$\cdot$» επί του συνόλου A, όπου A είναι ένα από τα γνωστά μας σύνολα αριθμών $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}$, $\mathbb{C}$, γνωρίζουμε ότι υπάρχουν διακεκριμένα στοιχεία, το 0 και το 1, έτσι ώστε για στοιχείο $x\in A$: $x+0=x=0+x$ και αντίστοιχα: $x\cdot 1=x=1\cdot x$. Δηλαδή τα στοιχεία 0 και 1, συμπεριφέρονται «ουδέτερα» ή «ταυτοτικά» ως προς τις πράξεις πρόσθεσης και πολλαπλασιασμού αντίστοιχα.

Γενικεύοντας, ας υποθέσουμε ότι για την πράξη «$\star$» επί του συνόλου X υπάρχει ένα στοιχείο $e\in X$ έτσι ώστε: $x\star e=x=e\star x$, $\forall x\in X$. Ισχυρισμος: Το στοιχείο e είναι το μοναδικό στοιχείο του X το οποίο ικανοποιεί αυτή την ιδιότητα. Πράγματι, έστω $e,e'\in X$ στοιχεία του X έτσι ώστε $\forall x\in X$:

$$x\star e=x=e\star x \tag{1.1α′}$$

$$x\star e'=x=e'\star x \tag{1.1β′}$$

Τότε, θέτοντας $x=e'$ στην 1.1α′ και $x=e$ στην 1.1β′, θα έχουμε:

$$e'\star e=e'=e\star e' \quad \text{και} \quad e\star e'=e=e'\star e \quad \text{και άρα:} \quad e=e' \tag{1.2}$$

Ορισμός 1.3.4. *Έστω «$\star$» μια πράξη επί ενός συνόλου X. Ένα στοιχείο $e\in X$ καλείται* **ουδέτερο** *ή* **ταυτοτικό** *στοιχείο του X ως προς την πράξη «$\star$», αν ισχύει:*

$$\forall x\in X: \qquad x\star e=x=e\star x$$

Το στοιχείο e, αν υπάρχει, λόγω της (1.2) είναι μοναδικό.

Υποθέτουμε ότι «$\star$» είναι μια προσεταιριστική πράξη επί του X, για την οποία υπάρχει ουδέτερο στοιχείο $e\in X$. Έστω επίσης $x\in X$ ένα στοιχείο για το οποίο υπάρχει στοιχείο $x'\in X$, έτσι ώστε: $x\star x'=e=x'\star x$. Ισχυρισμος: Το στοιχείο x' είναι το μοναδικό στοιχείο του X το οποίο ικανοποιεί αυτή την ιδιότητα. Πράγματι, έστω $x',x''\in X$ στοιχεία του X έτσι ώστε, $\forall x\in X$:

$$x\star x'=e=x'\star x \tag{1.3α′}$$

$$x\star x''=e=x''\star x \tag{1.3β′}$$

Τότε, χρησιμοποιώντας ότι η πράξη «$\star$» είναι προσεταιριστική, ότι το e είναι το ουδέτερο στοιχείο για την πράξη «$\star$» επί του X, και τις σχέσεις 1.3α′ και 1.3β′, θα έχουμε:

$$x\star x'=e \implies x''\star(x\star x')=x''\star e \implies (x''\star x)\star x'=x'' \implies e\star x'=x'' \implies x'=x'' \tag{1.4}$$

Ορισμός 1.3.5. *Έστω «⋆» μια προσεταιριστική πράξη επί ενός συνόλου X, και υποθέτουμε ότι υπάρχει ουδέτερο στοιχείο $e \in X$ ως προς την πράξη «⋆». Ένα στοιχείο $x \in X$ καλείται* **αντιστρέψιμο ως προς την πράξη** *«⋆», αν υπάρχει στοιχείο $x' \in X$ έτσι ώστε:*

$$x \star x' = e = x' \star x$$

Δεδομένου του στοιχείου $x \in X$, το στοιχείο x', αν υπάρχει, καλείται **αντίστροφο** *(ή* **αντίθετο***) του x, και είναι λόγω της (1.4) μοναδικό. Το* **σύνολο όλων των αντιστρέψιμων** *ή* **αντίθετων στοιχείων** *για την πράξη «⋆» επί του X συμβολίζεται με:*

$$\mathsf{U}(X, \star) = \{x \in X \mid \exists x' \in X : \ x \star x' = e = x' \star x\}$$

Παρατήρηση 1.3.6. Παρατηρούμε ότι, αν η πράξη «⋆» είναι προσεταιριστική και υπάρχει ουδέτερο στοιχείο $e \in X$ ως προς την πράξη, τότε προφανώς $e \in \mathsf{U}(X, \star)$ και επομένως: $\mathsf{U}(X, \star) \neq \emptyset$.

Όταν δεν υπάρχει κίνδυνος σύγχυσης, συνήθως θα γράφουμε απλώς $\mathsf{U}(X)$ για το σύνολο $\mathsf{U}(X, \star)$ των αντιστρέψιμων στοιχείων του X ως προς την πράξη «⋆». ▲

Πρόταση 1.3.7. *Έστω «⋆» μια προσεταιριστική πράξη επί ενός συνόλου X, και υποθέτουμε ότι υπάρχει ουδέτερο στοιχείο $e \in X$ ως προς την πράξη «⋆».*

1. *Αν x είναι ένα αντιστρέψιμο στοιχείο του x με αντίστροφο το στοιχείο x', τότε το στοιχείο x' είναι αντιστρέψιμο με αντίστροφο το στοιχείο x:*

$$x \in \mathsf{U}(X, \star) \implies x' \in \mathsf{U}(X, \star) \quad \textit{και} \quad (x')' := x'' = x$$

2. *Αν x, y είναι δύο αντιστρέψιμα στοιχεία του X με αντίστροφα στοιχεία x' και y' αντίστοιχα, τότε το στοιχείο $x \star y$ είναι αντιστρέψιμο και το αντίστροφό του είναι το στοιχείο $y' \star x'$:*

$$x, y \in \mathsf{U}(X, \star) \implies x \star y \in \mathsf{U}(X, \star) \quad \textit{και} \quad (x \star y)' = y' \star x'$$

Απόδειξη. 1. Επειδή:

$$x \star x' = e = x' \star x$$

από τον Ορισμό 1.3.5 έπεται ότι το στοιχείο x' είναι αντιστρέψιμο με αντίστροφο το στοιχείο x: $x'' = x$.

2. Από τον Ορισμό 1.3.5 έπεται ότι $x \star x' = e = x' \star x$ και $y \star y' = e = y' \star y$. Χρησιμοποιώντας την προσεταιριστική ιδιότητα θα έχουμε τότε τις ακόλουθες σχέσεις :

$$(x \star y) \star (y' \star x) = x \star (y \star (y' \star x')) = x \star ((y \star y') \star x') = x \star (e \star x') = x \star x' = e$$

$$(y' \star x') \star (x \star y) = y' \star (x' \star (x \star y)) = y' \star ((x' \star x) \star y) = y' \star (e \star y) = y' \star y = e$$

από τις οποίες προκύπτει ότι το στοιχείο $x \star y$ είναι αντιστρέψιμο με αντίστροφο το στοιχείο $y' \star x'$. ■

Παράδειγμα 1.3.8. Κλείνουμε την παρούσα υποενότητα με μια σειρά ενδεικτικών παραδειγμάτων.

1. Θεωρούμε το ζεύγος $(X, +)$, όπου X είναι ένα εκ των συνόλων αριθμών $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, και «+» είναι η συνήθης πράξη πρόσθεσης αριθμών. Τότε η πράξη «+» είναι προσεταιριστική και μεταθετική. Αν $X = \mathbb{N}$, τότε για την πράξη «+» δεν υπάρχει ουδέτερο στοιχείο (αν υπήρχε ένα τέτοιο στοιχείο $e \in \mathbb{N}$, θα έπρεπε να ίσχυε $e + x = x$, $\forall x \in \mathbb{N}$, απο όπου έπεται ότι $e = 0$, το οποίο είναι άτοπο διότι $0 \notin \mathbb{N}$). Αντίθετα, αν το σύνολο X είναι ένα εκ των $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$, τότε υπάρχει ουδέτερο στοιχείο, ο αριθμός 0, για την πράξη «+». Για τα σύνολα των αντίθετων (ή αντιστρέψιμων) στοιχείων ως προς την πράξη «+», έχουμε:

$$\mathsf{U}(\mathbb{N}_0, +) = \{0\}, \quad \mathsf{U}(\mathbb{Z}, +) = \mathbb{Z}, \quad \mathsf{U}(\mathbb{Q}, +) = \mathbb{Q}, \quad \mathsf{U}(\mathbb{R}, +) = \mathbb{R}, \quad \mathsf{U}(\mathbb{C}, +) = \mathbb{C}$$

2. Θεωρούμε το ζεύγος $(X,\cdot)$, όπου X είναι ένα εκ των συνόλων αριθμών $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, και «$\cdot$» είναι η συνήθης πράξη πολαπλασιασμού αριθμών. Τότε η πράξη «$\cdot$» είναι προσεταιριστική και μεταθετική, και υπάρχει ουδέτερο στοιχείο, ο αριθμός 1. Για τα σύνολα των αντιστρέψιμων στοιχείων ως προς την πράξη «$\cdot$», έχουμε:

$$\mathsf{U}(\mathbb{N},\cdot)=\{1\},\quad \mathsf{U}(\mathbb{Z},\cdot)=\{1,-1\},\quad \mathsf{U}(\mathbb{Q},\cdot)=\mathbb{Q}^*,\quad \mathsf{U}(\mathbb{R},\cdot)=\mathbb{R}^*,\quad \mathsf{U}(\mathbb{C},\cdot)=\mathbb{C}^*$$

3. Θεωρούμε το ζεύγος $(\mathsf{Map}(X),\circ)$, όπου $\mathsf{Map}(X)=\{f\colon X\longrightarrow X \mid f:\text{απεικόνιση}\}$ είναι το σύνολο των απεικονίσεων επί ενός μη κενού συνόλου X, και «$\circ$» είναι η πράξη της σύνθεσης απεικονίσεων:

$$\circ\colon \mathsf{Map}(X)\times\mathsf{Map}(X)\longrightarrow \mathsf{Map}(X),\quad (f,g)\longmapsto f\circ g$$

Η πράξη της σύνθεσης «$\circ$» είναι προσεταιριστική, αλλά γενικά, όπως προκύπτει από την Παρατήρηση 0.2.7, δεν είναι μεταθετική. Η ταυτοτική απεικόνιση Id_X αποτελεί ουδέτερο στοιχείο για την πράξη «$\circ$», και, όπως προκύπτει από την Πρόταση 0.2.8, για το σύνολο των αντιστρέψιμων στοιχείων, έχουμε:

$$\mathsf{U}(\mathsf{Map}(X),\circ)=\{f\colon X\longrightarrow X \mid f:\text{απεικόνιση «1-1» και «επί»}\}$$

Από τώρα και στο εξής, το σύνολο $\mathsf{U}(\mathsf{Map}(X),\circ)$ θα το συμβολίζουμε με $\mathsf{S}(X)$ και θα καλούμε τα στοιχεία του **μεταθέσεις** του συνόλου X. Δηλαδή μια μετάθεση του X είναι μια «1-1» και «επί» απεικόνιση $f\colon X\longrightarrow X$. Αν $X=\mathbb{N}_n$, θα γράφουμε $\mathsf{S}(\mathbb{N}_n)=\mathsf{S}_n$. Για μια εκτενή ανάλυση της δομής του ζεύγους $(\mathsf{S}(X),\circ)$ παραπέμπουμε στην υποενότητα 1.3.4 και στο Κεφάλαιο 5.

4. Θεωρούμε το σύνολο $\mathbb{R}^3=\{\vec{x}=(x_1,x_2,x_3)\mid x_i\in\mathbb{R},\ 1\le i\le 3\}$ των διατεταγμένων τριάδων πραγματικών αριθμών, τις οποίες θεωρούμε ως διανύσματα στον χώρο, στο οποίο ορίζουμε μια πράξη ως εξής:

$$\times:\mathbb{R}^3\times\mathbb{R}^3\longrightarrow\mathbb{R}^3,\quad (x_1,x_2,x_3)\times(y_1,y_2,y_3)=(x_2y_3-y_2x_3,\ x_3y_1-y_3x_1,\ x_1y_2-y_1x_2)$$

Δηλαδή η πράξη «$\times$» είναι το εξωτερικό γινόμενο διανυσμάτων του $\mathbb{R}^3$. Τότε η πράξη «$\times$» δεν είναι προσεταιριστική ούτε μεταθετική,[5] διότι, για παράδειγμα, θέτοντας $\vec{e}_1=(1,0,0)$, $\vec{e}_2=(0,1,0)$, $\vec{e}_3=(0,0,1)$, και $\vec{0}=(0,0,0)$, έχουμε:

$$\vec{e}_1\times\vec{e}_2=\vec{e}_3\neq-\vec{e}_3=\vec{e}_2\times\vec{e}_1$$

$$(\vec{e}_1\times\vec{e}_1)\times\vec{e}_2=\vec{0}\neq-\vec{e}_2=\vec{e}_1\times(\vec{e}_1\times\vec{e}_2)$$

Τέλος, για την πράξη «$\times$» δεν υπάρχει ουδέτερο στοιχείο: αν υπήρχε ουδέτερο στοιχείο $\vec{e}\in\mathbb{R}^3$, τότε θα έπρεπε να ισχύει ότι $\vec{e}\times\vec{x}=\vec{x}=\vec{x}\times\vec{e}$, $\forall\vec{x}\in\mathbb{R}^3$. Επειδή, όπως μπορούμε να δούμε εύκολα, ισχύει ότι $\vec{x}\times\vec{y}=-(\vec{y}\times\vec{x})$, $\forall\vec{x},\vec{y}\in\mathbb{R}^3$, έπεται ότι $\vec{x}=\vec{x}\times\vec{e}=-(\vec{e}\times\vec{x})=-\vec{x}$ και επομένως $\vec{x}=\vec{0}$. Άρα, αν $\vec{x}\neq\vec{0}$, τότε $\vec{x}=\vec{x}\times\vec{e}=\vec{0}\neq\vec{x}$, το οποίο είναι άτοπο.

5. Θεωρούμε τα ζεύγη $(\mathbb{N},\star)$ και $(\mathbb{Z},-)$, όπου $n\star m=n^m$, $\forall n,m\in\mathbb{N}$, και «$-$» είναι η συνήθης πράξη αφαίρεσης ακεραίων (η αφαίρεση δεν ορίζει πράξη επί του $\mathbb{N}$). Τότε οι πράξεις αυτές δεν είναι προσεταιριστικές, διότι για παράδειγμα:

$$2\star(2\star3)=2\star2^3=2\star8=2^8\neq2^6=(2^2)^3=(2\star2)\star3\quad\text{και}\quad 1-(2-3)=1-(-1)=2\neq-4=-1-3=(1-2)-3$$

6. Έστω $\mathsf{M}_{m\times n}(\mathbb{R})$ το σύνολο όλων των $m\times n$ πινάκων A με στοιχεία πραγματικούς αριθμούς:

$$\mathsf{M}_{m\times n}(\mathbb{R})=\{A=(a_{ij})\mid a_{ij}\in\mathbb{R},\ 1\le i\le m,\ 1\le j\le n\},\quad\text{όπου}\quad A=(a_{ij})=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\a_{m1}&a_{m2}&\cdots&a_{mn}\end{pmatrix}$$

[5] Η πράξη «$\times$» ικανοποιεί ασθέστερες εκδοχές προσεταιριστικότητας και μεταθετικότητας:

$$\forall\vec{x},\vec{y},\vec{z}\in\mathbb{R}^3:\quad \vec{x}\times\vec{y}=-(\vec{y}\times\vec{x})\quad\text{και}\quad \vec{x}\times(\vec{y}\times\vec{z})+\vec{y}\times(\vec{z}\times\vec{x})+\vec{z}\times(\vec{x}\times\vec{y})=\vec{0}$$

Συνήθως ένας $m \times n$ πίνακας A θα παριστάται σε συντομευμένη μορφή ως $A = (A_{ij})$ ή $A = (a_{ij})$, υπονοώντας ότι το στοιχείο στην (i,j)-θέση του πίνακα A, δηλαδή στην τομή της i-γραμμής με την j-στήλη, είναι ο αριθμός A_{ij} ή a_{ij} αντίστοιχα.

Στο σύνολο $\mathsf{M}_{m\times n}(\mathbb{R})$ θεωρούμε τη συνήθη πράξη πρόσθεσης πινάκων: αν $A = (a_{ij})$ και $B = (b_{ij})$, τότε $A + B = (c_{ij})$, όπου $c_{ij} = a_{ij} + b_{ij}$, $1 \le i \le m$, $1 \le j \le n$. Η πράξη «+» επί του συνόλου $\mathsf{M}_{m\times n}(\mathbb{R})$ είναι προσεταιριστική, μεταθετική, ο *μηδενικός πίνακας* $\mathsf{O} = (x_{ij})$, όπου $x_{ij} = 0$, $1 \le i \le m$, $1 \le j \le n$, είναι το ουδέτερο στοιχείο, και για το σύνολο των αντίθετων στοιχείων ως προς την πράξη «+» έχουμε προφανώς $\mathsf{U}(\mathsf{M}_{m\times n}(\mathbb{R}),+) = \mathsf{M}_{m\times n}(\mathbb{R})$, διότι για κάθε πίνακα $A = (a_{ij})$ υπάρχει ο πίνακας $-A := (-a_{ij})$ έτσι ώστε $A + (-A) = \mathsf{O} = (-A) + A$.

Όταν $m = n$, μπορούμε να ορίσουμε στο σύνολο $\mathsf{M}_n(\mathbb{R}) := \mathsf{M}_{n\times n}(\mathbb{R})$ μια νέα πράξη, την πράξη του πολλαπλασιασμού πινάκων:

$$\text{Αν } A = (a_{ij}) \text{ και } B = (b_{ij}), \text{ τότε: } A \cdot B = (c_{ij}), \text{ όπου } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad 1 \le i, j \le n$$

Όπως μπορούμε να δούμε εύκολα, η πράξη «$\cdot$» πολλαπλασιασμού πινάκων είναι προσεταιριστική.[6] Όμως, όταν $n > 1$, η πράξη «$\cdot$» δεν είναι μεταθετική διότι, για παράδειγμα:

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} = \begin{pmatrix} n & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Προφανώς ο μοναδιαίος πίνακας

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

αποτελεί το ουδέτερο στοιχείο για την πράξη «$\cdot$», και το σύνολο $\mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot)$ των αντιστρέψιμων στοιχείων του $\mathsf{M}_n(\mathbb{R})$ ως προς την πράξη «$\cdot$» πολλαπλασιασμού πινάκων αποτελείται από το σύνολο $\mathsf{GL}(n,\mathbb{R})$ των αντιστρέψιμων $n \times n$ πινάκων πραγματικών αριθμών:

$$\mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot) := \mathsf{GL}(n,\mathbb{R}) = \{A \in \mathsf{M}_n(\mathbb{R}) \mid A: \text{ αντιστρέψιμος}\}$$

Σημειώνουμε ότι, όπως γνωρίζουμε από την Γραμμική Άλγεβρα, ισχύει ότι

$$\mathsf{GL}(n,\mathbb{R}) = \{A \in \mathsf{M}_n(\mathbb{R}) \mid \mathsf{Det}(A) \neq 0\}$$

7. Θεωρούμε τα ζεύγη $(\mathbb{N},(,))$ και $(\mathbb{N},[,])$, όπου «$(,)$» και «$[,]$» είναι οι ακόλουθες πράξεις επί του $\mathbb{N}$:

$$(,) : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}, \quad (n,m) = \text{μέγιστος κοινός διαιρέτης των } n, m$$

$$[,] : \mathbb{N}\times\mathbb{N} \longrightarrow \mathbb{N}, \quad [n,m] = \text{ελάχιστο κοινό πολλαπλάσιο των } n, m$$

Οι πράξεις «$(,)$» και «$[,]$» επί του $\mathbb{N}$ είναι προσεταιριστικές και μεταθετικές, αλλά δεν υπάρχει ουδέτερο στοιχείο για τις πράξεις αυτές.

---

[6] Έστω ότι $A = (A_{ij})$, $B = (B_{ij})$, και $C = (C_{ij})$ είναι τρεις $n \times n$ πίνακες με στοιχεία πραγματικούς αριθμούς. Τότε, για κάθε $1 \le i, j \le n$, θα έχουμε ότι το στοιχείο στην (i,j)-θέση του πίνακα $A \cdot (B \cdot C)$ είναι:

$$[A\cdot(B\cdot C)]_{ij} = \sum_{k=1}^{n} A_{ik}(B\cdot C)_{kj} = \sum_{k=1}^{n} A_{ik}\Big(\sum_{m=1}^{n} B_{km}C_{mj}\Big) = \sum_{k=1}^{n}\sum_{m=1}^{n} A_{ik}(B_{km}C_{mj}) = \sum_{m=1}^{n}\sum_{k=1}^{n} (A_{ik}B_{km})C_{mj} = \sum_{m=1}^{n} (A\cdot B)_{im}C_{mj} = [(A\cdot B)\cdot C]_{ij}$$

δηλαδή είναι ίσο με το στοιχείο στην (i,j)-θέση του πίνακα $(A \cdot B) \cdot C$. Επομένως οι πίνακες $A \cdot (B \cdot C)$ και $(A \cdot B) \cdot C$ έχουν ίσα στοιχεία στις αντίστοιχες θέσεις και άρα: $A \cdot (B \cdot C) = (A \cdot B) \cdot C$.

8. Έστω A ένα μη κενό σύνολο, και έστω $\mathscr{P}(A)$ το δυναμοσύνολο του A. Θεωρούμε τα ζεύγη $(\mathscr{P}(A),\cap)$ και $(\mathscr{P}(A),\cup)$, όπου $\forall X,Y\in\mathscr{P}(A)$: $X\cap Y$ είναι η τομή και $X\cup Y$ είναι η ένωση των των υποσυνόλων X και Y του A. Τότε οι πράξεις «$\cap$» και «$\cup$» είναι προσεταιριστικές και μεταθετικές. Το σύνολο A αποτελεί το ουδέτερο στοιχείο για την πράξη «$\cap$» επί του $\mathscr{P}(A)$, και το κενό σύνολο $\emptyset$ αποτελεί το ουδέτερο στοιχείο για την πράξη «$\cup$» επί του $\mathscr{P}(A)$. Τέλος, για τα σύνολα των αντιστρέψιμων στοιχείων, έχουμε:

$$\mathsf{U}\big(\mathscr{P}(A),\cap\big)=\{A\}\qquad\text{και}\qquad\mathsf{U}\big(\mathscr{P}(A),\cup\big)=\{\emptyset\}$$

Επί του συνόλου $\mathscr{P}(A)$ μπορούμε να ορίσουμε και μια τρίτη ενδιαφέρουσα πράξη, την «*συμμετρική διαφορά*» υποσυνόλων του A:

$$\Delta:\mathscr{P}(A)\times\mathscr{P}(A)\longrightarrow\mathscr{P}(A),\quad X\Delta Y=(X\cup Y)\setminus(X\cap Y)$$

Η πράξη «Δ» είναι προσεταιριστική και μεταθετική. Υπάρχει ουδέτερο στοιχείο, το κενό σύνολο $\emptyset$, για την πράξη «Δ», και για το σύνολο $\mathsf{U}\big(\mathscr{P}(A),\Delta\big)$ των αντιστρέψιμων στοιχείων του $\mathscr{P}(A)$ ως προς την πράξη Δ έχουμε: $\mathsf{U}\big(\mathscr{P}(A),\Delta\big)=\mathscr{P}(A)$, διότι για κάθε $X\in\mathscr{P}(A)$ έχουμε: $X\Delta X=\emptyset$, δηλαδή το αντίστροφο ως προς την πράξη Δ του X υπάρχει και συμπίπτει με το X.

9. Έστω $\mathscr{F}(X,\mathbb{R})=\{f:X\longrightarrow\mathbb{R}\mid f:\text{απεικόνιση}\}$ το σύνολο όλων των πραγματικών απεικονίσεων οι οποίες είναι ορισμένες επί του υποσυνόλου X της πραγματικής ευθείας. Το σύνολο $\mathscr{F}(X,\mathbb{R})$ είναι εφοδιασμένο με τις εξής πράξεις πρόσθεσης και πολλαπλασιασμού συναρτήσεων:

$$\forall f,g:X\longrightarrow\mathbb{R},\quad f+g,\ f\cdot g:X\longrightarrow\mathbb{R},\quad\text{όπου}\quad(f+g)(x)=f(x)+g(x),\quad(f\cdot g)(x)=f(x)\cdot g(x)$$

Επειδή οι πράξεις «$+$» και «$\cdot$» επί του συνόλου $\mathscr{F}(X,\mathbb{R})$ με χρήση των αντίστοιχων πράξεων «$+$» και «$\cdot$» επί του $\mathbb{R}$ οι οποίες είναι προσεταιριστικές και μεταθετικές, έπεται ότι οι πράξεις «$+$» και «$\cdot$» επί του συνόλου $\mathscr{F}(X,\mathbb{R})$ είναι προσεταιριστικές και μεταθετικές. Οι απεικονίσεις

$$0:X\longrightarrow\mathbb{R},\ \ 0(x)=0\qquad\text{και}\qquad 1:X\longrightarrow\mathbb{R},\ \ 1(x)=1$$

αποτελούν ουδέτερο στοιχείο για τις πράξεις «$+$» και «$\cdot$» επί του συνόλου $\mathscr{F}(X,\mathbb{R})$ αντίστοιχα.

10. Έστω ότι $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, καθένα εκ των οποίων θεωρείται εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού. Υπενθυμίζουμε ότι μια *ακολουθία στοιχείων* του $\mathbb{K}$ ορίζεται να είναι μια απεικόνιση

$$\mathsf{a}:\mathbb{N}_0\longrightarrow\mathbb{K},\quad\mathsf{a}(n):=a_n$$

Συνήθως μια ακολουθία a την συμβολίζουμε με $\mathsf{a}=(a_n)_{n\geq0}$. Θεωρούμε το ακόλουθο σύνολο των **ακολουθιών** με στοιχεία από το $\mathbb{K}$:

$$\mathsf{A}(\mathbb{K})=\{\mathsf{a}=(a_n)_{n\geq0}\mid a_n\in\mathbb{K},\ \forall n\geq0\}$$

επί του οποίου ορίζουμε *πράξη πρόσθεσης* «$+$» και *πράξη πολλαπλασιασμού* «$\cdot$», ως εξής. Αν $\mathsf{a}=(a_n)_{n\geq0}$ και $\mathsf{b}=(b_n)_{n\geq0}$ είναι στοιχεία του $\mathsf{A}(\mathbb{K})$, τότε:

$$+:\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad\mathsf{a}+\mathsf{b}=\mathsf{c}=(c_n)_{n\geq0},\quad\text{όπου}\quad c_n=a_n+b_n,\ \ \forall n\geq0$$

$$\cdot:\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad\mathsf{a}\cdot\mathsf{b}=\mathsf{d}=(d_n)_{n\geq0},\quad\text{όπου}\quad d_n=\sum_{k=0}^{n}a_kb_{n-k},\ \ \forall n\geq0$$

Έτσι αποκτούμε τα ζεύγη $(\mathsf{A}(\mathbb{K}),+)$ και $(\mathsf{A}(\mathbb{K}),\cdot)$, και όπως προκύπτει εύκολα, βλέπε την Άσκηση 1.5.25, οι πράξεις «$+$» και «$\cdot$» είναι προσεταιριστικές.

Η ακολουθία $0=(a_n)_{n\geq0}$, όπου $a_n=0$, $\forall n\geq0$, είναι προφανώς ουδέτερο στοιχείο για την πράξη της πρόσθεσης ακολουθιών και ισχύει ότι:

$$\mathsf{U}(\mathsf{A}(\mathbb{K}),+)=\mathsf{A}(\mathbb{K})$$

Από την άλλη πλευρά, η ακολουθία $1=(a_n)_{n\geq0}$, όπου $a_0=1$ και $a_n=0$, $\forall n\geq1$, είναι ουδέτερο στοιχείο για την πράξη του πολλαπλασιασμού ακολουθιών, και ισχύει ότι, βλέπε Άσκηση 1.5.25:

$$\mathsf{U}(\mathsf{A}(\mathbb{K}),\cdot)=\{\mathsf{a}=(a_n)_{n\geq0}\mid a_0\in\mathsf{U}(\mathbb{K},\cdot)\text{ και }a_n=0,\forall n\geq1\}$$

11. Θεωρούμε το σύνολο $\mathscr{A}$ των **αριθμητικών συναρτήσεων** δηλαδή το σύνολο

$$\mathscr{A} = \{f : \mathbb{N} \longrightarrow \mathbb{C} \mid f : \text{συνάρτηση}\}$$

Για παράδειγμα: (α) αν $k \in \mathbb{N}$, η συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{C}$, $f(n) = n^k$, είναι αριθμητική, (β) η συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{C}$, $f(n) = e^{in}$, είναι αριθμητική, και (γ) η συνάρτηση $f : \mathbb{N} \longrightarrow \mathbb{C}$, $f(n) = n!$, είναι αριθμητική. Στο σύνολο $\mathscr{A}$ ορίζουμε τις ακόλουθες πράξεις «+» και «∗». Για κάθε $f, g \in \mathscr{A}$:

$$+ : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}, \quad (f,g) \longmapsto f+g : \mathbb{N} \longrightarrow \mathbb{C}, \quad (f+g)(n) = f(n)+g(n)$$

$$* : \mathscr{A} \times \mathscr{A} \longrightarrow \mathscr{A}, \quad (f,g) \longmapsto f*g : \mathbb{N} \longrightarrow \mathbb{C}, \quad (f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

Εύκολα βλέπουμε ότι η πράξη «+» είναι μεταθετική και προσεταιριστική, και η αριθμητική συνάρτηση $0 : \mathbb{N} \longrightarrow \mathbb{C}$, $0(n) = 0$, $\forall n \in \mathbb{N}$, είναι ουδέτερο στοιχείο για την πράξη «+» στο σύνολο $\mathscr{A}$.

Από την άλλη πλευρά, η τιμή $(f*g)(n)$ προκύπτει αθροίζοντας όλα τα δυνατά γινόμενα $f(d)g(\frac{n}{d})$ όταν το d διατρέχει όλους τους θετικούς διαιρέτες του n. Για παράδειγμα, αν $n = 12$, τότε, επειδή οι θετικοί διαιρέτες του 12 είναι οι $1,2,3,4,6,12$, θα έχουμε: $(f*g)(12) = f(1)g(12)+f(2)g(6)+f(3)g(4)+f(4)g(3)+f(6)g(12)+f(12)g(1)$. Η πράξη «∗» επί του $\mathscr{A}$ καλείται *ευελικτικό γινόμενο* ή *γινόμενο Dirichlet*,[7] και διαδραματίζει σημαντικό ρόλο στη Θεωρία Αριθμών, όπου και αποδεικνύεται ότι είναι μεταθετική και προσεταιριστική πράξη, με ουδέτερο στοιχείο την αριθμητική συνάρτηση

$$\varepsilon : \mathbb{N} \longrightarrow \mathbb{C}, \quad \varepsilon(n) = \begin{cases} 1, & \text{αν } n = 1 \\ 0, & \text{αν } n \geq 2 \end{cases} \qquad \surd$$

1.3.2 Ο Πίνακας Cayley μιας Διμελούς Πράξης

Θεωρούμε ένα ζεύγος $(X, \star)$, όπου $X = \{x_1, x_2, \cdots, x_n\}$ είναι ένα πεπερασμένο σύνολο και «$\star$» είναι μια πράξη επί του X. Όλες οι βασικές πληροφορίες οι οποίες αφορούν την πράξη «$\star$» εμπεριέχονται στον πίνακα Cayley της πράξης ο οποίος ορίζεται παρακάτω. Υπενθυμίζουμε πρώτα ότι, αν $A = (a_{ij})$ είναι ένας $n \times n$ πίνακας με στοιχεία από ένα σύνολο X, τότε το στοιχείο a_{ij} βρίσκεται στην τομή της i-γραμμής και της j-στήλης.

Ορισμός 1.3.9. *Ο τετραγωνικός $n \times n$ πίνακας $\mathsf{C}(X, \star) = (x_{ij})$ στοιχείων του X, όπου:*

$$x_{ij} := x_i \star x_j, \quad 1 \leq i, j \leq n$$

καλείται ***πίνακας Cayley***[8] *της αλγεβρικής δομής $(X, \star)$, και παριστάται όπως στο παρακάτω σχήμα 1.1:*

Παρατήρηση 1.3.10. 1. Όταν είναι γνωστός ο πίνακας Cayley $\mathsf{C}(X, \star)$ μιας αλγεβρικής δομής $(X, \star)$, τότε μπορεί να διαπιστωθεί αμέσως αν η πράξη «$\star$» είναι μεταθετική ή όχι. Πράγματι, είναι αρκετό να παρατηρήσει κανείς ότι για κάθε i, j με $1 \leq i, j \leq n$, τα στοιχεία $x_{ij} = x_i \star x_j$ και $x_{ji} = x_j \star x_i$, βρίσκονται συμμετρικά ως προς την κύρια διαγώνιο του πίνακα η οποία αποτελείται από τα στοιχεία $x_{ii} = x_i \star x_i$, $1 \leq i \leq n$. Συνεπώς η πράξη είναι μεταθετική αν και μόνο αν τα στοιχεία του πίνακα $\mathsf{C}(X, \star)$ που κείνται συμμετρικά ως προς την κύρια διαγώνιό του είναι ίσα.

Επομένως η πράξη «$\star$» επί του X είναι μεταθετική αν και μόνο αν ο πίνακας Cayley $\mathsf{C}(X, \star)$ της πράξης «$\star$» είναι συμμετρικός[9]: $\mathsf{C}(X, \star) = {}^t\mathsf{C}(X, \star)$.

---

[7] Peter Gustav Lejeune Dirichlet (1805-1859) [http://en.wikipedia.org/wiki/Peter_Gustav_Lejeune_Dirichlet], Γερμανός μαθηματικός με θεμελιώδη συμβολή στη Θεωρία Αριθμών, και την Μαθηματική Ανάλυση.

[8] Arthur Cayley (16 Αυγούστου 1821 - 26 Ιανουαρίου 1895) [https://en.wikipedia.org/wiki/Arthur_Cayley]: Βρετανός μαθηματικός, με συμβολή στην Άλγεβρα και ιδιαίτερα στη Θεωρία Ομάδων. Υπήρξε ο πρώτος ο οποίος όρισε την έννοια της ομάδας με την μορφή που γνωρίζουμε σήμερα.

[9] Υπενθυμίζουμε ότι ο *ανάστροφος* πίνακας ${}^tA$ ενός πίνακα $A = (a_{ij})$, είναι ο πίνακας ${}^tA = (a_{ji})$, δηλαδή στην τομή της i-γραμμής και της j-στήλης βρίσκεται το στοιχείο a_{ji} του πίνακα A. Εξ ορισμού ο πίνακας A είναι *συμμετρικός* αν συμπίπτει με τον ανάστροφό του: $A = {}^tA$.

$\star$	$\mathbf{x_1}$	$\mathbf{x_2}$	$\cdots$	$\mathbf{x_i}$	$\cdots$	$\mathbf{x_j}$	$\cdots$	$\mathbf{x_n}$
$\mathbf{x_1}$	$x_1 \star x_1$	$x_1 \star x_2$	$\ldots$	$x_1 \star x_i$	$\ldots$	$x_1 \star x_j$	$\ldots$	$x_1 \star x_n$
$\mathbf{x_2}$	$x_2 \star x_1$	$x_2 \star x_2$	$\ldots$	$x_2 \star x_i$	$\ldots$	$x_2 \star x_j$	$\ldots$	$x_2 \star x_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{x_i}$	$x_i \star x_1$	$x_i \star x_2$	$\cdots$	$x_i \star x_i$	$\cdots$	$x_i \star x_j$	$\cdots$	$x_i \star x_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{x_j}$	$x_j \star x_1$	$x_j \star x_2$	$\cdots$	$x_j \star x_i$	$\cdots$	$x_j \star x_j$	$\cdots$	$x_j \star x_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\mathbf{x_n}$	$x_n \star x_1$	$x_n \star x_2$	$\cdots$	$x_n \star x_i$	$\cdots$	$x_n \star x_j$	$\cdots$	$x_n \star x_n$

Σχήμα 1.1: Ο πίνακας Cayley της αλγεβρικής δομής $(X, \star)$.

2. Αν $X = \{x_1, x_2, \ldots, x_n\}$ είναι ένα σύνολο με n στοιχεία, τότε κάθε πίνακας με n γραμμές και n στήλες, ο οποίος αποτελείται από στοιχεία του X, ορίζει μια πράξη επί του X ως ακολούθως:

   $\star : X \times X \longrightarrow X, \ (x_i, x_j) \longmapsto x_i \star x_j :=$ το στοιχείο τού X που βρίσκεται στην (i, j)-θέση του πίνακα.

3. Όταν υπάρχει ουδέτερο στοιχείο $e \in X$ για την πράξη «$\star$» επί του πεπερασμένου συνόλου $X = \{x_1, x_2, \cdots, x_n\}$, τότε, αναδιατάσσοντας, αν είναι ανάγκη, τα στοιχεία του X, μπορούμε να υποθέσουμε ότι $e = x_1$. Τότε θα έχουμε $x_1 \star x_k = x_k = x_k \star x_1$, $1 \leq k \leq n$, και επομένως η πρώτη γραμμή $x_{1k} = x_1 \star x_k$, $1 \leq k \leq n$, και η πρώτη στήλη $x_{k1} = x_k \star x_1$, $1 \leq k \leq n$, του πίνακα Cayley στο Σχήμα 1.1 αποτελείται από τα στοιχεία $x_1, x_2, \cdots, x_n$ με την ίδια σειρά. ▲

Παράδειγμα 1.3.11. Έστω $X = \{x, y\}$ ένα σύνολο με δύο στοιχεία. Τότε επί του X μπορούν να οριστούν 16 (διμελείς) πράξεις. Πράγματι, μια πράξη «$\star$» επί του X είναι μια απεικόνιση $\star : X \times X \longrightarrow X$, και γνωρίζουμε ότι το πλήθος των απεικονίσεων από ένα σύνολο με n στοιχεία σε ένα σύνολο με m στοιχεία είναι ίσο με m^n. Άρα το πλήθος των δυνατών πράξεων επί του X είναι $|X|^{|X \times X|} = 2^{2 \cdot 2} = 2^4 = 16$. Από αυτές τις 16 πράξεις, ας περιοριστούμε στις πράξεις «$\star$» για τις οποίες υπάρχει ουδέτερο στοιχείο $e \in X$. Χωρίς βλάβη της γενικότητας, έστω ότι $e = y$. Τότε $X = \{e, x\}$ και θα έχουμε: $e \star e = e$ και $e \star x = x = x \star e$. Επομένως, για να περιγράψουμε την πράξη «$\star$» μένει να ορίσουμε το στοιχείο $x \star x$ για το οποίο έχουμε δύο επιλογές: είτε $x \star x = e$ είτε $x \star x = x$. Έτσι προκύπτουν δύο πράξεις επί του X με αντίστοιχους πίνακες Cayley τους εξής:

$\star$	$\mathbf{e}$	$\mathbf{x}$
$\mathbf{e}$	e	x
$\mathbf{x}$	x	e

και

$\diamond$	$\mathbf{e}$	$\mathbf{x}$
$\mathbf{e}$	e	x
$\mathbf{x}$	x	x

Επομένως υπάρχουν μόνο δύο πράξεις «$\star$» και «$\diamond$» επί του X για τις οποίες υπάρχει ουδέτερο στοιχείο. Εύκολα βλέπουμε ότι οι πράξεις «$\star$» και «$\diamond$» είναι προσεταιριστικές, και επομένως υπάρχουν ακριβώς δύο δομές $(X, \star)$ και $(X, \diamond)$, επί ενός συνόλου X με δύο στοιχεία, όπου οι πράξεις είναι προσεταιριστικές και υπάρχει γι' αυτές ουδέτερο στοιχείο. Επιπρόσθετα και για τις δύο αυτές δομές, οι πράξεις οι οποίες τις ορίζουν είναι προφανώς μεταθετικές. Αν επιπλέον αναζητούμε τις πιθανές δομές επί του X ως προς τις οποίες κάθε στοιχείο είναι αντιστρέψιμο, έπεται ότι θα πρέπει να απορρίψουμε την αλγεβρική δομή $(X, \diamond)$ διότι, επειδή το x είναι αντιστρέψιμο, με αντίστροφο έστω το στοιχείο x', θα πρέπει $x \diamond x' = e = x' \diamond x$. Για το x' έχουμε δύο επιλογές: είτε $x' = x$ είτε $x' = e$. Η πρώτη επολογή απορρίπτεται διότι από τον πίνακα Cayley έχουμε $x \diamond x = x \neq e$, και η δεύτερη επιλογή απορρίπτεται διότι από τον πίνακα Cayley έχουμε $x \diamond e = x \neq e$. Άρα υπάρχει ακριβώς μια αλγεβρική δομή $(X, \star)$ επί ενός συνόλου X με δύο στοιχεία, για το οποίο η πράξη «$\star$» είναι προσεταιριστική, υπάρχει γι' αυτήν ουδέτερο στοιχείο, και κάθε στοιχείο του X είναι αντιστρέψιμο ως προς την πράξη «$\star$». $\surd$

Παράδειγμα 1.3.12. Θεωρούμε το σύνολο $X = \{x, y, z\}$. Τότε, όπως στο Παράδειγμα 1.3.11, επί του X μπορούν να οριστούν $3^{3\cdot 3} = 3^9 = 19683$ διαφορετικές πράξεις. Μία από αυτές τις πράξεις είναι η πράξη «$\star$» επί του X η οποία ορίζεται από τις ακόλουθες σχέσεις:

$$x \star x = x, \quad x \star y = y, \quad x \star z = z$$

$$y \star x = y, \quad y \star y = y, \quad y \star z = x,$$

$$z \star x = z, \quad z \star y = x, \quad z \star z = y$$

Ο πίνακας Cayley τής αλγεβρικής δομής $(X, \star)$ παρουσιάζεται στο Σχήμα 1.2 παρακάτω.

$\star$	**x**	**y**	**z**
x	x	y	z
y	y	z	x
z	z	x	y

Σχήμα 1.2: Ο πίνακας τής πράξης «$\star$» επί τού συνόλου T.

Προφανώς πρόκειται για μια μεταθετική πράξη. Αφήνεται ως άσκηση στον αναγνώστη να εξετάσει αν η πράξη αυτή είναι προσεταιριστική. $\surd$

Παρατήρηση 1.3.13. Το πλήθος των «διαφορετικών»[10] αλγεβρικών δομών $(X, \star)$, οι οποίες μπορεί να οριστούν επί ενός συνόλου X με πλήθος στοιχείων ίσο με n και για τις οποίες η πράξη «$\star$» είναι προσεταιριστική και υπάρχει ουδέτερο στοιχείο γι' αυτήν στο X, αυξάνεται εντυπωσιακά όταν το n αυξάνει.

Έτσι ορίζοντας την συνάρτηση

$$\mu\colon \mathbb{N} \longrightarrow \mathbb{N}, \quad \mu(n) = \text{πλήθος διαφορετικών προσεταιριστικών πράξεων με ουδέτερο στοιχείο}$$

$$\text{επί ενός συνόλου με } n \text{ το πληθος στοιχεία}$$

έχουμε[11]:

$$\mu(1) = 1, \quad \mu(2) = 2, \quad \mu(3) = 7, \quad \mu(4) = 35, \quad \mu(5) = 228, \quad \mu(6) = 2237, \quad \mu(7) = 31559, \quad \mu(8) = 1668997 \quad \blacktriangle$$

1.3.3 Ο Γενικός Προσεταιριστικός και Μεταθετικός Νόμος - Δυνάμεις Στοιχείων

Στην παρούσα υποενότητα θα αποδείξουμε κάποιες βασικές ιδιότητες που αφορούν προσεταιριστικές πράξεις επί συνόλων, και οι οποίες θα μας είναι πολύ χρήσιμες στα επόμενα κεφάλαια. Επίσης θα ορίσουμε δυνάμεις (ή ακέραια πολλαπλάσια) στοιχείων ως προς μια πράξη σε ένα σύνολο και θα αποδείξουμε κάποιες βασικές ιδιότητες οι οποίες γενικεύουν γνωστές μας ιδιότητες πολλαπλασιασμού (ή πρόσθεσης) σε οικεία σύνολα αριθμών. Τέλος, θα εισαγάγουμε συμβολισμό ο οποίος θα απλουστεύσει σημαντικά την ανάπτυξη και ανάλυση των εννοιών τις οποίες θα μελετήσουμε αργότερα.

[10] Δηλαδή αλγεβρικών δομών με διαφορετικό πίνακα Cayley και χωρίς να λαμβάνεται υπόψη η φύση ή η διάταξη των στοιχείων τους.
[11] Για περισσότερες πληροφορίες παραπέμπουμε στον ιστότοπο [http://oeis.org/A058129].

Ο Γενικός Προσεταιριστικός Νόμος

Έστω $(X,\star)$ ένα ζεύγος, όπου «$*$» είναι μια πράξη επί ενός μη κενού συνόλου X. Αν a,b,c είναι στοιχεία του X, τότε το «στοιχείο» $a\star b\star c$ δεν είναι μονοσήμαντα ορισμένο, καθώς μπορεί να είναι οποιοδήποτε από τα μονοσήμαντα ορισμένα στοιχεία $(a\star b)\star c$ και $a\star(b\star c)$, τα οποία ενδεχομένως να μην είναι ίσα. Αυτά τα στοιχεία είναι ίσα, αν ισχύει η προσεταιριστική ιδιότητα για την πράξη «$\star$».

Γενικότερα, αν a,b,c,d είναι διακεκριμένα στοιχεία του X, τότε το «στοιχείο» $a\star b\star c\star d$ δεν είναι μονοσήμαντα ορισμένο, καθώς μπορεί να είναι οποιοδήποτε από τα μονοσήμαντα ορισμένα στοιχεία

$$(a\star b)\star(c\star d),\quad (a\star(b\star c))\star d,\quad ((a\star b)\star c)\star d,\quad a\star((b\star c)\star d),\quad a\star(b\star(c\star d))$$

τα οποία ενδεχομένως να μην είναι όλα ίσα μεταξύ τους. Τα παραπάνω στοιχεία προκύπτουν ομαδοποιώντας κατάλληλα τα στοιχεία a,b,c,d, εισάγοντας παρενθέσεις οι οποίες υποδεικνύουν με ποια σειρά εκτελούνται οι εμπλεκόμενες πράξεις. Για παράδειγμα, το στοιχείο $(a\star(b\star c))\star d$ προκύπτει υπολογίζοντας πρώτα το αποτέλεσμα της πράξης «$\star$» στα στοιχεία b και c, οπότε θα προκύπει ένα νέο στοιχείο $b\star c$, ακολούθως υπολογίζουμε το αποτέλεσμα της πράξης στα στοιχεία a και $b\star c$, οπότε θα προκύψει το νέο στοιχείο $a\star(b\star c)$, και τέλος υπολογίζουμε το αποτέλεσμα της πράξης «$\star$» στα στοιχεία $a\star(b\star c)$ και d, οπότε θα προκύψει το στοιχείο $(a\star(b\star c))\star d$.

Το επόμενο αποτέλεσμα μάς επιτρέπει να ορίσουμε μονοσήμαντα στοιχεία της μορφής

$$a_1\star a_2\star\cdots\star a_n$$

σε ένα σύνολο X εφοδιασμένο με μια *προσεταιριστική* πράξη «$\star$». Δηλαδή όλες οι δυνατές ομαδοποιήσεις των στοιχείων $a_1,a_2,\cdots,a_n$, με εισαγωγή παρενθέσεων, οι οποίες είναι απαραίτητες για τον υπολογισμό του στοιχείου $a_1\star a_2\star\cdots\star a_n$, μας δίνουν το ίδιο αποτέλεσμα.

Πρόταση 1.3.14 (Ο Γενικός Προσεταιριστικός Νόμος)**.** *Έστω «$\star$» μια προσεταιριστική πράξη επί του μη κενού συνόλου X. Αν $a_1,a_2,\cdots,a_n$ είναι στοιχεία του X, τότε το στοιχείο $a_1\star a_2\star\cdots\star a_n$ είναι μονοσήμαντα ορισμένο.*

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στο πλήθος n των στοιχείων $a_1,a_2,\cdots,a_n$ του X.

1. Αν $n=1$ ή 2, ο ισχυρισμός είναι προφανής.
2. Αν $n=3$, τότε ο ισχυρισμός είναι αληθής επειδή η πράξη «$\star$» είναι προσεταιριστική.
3. <u>*Επαγωγική Υπόθεση*</u>: Αν $a_1,a_2,\cdots,a_k$ είναι στοιχεία του X, όπου $k<n$, τότε το στοιχείο $a_1\star a_2\star\cdots\star a_k$ είναι μονοσήμαντα ορισμένο, δηλαδή όλες οι δυνατές επιλογές για τον υπολογισμό του με εισαγωγή παρενθέσεων δίνουν το ίδιο αποτέλεσμα.
4. Για την γενική περίπτωση $k=n$, έστω ότι έχουμε δύο τυχούσες ομαδοποιήσεις των στοιχείων a_1, a_2, $\cdots$, a_n. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι για κάποια $i,j<n$, αυτές οι ομαδοποιήσεις είναι της μορφής

   $$M=(a_1\star\cdots\star a_i)\star(a_{i+1}\star\cdots\star a_n)\qquad\text{και}\qquad N=(a_1\star\cdots\star a_j)\star(a_{j+1}\star\cdots\star a_n)$$

   Σημειώνουμε ότι, με χρήση της επαγωγικής υπόθεσης, μέσα στις παρενθέσεις τα στοιχεία $a_1\star\cdots\star a_i$, $a_1\star\cdots\star a_j$, $a_{i+1}\star\cdots\star a_n$, και $a_{j+1}\star\cdots\star a_n$ είναι μονοσήμαντα ορισμένα.

   Θα δείξουμε ότι $M=N$.

   (α′) Αν $i=j$, τότε προφανώς $M=N$.

   (β′) Έστω $i\neq j$. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $i<j$. Τότε, με χρήση της επαγωγικής υπόθεσης, τα στοιχεία M και N μπορούν να γραφούν ως εξής:

   $$M=(a_1\star\cdots\star a_i)\star\big((a_{i+1}\star\cdots\star a_j)\star(a_{j+1}\star\cdots\star a_n)\big)=x\star(y\star z)$$

   $$N=\big((a_1\star\cdots\star a_i)\star(a_{i+1}\star\cdots\star a_j)\big)\star(a_{j+1}\star\cdots\star a_n)=(x\star y)\star z$$

όπου θέσαμε:

$$x = a_1 \star \cdots \star a_i, \qquad y = a_{i+1} \star \cdots \star a_j, \qquad z = a_{j+1} \star \cdots \star a_n$$

Σημειώνουμε ότι τα x, y, z είναι μονοσήμαντα ορισμένα στοιχεία του X από την Επαγωγική Υπόθεση. Επειδή η πράξη $*$ είναι προσεταιριστική, θα έχουμε

$$x \star (y \star z) = (x \star y) \star z \qquad \text{και άρα} \qquad M = N$$ ■

Ο Γενικός Μεταθετικός Νόμος

Έστω ότι $(X, \star)$ είναι ένα μη κενό σύνολο X εφοδιασμένο με μια προσεταιριστική και μεταθετική πράξη πράξη «$\star$» επί του X. Αν $a_1, a_2, a_3 \in X$, τότε χρησιμοποιώντας την προσεταιριστική και μεταθετική ιδιότητα της πράξης «$\star$» έχουμε:

$$a_1 \star a_2 \star a_3 = a_1 \star a_3 \star a_2 = a_2 \star a_1 \star a_3 = a_3 \star a_2 \star a_1 = a_3 \star a_1 \star a_2 = a_2 \star a_3 \star a_1$$

δηλαδή όλοι οι δυνατοί συνδυασμοί στοιχείων $a_i \star a_j \star a_k$ του X, όπου i, j, k είναι οι αριθμοί $1, 2, 3$ ενδεχομένως με διαφορετική σειρά, οι οποίοι μπορούν να οριστούν με χρήση της πράξης «$\star$» και των στοιχείων a_1, a_2, a_3, ορίζουν το ίδιο στοιχείο του X. Οι 6 δυνατοί συνδυασμοί αντιστοιχούν στις 6 δυνατές μεταθέσεις του $\mathbb{N}_3$, δηλαδή στις 6 δυνατές «1-1» και «επί» απεικονίσεις $\mathbb{N}_3 \longrightarrow \mathbb{N}_3$ οι οποίες μπορούν να οριστούν από το σύνολο $\mathbb{N}_3 = \{1, 2, 3\}$ στον εαυτό του, βλέπε την Πρόταση 1.3.23. Η επόμενη πρόταση περιγράφει τι συμβαίνει στην γενική περίπτωση.

Πρόταση 1.3.15 (Ο Γενικός Μεταθετικός Νόμος). *Έστω «$\star$» μια προσεταιριστική πράξη επί του μη κενού συνόλου X, και υποθέτουμε ότι $a_1, a_2, \cdots, a_n$ είναι στοιχεία του X, έτσι ώστε: $a_i \star a_j = a_j \star a_i$, $1 \le i, j \le n$.*

Τότε για κάθε μετάθεση $\sigma \in \mathsf{S}_n$, δηλαδή για κάθε «1-1» και «επί» απεικόνιση $\sigma : \mathbb{N}_n \longrightarrow \mathbb{N}_n$, ισχύει ότι:

$$a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(n)} = a_1 \star a_2 \star \cdots \star a_n \tag{1.5}$$

Απόδειξη. Για τις ανάγκες της απόδειξης, καλούμε ένα υποσύνολο $\{a_1, a_2, \cdots, a_m\} \subseteq X$ *μεταθετικό*, αν: $a_i \star a_j = a_j \star a_i$, $1 \le i, j \le m$. Θεωρούμε το ακόλουθο σύνολο θετικών ακεραίων:

$$S = \left\{ n \in \mathbb{N} \mid \text{η (1.5) ισχύει για κάθε } \sigma \in \mathsf{S}_n \text{ και για κάθε μεταθετικό σύνολο στοιχείων } \{a_1, \cdots, a_n\} \text{ του } X \right\}$$

Το υποσύνολο $S \subseteq \mathbb{N}$ δεν είναι κενό διότι $1 \in S$. Υποθέτοντας ότι $n \in S$, θα δείξουμε ότι $n+1 \in S$. Γι' αυτόν τον λόγο θεωρούμε ένα μεταθετικό υποσύνολο $\{a_1, a_2, \cdots, a_{n+1}\} \subseteq X$, δηλαδή: $a_i \star a_j = a_j \star a_i$, $1 \le i, j \le n+1$, και έστω $\sigma \in \mathsf{S}_{n+1}$ μια μετάθεση του $\mathbb{N}_{n+1}$.

Τότε $n+1 = \sigma(t)$, για κάποιο $t \in \mathbb{N}_{n+1}$. Διακρίνουμε τις ακόλουθες περιπτώσεις:

1. Υποθέτουμε ότι $\sigma(n+1) = n+1$. Τότε προφανώς ο περιορισμός της σ στο υποσύνολο $\mathbb{N}_n \subseteq \mathbb{N}_{n+1}$ ορίζει μια μετάθεση $\tau = \sigma|_{\mathbb{N}_n}$ του $\mathbb{N}_{n+1}$, και επομένως απο την υπόθεση θα έχουμε ότι ισχύει η σχέση (1.5). Τότε χρησιμοποιώντας την προσεταιριστικότητα της πράξης «$\star$» θα έχουμε:

$$a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(n)} \star a_{\sigma(n+1)} = (a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(n)}) \star a_{\sigma(n+1)} = (a_1 \star a_2 \star \cdots \star a_n) \star a_{n+1} =$$

$$= a_1 \star a_2 \star \cdots \star a_n \star a_{n+1}$$

2. Υποθέτουμε ότι $\sigma(1) = n+1$. Τότε, θέτοντας $\tau(r) = \sigma(r+1)$, $1 \le r \le n$, αποκτούμε μια μετάθεση $\tau \in S_n$. Πράγματι $\tau(r) \neq n+1$ διότι, αν $\tau(r) = n+1$ για κάποιο $r \in \mathbb{N}_n$, τότε θα έχουμε: $\tau(r) = \sigma(r+1) = n+1 = \sigma(1)$, από όπου, επειδή η σ είναι «1-1», έπεται ότι $r+1 = 1$, το οποίο είναι άτοπο. Έτσι έχουμε μια απεικόνιση $\tau : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ η οποία είναι «1-1» διότι, αν $\tau(r) = \tau(s)$, όπου $r, s \in \mathbb{N}_n$, τότε θα έχουμε $\sigma(r+1) = \sigma(s+1)$, από όπου $r+1 = s+1$, δηλαδή $r = s$. Τότε η τ είναι προφανώς και «επί», δηλαδή $\tau \in \mathsf{S}_n$. Χρησιμοποιώντας διαδοχικά την προσεταιριστικότητα της πράξης «$\star$», την μεταθετικότητα του υποσυνόλου $\{a_1, a_2, \cdots, a_{n+1}\}$ και την επαγωγική υπόθεση $n \in S$, θα έχουμε:

$$\begin{aligned} a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(n)} \star a_{\sigma(n+1)} &= a_{\sigma(1)} \star (a_{\sigma(2)} \star \cdots \star a_{\sigma(n)} \star a_{\sigma(n+1)}) \\ &= a_{n+1} \star (a_{\tau(1)} \star \cdots \star a_{\tau(n-1)} \star a_{\tau(n)}) \\ &= a_{n+1} \star (a_1 \star \cdots \star a_{n-1} \star a_n) \\ &= a_1 \star \cdots \star a_{n-1} \star a_n \star a_{n+1} \end{aligned}$$

3. Υποθέτουμε ότι $\sigma(m) = n+1$, όπου $2 \le m \le n$. Τότε η απεικόνιση $\rho\colon \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_{n+1}$, όπου $\rho(r) = \sigma(r)$, $1 \le r \le m-1$, $\rho(r) = \sigma(r+1)$, $m \le r \le n$, και $\rho(n+1) = n+1$, είναι μια μετάθεση του $\mathbb{N}_{n+1}$, δηλαδή $\rho \in \mathsf{S}_{n+1}$, η οποία ικανοποιεί την υπόθεση της περίπτωσης 1. Επομένως θα έχουμε:

$$a_{\rho(1)} \star a_{\rho(2)} \star \cdots \star a_{\rho(n)} \star a_{\rho(n+1)} = a_1 \star a_2 \star \cdots \star a_n \star a_{n+1}$$

Τότε, χρησιμοποιώντας τον Γενικό Προσεταιριστικό Νόμο της Πρότασης 1.3.14, την μεταθετικότητα του υποσυνόλου $\{a_1, a_2, \cdots, a_{n+1}\}$, και τον ορισμό της μετάθεσης ρ, θα έχουμε:

$$\begin{aligned}
a_1 \star a_2 \star \cdots \star a_n \star a_{n+1} &= a_{\rho(1)} \star a_{\rho(2)} \star \cdots \star a_{\rho(n)} \star a_{\rho(n+1)} \\
&= (a_{\rho(1)} \star a_{\rho(2)} \star \cdots \star a_{\rho(m-1)}) \star ((a_{\rho(m)} \star a_{\rho(m+1)} \star \cdots \star a_{\rho(n)}) \star a_{\rho(n+1)}) \\
&= (a_{\rho(1)} \star a_{\rho(2)} \star \cdots \star a_{\rho(m-1)}) \star (a_{\rho(n+1)} \star (a_{\rho(m)} \star \cdots \star a_{\rho(n)}) \\
&= (a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(m-1)}) \star (a_{\sigma(m)} \star (a_{\sigma(m+1)} \star \cdots \star a_{\sigma(n+1)}) \\
&= a_{\sigma(1)} \star a_{\sigma(2)} \star \cdots \star a_{\sigma(n)} \star a_{\sigma(n+1)}
\end{aligned}$$

Επομένως σε κάθε περίπτωση ισχύει το ζητούμενο $n+1 \in S$. Από την Αρχή Μαθηματικής Επαγωγής έπεται ότι $S = \mathbb{N}$, και άρα η σχέση (1.5) ισχύει για κάθε $n \in \mathbb{N}$. ■

Δυνάμεις Στοιχείων

Θεωρούμε ένα ζεύγος $(X, \star)$, όπου X είναι ένα μη κενό σύνολο και «$\star$» είναι μια διμελής προσεταιριστική πράξη επί του X για την οποία υπάρχει ουδέτερο στοιχείο $e \in X$. Στην παρούσα υποενότητα θα ορίσουμε δυνάμεις ή ακέραια πολλαπλάσια στοιχείων του X ως προς την πράξη «$\star$» και θα αποδείξουμε βασικές ιδιότητες οι οποίες μας είναι οικείες από τις συνήθεις πράξεις πολλαπλασιασμού ή πρόσθεσης σε γνωστά σύνολα αριθμών.

Ορισμός 1.3.16. *Αν $x \in X$ και $n \ge 0$, τότε ορίζουμε την n-**οστή δύναμη** $\star^n x$ του στοιχείου x ως προς την πράξη «$\star$» ως εξής:*

$$\star^n x := \begin{cases} \underbrace{x \star x \star \cdots \star x}_{n-\text{παράγοντες}}, & \text{αν } n \ge 1 \\ e, & \text{αν } n = 0 \end{cases}$$

Αν επιπλέον το στοιχείο x έχει αντίστροφο ως προς την πράξη «$\star$» το στοιχείο $x' \in X$, και $n \ge 1$, τότε ορίζουμε:

$$\star^{-n} x := \underbrace{x' \star x' \star \cdots \star x'}_{n-\text{παράγοντες}}$$

Παρατήρηση 1.3.17. • (Πολλαπλασιαστικός Συμβολισμός) Αν ο συμβολισμός της διμελούς πράξης είναι «πολλαπλασιαστικός», δηλαδή προσομοιάζει με την συνήθη πράξη πολλαπλασιασμού σε ένα σύνολο αριθμών, οπότε χρησιμοποιούμε ως σύμβολο της διμελούς πράξης το σύμβολο «$\cdot$», τότε θα γράφουμε $\cdot^n x := x^n$ και ο ορισμός 1.3.16 παίρνει την ακόλουθη μορφή:

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \cdots \cdot x}_{n-\text{παράγοντες}}, & \text{αν } n \ge 1 \\ e, & \text{αν } n = 0 \end{cases}$$

Σημειώνουμε ότι στον πολλαπλασιαστικό συμβολισμό, συνήθως το ουδέτερο στοιχείο e συμβολίζεται με 1. Αν επιπλέον το στοιχείο x έχει αντίστροφο ως προς την πράξη «$\star$» το στοιχείο $x^{-1} \in X$, και $n \ge 1$, τότε:

$$x^{-n} := \underbrace{x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{n-\text{παράγοντες}}$$

Το στοιχείο x^n καλείται η n-**οστή δύναμη** (φυσική ή ακέραια) του x ως προς την πράξη «$\cdot$».

• (Προσθετικός Συμβολισμός) Αν ο συμβολισμός της διμελούς πράξης είναι «προσθετικός», δηλαδή προσομοιάζει με την συνήθη πράξη πρόσθεσης σε ένα σύνολο αριθμών, οπότε χρησιμοποιούμε ως σύμβολο της διμελούς πράξης το σύμβολο «+», τότε θα γράφουμε $+^n x := nx$, και ο ορισμός 1.3.16 παίρνει την ακόλουθη μορφή:

$$nx := \begin{cases} \underbrace{x+x+\cdots+x}_{n-\text{παράγοντες}}, & \text{αν } n \geq 1 \\ e, & \text{αν } n = 0 \end{cases}$$

Σημειώνουμε ότι στον προσθετικό συμβολισμό, συνήθως το ουδέτερο στοιχείο e συμβολίζεται και με 0. Αν επιπλέον το στοιχείο x έχει αντίστροφο ως προς την πράξη «$\star$» το στοιχείο $-x \in X$, και $n \geq 1$, τότε:

$$(-n)x := \underbrace{(-x)+(-x)+\cdots+(-x)}_{n-\text{παράγοντες}}$$

Το στοιχείο nx καλείται το n-**οστό πολλαπλάσιο** (φυσικό ή ακέραιο) του x ως προς την πράξη «+».

Σημειώνουμε ότι παραδοσιακά ο προσθετικός συμβολισμός για μια πράξη χρησιμοποιείται συνήθως (αλλά όχι πάντα) όταν η πράξη είναι μεταθετική. ▲

Χάριν απλότητας του συμβολισμού, στην ακόλουθη πρόταση, η οποία περιγράφει τις βασικές ιδιότητες δυνάμεων στοιχείων, χρησιμοποιούμε τον πολλαπλασιαστικό συμβολισμό για μια πράξη ορισμένη επί ενός συνόλου.

Πρόταση 1.3.18. *Έστω $(X,\cdot)$ ένα ζεύγος αποτελούμενο από ένα μη κενό σύνολο X και μια προσεταιριστική πράξη «$\cdot$» επί του X για την οποία υπάρχει ουδέτερο στοιχείο $e \in X$. Τότε για κάθε στοιχείο $x \in X$ θα έχουμε:*

1. *Ισχύει ότι: $x^{n+m} = x^n \cdot x^m$, $\forall\, n,m \in \mathbb{N}_0$. Αν το x είναι αντιστρέψιμο ως προς την πράξη «$\cdot$», τότε:*

$$\forall\, n,m \in \mathbb{Z}: \qquad x^{n+m} = x^n \cdot x^m \tag{1.6}$$

2. *Ισχύει ότι: $(x^n)^m = x^{nm}$, $\forall\, n,m \in \mathbb{N}_0$. Αν το x είναι αντιστρέψιμο ως προς την πράξη «$\cdot$», τότε:*

$$\forall\, n,m \in \mathbb{Z}: \qquad (x^n)^m = x^{nm} \tag{1.7}$$

Ιδιαίτερα αν το x είναι αντιστρέψιμο ως προς την πράξη «$\cdot$» με αντίστροφο το στοιχείο x^{-1}, τότε:

$$\forall\, n \in \mathbb{Z}: \qquad (x^n)^{-1} = x^{-n} = (x^{-1})^n \tag{1.8}$$

Απόδειξη. 1. Αν $n=0$, τότε: $x^{n+m} = x^{0+m} = x^m = x^m \cdot e = x^m \cdot x^0 = x^m \cdot x^n$. Παρόμοια βλέπουμε ότι ισχύει η ζητούμενη σχέση αν $m=0$. Επομένως μπορούμε να υποθέσουμε ότι $n,m \in \mathbb{N}$. Σταθεροποιούμε έναν τυχόντα θετικό ακέραιο n και εφαρμόζουμε την Αρχή Μαθηματικής Επαγωγής για τις τιμές του θετικού ακεραίου m. Αν $m=1$, τότε χρησιμοποιώντας τον ορισμό και την προσεταιριστικότητα της πράξης «$\cdot$» θα έχουμε:

$$x^{n+1} = \underbrace{x\cdot x\cdot \cdots \cdot x}_{(n+1)-\text{παράγοντες}} = (\underbrace{x\cdot x\cdot \cdots \cdot x}_{n-\text{παράγοντες}})\cdot x = x^n \cdot x = x^n \cdot x^1$$

Άρα η ζητούμενη σχέση (1.6) ισχύει αν $m=1$. Υποθέτοντας ότι η (1.6) ισχύει για τον θετικό ακέραιο m, δηλαδή ισχύει ότι $x^{n+m} = x^n \cdot x^m$, θα έχουμε:

$$x^{n+m+1} = \underbrace{x\cdot x\cdot \cdots \cdot x}_{(n+m+1)-\text{παράγοντες}} = (\underbrace{x\cdot x\cdot \cdots \cdot x}_{(n+m)-\text{παράγοντες}})\cdot x = (x^n \cdot x^m)\cdot x = x^n \cdot (x^m \cdot x^1) = x^n \cdot x^{m+1}$$

Επομένως η σχέση (1.6) ισχύει για κάθε $m \in \mathbb{N}$. Επειδή ο θετικός ακέραιος n ήταν τυχαίος, έπεται ότι η σχέση (1.6) ισχύει για κάθε $n,m \in \mathbb{N}_0$. Υποθέτουμε τώρα ότι το στοιχείο x είναι αντιστρέψιμο με αντίστροφο το στοιχείο x^{-1}, και έστω $n \geq 1$. Τότε εξ ορισμού $x^{-n} = x^{-1}\cdot x^{-1}\cdot\cdots\cdot x^{-1} = (x^{-1})^n$. Επειδή

$$\begin{aligned} x^{-n}\cdot x^n &= \underbrace{x^{-1}\cdot x^{-1}\cdot\cdots\cdot x^{-1}}_{(n)-\text{παράγοντες}}\cdot \underbrace{x\cdot x\cdot\cdots\cdot x}_{(n)-\text{παράγοντες}} = \underbrace{x^{-1}\cdot x^{-1}\cdot\cdots\cdot x^{-1}}_{(n-1)-\text{παράγοντες}}\cdot e\cdot \underbrace{x\cdot x\cdot\cdots\cdot x}_{(n-1)-\text{παράγοντες}} \\ &= \underbrace{x^{-1}\cdot x^{-1}\cdot\cdots\cdot x^{-1}}_{(n-1)-\text{παράγοντες}}\cdot \underbrace{x\cdot x\cdot\cdots\cdot x}_{(n-1)-\text{παράγοντες}} = \cdots = x^{-1}\cdot x = e \end{aligned}$$

και επειδή παρόμοια έχουμε $x^n \cdot x^{-n} = e$, έπεται ότι: $x^{-n} = (x^{-1})^n = (x^n)^{-1}$.

Τέλος, δείχνουμε ότι $x^{n+m} = x^n \cdot x^m$, $\forall n, m \in \mathbb{Z}$. Έχουμε ήδη δείξει την ζητούμενη σχέση όταν $n, m \geq 0$. Έτσι μένουν οι ακόλουθες περιπτώσεις:

(α') Υποθέτουμε πρώτα ότι $n < 0$ και $m \geq 0$. Τότε $n = -k$, όπου $k \geq 1$. Αν $k \leq m$, τότε $m = k + l$ για κάποιο $l \geq 0$, και τότε:

$$x^n \cdot x^m = x^{-k} \cdot x^m = (x^k)^{-1} \cdot x^m = (x^k)^{-1} \cdot x^{k+l} = (x^k)^{-1} \cdot x^k \cdot x^l = e \cdot x^l = x^l = x^{-k+m} = x^{n+m}$$

Αν $k > m$, οπότε $k = l + m$ για κάποιο $l \geq 1$, τότε, επειδή

$$(x^{l+m})^{-1} = \underbrace{x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{(l+m)-\text{παράγοντες}} = \underbrace{x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{l-\text{παράγοντες}} \cdot \underbrace{x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{m-\text{παράγοντες}} = (x^l)^{-1} \cdot (x^m)^{-1}$$

θα έχουμε:

$$x^n \cdot x^m = x^{-k} \cdot x^m = (x^k)^{-1} \cdot x^m = (x^{l+m})^{-1} \cdot x^m = (x^l)^{-1} \cdot (x^m)^{-1} \cdot x^m = (x^l)^{-1} \cdot e = x^{-l} = x^{-k+m} = x^{n+m}$$

(β') Αν $n \geq 0$ και $m < 0$, τότε εργαζόμαστε ανάλογα όπως στο (α').

(γ') Αν $n, m \leq 0$, τότε $n = -k$ και $m = -l$ για κάποιους μη αρνητικούς ακεραίους k, l. Τότε χρησιμοποιώντας την Πρόταση 1.3.7 θα έχουμε:

$$x^n \cdot x^m = x^{-k} \cdot x^{-l} = (x^k)^{-1} \cdot (x^l)^{-1} = (x^l \cdot x^k)^{-1} = (x^{l+k})^{-1} = x^{-k-l} = x^{n+m}$$

2. Αν $n = 0 = m$, τότε $(x^n)^m = (x^0)^0 = e^0 = e = e^{0 \cdot 0} = x^{n \cdot m}$. Αν $n = 0$ και $m \geq 1$, τότε, επειδή προφανώς $e^k = e \cdot e \cdot \cdots \cdot e = e$ (k-παράγοντες), $\forall k \geq 1$, θα έχουμε: $(x^n)^m = (x^0)^m = e^m = e = x^0 = x^{0 \cdot m} = x^{n \cdot m}$. Αν $n \geq 1$ και $m = 0$, τότε $(x^n)^m = (x^n)^0 = e = x^0 = x^{n \cdot 0} = x^{n \cdot m}$. Σταθεροποιούμε τώρα έναν τυχόντα θετικό ακέραιο n και εφαρμόζουμε την Αρχή Μαθηματικής Επαγωγής για τις τιμές του θετικού ακεραίου m. Αν $m = 1$, τότε $(x^n)^m = (x^n)^1 = x^n = x^{n \cdot 1} = x^{n \cdot m}$, και άρα η ζητούμενη σχέση (1.7) ισχύει αν $m = 1$. Υποθέτοντας ότι η (1.7) ισχύει για τον θετικό ακέραιο m, δηλαδή ισχύει ότι $x^{n+m} = x^n \cdot x^m$, και χρησιμοποιώντας τον ορισμό και την προσεταιριστικότητα της πράξης «$\cdot$», από το μέρος 1. θα έχουμε:

$$(x^n)^{m+1} = (x^n)^m \cdot (x^n)^1 = x^{n \cdot m} \cdot x^{n \cdot 1} = x^{n \cdot m + n} = x^{n \cdot (m+1)}$$

Επομένως η σχέση (1.7) ισχύει για κάθε $m \in \mathbb{N}$.

Υποθέτουμε τώρα ότι το στοιχείο x είναι αντιστρέψιμο με αντίστροφο το στοιχείο x^{-1}, και έστω $n \geq 1$. Θα δείξουμε τη σχέση $(x^n)^m = x^{nm}$, για κάθε $n, m \in \mathbb{Z}$. Έχουμε δείξει την ζητούμενη σχέση όταν $n, m \geq 0$, και άρα μένουν οι ακόλουθες περιπτώσεις:

(α') Αν $n < 0$ και $m \geq 0$, τότε $n = -k$ για κάποιο $k > 0$. Με χρήση του μέρους 1., θα έχουμε:

$$(x^n)^m = (x^{-k})^m = ((x^{-1})^k)^m = (x^{-1})^{k \cdot m} = x^{-(k \cdot m)} = x^{(-k) \cdot m} = x^{n \cdot m}$$

(β') Αν $n \geq 0$ και $m < 0$, τότε $m = -k$ για κάποιο $k > 0$. Με χρήση του μέρους 1., θα έχουμε:

$$(x^n)^m = (x^n)^{-k} = ((x^n)^k)^{-1} = (x^{n \cdot k})^{-1} = x^{-(n \cdot k)} = x^{n \cdot (-k)} = x^{n \cdot m}$$

(γ') Αν $n < 0$ και $m < 0$, τότε $n = -k$ και $m = -l$ για κάποια $k, l > 0$. Με χρήση του μέρους (β') θα έχουμε:

$$(x^n)^m = (x^{-k})^{-l} = ((x^{-1})^k)^{-l} = (x^{-1})^{k \cdot (-l)} = x^{-(k \cdot (-l))} = x^{(-k) \cdot (-l)} = x^{n \cdot m}$$ ■

Συνδυάζοντας τις Πρότασεις 1.3.15 και 1.3.18, προκύπτει εύκολα το ακόλουθο χρήσιμο αποτέλεσμα.

Πόρισμα 1.3.19. *Έστω $(X,\cdot)$ ένα ζεύγος αποτελούμενο από ένα μη κενό σύνολο X και μια προσεταιριστική πράξη «$\cdot$» επί του X για την οποία υπάρχει ουδέτερο στοιχείο $e \in X$. Αν $x, y \in X$ και ισχύει $x \cdot y = y \cdot x$, τότε:*

$$(x \cdot y)^n = x^n \cdot y^n \tag{1.9}$$

για κάθε $n = 0, 1, 2, \cdots$. Αν τα στοιχεία x, y είναι αντιστρέψιμα ως προς την πράξη «$\cdot$», τότε η σχέση (1.9) ισχύει για κάθε $n \in \mathbb{Z}$.

Παρατήρηση 1.3.20. Χρησιμοποιώντας προσθετικό συμβολισμό «+» για μια προσεταιριστική πράξη επί ενός συνόλου X, για την οποία υπάρχει ουδέτερο στοιχείο, η Πρόταση 1.3.18 και το Πόρισμα 1.3.19 παίρνουν την ακόλουθη μορφή:

1. Ισχύει ότι: $(n+m)x = nx + mx$, $\forall n, m \in \mathbb{N}_0$. Αν το x είναι αντιστρέψιμο ως προς την πράξη «+», τότε: $(n+m)x = nx + mx$, $\forall n, m \in \mathbb{Z}$.
2. Ισχύει ότι: $n(mx) = (nm)x$, $\forall n, m \in \mathbb{N}_0$. Αν το x είναι αντιστρέψιμο ως προς την πράξη «+», τότε: $n(mx) = (nm)x$, $\forall n, m \in \mathbb{Z}$.
3. Αν το x είναι αντιστρέψιμο ως προς την πράξη «+» με αντίστροφο το στοιχείο $-x$, τότε: $-(nx) = (-n)x = n(-x)$, $\forall n \in \mathbb{Z}$.
4. Αν $x + y = y + x$, τότε[12] $n(x+y) = nx + ny$, $\forall n \in \mathbb{N}_0$. Αν επιπλέον τα στοιχεία x, y είναι αντιστρέψιμα ως προς την πράξη «+», τότε η παραπάνω σχέση ισχύει για κάθε $n \in \mathbb{Z}$. ▲

1.3.4 Σύνολα Μεταθέσεων

Στην παρούσα ενότητα θα εισαγάγουμε και θα αναλύσουμε εν συντομία ένα σημαντικό παράδειγμα αλγεβρικής δομής η οποία βασίζεται σε μετασχηματισμούς στοιχείων ενός συνόλου, και η οποία, όπως θα δούμε αργότερα, αποτελεί πρότυπο για αλγεβρικές δομές παρόμοιου τύπου.

Έστω X ένα μη κενό σύνολο και θεωρούμε το σύνολο

$$\mathsf{S}(X) = \{f : X \longrightarrow X \mid f : \text{«1-1» και «επί»}\}$$

Ορισμός 1.3.21. *Τα στοιχεία του συνόλου $\mathsf{S}(X)$ καλούνται* **μεταθέσεις** *του συνόλου X. Η σύνθεση $\sigma \circ \tau$ απεικονίσεων $\sigma, \tau \in \mathsf{S}(X)$ καλείται* **γινόμενο των μεταθέσων** *σ και τ και συμβολίζεται με $\sigma \cdot \tau$ ή απλά $\sigma\tau$. Επίσης, από τώρα και στο εξής, το σύνολο $\mathsf{S}(\mathbb{N}_n)$ θα συμβολίζεται με:*

$$\mathsf{S}_n := \mathsf{S}(\mathbb{N}_n) = \{\sigma : \mathbb{N}_n \longrightarrow \mathbb{N}_n \mid \sigma : \text{«1-1» και «επί»}\}$$

Αν f, g είναι δύο μεταθέσεις του συνόλου X, τότε, επειδή η σύνθεση «1-1» και «επί» απεικονίσεων είναι «1-1» και «επί» απεικόνιση, έπεται ότι το γινόμενο $f \cdot g = f \circ g$ των μεταθέσεων f και g είναι επίσης μετάθεση του συνόλου X και επομένως $f \circ g \in \mathsf{S}(X)$. Με άλλα λόγια, ορίζεται η πράξη

$$\cdot : \mathsf{S}(X) \times \mathsf{S}(X) \longrightarrow \mathsf{S}(X), \quad (f, g) \longmapsto f \cdot g = f \circ g$$

Το επόμενο Πόρισμα συνοψίζει τις βασικές ιδιότητες της αλγεβρικής δομής $(\mathsf{S}(X), \cdot)$, όπως αυτές προκύπτουν από την υποενότητα 0.2.1.

Πόρισμα 1.3.22. *Έστω X ένα μη κενό σύνολο και έστω $\mathsf{S}(X)$ το σύνολο μεταθέσεων επί του X. Τότε στο ζεύγος $(\mathsf{S}(X), \circ)$ η πράξη «$\circ$» της σύνθεσης απεικονίσεων ικανοποιεί τις ακόλουθες ιδιότητες:*

(α) *Η πράξη «$\circ$» είναι προσεταιριστική. Η πράξη «$\circ$» είναι μεταθετική αν και μόνο αν $|X| \leq 2$.*

[12] Προσοχή: η προσθετική εκδοχή της σχέσης (1.9) **δεν είναι** η σχέση $(x+y)^n = x^n + y^n$ η οποία γενικά δεν είναι αληθής.

(β) *Υπάρχει ουδέτερο στοιχείο για την πράξη «∘», η ταυτοτική απεικόνιση* $\mathsf{Id}_X \in \mathsf{S}(X)$, *και*

(γ) *κάθε στοιχείο του συνόλου* $\mathsf{S}(X)$ *είναι αντιστρέψιμο ως προς την πράξη «∘».*

Η ακόλουθη Πρόταση προσδιορίζει το πλήθος των στοιχείων του συνόλου μεταθέσεων $\mathsf{S}(X)$ του πεπερασμένου συνόλου X.

Πρόταση 1.3.23. *Έστω X ένα μη-κενό πεπερασμένο σύνολο. Τότε $|\mathsf{S}(X)| < \infty$, και μάλιστα:*

$$|X| = n \quad \Longrightarrow \quad |\mathsf{S}(X)| = n!$$

Απόδειξη. Έστω $X = \{x_1, x_2, \cdots, x_n\}$ και $f\colon X \longrightarrow X$ μια «1-1» και «επί» απεικόνιση. Επειδή η f είναι «1-1», τα στοιχεία $f(x_1), f(x_2), \cdots, f(x_n)$ του X είναι ανά δύο διαφορετικά, και επομένως είναι τα στοιχεία $x_1, x_2, \cdots, x_n$, ενδεχομένως με διαφορετική σειρά. Οι δυνατές τιμές τις οποίες μπορεί να λάβει το στοιχείο $f(x_1)$ είναι οποιαδήποτε εκ των $x_1, x_2, \cdots, x_n$, και άρα υπάρχουν n το πληθος επιλογές για το $f(x_1)$. Έχοντας επιλέξει το στοιχείο $f(x_1)$, οι δυνατές τιμές τις οποίες μπορεί να λάβει το στοιχείο $f(x_2)$ είναι οποιαδήποτε εκ των $x_1, x_2, \cdots, x_n$, με εξαίρεση την τιμή $f(x_1)$ διότι, αν $f(x_2) = f(x_1)$, τότε, επειδή η f είναι «1-1», έπεται ότι $x_1 = x_2$ το οποίο είναι άτοπο. Άρα υπάρχουν $n-1$ το πληθος επιλογές για το $f(x_2)$, και τότε υπάρχουν $n \cdot (n-1)$ δυνατές επιλογές για να οριστούν τα στοιχεία $f(x_1)$ και $f(x_2)$. Συνεχίζοντας αυτή την διαδικασία, έχοντας επιλέξει τα στοιχεία $f(x_1), f(x_2), \cdots, f(x_k)$, και υπάρχουν $n \cdot (n-1) \cdots (n-(k-1))$ τέτοιες επιλογές, το στοιχείο $f(x_{k+1})$ μπορεί να επιλεγεί να είναι οποιοδήποτε από τα στοιχεία $x_1, x_2, \cdots, x_n$, με εξαίρεση τις τιμές $f(x_1), f(x_2), \cdots, f(x_k)$, πάλι επειδή η f είναι «1-1». Τέτοιες επιλογές υπάρχουν σε πλήθος $n-k$, και επομένως υπάρχουν σε πλήθος $n \cdot (n-1) \cdots (n-k+1) \cdot (n-k)$ τέτοιες επιλογές. Έτσι μετά από $n-1$ το πλήθος βήματα, έχοντας επιλέξει τα στοιχεία $f(x_1), f(x_2), \cdots, f(x_{n-1})$, και υπάρχουν $n \cdot (n-1) \cdots (n-k) \cdots (n-(n-2)) = n \cdot (n-1) \cdots (n-k) \cdots 2$ τέτοιες επιλογές, υπάρχει μόνο μία επιλογή για το $f(x_n)$ η οποία είναι το στοιχείο του μονοσυνόλου $X \setminus \{f(x_1), f(x_2), \cdots, f(x_{n-1})\}$. Επομένως, συνοψίζοντας, για να οριστεί η τυχούσα «1-1» και «επί» απεικόνιση f, υπάρχουν $n \cdot (n-1) \cdots 2 \cdot 1 = n!$ διαφορετικοί τρόποι. Αυτό σημαίνει ότι το πλήθος των στοιχείων του συνολου $\mathsf{S}(X)$ είναι $|\mathsf{S}(X)| = n!$. ■

Το επόμενο αποτέλεσμα δείχνει ότι το σύνολο $\mathsf{S}(X)$ των μεταθέσεων του συνόλου X εξαρτάται ουσιαστικά μόνο από το πλήθος και όχι την φύση των στοιχείων του συνόλου X, με την ακόλουθη έννοια: αν Y είναι ένα άλλο σύνολο ίσου πλήθους στοιχείων με το X, τότε τα σύνολα των μεταθέσεων $\mathsf{S}(X)$ και $\mathsf{S}(Y)$ είναι σε «1-1» και «επί» αντιστοιχία μέσω της οποίας διατηρείται η σύνθεση απεικονίσεων.

Πρόταση 1.3.24. *Έστω X και Y δύο μη κενά σύνολα, και υποθέτουμε ότι $|X| = |Y|$. Τότε $|\mathsf{S}(X)| = |\mathsf{S}(Y)|$. Αναλυτικότερα, αν $\varphi\colon X \longrightarrow Y$ είναι μια «1-1» και «επί» απεικόνιση, τότε η απεικόνιση*

$$\Phi : \mathsf{S}(X) \longrightarrow \mathsf{S}(Y), \quad \Phi(f) = \varphi \circ f \circ \varphi^{-1}$$

είναι «1-1» και «επί», και επιπλέον η Φ διατηρεί την σύνθεση απεικονίσεων, δηλαδή $\forall f, g \in \mathsf{S}(X)$:

$$\Phi(f \circ g) = \Phi(f) \circ \Phi(g)$$

Απόδειξη. Επειδή $|X| = |Y|$, έπεται ότι υπάρχει μια «1-1» και «επί» απεικόνιση $\varphi\colon X \longrightarrow Y$. Ορίζουμε μια απεικόνιση:

$$\Phi\colon \mathsf{S}(X) \longrightarrow \mathsf{S}(Y), \quad \Phi(f) = \varphi \circ f \circ \varphi^{-1}$$

Δηλαδή η απεικόνιση Φ στέλνει την «1-1» και «επί» απεικόνιση $f\colon X \longrightarrow X$ στην απεικόνιση $\Phi(f)\colon Y \longrightarrow Y$ η οποία ορίζεται ως η εξής σύνθεση:

$$\begin{array}{ccc} Y & \overset{\Phi(f)}{\dashrightarrow} & Y \\ {\scriptstyle \varphi^{-1}}\downarrow & & \uparrow{\scriptstyle \varphi} \\ X & \xrightarrow{\quad f \quad} & X \end{array}$$

1. *Η Φ είναι καλά ορισμένη*: Έστω $f \in \mathsf{S}(X)$. Θα δείξουμε ότι η απεικόνιση $\Phi(f)$ ανήκει στο σύνολο $\mathsf{S}(Y)$, δηλαδή είναι «1-1» και «επί». Αυτό όμως είναι άμεσο, διότι $\Phi(f) = \varphi \circ f \circ \varphi^{-1}\colon Y \longrightarrow Y$ είναι «1-1» και «επί» ως σύνθεση απεικονίσεων οι οποίες είναι «1-1» και «επί».

2. *Η Φ είναι «1-1»*: Έστω $f,g\in \mathsf{S}(X)$, και υποθέτουμε ότι $\Phi(f)=\Phi(g)$. Τότε, χρησιμοποιώντας την προσεταιριστική ιδιότητα της σύνθεσης απεικονίσεων και την Πρόταση 0.2.8, συνθέτοντας από αριστερά με την φ^{-1} και από τα δεξιά με την φ, θα έχουμε:

$$\Phi(f)=\Phi(g) \implies \varphi\circ f\circ\varphi^{-1}=\varphi\circ g\circ\varphi^{-1} \implies \varphi^{-1}\circ\varphi\circ f\circ\varphi^{-1}=\varphi^{-1}\circ\varphi\circ g\circ\varphi^{-1} \implies \mathsf{Id}_Y\circ f\circ\varphi^{-1}=\mathsf{Id}_Y\circ g\circ\varphi^{-1}$$

$$\implies f\circ\varphi^{-1}=g\circ\varphi^{-1} \implies f\circ\varphi^{-1}\circ\varphi=g\circ\varphi^{-1}\circ\varphi \implies f\circ\mathsf{Id}_X=g\circ\mathsf{Id}_X \implies f=g$$

Επομένως η Φ είναι «1-1».

3. *Η Φ είναι «επί»*: Αν $h\colon Y\longrightarrow Y$ είναι μια «1-1» και «επί» απεικόνιση, δηλαδή είναι ένα στοιχείο του συνόλου $\mathsf{S}(Y)$, τότε θεωρούμε την απεικόνιση

$$\varphi^{-1}\circ h\circ\varphi\colon X\longrightarrow X$$

η οποία είναι «1-1» και «επί» ως σύνθεση απεικονίσεων οι οποίες είναι «1-1» και «επί», και άρα ανήκει στο σύνολο $\mathsf{S}(X)$. Επιπλέον

$$\Phi(\varphi^{-1}\circ h\circ\varphi)=\varphi\circ\varphi^{-1}\circ h\circ\varphi\circ\varphi^{-1}=h$$

Επομένως η απεικόνιση Φ είναι «επί».

4. *Η Φ διατηρεί τη σύνθεση*: Έστω $f,g\in\mathsf{S}(X)$. Τότε:

$$\Phi(f\circ g)=\varphi\circ(f\circ g)\circ\varphi^{-1}=\varphi\circ f\circ g\circ\varphi^{-1}=\varphi\circ f\circ\mathrm{Id}_X\circ g\circ\varphi^{-1}=$$

$$=\varphi\circ f\circ\varphi^{-1}\circ\varphi\circ g\circ\varphi^{-1}=\Phi(f)\circ\Phi(g)$$

Επομένως η απεικόνιση $\Phi\colon\mathsf{S}(X)\longrightarrow\mathsf{S}(Y)$ είναι «1-1» και «επί» και διατηρεί την πράξη της σύνθεσης απεικονίσεων. ■

Πόρισμα 1.3.25. *Έστω X ένα σύνολο με n το πλήθος στοιχεία: $|X|=n$, και έστω $\varphi\colon X\longrightarrow\mathbb{N}_n$ μια «1-1» και «επί» απεικόνιση. Τότε η απεικόνιση $\Phi\colon\mathsf{S}(X)\longrightarrow\mathsf{S}(\mathbb{N}_n)=\mathsf{S}_n$, $\Phi(f)=\varphi\circ f\circ\varphi^{-1}$ είναι «1-1» και «επί», και επιπλέον η Φ διατηρεί τη σύνθεση απεικονίσεων, δηλαδή $\forall\, f\in\mathsf{S}(X)$: $\Phi(f\circ g)=\Phi(f)\circ\Phi(g)$.*

Παρατήρηση 1.3.26. Έστω $X=\{x_1,x_2,\cdots,x_n\}$ ένα σύνολο με n το πλήθος στοιχεία. Τότε προφανώς η απεικόνιση $\varphi\colon X\longrightarrow\mathbb{N}_n$, $\varphi(x_i)=i$ είναι «1-1» και «επί». Μέσω της «1-1» και «επί» απεικόνισης $\Phi\colon\mathsf{S}(X)\longrightarrow\mathsf{S}_n$, $\Phi(f)=\varphi\circ f\circ\varphi^{-1}$ η οποία διατηρεί την σύνθεση απεικονίσεων, όλες οι βασικές ιδιότητες της άλγεβρας απεικονίσεων επί του συνόλου X μεταφέρονται στις αντίστοιχες ιδιότητες της άλγεβρας απεικονίσεων επί του συνόλου $\mathbb{N}_n=\{1,2,\cdots,n\}$. Αυτή η παρατήρηση θα διαδραματίσει σημαντικό ρόλο στην βαθύτερη μελέτη και ανάλυση ιδιοτήτων που αφορούν σύνολα μεταθέσεων επί πεπερασμένων συνόλων. ▲

Συμβολισμός 1.3.27. Όπως θα δούμε αργότερα, για την περαιτέρω ανάπτυξη της θεωρίας μεταθέσεων επί ενός συνόλου, είναι απαραίτητη η χρήση όσο γίνεται απλούστερου συμβολισμού. Εδώ θα αναλύσουμε εν συντομία δύο βασικούς συμβολισμούς μεταθέσεων: (α) τον συμβολισμό με χρήση πινάκων και (β) τον κυκλικό συμβολισμό.

(**a**) Αν $\sigma\in\mathsf{S}_n$ είναι μια μετάθεση του συνόλου $\mathbb{N}_n=\{1,2,\cdots,n\}$, τότε είναι χρήσιμο για λόγους εποπτείας να παριστάνουμε την «1-1» και «επί» απεικόνιση

$$\sigma\colon\{1,2,\cdots,n\}\longrightarrow\{1,2,\cdots,n\},\quad i\longmapsto\sigma(i)$$

με έναν $2\times n$ πίνακα

$$\sigma=\begin{pmatrix}1 & 2 & \cdots & i & \cdots & n-1 & n\\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(n-1) & \sigma(n)\end{pmatrix}$$

του οποίου η πρώτη γραμμή περιέχει τα στοιχεία του συνόλου $\mathbb{N}_n$ και η δεύτερη γραμμή περιέχει τις εικόνες των στοιχείων αυτών μέσω της μετάθεσης σ.

Για παράδειγμα, έχουμε τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in \mathsf{S}_3, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in \mathsf{S}_5, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 2 & 5 & 8 & 7 \end{pmatrix} \in \mathsf{S}_8$$

Για την μετάθεση σ έχουμε: $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 2$, και παρόμοια για τις μεταθέσεις ρ και τ.

Έστω $\sigma, \tau \in \mathsf{S}_n$. Τότε για το γινόμενο $\sigma \cdot \tau$ των μεταθέσεων σ και τ, δηλαδή για τη σύνθεση των απεικονίσεων σ και τ, όπου πρώτα εφαρμόζουμε τη συνάρτηση τ, θα έχουμε

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix} \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \tau(1) & \tau(2) & \cdots & \tau(n-1) & \tau(n) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n-1)) & \sigma(\tau(n)) \end{pmatrix}$$

Για παράδειγμα:

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$$

Η ταυτοτική μετάθεση, δηλαδή η ταυτοτική απεικόνιση $\mathrm{Id}_{\mathbb{N}_n}$, συμβολίζεται συνήθως με ι και είναι η

$$\iota = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$$

(**b**) Αν $\{a_1, a_2, \cdots, a_k\} \subseteq \{1, 2, \cdots, n\}$, όπου $1 \leq k \leq n$, είναι ένα υποσύνολο του $\mathbb{N}_n$ με k το πλήθος στοιχεία, τότε καλούμε k-**κύκλο** των στοιχείων $a_1, a_2, \cdots, a_n$ με αυτή τη σειρά αναγραφής, την μετάθεση $\sigma \in \mathsf{S}_n$ η οποία μεταθέτει κυκλικά τα στοιχεία $a_1, a_2, \cdots, a_k$, και διατηρεί σταθερά τα υπόλοιπα στοιχεία του συνόλου $\{1, 2, , \cdots, n\}$:

$$\sigma(a_k) = \begin{cases} a_{k+1}, & \text{αν } 1 \leq k \leq n-1 \\ a_1, & \text{αν } k = n \end{cases} \qquad \text{και} \qquad \sigma(x) = x, \quad \text{αν } x \in \{1, 2, \cdots, n\} \setminus \{a_1, a_2, \cdots, a_k\}$$

Ο k-κύκλος σ των στοιχείων $\{a_1, a_2, \cdots, a_k\}$ συμβολίζεται ως εξής:

$$\sigma = \begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \end{pmatrix}$$

δηλαδή παραλείπονται τα στοιχεία x του συνόλου $\{1, 2, \cdots, n\} \setminus \{a_1, a_2, \cdots, a_k\}$ τα οποία παραμένουν σταθερά από την μετάθεση σ (φυσικά τα στοιχεία αυτά υπονοούνται χωρίς να αναφέρονται στον συμβολισμό). Δύο κύκλοι, ο k-κύκλος $\begin{pmatrix} a_1 & a_2 & \cdots & a_{k-1} & a_k \end{pmatrix}$ και ο l-κύκλος $\begin{pmatrix} b_1 & b_2 & \cdots & b_{l-1} & b_l \end{pmatrix}$, καλούνται **ξένοι κύκλοι**, αν $\{a_1, a_2, \cdots, a_k\} \bigcap \{b_1, b_2, \cdots, b_l\} = \emptyset$.

Χρησιμοποιώντας τον κυκλικό συμβολισμό, θα αναλύσουμε τις μεταθέσεις σ, ρ και τ, ως γινόμενα ξένων κύκλων. Η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in \mathsf{S}_3$ μεταθέτει κυκλικά τα στοιχεία 1,3,2 (με αυτή τη σειρά), και άρα: $\sigma = (132)$. Στην μετάθεση $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \in \mathsf{S}_5$ περιέχονται δύο κύκλοι: ο 2-κύκλος $\rho_1 = (12)$ ο οποίος μεταθέτει τα στοιχεία 1,2 (με αυτή τη σειρά) και διατηρεί σταθερά τα υπόλοιπα, και ο 3-κύκλος $\rho_2 = (345)$ ο οποίος μεταθέτει κυκλικά τα στοιχεία 3,4,5 (με αυτή τη σειρά) και διατηρεί σταθερά τα υπόλοιπα. Παρατηρούμε ότι η μετάθεση ρ γράφεται ως γινόμενο ξένων κύκλων: $\rho = \rho_1 \circ \rho_2 = (12) \circ (345)$. Στη μετάθεση $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 2 & 5 & 8 & 7 \end{pmatrix} \in \mathsf{S}_8$ περιέχονται τρεις κύκλοι: ο 2-κύκλος $\tau_1 = (13)$ ο οποίος μεταθέτει κυκλικά τα στοιχεία 1,3 (με αυτή τη σειρά) και διατηρεί σταθερά τα υπόλοιπα, ο 4-κύκλος $\tau_2 = (2465)$ ο οποίος μεταθέτει κυκλικά τα στοιχεία 1,3 (με αυτή τη σειρά) και διατηρεί σταθερά τα υπόλοιπα, και ο 2-κύκλος $\tau_3 = (78)$ ο οποίος μεταθέτει κυκλικά τα στοιχεία 7,8 (με αυτή τη σειρά) και διατηρεί

σταθερά τα υπόλοιπα. Παρατηρούμε ότι η μετάθεση τ γράφεται ως γινόμενο ξένων κύκλων: $\tau = \tau_1 \circ \tau_2 \circ \tau_3 = (13) \circ (2465) \circ (78)$. Επομένως οι μεταθέσεις σ, ρ και τ γράφονται χρησιμοποιώντας κυκλικό συμβολισμό ως εξής:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}, \qquad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 2 & 5 & 8 & 7 \end{pmatrix} = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 & 6 & 5 \end{pmatrix} \circ \begin{pmatrix} 7 & 8 \end{pmatrix}$$

Όπως θα δούμε σε μεταγενέστερο κεφάλαιο, κάθε μετάθεση μπορεί να γραφεί μοναδικά ως γινόμενο ξένων κύκλων. ▲

1.3.5 Επαγόμενες Πράξεις

Έστω «$*$» μια (διμελής) πράξη επί ενός μη κενού συνόλου X. Αν S είναι ένα μη κενό υποσύνολο του X, τότε για κάθε δύο στοιχεία s_1, s_2 του υποσυνόλου S, το στοιχείο $s_1 \star s_2 \in X$, δεν είναι απαραίτητα στοιχείο του S. Για παράδειγμα, αν θεωρήσουμε την πράξη της αφαίρεσης $- : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $(n, m) \longmapsto n - m$, επί του συνόλου των ακεραίων $\mathbb{Z}$, και αν $S = \mathbb{N}$, τότε $3, 5 \in \mathbb{N}$, αλλά $3 - 5 = -2 \notin \mathbb{N}$.

Το υποσύνολο S του X είναι **κλειστό στην πράξη** «$\star$» επί του X, αν:

$$\forall s_1, s_2 \in S: \quad s_1 \star s_2 \in S$$

Πρόταση 1.3.28. *Έστω «$*$» μια πράξη επί ενός μη κενού συνόλου X, και S ένα μη κενό υποσύνολο του X, το οποίο είναι κλειστό στην πράξη «$*$». Τότε η πράξη «$*$» επάγει μια πράξη «$\star_S$» επί του συνόλου S ως εξής:*

$$\forall s_1, s_2 \in S: \quad s_1 \star_S s_2 = s_1 \star s_2$$

Επιπλέον:

1. *Αν η πράξη «$\star$» επί του X είναι προσεταιριστική ή μεταθετική, τότε η πράξη «$\star_S$» επί του S είναι προσεταιριστική ή μεταθετική αντίστοιχα.*
2. *Έστω $e \in X$ ένα ουδέτερο στοιχείο για την πράξη «$\star$» επί του X. Αν $e \in S$, τότε το e είναι ουδέτερο στοιχείο για την πράξη «$\star_S$» επί του S.*
3. *Υποθέτουμε ότι η πράξη «$\star$» έχει ένα ουδέτερο στοιχείο $e \in X$ έτσι ώστε $e \in S$, και έστω x ένα στοιχείο του S για το οποίο υπάρχει ένα αντίστροφο στοιχείο $x' \in X$ για την πράξη «$\star$» επί του X. Αν $x' \in S$, τότε το στοιχείο x' είναι ένα αντίστροφο στοιχείο του x για την πράξη «$\star_S$» επί του S.*

Απόδειξη. Επειδή το υποσύνολο S είναι κλειστό στην πράξη «$\star$», θέτοντας $s_1 \star_S s_2 = s_1 \star s_2$, $\forall s_1, s_2 \in S$, ορίζεται μια πράξη «$\star_S$» επί του S. Από τον τρόπο ορισμού της η πράξη «$\star_S$» επί του S είναι προσεταιριστική ή μεταθετική, αν η πράξη «$\star$» επί του X είναι προσεταιριστική ή μεταθετική αντίστοιχα. Έστω ότι η πράξη «$\star$» επί του X έχει ουδέτερο στοιχείο e και υποθέτουμε ότι $e \in S$. Τότε προφανώς $s \star_S e = s \star e = s = e \star s = e \star_S s$, $\forall s \in S$, και άρα το στοιχείο e είναι ουδέτερο στοιχείο για την πράξη «$\star_S$» επί του S. Τέλος, έστω ότι η πράξη «$\star$» έχει ένα ουδέτερο στοιχείο $e \in X$ έτσι ώστε $e \in S$, και έστω s ένα στοιχείο του S για το οποίο υπάρχει ένα αντίστροφο στοιχείο $s' \in X$. Αν $s \in S$, τότε: $s \star_S s' = s \star s' = e = s' \star s = s' \star_S s$, από όπου έπεται ότι το στοιχείο s' είναι αντίστροφο του στοιχείου s ως προς την πράξη $\star_S$ επί του S. ■

Η πράξη «$\star_S$» της Πρότασης 1.3.28 καλείται η **επαγόμενη πράξη** επί του S, και στο εξής θα συμβολίζεται απλά με το ίδιο σύμβολο «$\star$».

Παράδειγμα 1.3.29 (Παραδείγματα επαγόμενων πράξεων)**.**

1. Θεωρούμε το ζεύγος $(\mathbb{C}, \star)$, όπου «$\star$» είναι είτε η συνήθης πρόσθεση ή ο συνήθης πολλαπλασιασμός μιγαδικών αριθμών. Τότε το υποσύνολο $\mathbb{K} \subseteq \mathbb{C}$, όπου $\mathbb{K}$ είναι ένα εκ των $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, είναι κλειστό στην πράξη «$\star$».

2. Έστω $\mathsf{M}_n(\mathbb{K})$ το σύνολο των $n\times n$ πινάκων με στοιχεία από το σύνολο $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένα εκ των $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, το οποίο θεωρούμε εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού τετραγωνικών πινάκων όπως στο μέρος 6 του Παραδείγματος 1.3.8. Θεωρούμε το υποσύνολο $n\times n$ **άνω τριγωνικών πινάκων** με στοιχεία από το $\mathbb{K}$:

$$\mathsf{AT}_n(\mathbb{K}) = \{A=(a_{ij})\in \mathsf{M}_n(\mathbb{K}) \mid a_{ij}=0,\ 1\le j<i\le n\} \quad \text{δηλαδή} \quad A=(a_{ij})=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ 0 & a_{22} & \cdots & a_{2n}\\ \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & \cdots & a_{nn}\end{pmatrix}$$

και το υποσύνολο $n\times n$ **κάτω τριγωνικών πινάκων** με στοιχεία από το $\mathbb{K}$:

$$\mathsf{KT}_n(\mathbb{K}) = \{A=(a_{ij})\in \mathsf{M}_n(\mathbb{K}) \mid a_{ij}=0,\ 1\le i<j\le n\} \quad \text{δηλαδή} \quad A=(a_{ij})=\begin{pmatrix} a_{11} & 0 & \cdots & 0\\ a_{21} & a_{22} & \cdots & 0\\ \vdots & \vdots & \ddots & \vdots\\ a_{m1} & a_{m2} & \cdots & a_{nn}\end{pmatrix}$$

Τότε τα υποσύνολα $\mathsf{AT}_n(\mathbb{K})$ και $\mathsf{KT}_n(\mathbb{K})$ είναι, όπως εύκολα μπορούμε να δούμε, κλειστά στις πράξεις πρόσθεσης και πολλαπλασιασμού τετραγωνικών πινάκων.

3. Έστω $\mathscr{F}([0,1],\mathbb{R}) = \{f\colon [0,1]\longrightarrow\mathbb{R} \mid f : \text{απεικόνιση}\}$ το σύνολο όλων των πραγματικών απεικονίσεων οι οποίες είναι ορισμένες επί του κλειστού διαστήματος $[0,1]$ της πραγματικής ευθείας, το οποίο είναι εφοδιασμένο είτε με την πράξη της πρόσθεσης ή με την πράξη του πολλαπλασιασμού απεικονίσεων, βλέπε το μέρος 9 στο Παράδειγμα 1.3.8. Θεωρούμε το υποσύνολο $\mathscr{C}([0,1]),\mathbb{R}) = \{f\colon [0,1]\longrightarrow\mathbb{R} \mid f : \text{συνεχής απεικόνιση}\} \subseteq \mathscr{F}([0,1],\mathbb{R})$. Επειδή άθροισμα και πολλαπλασιασμός, όπως αυτές ορίστηκαν στο μέρος 9 στο Παράδειγμα 1.3.8, συνεχών απεικονίσεων είναι συνεχής απεικόνιση, έπεται ότι το υποσύνολο $\mathscr{C}([0,1]),\mathbb{R})$ είναι κλειστό στις πράξεις πρόσθεσης και πολλαπλασιασμού απεικονίσεων.

4. Θεωρούμε το ζεύγος $(\mathscr{A},*)$ όπου «$*$» είναι το γινόμενο Dirichlet επί του συνόλου $\mathscr{A}$ των αριθμητικών συναρτήσεων. Θεωρούμε το ακόλουθο υποσύνολο $\mathscr{M}$ το οποίο αποτελείται από τις *πολλαπλασιαστικές συναρτήσεις*:

$$\mathscr{M} = \{f\colon \mathbb{N}\longrightarrow\mathbb{C} \mid f\neq 0 \ \text{ και } \ (n,m)=1 \implies f(nm)=f(n)f(m)\}$$

Αποδεικνύεται[13] στη στοιχειώδη Θεωρία Αριθμών ότι $\forall f,g\in\mathscr{M}\colon\ f*g\in\mathscr{M}$, δηλαδή το υποσύνολο $\mathscr{M}$ του $\mathscr{A}$ είναι κλειστό στην πράξη του γινομένου Dirichlet.

5. Έστω ότι το σύνολο $\mathsf{A}(\mathbb{K})$ των ακολουθιών με στοιχεία από το σύνολο $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Θεωρούμε ότι το σύνολο $\mathsf{A}(\mathbb{K})$ είναι εφοδιασμένο με τις πράξεις πρόσθεσης και πολλαπλασιασμού ακολουθιών όπως στο μέρος 10 του Παραδείγματος 1.3.8.

   Θεωρούμε το ακόλουθο υποσύνολο του $\mathsf{A}(\mathbb{K})$:

$$\Pi(\mathbb{K}) = \{\mathsf{a}=(a_n)_{n\ge0}\in\mathsf{A}(\mathbb{K}) \mid \exists n\ge 0\colon\ a_k=0,\ \forall k>n\}$$

   Αν $\mathsf{a}=(a_n)_{n\ge0}$ και $\mathsf{b}=(b_n)_{n\ge0}$ είναι στοιχεία του $\Pi(\mathbb{K})$, τότε υπάρχουν μη αρνητικοί ακέραιοι n,m έτσι ώστε: $a_k=0,\ \forall k>n$ και $b_k=0,\ \forall k>m$. Θέτοντας $l=\max\{n,m\}$, θα έχουμε $a_k=0=b_k,\ \forall k>l$ και επομένως $c_k=a_k+b_k=0+0=0,\ \forall k>l$. Αυτό σημαίνει ότι η ακολουθία $\mathsf{c}=(c_n)_{n\ge0}=\mathsf{a}+\mathsf{b}$ ανήκει στο υποσύνολο $\Pi(\mathbb{K})$. Επομένως το υποσύνολο $\Pi(\mathbb{K})\subseteq\mathsf{A}(\mathbb{K})$ είναι κλειστό στην πράξη της πρόσθεσης.

   Θεωρούμε το γινόμενο $\mathsf{a}\cdot\mathsf{b}=\mathsf{d}=(d_n)_{d\ge0}$ των ακολουθιών a και b, και θέτουμε $l=n+m$. Τότε:

$$d_r=\sum_{k=0}^{r} a_k b_{n-k} = a_0b_r+a_1b_{r-1}+\cdots a_{r-1}b_1+a_rb_0 \quad \text{και άρα} \quad d_r=0, \quad \text{αν} \quad r>l$$

   Αυτό σημαίνει ότι η ακολουθία $\mathsf{d}=(c_d)_{n\ge0}=\mathsf{a}\cdot\mathsf{b}$ ανήκει στο υποσύνολο $\Pi(\mathbb{K})$. Επομένως το υποσύνολο $\Pi(\mathbb{K})\subseteq\mathsf{A}(\mathbb{K})$ είναι κλειστό στην πράξη του πολλαπλασιασμού.

[13] Βλέπε για παράδειγμα το βιβλίο [28].

Τα στοιχεία του συνόλου $\Pi(\mathbb{K})$ καλούνται πολυώνυμα μιας μεταβλητής υπεράνω του $\mathbb{K}$. Για μια δικαιολόγηση της ορολογίας και του συμβολισμού, παραπέμπουμε στην υποενότητα 7.2.14 του Κεφαλαίου 7. $\surd$

Παρατήρηση 1.3.30. Έστω το ζεύγος $(X,\star)$, όπου «$\star$» είναι μια προσεταιριστική πράξη επί του συνόλου X για την οποία υπάρχει ουδέτερο στοιχείο $e\in X$, και έστω $\mathsf{U}(X,\star)$ το σύνολο των αντιστρέψιμων στοιχείων του X. Από την Πρόταση 1.3.7 έπεται ότι το υποσύνολο $\mathsf{U}(X,\star)$ είναι κλειστό στην πράξη «$\star$», και επομένως από την Πρόταση 1.3.28, έπεται ότι στο ζεύγος $(\mathsf{U}(X,\star),\star)$ η πράξη «$\star$» είναι προσεταιριστική, υπάρχει ουδέτερο στοιχείο, και εκ κατασκευής ικανοποιείται η χαρακτηριστική ιδιότητα ότι κάθε στοιχείο του συνόλου $\mathsf{U}(X,\star)$ είναι αντιστρέψιμο ως προς την επαγόμενη πράξη.

Παραδείγματα ζευγών $(X,\star)$, για τα οποία η πράξη «$\star$» είναι προσεταιριστική περιλαμβάνουν, σύμφωνα με το Παράδειγμα 1.3.8, και τα εξής:

$$(\mathbb{Z},\cdot),\quad (\mathbb{Q},\cdot),\quad (\mathbb{R},\cdot),\quad (\mathbb{C},\cdot),\quad (\mathsf{M}_n(\mathbb{R}),\cdot),\quad (\mathsf{Map}(X),\circ)$$

Επομένως αποκτούμε τα ζεύγη

$$\mathsf{U}(\mathbb{Z},\cdot)=\{1,-1\},\quad \mathsf{U}(\mathbb{Q},\cdot)=\mathbb{Q}^*,\quad \mathsf{U}(\mathbb{R},\cdot)=\mathbb{R}^*,\quad \mathsf{U}(\mathbb{C},\cdot)=\mathbb{C}^*,\quad \mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot):=\mathsf{GL}(n,\mathbb{R}),\quad \mathsf{U}(\mathsf{Map}(X),\circ)=\mathsf{S}(X)$$

στα οποία η επαγόμενη πράξη είναι προσεταιριστική, υπάρχει αντίστροφο στοιχείο, και κάθε στοιχείο του αντίστοιχου συνόλου είναι αντιστρέψιμο. ▲

Η ακόλουθη πρόταση περιγράφει ένα σημαντικό παράδειγμα υποσυνόλου το οποίο είναι κλειστό στην πράξη ενός υπερσυνόλου.

Πρόταση 1.3.31. *Έστω $(X,\cdot)$ ένα ζεύγος, όπου «$\cdot$» είναι μια προσεταιριστική (πολλαπλασιαστική) πράξη επί του X για την οποία υπάρχει ουδέτερο στοιχείο $e\in X$. Για κάθε στοιχείο $x\in X$, το υποσύνολο:*

$$[x\rangle=\{x^n\in X\mid n\in\mathbb{N}_0\}$$

είναι κλειστό στην πράξη «$\cdot$» του X. Αν το στοιχείο x είναι αντιστρέψιμο ως προς την πράξη «$\cdot$», τότε το υποσύνολο

$$\langle x\rangle=\{x^n\in X\mid n\in\mathbb{Z}\}$$

είναι κλειστό στην πράξη «$\cdot$» του X.

Απόδειξη. Θεωρούμε τας στοιχεία x^n και x^m τα οποία ανήκουν στο υποσύνολο $[x\rangle$, όπου $n,m\geq 0$. Τότε από την Πρόταση 1.3.18 έπεται ότι $x^n\cdot x^m=x^{n+m}\in[x\rangle$ και άρα το υποσύνολο $[x\rangle$ είναι κλειστό στην πράξη «$\cdot$». Αν επιπλέον το x είναι αντιστρέψιμο ως προς την πράξη «$\cdot$», και x^n και x^m ανήκουν στο υποσύνολο $\langle x\rangle$, όπου $n,m\in\mathbb{Z}$, τότε από την Πρόταση 1.3.18 έπεται ότι $x^n\cdot x^m=x^{n+m}\in\langle x\rangle$ και άρα το υποσύνολο $\langle x\rangle$ είναι επίσης κλειστό στην πράξη «$\cdot$». ■

Παράδειγμα 1.3.32. Θεωρούμε το ζεύγος $(\mathsf{Map}(X),\circ)$ του μέρους 3 του Παραδείγματος 1.3.8, και έστω $f\colon X\longrightarrow X$ μια απεικόνιση, δηλαδή ένα στοιχείο του $\mathsf{Map}(X)$. Τότε το σύνολο $[f\rangle=\{f^0=\mathsf{Id}_X,f,f^2,\cdots\}\subseteq\mathsf{Map}(X)$ είναι κλειστό στην πράξη της σύνθεσης απεικονίσεων. Αν η απεικόνιση είναι «1-1» και «επί», δηλαδή ανήκει στο υποσύνολο $\mathsf{S}(X)$, τότε το υποσύνολο $\langle f\rangle=\{\cdots,f^{-2},f^{-1},f^0=\mathsf{Id}_X,f,f^2,\cdots\}\subseteq\mathsf{S}(X)$ είναι κλειστό στην πράξη της σύνθεσης απεικονίσεων. $\surd$

Παράδειγμα 1.3.33. Θεωρούμε το ζεύγος $(\mathsf{GL}(2,\mathbb{R}),\cdot)$ των αντιστρέψιμων πινάκων με στοιχεία πραγματικούς αριθμούς, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός πινάκων όπως στο Παράδειγμα 1.3.8. Αν $A=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, τότε, όπως μπορούμε να δούμε εύκολα, ο πίνακας A είναι αντιστρέψιμος και $A^{-1}=\begin{pmatrix}1&-1\\0&1\end{pmatrix}$. Υπολογίζουμε

$A^2 = A\cdot A = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$, και τότε, χρησιμοποιώντας της Αρχή Μαθηματικής Επαγωγής, βλέπουμε εύκολα ότι $A^n = \begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$, $\forall n\in\mathbb{N}_0$. Παρόμοια έπεται ότι $A^{-n} = \begin{pmatrix}1 & -n\\ 0 & 1\end{pmatrix}$, $\forall n\in\mathbb{N}_0$. Επομένως

$$\langle A\rangle = \left\{A^n \in \mathsf{GL}_n(\mathbb{R}) \mid n\in\mathbb{Z}\right\} = \left\{\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix} \in \mathsf{GL}(2,\mathbb{R}) \mid n\in\mathbb{Z}\right\} \quad \surd$$

Παράδειγμα 1.3.34. Θεωρούμε το ζεύγος $(\mathscr{A},*)$, όπου $\mathscr{A}$ είναι το σύνολο των αριθμητικών συναρτήσεων και «$*$» είναι το γινόμενο Dirichlet. Αποδεικνύεται στην στοιχειώδη Θεωρία Αριθμών[14] ότι το υποσύνολο $\mathsf{U}(\mathscr{A},*)$ των αντιστρέψιμων στοιχείων του $\mathscr{A}$ ως προς την πράξη «$*$» συμπίπτει με το σύνολο

$$\mathsf{U}(\mathscr{A},*) = \left\{f : \mathbb{N}\longrightarrow\mathbb{C} \mid f(1)\neq 0\right\}$$

το οποίο περιέχει και το υποσύνολο $\mathscr{M}$ των πολλαπλασιαστικών συναρτήσεων, δηλαδή: $\mathscr{M}\subseteq\mathsf{U}(\mathscr{A},*)$. $\surd$

Παρατήρηση 1.3.35. Χρησιμοποιώντας προσθετικό συμβολισμό, η Πρόταση 1.3.31 παίρνει την ακόλουθη μορφή. Έστω η προσεταιριστική πράξη «+» επί ενός συνόλου X, και έστω $x\in X$. Τότε το υποσύνολο:

$$[x\rangle = \left\{nx\in X \mid n\in\mathbb{N}_0\right\}$$

είναι κλειστό στην πράξη «+» του X. Αν το στοιχείο x είναι αντιστρέψιμο ως προς την πράξη «+», τότε το υποσύνολο

$$\langle x\rangle = \left\{nx\in X \mid n\in\mathbb{Z}\right\}$$

είναι κλειστό στην πράξη «+» του X.

Για παράδειγμα, θεωρούμε το ζεύγος $(\mathbb{Z},+)$, όπου «+» είναι η συνήθης πράξη της πρόσθεσης ακεραίων. Αν $x\in\mathbb{Z}$, τότε τα υποσύνολα $[x\rangle$, το οποίο συμπίπτει με τα μη αρνητικά ακέραια πολλαπλάσια του x, και το υποσύνολο $\langle x\rangle$, το οποίο συμπίπτει με όλα τα ακέραια πολλαπλάσια του x, είναι κλειστά στην πράξη της πρόσθεσης ακεραίων. ▲

Η χρησιμότητα των υποσυνόλων $[x,\rangle$ ή $\langle x\rangle$ της Πρότασης 1.3.31 έγκειται στο γεγονός ότι, αν και η πράξη «$\cdot$» επί του X μπορεί να είναι πολύπλοκη και επομένως δύσκολη στην μελέτη της, η πράξη «$\cdot$» είναι πολύ απλή όταν περιοριστεί σε υποσύνολα της μορφής $[x,\rangle$ ή $\langle x\rangle$, καθώς ουσιαστικά ανάγεται στην πρόσθεση ακεραίων. Αυτή η παρατήρηση θα μας οδηγήσει σε επόμενα Κεφάλαια στην μελέτη ιδιοτήτων μιας αλγεβρικής δομής της μορφής $(X,\cdot)$, με βάση ιδιότητες επαγόμενων δομών της μορφής $([x\rangle,\cdot)$ ή $(\langle x\rangle,\cdot)$, $x\in X$.

1.3.6 Πράξεις συμβιβαστές με σχέσεις ισοδυναμίας

Στα επόμενα εδάφια σημαντικό ρόλο θα παίξουν πράξεις $\star: X\times X\longrightarrow X$ επί συνόλων X οι οποίες είναι συμβιβαστές με μια δοσμένη σχέση ισοδυναμίας $\mathscr{R}\subseteq X\times X$ επί του συνόλου X, με την έννοια του ακόλουθου ορισμού.

Ορισμός 1.3.36. *Η σχέση ισοδυναμίας $\mathscr{R}$* **είναι συμβιβαστή με την πράξη** «$\star$» *επί του X αν ισχύει:*

$$\forall x,y,z,w\in X: \quad x\sim_{\mathscr{R}} z \quad \text{και} \quad y\sim_{\mathscr{R}} w \quad \Longrightarrow \quad x\star y \sim_{\mathscr{R}} z\star w$$

Η ακόλουθη Πρόταση εξηγεί γιατί η παραπάνω έννοια είναι σημαντική.

Πρόταση 1.3.37. *Έστω ότι $\star: X\times X\longrightarrow X$ μια πράξη επί του συνόλου X, και έστω $\mathscr{R}\subseteq X\times X$ μια σχέση ισοδυναμίας επί του συνόλου X η οποία είναι συμβιβαστή με την πράξη «$\star$».*

[14] Βλέπε το βιβλίο [28].

1. *Ορίζοντας*

$$\widetilde{\star} : X/\mathscr{R} \times X/\mathscr{R} \longrightarrow X/\mathscr{R}, \qquad \widetilde{\star}([x]_{\mathscr{R}}, [y]_{\mathscr{R}}) := [x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}} = [x \star y]_{\mathscr{R}}$$

αποκτούμε μια πράξη «$\widetilde{\star}$» επί του συνόλου πηλίκου $X/\mathscr{R}$.

2. *Αν η πράξη «$\star$» επί του X είναι προσεταιριστική ή μεταθετική, τότε η πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$ είναι προσεταιριστική ή μεταθετική αντίστοιχα.*

3. *Έστω $e \in X$ ένα ουδέτερο στοιχείο για την πράξη «$\star$» επί του X. Τότε το στοιχείο $[e]_{\mathscr{R}} \in X/\mathscr{R}$ είναι ουδέτερο στοιχείο για την πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$.*

4. *Υποθέτουμε ότι η πράξη «$\star$» έχει ένα ουδέτερο στοιχείο $e \in X$, και έστω x ένα στοιχείο του X για το οποίο υπάρχει ένα αντίστροφο στοιχείο $x' \in X$ ως προς την πράξη «$\star$». Τότε το στοιχείο $[x']_{\mathscr{R}}$ είναι ένα αντίστροφο στοιχείο του $[x]_{\mathscr{R}}$ για την πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$.*

Απόδειξη. **1.** Αρκεί το αποτέλεσμα της πράξης $[x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}} = [x \star y]_{\mathscr{R}}$, $\forall x, y \in X$, να είναι ανεξάρτητο της επιλογής αντιπροσώπων των κλάσεων ισοδυναμίας. Δηλαδή αρκεί να δείξουμε ότι:

$$\forall x, y, z, w \in X: \quad [x]_{\mathscr{R}} = [z]_{\mathscr{R}} \quad \text{και} \quad [y]_{\mathscr{R}} = [w]_{\mathscr{R}} \quad \Longrightarrow \quad [x \star y]_{\mathscr{R}} = [z \star w]_{\mathscr{R}}$$

Σύμφωνα με το Λήμμα 1.2.10, αρκεί να δείξουμε ισοδύναμα ότι

$$\forall x, y, z, w \in X: \quad x \sim_{\mathscr{R}} z \quad \text{και} \quad y \sim_{\mathscr{R}} w \quad \Longrightarrow \quad x \star y \;\sim_{\mathscr{R}}\; z \star w$$

Η τελευταία συνεπαγωγή όμως ισχύει ακριβώς διότι από την υπόθεση η σχέση $\mathscr{R}$ είναι συμβιβαστή με την πράξη «$\star$».

2. Υποθέτουμε ότι η πράξη «$\star$» επί του X είναι μεταθετική. Τότε η πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$ είναι μεταθετική διότι, $\forall\, [x]_{\mathscr{R}}, [y]_{\mathscr{R}} \in X/\mathscr{R}$:

$$[x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}} = [x \star y]_{\mathscr{R}} = [y \star x]_{\mathscr{R}} = [y]_{\mathscr{R}} \,\widetilde{\star}\, [x]_{\mathscr{R}}$$

Παρόμοια, αν η πράξη «$\star$» επί του X είναι προσεταιριστική, τότε η πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$ είναι προσεταιριστική διότι, $\forall\, [x]_{\mathscr{R}}, [y]_{\mathscr{R}}, [z]_{\mathscr{R}} \in X/\mathscr{R}$:

$$[x]_{\mathscr{R}} \,\widetilde{\star}\, \big([y]_{\mathscr{R}} \,\widetilde{\star}\, [z]_{\mathscr{R}}\big) = [x] \,\widetilde{\star}\, [y \star z]_{\mathscr{R}} = [x \star (y \star z)]_{\mathscr{R}} = [(x \star y) \star z]_{\mathscr{R}} = [x \star y]_{\mathscr{R}} \,\widetilde{\star}\, [z]_{\mathscr{R}} = \big([x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}}\big) \,\widetilde{\star}\, [z]_{\mathscr{R}}$$

3. Αν $e \in X$ είναι ουδέτερο στοιχείο της πράξης «$\star$», τότε το στοιχείο $[e]_{\mathscr{R}}$ είναι ουδέτερο στοιχείο για την πράξη $\widetilde{\star}$ επί του $X/\mathscr{R}$ διότι, $\forall\, [x]_{\mathscr{R}} \in X/\mathscr{R}$:

$$[x]_{\mathscr{R}} \,\widetilde{\star}\, [e]_{\mathscr{R}} = [x \star e]_{\mathscr{R}} = [x]_{\mathscr{R}} = [e \star x]_{\mathscr{R}} = [e]_{\mathscr{R}} \,\widetilde{\star}\, [x]_{\mathscr{R}}$$

4. Υποθέτουμε ότι η πράξη «$\star$» έχει ένα ουδέτερο στοιχείο $e \in X$, και έστω x ένα στοιχείο του X με αντίστροφο στοιχείο $x' \in X$ ως προς την πράξη «$\star$». Τότε θα έχουμε:

$$[x]_{\mathscr{R}} \,\widetilde{\star}\, [x']_{\mathscr{R}} = [x \star x']_{\mathscr{R}} = [e]_{\mathscr{R}} = [x' \star x]_{\mathscr{R}} = [x']_{\mathscr{R}} \,\widetilde{\star}\, [x]_{\mathscr{R}}$$

και επομένως το στοιχείο $[x']_{\mathscr{R}}$ είναι ένα αντίστροφο στοιχείο του $[x]_{\mathscr{R}}$ για την πράξη «$\widetilde{\star}$» επί του $X/\mathscr{R}$. ■

Παρατήρηση 1.3.38. Έστω $\star : X \times X \longrightarrow X$ μια πράξη επί του συνόλου X, και έστω $\mathscr{R} \subseteq X \times X$ μια σχέση ισοδυναμίας επί του συνόλου X η οποία είναι συμβιβαστή με την πράξη «$\star$». Τότε το ακόλουθο διάγραμμα απεικονίσεων μεταξύ συνόλων είναι μεταθετικό

$$\begin{array}{ccc} X \times X & \xrightarrow{\;\star\;} & X \\ {\scriptstyle \pi_{\mathscr{R}} \times \pi_{\mathscr{R}}} \downarrow & & \downarrow {\scriptstyle \pi_{\mathscr{R}}} \\ X/\mathscr{R} \times X/\mathscr{R} & \xrightarrow{\;\widetilde{\star}\;} & X/\mathscr{R} \end{array} \tag{1.10}$$

δηλαδή:

$$\widetilde{\star} \circ (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}}) = \pi_{\mathscr{R}} \circ \star \tag{1.11}$$

όπου η απεικόνιση $\pi_{\mathscr{R}} \times \pi_{\mathscr{R}}$ είναι η απεικόνιση γινόμενο, βλέπε το Παράδειγμα 0.2.6:

$$\pi_{\mathscr{R}} \times \pi_{\mathscr{R}} : X \times X \longrightarrow X/\mathscr{R} \times X/\mathscr{R}, \quad (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}})(x,y) = ([x]_{\mathscr{R}}, [y]_{\mathscr{R}})$$

Πράγματι, για τυχόντα στοιχεία $x, y \in X$, θα έχουμε:

$$\big(\widetilde{\star} \circ (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}})\big)(x,y) = \widetilde{\star}\big((\pi_{\mathscr{R}} \times \pi_{\mathscr{R}})(x,y)\big) = \widetilde{\star}\big(\pi_{\mathscr{R}}(x), \pi_{\mathscr{R}}(y)\big) = \widetilde{\star}([x]_{\mathscr{R}}, [y]_{\mathscr{R}}) =$$

$$= [x]_{\mathscr{R}} \widetilde{\star} [y]_{\mathscr{R}} = [x \star y]_{\mathscr{R}} = \pi_{\mathscr{R}}(x \star y) = (\pi_{\mathscr{R}} \circ \star)(x,y)$$

Άρα πράγματι: $\widetilde{\star} \circ (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}}) = \pi_{\mathscr{R}} \circ \star$.

Επιπλέον η πράξη «$\widetilde{\star}$»:

$$[x]_{\mathscr{R}} \widetilde{\star} [y]_{\mathscr{R}} := [x \star y]_{\mathscr{R}}$$

επί του $X/\mathscr{R}$ είναι η μοναδική πράξη επί του $X/\mathscr{R}$ η οποία ικανοποιεί την παραπάνω σχέση (1.11). Δηλαδή αν

$$\# : X/\mathscr{R} \times X/\mathscr{R} \longrightarrow X/\mathscr{R}, \quad \#([x]_{\mathscr{R}}, [y]_{\mathscr{R}}) := [x]_{\mathscr{R}} \# [y]_{\mathscr{R}}$$

είναι μια πράξη επί του $X/\mathscr{R}$ για την οποία ισχύει: $\# \circ (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}}) = \pi_{\mathscr{R}} \circ \star$, τότε: $\# = \widetilde{\star}$. Πράγματι, για τυχόντα στοιχεία $x, y \in X$ θα έχουμε:

$$\#([x]_{\mathscr{R}}, [y]_{\mathscr{R}}) = \#(\pi_{\mathscr{R}}(x), \pi_{\mathscr{R}}(y)) = \#\big((\pi_{\mathscr{R}} \times \pi_{\mathscr{R}})(x,y)\big) = \big(\# \circ (\pi_{\mathscr{R}} \times \pi_{\mathscr{R}})\big)(x,y) = (\pi_{\mathscr{R}} \circ \star)(x,y) =$$

$$= \pi_{\mathscr{R}}(\star(x,y)) = \pi_{\mathscr{R}}(x \star y) = [x \star y]_{\mathscr{R}} = [x]_{\mathscr{R}} \widetilde{\star} [y]_{\mathscr{R}} = \widetilde{\star}([x]_{\mathscr{R}}, [y]_{\mathscr{R}})$$

Άρα: $\# = \widetilde{\star}$. ▲

Φυσικά δεν είναι όλες οι πράξεις σε ένα σύνολο συμβιβαστές με μια δοσμένη σχέση ισοδυναμίας επί του συνόλου. Ας δούμε ένα παράδειγμα μιας σχέσης ισοδυναμίας $\mathscr{R}$ που ορίζεται επί ενός συνόλου X, η οποία δεν είναι συμβιβαστή με μία από τις πράξεις του συνόλου:

Παράδειγμα 1.3.39. Επί του συνόλου $\mathbb{Z}$ των ακέραιων αριθμών θεωρούμε τις συνήθεις πράξεις της πρόσθεσης και πολλαπλασιασμού:

$$+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (z_1, z_2) \longmapsto z_1 + z_2$$
$$\cdot : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}, \quad (z_1, z_2) \longmapsto z_1 \cdot z_2.$$

Επιπλέον, θεωρούμε την ακόλουθη διαμέριση Δ του $\mathbb{Z}$:

$$\mathbb{Z} = A \cup B, \quad \text{όπου} \qquad A = \{0, \pm 1\}, \qquad B = \{\pm 2, \pm 3, \pm 4, \ldots\}.$$

Η διαμέριση Δ, σύμφωνα με Πρόταση 1.2.20, ορίζει επί του $\mathbb{Z}$ την ακόλουθη σχέση ισοδυναμίας

$$\mathscr{R}_\Delta = \big\{(\alpha, \beta) \mid \alpha, \beta \in A\big\} \bigcup \big\{(\gamma, \delta) \mid \gamma, \delta \in B\big\}.$$

Η σχέση ισοδυναμίας $\mathscr{R}_\Delta$ *δεν είναι συμβιβαστή* με την πράξη της πρόσθεσης, αφού $[0]_{\mathscr{R}_\Delta} = [1]_{\mathscr{R}_\Delta}$, ενώ $[0]_{\mathscr{R}_\Delta} = [0+0]_{\mathscr{R}} \neq [2]_{\mathscr{R}_\Delta} = [1+1]_{\mathscr{R}_\Delta}$. Αντίθετα η σχέση $\mathscr{R}_\Delta$ *είναι συμβιβαστή* με την πράξη του πολλαπλασιασμού, αφού $[0]_{\mathscr{R}_\Delta} = [1]_{\mathscr{R}_\Delta} = [-1]_{R_\Delta}$, όπως επίσης $[\pm 2]_{\mathscr{R}_\Delta} = [\pm 3]_{\mathscr{R}_\Delta} = [\pm 4]_{R_\Delta} = \cdots$ και όλα τα δυνατά γινόμενα $\alpha \cdot \beta$, όπου $\alpha, \beta \in A$ ή B αντίστοιχα δίνουν και πάλι στοιχείο από το A ή το B αντίστοιχα. √

Ίσως το πιο χαρακτηριστικό παράδειγμα πράξης η οποία είναι συμβιβαστή με μια σχέση ισοδυναμίας είναι το ακόλουθο:

Παράδειγμα 1.3.40. Έστω $n \geq 1$. Όπως στο Παράδειγμα 1.2.5, στο σύνολο $\mathbb{Z}$ των ακεραίων θεωρούμε τη σχέση ισοδυναμίας $\mathscr{R}_n$, όπου:

$$\forall a, b \in \mathbb{Z}: \quad a \sim_{\mathscr{R}_n} b \iff n \mid a-b$$

Έστω $a, a', b, b' \in \mathbb{Z}$ και υποθέτουμε ότι: $a \sim_{\mathscr{R}_n} b$ και $a' \sim_{\mathscr{R}_n} b'$. Τότε θα έχουμε $n \mid a-b$ και $n \mid a'-b'$ και επομένως υπάρχουν ακέραιοι k, l έτσι ώστε:

$$a - b = k \cdot n \quad \text{και} \quad a' - b' = l \cdot n \tag{1.12}$$

Προσθέτοντας τις σχέσεις (1.12) θα έχουμε:

$$(a+a')-(b+b') = a-b+a'-b' = k\cdot n + l\cdot n = (k+l)\cdot n \implies n \mid (a+a')-(b+b') \implies (a+a') \sim_{\mathscr{R}_n} (b+b')$$

Πολλαπλασιάζοντας την πρώτη εκ των σχέσεων (1.12) με τον ακέραιο a' και την δεύτερη εκ των σχέσεων (1.12) με τον ακέραιο b, θα έχουμε:

$$a\cdot a' - b\cdot a' = k\cdot a'\cdot n \quad \text{και} \quad b\cdot a' - b\cdot b' = l\cdot b\cdot n \implies a\cdot a' - b\cdot b' = (k\cdot a' + l\cdot b)\cdot n \implies n \mid (a\cdot a' - b\cdot b')$$

$$\implies (a\cdot a') \sim_{\mathscr{R}_n} (b\cdot b')$$

Επομένως η σχέση ισοδυναμίας $\mathscr{R}_n$ είναι συμβιβαστή με την πράξη της πρόσθεσης και πολλαπλασιασμού ακεραίων. Σύμφωνα με την Πρόταση 1.3.37, ορίζοντας

$$\widetilde{+}: \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad [x]_n \,\widetilde{+}\, [y]_n = [x+y]_n$$

$$\widetilde{\cdot}: \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad [x]_n \,\widetilde{\cdot}\, [y]_n = [x\cdot y]_n$$

αποκτούμε καλά ορισμένες πράξεις επί του συνόλου πηλίκο $\mathbb{Z}_n$. Επειδή οι πράξεις «+» και «·» είναι προσεταιριστικές και μεταθετικές, και υπάρχει ουδέτερο στοιχείο γι' αυτές στο $\mathbb{Z}$, οι ακέραιοι 0 και 1 αντίστοιχα, από την Πρόταση 1.3.37 έπεται ότι οι πράξεις «$\widetilde{+}$» και «$\widetilde{\cdot}$» είναι προσεταιριστικές και μεταθετικές, και υπάρχει ουδέτερο στοιχείο γι' αυτές στο $\mathbb{Z}_n$, οι κλάσεις ισοδυναμίας $[0]_n$ και $[1]_n$ αντίστοιχα. Τέλος, επειδή κάθε στοιχείο z του $\mathbb{Z}$ είναι αντιστρέψιμο ως προς την πράξη «+», με αντίστροφο τον ακέραιο $-z$, έπεται ότι κάθε στοιχείο $[z]_n$ του $\mathbb{Z}_n$ είναι αντιστρέψιμο ως προς την πράξη «$\widetilde{+}$», με αντίστροφο την κλάση ισοδυναμίας $[-z]_n$.

Χάριν απλότητας και αν δεν δημιουργείται σύγχυση, συνήθως θα χρησιμοποιούμε τα σύμβολα «+» και «·» αντί των συμβόλων «$\widetilde{+}$» και «$\widetilde{\cdot}$» αντίστοιχα. $\surd$

Όπως είδαμε στην υποενότητα 1.2.4, βλέπε τη σχετική συζήτηση πρίν την Πρόταση 1.2.29, σχέσεις ισοδυναμίας επί ενός συνόλου X προκύπτουν με μοναδικό τρόπο ως σχέσεις ισοδυναμίας επαγόμενες από απεικονίσεις με πεδίο ορισμού το συνολο X. Επομένως είναι λογικό να εξετάσουμε πότε η σχέση ισοδυναμίας η οποία επάγεται από μια απεικόνιση $f: (X, \star) \longrightarrow (Y, *)$ μεταξύ συνόλων X και Y, τα οποία είναι εφοδιασμένα με διμελείς πράξεις «$\star$» και «$*$» αντίστοιχα, είναι συμβιβαστή με την πράξη «$\star$» του συνόλου X:

Παρατήρηση 1.3.41. Έστω $(X, \star)$ και $(Y, *)$ δύο ζεύγη αποτελούμενα από πράξεις «$\star$» και «$*$» επί των μηκενών συνόλων X και Y αντίστοιχα, και υποθέτουμε ότι $f: X \longrightarrow Y$ είναι μια απεικόνιση. Από τον Ορισμό 1.2.25 έπεται ότι η f επάγει μια σχέση ισοδυναμίας $\mathscr{R}_f$ επί του X ως εξής:

$$\forall x_1, x_2 \in X: \quad x_1 \sim_{\mathscr{R}_f} x_2 \iff f(x_1) = f(x_2)$$

Από την άλλη πλευρά, από τον Ορισμό 1.3.36, η σχέση ισοδυναμίας $\mathscr{R}_f$ είναι συμβιβαστή με την πράξη «$\star$» επί του X αν ισχύει, $\forall x_1, x_2, z_1, z_2 \in X$:

$$x_1 \sim_{\mathscr{R}_f} z_1 \quad \text{και} \quad x_2 \sim_{\mathscr{R}_f} z_2 \implies x_1 \star x_2 \sim_{\mathscr{R}_f} z_1 \star z_2$$

με άλλα λόγια, αν και μόνο αν

$$f(x_1) = f(z_1) \quad \text{και} \quad f(x_2) = f(z_2) \implies f(x_1 \star x_2) = f(z_1 \star z_2)$$

Μια σημαντική περίπτωση κατά την οποία οι παραπάνω σχέσεις ισχύουν, και άρα η σχέση ισοδυναμίας $\mathscr{R}_f$ την οποία επάγει επί του X η f είναι συμβιβαστή με την πράξη «$\star$» του X, είναι η περιπτωση κατά την οποία η απεικόνιση f ικανοποιεί την ακόλουθη σχέση:

$$\forall x_1, x_2 \in X: \quad f(x_1 \star x_2) = f(x_1) * f(x_2)$$

Πράγματι, τότε θα έχουμε $f(x_1 \star x_2) = f(x_1) * f(x_2) = f(z_1) * f(z_2) = f(z_1 \star z_2)$. Όπως θα δούμε αργότερα, η παραπάνω σχέση θα μας οδηγήσει στην σημαντική έννοια του ομομορφισμού μεταξύ αλγεβρικών δομών ίδιου τύπου. ▲

1.4 Μονοειδή

Στην παρούσα ενότητα θα μελετήσουμε την αλγεβρική δομή του μονοειδούς, η οποία είναι ίσως η απλούστερη αλγεβρική δομή με ενδιαφέρουσες ιδιότητες, βρίσκεται στην βάση των περισσότερων αλγεβρικών δομών τις οποίες θα μελετήσουμε στη συνέχεια, και έχει πολλές εφαρμογές και σε άλλες επιστήμες, όπως για παράδειγμα στην Θεωρητική Πληροφορική.

1.4.1 Βασικές Ιδιότητες και Παραδείγματα

Όπως μπορούμε να δούμε από τα παραδείγματα 1.3.8, σύνολα τα οποία είναι εφοδιασμένα με μια προσεταιριστική πράξη για την οποία υπάρχει ουδέτερο στοιχείο έχουν ευχάριστες ιδιότητες και επιπλέον πολλά γνωστά μας σύνολα είναι εφοδιασμένα με τέτοιες πράξεις. Έτσι οδηγούμαστε φυσιολογικά στον ακόλουθο ορισμό ο οποίος συνοψίζει αρκετά φαινόμενα τα οποία παρατηρήσαμε σε διάφορα παραδείγματα συνόλων εφοδιασμένα με μια πράξη.

Ορισμός 1.4.1. *Ένα ζεύγος $(X, \star)$, όπου «$\star$» είναι μια πράξη επί ενός συνόλου X καλείται* **μονοειδές**, *αν:*

1. *Η πράξη «$\star$» είναι προσεταιριστική.*
2. *Υπάρχει ουδέτερο στοιχείο e για την πράξη «$\star$» επί του X.*

Το μονοειδές $(X, \star)$ καλείται **μεταθετικό μονοειδές**, *αν η πράξη «$\star$» είναι μεταθετική. Όταν το σύνολο X είναι πεπερασμένο, ο πίνακας Cayley της πράξης «$\star$» καλείται ο* **πίνακας Cayley του μονοειδούς** $(X, \star)$.

Παρατήρηση 1.4.2. Όπως προκύπτει από τη σχέση 1.2, το ουδέτερο στοιχείο e ενός μονοειδούς $(X, \star)$ είναι μοναδικό. Επίσης, όπως προκύπτει από τη σχέση 1.4, αν x είναι ένα στοιχείο του X για το οποίο υπάρχει αντίστροφο στοιχείο x', τότε το αντίστροφο στοιχείο είναι μοναδικό. ▲

Μια γενικότερη έννοια από την έννοια του μονοειδούς, είναι η έννοια της ημιομάδας: μια **ημιομάδα** είναι ένα ζεύγος $(X, \star)$, όπου X είναι ένα μη κενό σύνολο και «$\star$» είναι μια προσεταιριστική πράξη επί του X. Όλα τα ζεύγη στο Παράδειγμα 1.3.8 αποτελούν ημιομάδες, εκτός από τα ζεύγη στο Παράδειγμα 1.3.8(4), 1.3.8(5). Στη συνέχεια δεν θα ασχοληθούμε αναλυτικά με την έννοια της ημιομάδας, και θα περιοριστούμε στην μελέτη μονοειδών των οποίων η θεωρία είναι περισσότερο πλούσια.

Παράδειγμα 1.4.3. Έστω $(X, \star)$ ένα μονοειδές με ουδέτερο στοιχείο e. Ορίζουμε επί του X μια νέα πράξη «$\star^{\mathsf{op}}$» ως εξής:

$$\star^{\mathsf{op}}: X \times X \longrightarrow X, \quad x \star^{\mathsf{op}} y = y \star x$$

Εύκολα βλέπουμε ότι το ζεύγος $(X, \star^{\mathsf{op}})$ είναι ένα μονοειδές με ουδέτερο στοιχείο e, το οποίο καλείται το **αντίθετο μονοειδές** του $(X, \star)$.

Παρατηρούμε ότι το μονοειδές $(X, \star)$ είναι μεταθετικό αν και μόνο αν τα μονοειδή $(X, \star)$ και $(X, \star^{\mathsf{op}})$ συμπίπτουν, δηλαδή αν και μόνο αν «$\star$» = «$\star^{\mathsf{op}}$». √

Παράδειγμα 1.4.4. Τα παρακάτω είναι βασικά παραδείγματα μονοειδών.

1. Έστω $X = \{x\}$ ένα μονοσύνολο, επί του οποίου ορίζουμε μια πράξη «$\star$» θέτοντας $x \star x = x$. Τότε το ζεύγος $(X, \star)$ είναι μονοειδές, το **τετριμμένο μονοειδές**.

2. Όλα τα ζεύγη στο παράδειγμα 1.3.8 είναι μονοειδή, εκτός από το ζεύγος $(\mathbb{N}, +)$ το οποίο δεν είναι μονοειδές διότι δεν υπάρχει ουδέτερο στοιχείο ως προς την πρόσθεση ($0 \notin \mathbb{N}$), και τα ζεύγη στο Παράδειγμα 1.3.8(4), 1.3.8(5), τα οποια δεν είναι ούτε ημιομάδες.

3. Όλα τα ζεύγη της μορφής $(X, \star)$ τα οποία οποία αναλύονται στο Παράδειγμα 1.3.29 είναι μονοειδή.

4. Τα ζεύγη $(\mathbb{Z}_n, +)$ και $(\mathbb{Z}_n, \cdot)$, όπου $\mathbb{Z}_n$ είναι το σύνολο των κλάσεων υπολοίπων mod n και «$+$», «$\cdot$» οι πράξεις οι οποίες ορίστηκαν στο Παράδειγμα 1.3.40, είναι μεταθετικά μονοειδή.

5. Έστω X ένα μη κενό σύνολο και $\mathsf{Rel}(X)$ το σύνολο των σχέσεων επί του X. Τότε το ζεύγος $\mathsf{Rel}(X), \circ)$, όπου «$\circ$» είναι η πράξη μεταξύ σχέσεων επί του X η οποία ορίστηκε στην υποενότητα 1.1.1, είναι ένα μονοειδές (βλέπε Άσκηση 1.5.6).

6. Έστω $X = \{x\}$ ένα τυχόν μονοσύνολο. Από το μονοσύνολο X μπορούμε να σχηματίσουμε το σύνολο $\mathsf{F}(X)$ των *λέξεων* με βάση το *γράμμα* x (δηλαδή μια πεπερασμένη ακολουθία $xxx\cdots x$) και την *κενή λέξη* e:
$$\mathsf{F}(X) = \{e,\ x,\ xx,\ xxx,\ \cdots,\ xxxxxxxxxxx\ (n \text{ παράγοντες}), \cdots\}$$
Δύο λέξεις θεωρούνται ίσες όταν το γράμμα x εμφανίζεται ίδιες φορές και στις δύο λέξεις. Ορίζοντας πράξη
$$(x_1 x_2 \cdots x_n) \star (y_1 y_2 \cdots y_m) = x_1 x_2 \cdots x_n y_1 y_2 \cdots y_m$$
$$e \star (x_1 x_2 \cdots x_n) = x_1 x_2 \cdots x_n = (x_1 x_2 \cdots x_n) \star e$$
για κάθε $x_1 x_2 \cdots x_n, y_1 y_2 \cdots y_m \in \mathsf{F}(X)$, όπου $x_i = x = y_j$, $1 \le i \le n$ και $1 \le j \le m$, αποκτούμε ένα μονοειδές $(\mathsf{F}(X), e)$ με ουδέτερο στοιχείο την κενή λέξη e, το οποίο καλείται το *ελεύθερο μονοειδές με βάση το σύνολο* X. $\surd$

Από την Πρόταση 1.3.37 προκύπτει άμεσα η ακόλουθη.

Πρόταση 1.4.5. *Έστω $(X, \star)$ ένα (μεταθετικό) μονοειδές και έστω ότι $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του X η οποία είναι συμβιβαστή με την πράξη «$\star$». Τότε το ζεύγος $(X/\mathscr{R}, \widetilde{\star})$, όπου «$\widetilde{\star}$» είναι η πράξη*
$$\widetilde{\star} : X/\mathscr{R} \times X/\mathscr{R} \longrightarrow X/\mathscr{R}, \qquad ([x]_{\mathscr{R}}, [y]_{\mathscr{R}}) \longmapsto [x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}} = [x \star y]_{\mathscr{R}}$$
είναι ένα (μεταθετικό) μονοειδές.

Το μονοειδές $(X/\mathscr{R}, \widetilde{\star})$, καλείται το **μονοειδές πηλίκο** του $(X, \star)$ ως προς τη σχέση ισοδυναμίας $\mathscr{R}$.

Παράδειγμα 1.4.6. 1. Έστω $(X, \cdot)$ ένα μονοειδές και $x \in X$. Τότε, όπως προκύπτει από την Πρόταση 1.3.31, το ζεύγος $([x\rangle, \cdot)$, όπου
$$[x\rangle = \{x^n \in X \mid n \in \mathbb{N}_0\}$$
είναι ένα μονοειδές, το οποίο καλείται το μονοειδές το οποίο παράγεται από το στοιχείο $x \in X$.

2. Θεωρούμε το μονοειδές $(\mathbb{Z}, +)$, και έστω το υποσύνολο $\mathbb{N}_0 \subseteq \mathbb{Z}$. Όπως μπορούμε να δούμε εύκολα, το υποσύνολο $\mathbb{N}_0$ είναι κλειστό στην πράξη της πρόσθεσης και το ζεύγος $(\mathbb{N}_0, +)$ είναι ένα μονοειδές. $\surd$

Το παραπάνω παράδειγμα δείχνει ότι κάποια υποσύνολα μονοειδών είναι επίσης μονοειδή με την επαγόμενη πράξη. Γενικεύοντας αποκτούμε την έννοια του υπομονοειδούς:

Ορισμός 1.4.7. *Έστω $(X, \star)$ ένα μονοειδές με ουδέτερο στοιχείο e και $S \subseteq X$ ένα υποσύνολο του X. Το υποσύνολο S καλείται* **υπομονοειδές** *του $(X, \star)$, αν $e \in S$ και το S είναι κλειστό στην πράξη «$\star$».*

Η ακόλουθη άμεση συνέπεια δίνει έναν τρόπο κατασκευής νέων μονοειδών από παλαιά.

Πόρισμα 1.4.8. *Έστω S ένα υπομονοειδές του μονοειδούς $(X,\star)$, Τότε το ζεύγος $(S,\star)$ είναι ένα μονοειδές.*

Απόδειξη. Επειδή το υποσύνολο S είναι κλειστό στην πράξη «$\star$» του X, ορίζεται η επαγόμενη πράξη επί του X η οποία είναι προφανώς προσεταιριστική. Επειδή το ουδέτερο στοιχείο e του X ανήκει στο S, προφανώς το e είναι ουδέτερο στοιχείο για την επαγόμενη πράξη «$\star$» επί του S, και άρα το ζεύγος $(S,\star)$ είναι μονοειδές. ■

Παράδειγμα 1.4.9. Έστω $(X,\cdot)$ ένα μονοειδές και $x\in X$ ένα στοιχείο του. Από την Πρόταση 1.3.31, το υποσύνολο $[x\rangle = \{x^n \in X \mid n\in\mathbb{N}_0\}$ είναι κλειστό στην πράξη του X, και επιπλέον περιέχει το ουδέτερο στοιχείο e του X, διότι $e=x^0$. Επομένως το υποσύνολο $[x\rangle$ είναι ένα υπομονοειδές του $(X,\cdot)$, το οποίο καλείται το **κυκλικό υπομονοειδές** του X το οποίο παράγεται από το στοιχείο x.

Αν Y είναι ένα υπομονοειδές του X το οποίο περιέχει το στοιχείο x, τότε προφανώς $e\in Y$ και λόγω της κλειστότητας του Y στην πράξη «$\cdot$» έπεται ότι $x^2=x\cdot x\in Y$, $x^3=x^2\cdot x\in Y$, και με χρήση της Αρχής Μαθηματικής Επαγωγής προκύπτει άμεσα ότι $x^n\in Y$, $\forall n\in\mathbb{N}_0$. Επομένως $[x\rangle\in Y$ και άρα το κυκλικό υπομονοειδές του X το οποίο παράγεται από το στοιχείο x είναι το μικρότερο υπομονοειδές του X το οποίο περιέχει το στοιχείο x.

Για παράδειγμα, έστω $X=\{1,2,3,4\}$ και έστω το μονοειδές $(\mathsf{Map}(X),\circ)$ των απεικονίσεων $f\colon X\longrightarrow X$ με πράξη την σύνθεση απεικονίσεων. Θεωρούμε την απεικόνιση $f\in\mathsf{Map}(X)$, όπου $f(1)=1$, $f(2)=1$, $f(3)=4$, και $f(4)=3$. Εύκολα υπολογίζουμε ότι $f=f^3$, και $f^2=f^4$ είναι η απεικόνιση $f^2(1)=1$, $f^2(2)=1$, $f^2(3)=3$, και $f^2(4)=4$. Επομένως $[f\rangle=\{\mathsf{Id}_X,f,f^2,f^3\}$. $\surd$

Παράδειγμα 1.4.10. Έστω $(X,\star)$ ένα μονοειδές, και $\mathsf{U}(X,\star)$ το υποσύνολο του X το οποίο αποτελείται από όλα τα αντιστρέψιμα στοιχεία του X ως προς την πράξη «$\star$». Τότε από την Παρατήρηση 1.3.30 έπεται ότι το υποσύνολο $\mathsf{U}(X,\star)$ περιέχει το ουδέτερο στοιχείο του X και είναι κλειστό στην πράξη «$\star$». Επομένως το υποσύνολο $\mathsf{U}(X,\star)$ είναι ένα υπομονοειδές, το **μονοειδές των αντιστρέψιμων στοιχείων** του $(X,\star)$.

Για παράδειγμα, τα ζεύγη

$$\mathsf{U}(\mathbb{Z},\cdot)=\{1,-1\},\quad \mathsf{U}(\mathbb{Q},\cdot)=\mathbb{Q}^*,\quad \mathsf{U}(\mathbb{R},\cdot)=\mathbb{R}^*,\quad \mathsf{U}(\mathbb{C},\cdot)=\mathbb{C}^*,\quad \mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot):=\mathsf{GL}(n,\mathbb{R}),\quad \mathsf{U}(\mathsf{Map}(X),\circ)=\mathsf{S}(X)$$

του παραδείγματος 1.3.30 είναι τα υπομονοειδή των αντιστρέψιμων στοιχείων των μονοειδών:

$$(\mathbb{Z},\cdot),\quad (\mathbb{Q},\cdot),\quad (\mathbb{R},\cdot),\quad (\mathbb{C},\cdot),\quad (\mathsf{M}_n(\mathbb{R}),\cdot),\quad (\mathsf{Map}(X),\circ)\quad \surd$$

Το ακόλουθο παράδειγμα δείχνει ιδιαίτερα ότι η συνθήκη $e\in S$ στον ορισμό υπομονοειδούς 1.4.7 δεν προκύπτει από την κλειστότητα της πράξης «$\star$».

Παράδειγμα 1.4.11. Θεωρούμε το μονοειδές $(\mathsf{M}_2(\mathbb{R}),\cdot)$ των 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς και πράξη τον συνήθη πολλαπλασιασμό πινάκων, το ουδέτερο στοιχείο του οποίου είναι ο μοναδιαίος 2×2 πίνακας $I_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Τότε το υποσύνολο

$$S=\left\{\begin{pmatrix}x&0\\0&0\end{pmatrix}\in\mathsf{M}_2(\mathbb{R})\mid x\in\mathbb{R}\right\}$$

είναι προφανώς κλειστό στην πράξη «$\cdot$» αλλά δεν είναι υπομονοειδές του $(\mathsf{M}_2(\mathbb{R}),\cdot)$, διότι το ουδέτερο στοιχείο $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ του μονοειδούς $(\mathsf{M}_2(\mathbb{R}),\cdot)$ δεν ανήκει στο υποσύνολο S. Παρατηρούμε ότι το ζεύγος $(S,\cdot)$ είναι μονοειδές με ουδέτερο στοιχείο τον πίνακα $\begin{pmatrix}1&0\\0&0\end{pmatrix}$. Άρα υπάρχουν μονοειδή $(X,\star)$ τα οποία περιέχουν ως υποσύνολα μονοειδή $(S,\star)$ τα οποία δεν είναι υπομονοειδή του $(X,\star)$. $\surd$

Πρόταση 1.4.12 (Νόμοι Διαγραφής σε Μονοειδή)**.** *Έστω $(X,\star)$ ένα μονοειδές. Τότε:*

$$\forall x,y\in X,\ \forall u\in\mathsf{U}(X,\star):\quad x\star u=y\star u\implies x=y\quad \textit{και}\quad u\star x=u\star y\implies x=y$$

Απόδειξη. Έστω u' το αντίστροφο του στοιχείου u. Χρησιμοποιώντας την προσεταιριστική ιδιότητα, θα έχουμε:

$$x\star u = y\star u \implies (x\star u)\star u' = (y\star u)\star u' \implies x\star(u\star u') = y\star(u\star u') \implies x\star e = y\star e \implies x = y$$

Παρόμοια θα έχουμε

$$u\star x = u\star y \implies u'\star(u\star x) = u'\star(u\star y) \implies (u'\star u)\star x = (u'\star u)\star y \implies e\star x = e\star y \implies x = y \ \blacksquare$$

Θα κλείσουμε την παρούσα ενότητα με δύο σημαντικές κατασκευές μονοειδών. Η πρώτη κατασκευή αφορά απεικονίσεις οι οποίες ξεκινούν από ένα μη κενό σύνολο και καταλήγουν σε ένα μονοειδές.

Πρόταση 1.4.13. *Έστω $(X,\star)$ ένα ζεύγος, όπου «$\star$» είναι μια πράξη επί του X. Για κάθε μη κενό σύνολο A, θεωρούμε το σύνολο*

$$\mathscr{F}(A,X) = \{f\colon A\longrightarrow X \mid f : \text{απεικόνιση}\}$$

επί του οποίου ορίζουμε πράξη:

$$\widetilde{\star}\ :\ \mathscr{F}(A,X)\times\mathscr{F}(A,X)\ \longrightarrow\ \mathscr{F}(A,X),\quad f\,\widetilde{\star}\,g\colon A\longrightarrow X,\ \ (f\,\widetilde{\star}\,g)(a) = f(a)\star g(a)$$

1. *Αν η πράξη «$\star$» επί του X είναι προσεταιριστική ή μεταθετική, τότε η πράξη «$\widetilde{\star}$» επί του $\mathscr{F}(A,X)$ είναι προσεταιριστική ή μεταθετική αντίστοιχα.*

2. *Αν υπάρχει ουδέτερο στοιχείο $e\in X$ για την πράξη «$\star$», τότε η (σταθερή) απεικόνιση*

$$\widetilde{e}\colon A\longrightarrow X,\quad \widetilde{e}(a) = e$$

αποτελεί ουδέτερο στοιχείο για την πράξη «$\widetilde{\star}$» επί του $\mathscr{F}(A,X)$.

3. *Αν το ζεύγος $(X,\star)$ είναι (μεταθετικό) μονοειδές, τότε και το ζεύγος $(\mathscr{F}(A,X),\widetilde{\star})$ είναι (μεταθετικό) μονοειδές.*

4. *Αν το ζεύγος $(X,\star)$ είναι μονοειδές και $\mathsf{U}(X,\star) = X$, τότε $\mathsf{U}(\mathscr{F}(A,X),\widetilde{\star}) = \mathscr{F}(A,X)$.*

Απόδειξη. **1.** Υποθέτουμε ότι η πράξη «$\star$» επί του X είναι προσεταιριστική. Έστω $f,g,h\in\mathscr{F}(A,X)$. Τότε, χρησιμοποιώντας την προσεταιριστικότητα της πράξης «$\star$» επί του X, για κάθε στοιχείο $a\in A$, θα έχουμε:

$$[(f\widetilde{\star}g)\widetilde{\star}h](a) = (f\widetilde{\star}g)(a)\star h(a) = \big(f(a)\star g(a)\big)\star h(a) = f(a)\star\big(g(a)\star h(a)\big) = f(a)\star(g\widetilde{\star}h)(a) = [f\widetilde{\star}(g\widetilde{\star}h)](a)$$

Επομένως θα έχουμε $(f\widetilde{\star}g)\widetilde{\star}h = f\widetilde{\star}(g\widetilde{\star}h)$ και άρα η πράξη $\widetilde{\star}$ επί του $\mathscr{F}(A,X)$ είναι προσεταιριστική.

Παρόμοια, αν η πράξη $\star$ επί του X είναι μεταθετική, τότε για κάθε στοιχείο $a\in A$, θα έχουμε:

$$(f\widetilde{\star}g)(a) = f(a)\star g(a) = g(a)\star f(a) = (g\widetilde{\star}f)(a)$$

Επομένως θα έχουμε $f\widetilde{\star}g = g\widetilde{\star}f$ και άρα η πράξη «$\widetilde{\star}$» επί του $\mathscr{F}(A,X)$ είναι μεταθετική.

2. Για κάθε στοιχείο $f\in\mathscr{F}(A,X)$, και για κάθε στοιχείο $a\in A$, θα έχουμε:

$$(f\widetilde{\star}\widetilde{e})(a) = f(a)\star\widetilde{e}(a) = f(a)\star e = f(a)\qquad\text{και}\qquad(\widetilde{e}\widetilde{\star}f)(a) = \widetilde{e}(a)\star f(a) = e\star f(a) = f(a)$$

Επομένως $f\widetilde{\star}\widetilde{e} = f = \widetilde{e}\widetilde{\star}f$, $\forall f\in\mathscr{F}(A,X)$, και άρα η απεικόνιση $\widetilde{e}$ είναι ουδέτερο στοιχείο για την πράξη $\widetilde{\star}$ επί του $\mathscr{F}(A,X)$.

3. Προκύπτει άμεσα από τα μέρη **1.** και **2.**, και τον ορισμό του μονοειδούς.

4. Υποθέτουμε ότι $\mathsf{U}(X,\star) = X$, δηλαδή για κάθε στοιχείο $x\in X$ υπάρχει αντίστροφο στοιχείο x' του x ως προς την πράξη «$\star$». Αν $f\colon A\longrightarrow X$ είναι τυχόν στοιχείο του συνόλου $\mathscr{F}(A,X)$, τότε ορίζουμε την απεικόνιση

$$f'\colon A\longrightarrow X,\quad f'(a) = f(a)'$$

Τότε θα έχουμε:

$$(f\widetilde{\star}f')(a) = f(a)\star f'(a) = f(a)\star f(a)' = e = \widetilde{e}(a)\qquad\text{και}\qquad(f'\widetilde{\star}f)(a) = f'(a)\star f(a) = f(a)'\star f(a) = e = \widetilde{e}(a)$$

Επομένως $f\widetilde{\star}f' = \widetilde{e} = f'\widetilde{\star}f$, και άρα η απεικόνιση f' είναι το αντίστροφο στοιχείο του f επί του $\mathscr{F}(A,X)$, ως προς την πράξη «$\widetilde{\star}$», δηλαδή: $\mathsf{U}\big(\mathscr{F}(A,X),\widetilde{\star}\big) = \mathscr{F}(A,X)$. $\blacksquare$

Παράδειγμα 1.4.14. Για κάθε μη κενό σύνολο A, επιλέγοντας $(X,\star)=(\mathbb{N}_0,+)$ ή $(X,\star)=(\mathbb{N},\cdot)$, ή $(X,\star)=(\mathbb{Z},+)$, $\cdots$, αποκτούμε νέα μονοειδή $\mathscr{F}(A,\mathbb{N}_0)$ ή $\mathscr{F}(A,\mathbb{N})$, ή $\mathscr{F}(A,\mathbb{Z})$, $\cdots$. Από την άλλη πλευρά, αν επιλέξουμε $A=\mathbb{N}_0$, και $(X,\star)$ ένα τυχαίο μονοειδές, τότε αποκτούμε το μονοειδές $(\mathscr{F}(\mathbb{N}_0,X),\widetilde{\star})$ όλων των ακολουθιών $(x_n)_{n\geq 0}$ με στοιχεία από το μονοειδές $(X,\star)$, όπου, χάριν ευκολίας, ταυτίζουμε μια απεικόνιση $f\colon \mathbb{N}_0\longrightarrow X$ με την ακολουθία των τιμών της: $f(n)=x_n$, $\forall n\geq 0$. Με βάση την παραπάνω ταύτιση, η πράξη «$\widetilde{\star}$» την οποία περιγράφει η Πρόταση 1.4.13 μεταξύ απεικονίσεων $f,g\colon A\longrightarrow X$, αντιστοιχεί στην ακόλουθη πράξη μεταξύ ακολουθιών στοιχείων του X: $(x_n)_{n\geq 0}\,\widetilde{\star}\,(y_n)_{n\geq 0}=(z_n)_{n\geq 0}$, όπου $z_n=x_n\star y_n$, $\forall n\geq 0$. $\quad\surd$

Υποθέτουμε τώρα ότι τα ζεύγη $(X_1,\star_1)$, $(X_2,\star_2)$, $\cdots$, $(X_n,\star_n)$ είναι μονοειδή με ουδέτερο στοιχείο e_i αντίστοιχα, όπου $1\leq i\leq n$. Η ακόλουθη Πρόταση ορίζει μια σημαντική κατασκευή ενός νέου μονοειδούς επί του καρτεσιανού γινομένου $\prod_{k=1}^n X_k=X_1\times X_2\times\cdots\times X_n$.

Πρόταση 1.4.15. *Με τους παραπάνω συμβολισμούς, το ζεύγος* $(\prod_{k=1}^n X_k,\star)$, *όπου*

$$(x_1,x_2,\cdots,x_n)\star(y_1,y_2,\cdots,y_n)=\big(x_1\star_1 y_1,\,x_2\star_2 y_2,\cdots,x_n\star_n y_n\big)$$

είναι μονοειδές, το **ευθύ γινόμενο των μονοειδών** $(X_i,\star_i)$. *Επιπρόσθετα:*

$$\mathsf{U}\Big(\prod_{k=1}^n X_k,\star\Big)=\prod_{k=1}^n \mathsf{U}(X_k,\star_k)$$

Απόδειξη. Έστω $\mathsf{x}=(x_1,x_2,\cdots,x_n)$, $\mathsf{y}=(y_1,y_2,\cdots,y_n)$, και $\mathsf{z}=(z_1,z_2,\cdots,z_n)\in X:=\prod_{k=1}X_k$. Τότε, χρησιμοποιώντας την προσεταιριστικότητα των σχέσεων «$\star_i$» επί των συνόλων X_i, $1\leq i\leq n$, θα έχουμε:

$$\mathsf{x}\star(\mathsf{y}\star\mathsf{z})=(x_1,x_2,\cdots,x_n)\star\big((y_1,y_2,\cdots,y_n)\star(z_1,z_2,\cdots,z_n)\big)=(x_1,x_2,\cdots,x_n)\star\big(y_1\star_1 z_1,y_2\star_2 z_2,\cdots,y_n\star_n z_n\big)=$$

$$=\big(x_1\star_1(y_1\star_1 z_1),\;x_2\star_2(y_2\star_2 z_2),\;\cdots,\;x_n\star_n(y_n\star_n z_n)\big)=\big((x_1\star_1 y_1)\star_1 z_1,\;(x_2\star_2 y_2)\star_2 z_2,\;\cdots,\;(x_n\star_n y_n)\star_n z_n\big)=$$

$$=\big(x_1\star_1 y_1,x_2\star_2 y_2,\cdots,x_n\star_n y_n\big)\star(z_1,z_2,\cdots,z_n)=\big((x_1,x_2,\cdots,x_n)\star(y_1,y_2,\cdots,y_n)\big)\star(z_1,z_2,\cdots,z_n)=(\mathsf{x}\star\mathsf{y})\star\mathsf{z}$$

Άρα η πράξη «$\star$» επί του X είναι προσεταιριστική. Θα δείξουμε ότι το στοιχείο

$$e=(e_1,e_2,\cdots,e_n)\;\in\;X$$

όπου e_i είναι το ουδέτερο στοιχείο για την πράξη «$\star_i$» επί του X_i, $1\leq i\leq n$, είναι το ουδέτερο στοιχείο για την πράξη «$\star$» επί του X. Πράγματι, $\forall\mathsf{x}=(x_1,x_2,\cdots,x_n)\in X$:

$$\mathsf{x}\star e=(x_1,x_2,\cdots,x_n)\star(e_1,e_2,\cdots,e_n)=(x_1\star_1 e_1,\,x_2\star_2 e_2,\cdots,x_n\star_n e_n)=(x_1,x_2,\cdots,x_n)=\mathsf{x}$$

$$e\star\mathsf{x}=(e_1,e_2,\cdots,e_n)\star(x_1,x_2,\cdots,x_n)=(e_1\star_1 x_1,\,e_2\star_2 x_2,\cdots,e_n\star_n x_n)=(x_1,x_2,\cdots,x_n)=\mathsf{x}$$

Οι παραπάνω σχέσεις δείχνουν ότι το e είναι το ουδέτερο στοιχείο για την πράξη «$\star$» επί του X, και επομένως το ζεύγος $(X,\star)$ είναι μονοειδές.

Τέλος, έστω $\mathsf{x}=(x_1,x_2,\cdots,x_n)\in\prod_{k=1}^n X_k$. Αν το στοιχείο x είναι αντιστρέψιμο ως προς την πράξη «$\star$», τότε υπάρχει στοιχείο $\mathsf{x}'=(x_1',x_2',\cdots,x_n')\in X$, έτσι ώστε: $\mathsf{x}\star\mathsf{x}'=e=\mathsf{x}'\star\mathsf{x}$. Επομένως:

$$(x_1\star_1 x_1',\,x_2\star_2 x_2',\cdots,x_n\star_n x_n')=(e_1,e_2,\cdots,e_n)\quad\Longrightarrow\quad x_k\star x_k'=e_k,\quad 1\leq k\leq n$$

$$(x_1'\star_1 x_1,\,x_2'\star_2 x_2,\cdots,x_n'\star_n x_n)=(e_1,e_2,\cdots,e_n)\quad\Longrightarrow\quad x_k'\star x_k=e_k,\quad 1\leq k\leq n$$

Οι παραπάνω σχέσεις δείχνουν ότι το στοιχείο $x_k\in X_k$ είναι αντιστρέψιμο ως προς την πράξη «$\star_k$» με αντίστροφο το στοιχείο x_k', $1\leq k\leq n$. Επομένως $\mathsf{U}(\prod_{k=1}^n X_k,\star)\subseteq\prod_{k=1}^n\mathsf{U}(X_k,\star_k)$. Αντίστροφα, έστω $\mathsf{x}=(x_1,x_2,\cdots,x_n)\in\prod_{k=1}^n X_k$, όπου $x_k\in\mathsf{U}(X_k,\star_k)$, $1\leq k\leq n$. Τότε $x_k\star_k x_k'=e_k=x_k'\star_k x_k$, για κάποια στοιχεία $x_k'\in X_k$, $1\leq k\leq n$, και τότε θέτοντας $\mathsf{x}'=(x_1',x_2',\cdots,x_n')\in\prod_{k=1}^n X_k$, θα έχουμε:

$$\mathsf{x}\star\mathsf{x}'=(x_1,x_2,\cdots,x_n)\star(x_1',x_2',\cdots,x_n')=(x_1\star_1 x_1',x_2\star_2 x_2',\cdots,x_n\star_n x_k')=(e_1,e_2,\cdots,e_n)=e$$

$$\mathsf{x}'\star\mathsf{x}=(x_1',x_2',\cdots,x_n')\star(x_1,x_2,\cdots,x_n)=(x_1'\star_1 x_1,x_2'\star_2 x_2,\cdots,x_n'\star_n x_k)=(e_1,e_2,\cdots,e_n)=e$$

Άρα $\mathsf{x}\in\mathsf{U}(\prod_{k=1}^n X_k,\star)$ και επομένως $\prod_{k=1}^n\mathsf{U}(X_k,\star_k)\subseteq\mathsf{U}(\prod_{k=1}^n X_k,\star)$. Συνοψίζοντας, δείξαμε ότι $\prod_{k=1}^n\mathsf{U}(X_k,\star_k)=\mathsf{U}(\prod_{k=1}^n X_k,\star)$. ■

Παράδειγμα 1.4.16. Έστω ότι $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ το οποίο θεωρούμε εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού. Τότε έχουμε τα μεταθετικά μονοειδή $(\mathbb{K},+)$ και $(\mathbb{K},\cdot)$. Σύμφωνα με την Πρόταση 1.4.35, το καρτεσιανό γινόμενο $\mathbb{K}^n$ είναι εφοδιασμένο με τις ακόλουθες πράξεις:

$$+ : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}^n, \quad (x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$

$$\cdot : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}^n, \quad (x_1, x_2, \cdots, x_n) \cdot (y_1, y_2, \cdots, y_n) = (x_1 y_1, x_2 y_2, \cdots, x_n y_n)$$

και τα ζεύγη $(\mathbb{K}^n,+)$ και $(\mathbb{K}^n,\cdot)$ είναι μεταθετικά μονοειδή. $\surd$

Κλείνουμε την παρούσα υποενότητα επισημαίνοντας ότι ο ορισμός του ευθέος γινομένου μονοειδών $\{(X_i,\star_i)\}_{i\in I}$, όπου $I = \{1,2,\cdots,n\}$, επεκτείνεται ακριβώς με τον ίδιο τρόπο και για άπειρες οικογένειες μονοειδών, δηλαδή όταν το σύνολο δεικτών I είναι άπειρο.

1.4.2 Ομομορφισμοί Μονοειδών

Αν X και Y είναι δύο σύνολα χωρίς επιπλέον δομή, ο φυσιολογικός τρόπος με τον οποίο μπορούμε να τα συγκρίνουμε ή να τα συσχετίσουμε ή να αναλύσουμε κοινές τους ιδιότητες είναι μέσω μιας απεικόνισης $f\colon X \longrightarrow Y$. Ανάλογα, αν τα σύνολα X και Y είναι εφοδιασμένα με επιπλέον αλγεβρική δομή παρόμοιου τύπου, τότε ο φυσιολογικός τρόπος σύγκρισής τους ή συσχέτισής τους είναι μέσω μιας απεικόνισης f η οποία διατηρεί την κοινή αλγεβρική δομή. Από την άλλη πλευρά, σύμφωνα με την Παρατήρηση 1.3.41, η επαγόμενη από την απεικόνιση f σχέση ισοδυναμίας $\mathscr{R}_f$ επί του X είναι συμβιβαστή με την πράξη επί του X η οποία ορίζει την αλγεβρική δομή του X, αν η απεικόνιση f διατηρεί τις πράξεις οι οποίες ορίζουν την αλγεβρική δομή επί των X και Y.

Με βάση αυτές τις παρατηρήσεις και λαμβάνοντας υπόψη ότι η αλγεβρική δομή ενός μονοειδούς $(X,\star)$ καθορίζεται από την πράξη «$\star$» επί του X και το ουδέτερο στοιχείο της $e_X \in X$, οδηγούμαστε φυσιολογικά στην έννοια του *ομομορφισμού μονοειδών* $(X,\star)$ και $(Y,*)$ η οποία είναι η κάταλληλη έννοια σύγκρισης ή συσχέτισης μονοειδών.

Ορισμός 1.4.17. *Έστω $(X,\star)$ και $(Y,*)$ δύο μονοειδή. Μια απεικόνιση $f\colon X \longrightarrow Y$ καλείται* **ομομορφισμός μονοειδών** *αν:*

$$\forall x_1, x_2 \in X\colon \quad f(x_1 \star x_2) = f(x_1) * f(x_2) \qquad \text{και} \qquad f(e_X) = e_Y$$

όπου e_X, αντίστοιχα e_Y, είναι το ουδέτερο στοιχείο του μονοειδούς X, αντίστοιχα Y. Το σύνολο όλων των ομομορφισμών μονοειδών από το μονοειδές $(X,\star)$ στο μονοειδές $(Y,*)$ συμβολίζεται με:

$$\mathsf{Hom}_{\mathrm{Mon}}(X,Y) = \{f\colon X \longrightarrow Y \mid f\colon \textit{ομομορφισμός μονοειδών}\}$$

Γενικότερα, αν τα ζεύγη $(X,\star)$ και $(Y,*)$ είναι ημιομάδες, δηλαδή οι πράξεις «$\star$» και «$*$» είναι προσεταιριστικές αλλά δεν υπάρχει απαραίτητα ουδέτερο στοιχείο για τις πράξεις «$\star$» και «$*$» αντίστοιχα, τότε μια απεικόνιση απεικόνιση $f\colon X \longrightarrow Y$ καλείται **ομομορφισμός ημιομάδων** αν: $\forall x_1, x_2 \in X\colon\ f(x_1 \star x_2) = f(x_1) * f(x_2)$.

Παράδειγμα 1.4.18. Τα ακόλουθα είναι βασικά παραδείγματα ομομορφισμών μονοειδών.

1. Θεωρούμε μονοειδή $(X,\star)$ και $(Y,*)$ με ουδέτερα στοιχεία e_X και e_Y αντίστοιχα.

   (α') Η ταυτοτική απεικόνιση $\mathrm{Id}_X\colon X \longrightarrow X$ είναι ομομορφισμός μονοειδών.

   (β') Η απεικόνιση $\mathsf{e}\colon X \longrightarrow Y$, $\mathsf{e}(x) = e_Y$, $\forall x \in X$, είναι ομομορφισμός μονοειδών, ο οποίος καλείται ο **τετριμμένος ομομορφισμός** μονοειδών.

2. Θεωρούμε τα μονοειδή $(\mathbb{R},+)$ και $(\mathbb{R}^+,\cdot)$, όπου $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ και «+», «$\cdot$» είναι οι συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών αντίστοιχα. Θεωρούμε την εκθετική και λογαριθμική απεικόνιση αντίστοιχα

$$f\colon \mathbb{R} \longrightarrow \mathbb{R}^+, \quad f(x) = e^x \qquad \text{και} \qquad g\colon \mathbb{R}^+ \longrightarrow \mathbb{R}, \quad g(x) = \log_e(x)$$

Τότε για τυχόντες πραγματικούς αριθμούς x, y και για τυχόντες θετικούς πραγματικούς αριθμούς z, w, θα έχουμε:

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y) \qquad \text{και} \qquad f(0) = e^0 = 1$$

$$g(x \cdot y) = \log_e(x \cdot y) = \log_e(x) + \log_e(y) = g(x) + g(y) \qquad \text{και} \qquad g(1) = \log_e(1) = 0$$

Επομένως οι απεικονίσεις f και g είναι ομομορφισμοί μονοειδών.

3. Θεωρούμε ένα μονοειδές $(X, \cdot)$ με ουδέτερο στοιχείο e, και έστω $(\mathbb{N}_0, +)$ το προσθετικό μονοειδές των μη αρνητικών ακεραίων. Για κάθε στοιχείο $x \in X$, η απεικόνιση

$$f_x \colon \mathbb{N}_0 \longrightarrow X, \quad f_x(n) = x^n$$

είναι ένας ομομορφισμός μονοειδών. Πράγματι, χρησιμοποιώντας τις ιδιότητες δυνάμεων όπως περιγράφονται στην Πρόταση 1.3.18, θα έχουμε $f_x(0) = x^0 = e$ και $\forall\, n, m \in \mathbb{N}_0$: $f_x(n+m) = x^{n+m} = x^n \cdot x^m = f_x(n) \cdot f_x(m)$. Επομένως η απεικόνιση f_x είναι ομομορφισμός μονοειδών.

4. Αν $(S, \star)$ είναι υπομονοειδές του μονοειδούς $(X, \star)$, δηλαδή το υποσύνολο $S \subseteq X$ είναι κλειστό στην πράξη «$\star$» του X και $e_X \in S$ και άρα το ζεύγος $(S, \star)$ είναι μονοειδές με την επαγόμενη πράξη, τότε η απεικόνιση έγκλεισης $\iota_S \colon S \longrightarrow X$, $\iota_S(x) = x$, είναι προφανώς ένας ομομορφισμός μονοειδών.

5. Έστω ότι $(X, \star)$ είναι ένα μονοειδές και έστω ότι $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του X η οποία είναι συμβιβαστή με την πράξη «$\star$». Θεωρούμε το μονοειδές πηλίκο $(X/\mathscr{R}, \widetilde{\star})$, και την απεικόνιση

$$\pi_{\mathscr{R}} : X \longrightarrow X/\mathscr{R}, \quad \pi_{\mathscr{R}}(x) = [x]_{\mathscr{R}}$$

Τότε, με χρήση της Πρότασης 1.3.37, θα έχουμε $\pi_{\mathscr{R}}(e_X) = [e_X]_{\mathscr{R}} = e_{X/\mathscr{R}}$, και αν $x, y \in X$, τότε:

$$\pi_{\mathscr{R}}(x \star y) = [x \star y]_{\mathscr{R}} = [x]_{\mathscr{R}} \,\widetilde{\star}\, [y]_{\mathscr{R}} = \pi_{\mathscr{R}}(x) \,\widetilde{\star}\, \pi_{\mathscr{R}}(y)$$

Επομένως η απεικόνιση $\pi_{\mathscr{R}}$ είναι ένας ομομορφισμός μονοειδών ο οποίος καλείται **κανονική προβολή** του μονοειδούς X στο μονοειδές πηλίκο $X/\mathscr{R}$.

6. Θεωρούμε μονοειδή $(X_1, \star_1)$, $(X_2, \star_2)$, $\cdots$, $(X_n, \star_n)$ με ουδέτερο στοιχείο e_i αντίστοιχα, όπου $1 \leq i \leq n$, και έστω $(X = \prod_{k=1}^n X_k, \star)$ το μονοειδές ευθύ γινόμενο, βλέπε την Πρόταση 1.4.35. Τότε, για κάθε δείκτη $k = 1, 2, \cdots, n$, η απεικόνιση προβολής, βλέπε το Παράδειγμα 0.2.5:

$$\pi_k : \prod_{k=1}^n X_k \longrightarrow X_k, \quad \pi_k(x_1, x_2, \cdots, x_n) = x_k$$

είναι ένας ομομορφισμός μονοειδών. Πράγματι, θα έχουμε

$$\pi_k(e_X) = \pi_k(e_1, e_2, \cdots, e_n) = e_k = e_{X_k}$$

και αν $\mathsf{x} = (x_1, x_2, \cdots, x_n)$ και $\mathsf{y} = (y_1, y_2, \cdots, y_n)$ είναι στοιχεία του $X = \prod_{k=1}^n X_k$, τότε:

$$\pi_k\big(\mathsf{x} \star \mathsf{y}\big) = \pi_k\big((x_1 \star_1 y_1, x_2 \star_2 y_2, \cdots, x_n \star_n y_n)\big) = x_k \star_k y_k = \pi_k(\mathsf{x}) \star_k \pi_k(\mathsf{y})$$

Οι ομομορφισμοί μονοειδών π_k, $1 \leq k \leq n$, καλούνται **ομομορφισμοί κανονικής προβολής** από το μονοειδές ευθύ γινόμενο $(\prod_{k=1}^n X_k, \star)$ στα μονοειδή παράγοντες $(X_k, \star_k)$. $\surd$

Παράδειγμα 1.4.19. Έστω $(X, \star)$ ένα μονοειδές. Θεωρούμε το μονοειδές $(\mathsf{Map}(X), \circ)$, όπου $\mathsf{Map}(X) = \{f \colon X \longrightarrow X \mid f : \text{απεικόνιση}\}$ είναι το σύνολο των απεικονίσεων επί του X, και «$\circ$» είναι η πράξη της σύνθεσης απεικονίσεων:

$$\circ : \mathsf{Map}(X) \times \mathsf{Map}(X) \longrightarrow \mathsf{Map}(X), \quad (f, g) \longmapsto f \circ g$$

Ορίζουμε απεικονίσεις

$$\mathsf{L} : X \longrightarrow \mathsf{Map}(X), \quad x \longmapsto \mathsf{L}(x) := \mathsf{L}_x \colon X \longrightarrow X, \quad y \longmapsto \mathsf{L}_x(y) = x \star y$$

$$\mathsf{R}\colon X \longrightarrow \mathsf{Map}(X), \quad x \longmapsto \mathsf{R}(x) := \mathsf{R}_x\colon X \longrightarrow X, \quad y \longmapsto \mathsf{R}_x(y) = y \star x$$

Θα δείξουμε ότι η απεικόνιση $\mathsf{L}\colon (X,\star) \longrightarrow (\mathsf{Map}(X),\circ)$ είναι ένας ομομορφισμός μονοειδών και η απεικόνιση $\mathsf{R}\colon (X,\star^{\mathsf{op}}) \longrightarrow (\mathsf{Map}(X),\circ)$ είναι ένας ομομορφισμός μονοειδών, όπου $(X,\star^{\mathsf{op}})$ είναι το αντίθετο μονοειδές του $(X,\star)$, βλ. Παράδειγμα 1.4.3. Σημειώνουμε ότι το ουδέτερο στοιχείο e του μονοειδούς $(X,\star)$ συμπίπτει με το ουδέτερο στοιχείο του αντίθετου μονοειδούς $(X,\star^{\mathsf{op}})$.

Η απεικόνιση $\mathsf{L}(e) = \mathsf{L}_e\colon X \longrightarrow X$, $\mathsf{L}_e(y) = e \star y = y$, είναι προφανώς η ταυτοτική απεικόνιση Id_X, δηλαδή το ουδέτερο στοιχείο του μονοειδούς $(\mathsf{Map}(X),\circ)$, και άρα $\mathsf{L}(e) = \mathsf{Id}_X$. Παρόμοια $\mathsf{R}(e) = \mathsf{Id}_X$. Αν x_1, x_2 είναι στοιχεία του X, τότε θα έχουμε:

$$\mathsf{L}_{x_1\star x_2}\colon X \longrightarrow X, \quad \mathsf{L}_{x_1\star x_2}(y) = (x_1 \star x_2)\star y = x_1 \star (x_2 \star y)$$

$$\mathsf{L}_{x_1} \circ \mathsf{L}_{x_2}\colon X \longrightarrow X, \quad (\mathsf{L}_{x_1} \circ \mathsf{L}_{x_2})(y) = \mathsf{L}_{x_1}(\mathsf{L}_{x_2}(y)) = x_1 \star \mathsf{L}_{x_2}(y) = x_1 \star (x_2 \star y)$$

Οι παραπάνω σχέσεις δείχνουν ότι $\mathsf{L}(x_1 \star x_2) = \mathsf{L}(x_1) \circ \mathsf{L}(x_2)$ και επομένως η απεικόνιση L είναι ομομορφισμός μονοειδών. Παρόμοια, αν x_1, x_2 είναι στοιχεία του X, τότε θα έχουμε:

$$\mathsf{R}_{x_1\star^{\mathsf{op}}x_2}\colon X \longrightarrow X, \quad \mathsf{R}_{x_1\star^{\mathsf{op}}x_2}(y) = y \star (x_1 \star^{\mathsf{op}} x_2) = y \star (x_2 \star x_1) = (y \star x_2) \star x_1$$

$$\mathsf{R}_{x_1} \circ \mathsf{R}_{x_2}\colon X \longrightarrow X, \quad (\mathsf{R}_{x_1} \circ \mathsf{R}_{x_2})(y) = \mathsf{R}_{x_1}(\mathsf{R}_{x_2}(y)) = \mathsf{R}_{x_2}(y) \star x_1 = (y \star x_2) \star x_1$$

Οι παραπάνω σχέσεις δείχνουν ότι $\mathsf{R}(x_1 \star^{\mathsf{op}} x_2) = \mathsf{R}(x_1) \circ \mathsf{R}(x_2)$ και επομένως η απεικόνιση R είναι ομομορφισμός μονοειδών. $\surd$

Ορισμός 1.4.20. *Έστω $(X,\star)$ ένα μονοειδές. Με τους συμβολισμούς του Παραδείγματος 1.4.19, ο ομομορφισμός μονοειδών $\mathsf{L}\colon (X,\star) \longrightarrow (\mathsf{Map}(X),\circ)$ καλείται η* **αριστερή κανονική αναπαράσταση** *του μονοειδούς $(X,\star)$, και ο ομομορφισμός μονοειδών $\mathsf{R}\colon (X,\star^{\mathsf{op}}) \longrightarrow (\mathsf{Map}(X),\circ)$ καλείται η* **δεξιά κανονική αναπαράσταση** *του μονοειδούς $(X,\star)$.*

Παράδειγμα 1.4.21. Θεωρούμε πεπερασμένες οικογένειες μονοειδών $\{(X_k,\star_k)\}_{k=1}^n$ και $\{(Y_k,*_k)\}_{k=1}^n$, με ουδέτερα στοιχεία e_k και ϵ_k, $1 \le k \le n$, αντίστοιχα. Θεωρούμε το μονοειδές ευθύ γινόμενο $(\prod_{k=1}^n X_k, \star)$ με ουδέτερο στοιχείο $e = e_{\prod_{k=1}^n X_k} = (e_1, e_2, \cdots, e_n)$ και το μονοειδές ευθύ γινόμενο $(\prod_{k=1}^n Y_k, *)$ με ουδέτερο στοιχείο $\epsilon = \epsilon_{\prod_{k=1}^n Y_k} = (\epsilon_1, \epsilon_2, \cdots, \epsilon_n)$.

Για κάθε πεπερασμένη οικογένεια ομομορφισμών μονοειδών $f_k\colon (X_k,\star_k) \longrightarrow (Y_k,\star_k)$, $1 \le k \le n$, η επαγόμενη απεικόνιση ευθύ γινόμενο

$$\prod_{k=1}^n f_k : \prod_{k=1}^n X_k \longrightarrow \prod_{k=1}^n Y_k, \quad (\prod_{k=1}^n f_k)(x_1, x_2, \cdots, x_n) = \big(f_1(x_1), f(x_2), \cdots, f_n(x_n)\big)$$

είναι ένας ομομορφισμός μονοειδών. Πράγματι, επειδή κάθε f_k είναι ομομορφισμός μονοειδών, έπεται ότι $f_k(e_k) = \epsilon_k, 1 \le k \le n$, και τότε θα έχουμε:

$$(\prod_{k=1}^n f_k)(e) = (\prod_{k=1}^n f_k)(e_1, e_2, \cdots, e_n) = \big(f_1(e_1), f(e_2), \cdots, f_n(e_n)\big) = \big(\epsilon_1, \epsilon_2, \cdots, \epsilon_n\big) = \epsilon$$

Επιπλέον, αν $\mathsf{x} = (x_1, x_2, \cdots, x_n)$ και $\mathsf{y} = (y_1, y_2, \cdots, y_n)$ είναι στοιχεία του $X = \prod_{k=1}^n X_k$, τότε χρησιμοποιώντας ότι κάθε f_k, $1 \le k \le n$, είναι ομομορφισμός μονοειδών, θα έχουμε:

$$(\prod_{k=1}^n f_k)(\mathsf{x}\star\mathsf{y}) = (\prod_{k=1}^n f_k)\big((x_1, \cdots, x_n)\star(y_1, \cdots, y_n)\big) = (\prod_{k=1}^n f_k)\big(x_1\star_1 y_1, \cdots, x_n\star_n y_n\big) = \big(f_1(x_1\star_1 y_1), \cdots, f_n(x_n\star_n y_n)\big) =$$

$$= \big(f_1(x_1) *_1 f_1(y_1), \cdots, f_n(x_n) *_n f_n(y_n)\big) = \big(f_1(x_1), \cdots, f_n(x_n)\big) * \big(f_1(y_1), \cdots, f_n(y_n)\big) = (\prod_{k=1}^n f_k)(\mathsf{x}) * (\prod_{k=1}^n f_k)(\mathsf{y})$$

Επομένως η απεικόνιση $\prod_{k=1}^n f_k\colon (\prod_{k=1}^n X_k,\star) \longrightarrow (\prod_{k=1}^n Y_k,*)$ είναι ομομορφισμός μονοειδών, ο **ομομορφισμός ευθύ γινόμενο** των ομομορφισμών $f_k\colon (X_k,\star_k) \longrightarrow (Y_k,*_k)$, $1 \le k \le n$. $\surd$

Η επόμενη πρόταση περιγράφει κάποιες βασικές ιδιότητες ομομορφισμών μονοειδών.

Πρόταση 1.4.22. *Ισχύουν τα ακόλουθα:*

1. *Αν $f\colon (X,\star) \longrightarrow (Y,*)$ είναι ένας ομομορφισμός μονοειδών, τότε, $\forall x_1, x_2, \cdots, x_n$:*
$$f(x_1 \star x_2 \cdots \star x_n) = f(x_1) * f(x_2) \cdots * f(x_n)$$
2. *Σύνθεση ομομορφισμών μονοειδών, όταν ορίζεται, είναι ομομορφισμός μονοειδών.*
3. *Αν $f\colon (X,\star) \longrightarrow (Y,*)$ είναι ένας ομομορφισμός μονοειδών και η απεικόνιση f είναι «1-1» και «επί», τότε η αντίστροφη απεικόνιση $f^{-1}\colon X \longrightarrow Y$ είναι ένας ομομορφισμός μονοειδών.*

Απόδειξη. 1. Η ζητούμενη σχέση ισχύει προφανώς όταν $n = 1$ και όταν $n = 2$, διότι η f είναι ομομορφισμός μονοειδών. Υποθέτουμε ότι η ζητούμενη σχέση ισχύει για n το πλήθος στοιχεία, και έστω $x_1, x_2, \cdots, x_{n+1} \in X$. Χρησιμοποιώντας ότι η f είναι ομομορφισμός και την επαγωγική υπόθεση, θα έχουμε:
$$f(x_1 \star \cdots \star x_n \star x_{n+1}) = f(x_1 \star \cdots \star x_n) * f(x_{n+1}) = f(x_1) * \cdots * f(x_n) * f(x_{n+1})$$
και άρα, από την Αρχή Μαθηματικής Επαγωγής, η ζητούμενη σχέση ισχύει για κάθε $n \geq 1$.

2. Θεωρούμε μονοειδή $(X_1,\star_1)$, $(X_2,\star_2)$, και $(X_3,\star_3)$ με ουδέτερα στοιχεία e_1, e_2, και e_3 αντίστοιχα. Αν $f\colon (X_1,\star_1) \longrightarrow (X_2,\star_2)$ και $g\colon (X_2,\star_2) \longrightarrow (X_3,\star_3)$ είναι ομομορφισμοί μονοειδών, τότε:
$$(g \circ f)(e_1) = g(f(e_1)) = g(e_2) = e_3$$
Επίσης, αν $x, y \in X_1$, τότε θα έχουμε:
$$(g \circ f)(x \star_1 y) = g(f(x \star_1 y)) = g(f(x) \star_2 f(y)) = g(f(x)) \star_3 g(f(y)) = (g \circ f)(x) \star_3 (g \circ f)(y)$$
Επομένως η σύνθεση $g \circ f$ είναι ομομορφισμός μονοειδών.

3. Έστω $f\colon (X,\star) \longrightarrow (Y,*)$ ένας ομομορφισμός μονοειδών, υποθέτουμε ότι η απεικόνιση f είναι «1-1» και «επί», και θεωρούμε την αντίστροφη απεικόνιση $f^{-1}\colon Y \longrightarrow X$.

   Αν e_X και e_Y είναι τα ουδέτερα στοιχεία των X και Y αντίστοιχα, και αν $\epsilon = f^{-1}(e_Y)$, τότε $f(\epsilon) = f(f^{-1}(e_Y) = e_Y$. Όμως $f(e_X) = e_Y$, διότι η f είναι ομομορφισμός μονοειδών, και επομένως θα έχουμε $f(\epsilon) = e_Y = f(e_X)$. Επειδή η f είναι «1-1», έπεται ότι $\epsilon = e_X$ και επομένως $f^{-1}(e_Y) = e_X$.

   Έστω $y_1, y_2 \in Y$, και θέτουμε $f^{-1}(y_1) = x_1$, $f^{-1}(y_2) = x_2$, και $f^{-1}(y_1 * y_2) = x_3$. Τότε θα έχουμε $f(x_1) = y_1$, $f(x_2) = y_2$, και $f(x_3) = y_1 * y_2$. Επειδή η f είναι «1-1» και ομομορφισμός μονοειδών, θα έχουμε:
$$f(x_3) = y_1 * y_2 = f(x_1) * f(x_2) = f(x_1 \star x_2) \quad \Longrightarrow \quad x_3 = x_1 \star x_2 \quad \Longrightarrow \quad f^{-1}(y_1 * y_2) = f^{-1}(y_1) \star f^{-1}(y_2)$$
   Επομένως η f^{-1} είναι ομομορφισμός μονοειδών. ■

Η ακόλουθη Πρόταση δείχνει ότι ένας ομομορφισμός μονοειδών επάγει έναν ομομορφισμό μεταξύ των αντίστοιχων μονοειδών των αντιστρέψιμων στοιχείων τους.

Πρόταση 1.4.23. *Κάθε ομομορφισμός μονοειδών $f\colon (X,\star) \longrightarrow (Y,*)$ διατηρεί αντιστρέψιμα στοιχεία και επομένως επάγει έναν ομομορφισμό μονοειδών*
$$\mathsf{U}(f)\colon \mathsf{U}(X,\star) \longrightarrow \mathsf{U}(Y,*), \quad \mathsf{U}(f)(x) = f(x)$$

Απόδειξη. Έστω $e \in X$ και $\epsilon \in Y$ τα ουδέτερα στοιχεία των μονοειδών $(X,\star)$ και $(Y,*)$ αντίστοιχα, και έστω $x \in \mathsf{U}X,\star)$ ένα αντιστρέψιμο στοιχείο του X ως προς την πράξη «$\star$». Τότε υπάρχει στοιχείο $x' \in X$ έτσι ώστε: $x \star x' = e = x' \star x$. Εφαρμόζοντας τον ομομορφισμό f, θα έχουμε:
$$f(x \star x') = f(e) = f(x' \star x) \quad \Longrightarrow \quad f(x) * f(x') = \epsilon = f(x') \star f(x)$$
Οι παραπάνω σχέσεις δείχνουν ότι το στοιχείο $f(x)$ του $(Y,*)$ είναι αντιστρέψιμο ως προς την πράξη «$*$» και το αντίστροφό του είναι το στοιχείο $f(x')$, δηλαδή: $f(x)' = f(x')$. Επομένως η f στέλνει αντιστρέψιμα στοιχεία του μονοειδούς X σε αντιστρέψιμα στοιχεία του μονοειδούς Y, και επομένως επάγει μια απεικόνιση $\mathsf{U}(f)\colon \mathsf{U}(X,\star) \longrightarrow \mathsf{U}(Y,*)$, όπου $\mathsf{U}(f)(x) = f(x)$, η οποία είναι προφανώς ένας ομομορφισμός μονοειδών. ■

Πρόταση 1.4.24. *Έστω $f\colon (X,\star)\longrightarrow(Y,*)$ ένας ομομορφισμός μονοειδών.*

1. *Το υποσύνολο*
$$\mathsf{Ker}(f)=\big\{x\in X\mid f(x)=e_Y\big\}$$
είναι ένα υπομονοειδές του X, το οποίο καλείται **πυρήνας** *του f.*

2. *Το υποσύνολο*
$$\mathsf{Im}(f)=\big\{f(x)\in Y\mid x\in X\big\}$$
είναι ένα υπομονοειδές του Y, το οποίο καλείται **εικόνα** *του f.*

Απόδειξη. 1. Επειδή η απεικόνιση f είναι ομομορφισμός μονοειδών, θα έχουμε $f(e_X)=e_Y$ και άρα $e_X\in\mathsf{Ker}(f)$. Αν $x_1,x_2\in\mathsf{Ker}(f)$, τότε $f(x_1\star x_2)=f(x_1)*f(x_2)=e_Y*e_Y=e_Y$, και άρα $x_1\star x_2\in\mathsf{Ker}(f)$, δηλαδή το υποσύνολο $\mathsf{Ker}(f)$ είναι κλειστό στην πράξη «$\star$» του X και επομένως το υποσύνολο $\mathsf{Ker}(f)$ είναι ένα υπομονοειδές του X.

2. Επειδή η απεικόνιση f είναι ομομορφισμός μονοειδών θα έχουμε $f(e_X)=e_Y$ και άρα $e_Y\in\mathsf{Im}(f)$. Αν $y_1,y_2\in\mathsf{Im}(f)$, τότε $y_1=f(x_1)$ και $y_2=f(x_2)$ για κάποια στοιχεία $x_1,x_2\in X$. Τότε $y_1*y_2=f(x_1)*f(x_2)=f(x_1\star x_2)\in\mathsf{Im}(f)$, δηλαδή το υποσύνολο $\mathsf{Im}(f)$ είναι κλειστό στην πράξη «$*$» του Y και επομένως το υποσύνολο $\mathsf{Im}(f)$ είναι ένα υπομονοειδές του Y. ■

Παρατήρηση 1.4.25. Είδαμε στην αρχή της παρούσας υποενότητας ότι ο κατάλληλος τρόπος μέσω του οποίου μπορούμε να συσχετίσουμε ή να συγκρίνουμε δύο μονοειδή είναι μέσω ενός ομομορφισμού μονοειδών. Έτσι, αν μια απεικόνιση $f\colon(X,\star)\longrightarrow(Y,*)$ μεταξύ μονοειδών είναι ομομορφισμός, τότε μπορούμε μέσω της f να συγκρίνουμε τα σύνολα X και Y ως μονοειδή, δηλαδή λαμβάνοντας υπόψη την επιπλέον δομή με την οποία είναι εφοδιασμένα. Σ' αυτό το πλαίσιο τίθεται φυσιολογικά το ερώτημα:

Πότε δύο μονοειδή είναι «δομικά ίδια»;

δηλαδή πότε μπορούμε να ταυτίσουμε δύο μονοειδή, με βάση τις ιδιότητες οι οποίες απορρέουν από τα αξιώματα μονοειδούς και μη λαμβάνοντας υπόψη τη φύση των στοιχείων ή της πράξης με την οποία είναι εφοδιασμένα;

Αν ο ομομορφισμός μονοειδών $f\colon(X,\star)\longrightarrow(Y,*)$ είναι απεικόνιση «1-1» και «επί», τότε μέσω της f τα στοιχεία των συνόλων X και Y βρίσκονται σε αμφιμονοσήμαντη αντιστοιχία έτσι ώστε για κάθε $x_1,x_2\in X$, το στοιχείο $x_1\star x_2$ αντιστοιχεί με το στοιχείο $f(x_1)*f(x_2)$. Ώς άμεση συνέπεια, έπεται ότι κάθε ιδιότητα του μονοειδούς $(X,\star)$ η οποία απορρέει από την πράξη «$\star$» και τα αξιώματα τα οποία ικανοποιεί, μεταφέρεται σε ανάλογη ιδιότητα του μονοειδούς $(Y,*)$ και αντιστρόφως. Έτσι, για παράδειγμα, αν τα σύνολα X και Y είναι πεπερασμένα, τότε οι πίνακες Cayley των μονοειδών $(X,\star)$ και $(Y,*)$ είναι δομικά ίδιοι, δηλαδή, αν εξαιρέσουμε την φύση των στοιχείων και της πράξης με τα οποία τα σύνολα είναι εφοδιασμένα, οι πίνακες είναι ουσιαστικά ταυτόσημοι. Με βάση τις παραπάνω παρατηρήσεις, οδηγούμαστε φυσιολογικά στην έννοια του ισομορφισμού μονοειδών η οποία είναι η καταλληλότερη έννοια μέσω της οποίας μπορούμε να απαντήσουμε στο παραπάνω ερώτημα.

Ορισμός 1.4.26. *Ένας ομομορφισμός μονοειδών $f\colon(X,\star)\longrightarrow(Y,*)$ καλείται* **ισομορφισμός μονοειδών** *αν η απεικόνιση f είναι απεικόνιση «1-1» και «επί», και τότε θα συμβολίζουμε:*
$$f\colon(X,\star)\xrightarrow{\cong}(Y,*)$$
Ένας ισομορφισμός μονοειδών $f\colon(X,\star)\longrightarrow(X,\star)$ καλείται **αυτομορφισμός** *του $(X,\star)$.*

Γενικότερα ο ομομορφισμός μονοειδών $f\colon(X,\star)\longrightarrow(Y,*)$ καλείται:

1. **Μονομορφισμός μονοειδών** αν η f είναι απεικόνιση «1-1».

   Για παράδειγμα, αν S ένα υπομονοειδές του μονοειδούς $(X,\star)$, τότε η απεικόνιση έγκλεισης $\iota\colon S\longrightarrow X$ είναι ένας μονομορφισμός μονοειδών.

2. **Επιμορφισμός μονοειδών** αν η f είναι απεικόνιση «επί».

   Για παράδειγμα, έστω ότι $(X,\star)$ είναι ένα μονοειδές και έστω ότι $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί του X η οποία είναι συμβιβαστή με την πράξη «$\star$». Τότε η απεικόνιση κανονικής προβολής, όπως στο Παράδειγμα 1.4.18:
   $$\pi_{\mathscr{R}}: X \longrightarrow X/\mathscr{R}, \quad \pi_{\mathscr{R}}(x) = [x]_{\mathscr{R}}$$
   από το μονοειδές X στο μονοειδές πηλίκο $X/\mathscr{R}$ είναι προφανώς επιμορφισμός μονοειδών.

Παρατήρηση 1.4.27. Η **σχέση ισομορφίας** «$\cong$» η οποία ορίζεται στην κλάση[15] **Mon** όλων των μονοειδών ως εξής:

αν $(X,\star),(Y,*) \in$ **Mon** τότε: $(X,\star) \cong (Y,*) \iff$ υπάρχει ισομορφισμός μονοειδών $f:(X,\star) \longrightarrow (Y,*)$

είναι μια σχέση ισοδυναμίας επί της κλάσης **Mon**. Πράγματι: επειδή για κάθε μονοειδές $(X,\star)$, η ταυτοτική απεικόνιση $\mathsf{Id}_X: X \longrightarrow X$ είναι ομομορφισμός μονοειδών, έπεται ότι $(X,\star) \cong (X,\star)$. Αν $(X,\star)$ και $(Y,*)$ είναι μονοειδή και ισχύει $(X,\star) \cong (Y,*)$, τότε έστω $f:(X,\star) \longrightarrow (Y,*)$ ένας ισομορφισμός μονοειδών. Επειδή από την Πρόταση 1.4.22, η αντίστροφη απεικόνιση $f^{-1}:(Y,*) \longrightarrow (X,\star)$ είναι επίσης ισομορφισμός μονοειδών, έπεται ότι $(Y,*) \cong (X,\star)$. Τέλος, έστω ότι $(X,\star)$, $(Y,*)$, και $(Z,\cdot)$ είναι μονοειδή και ισχύει ότι $(X,\star) \cong (Y,*)$ και $(Y,*) \cong (Z,\cdot)$, τότε υπάρχουν ισομορφισμοί μονοειδών $f:(X,\star) \longrightarrow (Y,*)$ και $g:(Y,*) \longrightarrow (Z,\cdot)$. Επειδή από την Πρόταση 1.4.22 η σύνθεση ομομορφισμών είναι ομομορφισμός μονοειδών, έπεται ότι η σύνθεση $g \circ f:(X,\star) \longrightarrow (Z,\cdot)$ είναι ένας ισομορφισμός μονοειδών και επομένως: $(X,\star) \cong (Z,\cdot)$.

Η σχέση ισομορφίας διαμερίζει την κλάση **Mon** όλων των μονοειδών σε κλάσεις ισομορφίας και, σύμφωνα με την Παρατήρηση 1.4.25, δύο μονοειδή τα οποία ανήκουν στην ίδια κλάση ισομορφίας έχουν τις ίδιες δομικές ιδιότητες.

Τέλος, αν τα μονοειδή $(X,\star)$ και $(Y,*)$ δεν είναι ισόμορφα, τότε θα γράφουμε: $(X,\star) \ncong (Y,*)$. ▲

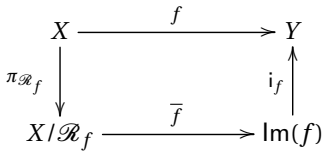
Το ακόλουθο βασικό αποτέλεσμα επιτρέπει την ανάλυση ενός ομομορφισμού μονοειδών ως σύνθεση ενός επιμορφισμού, ενός ισομορφισμού, και ενός μονομορφισμού μονοειδών.

Θεώρημα 1.4.28 (Θεώρημα Ισομορφισμών για Μονοειδή)**.** *Έστω $f:(X,\star) \longrightarrow (Y,*)$ ένας ομομορφισμός μονοειδών.*

1. *Η σχέση ισοδυναμίας $\mathscr{R}_f$ την οποία επάγει η απεικόνιση f επί του X είναι συμβιβαστή με την πράξη του μονοειδούς $(X,\star)$ και επομένως ορίζεται το μονοειδές πηλίκο $(X/\mathscr{R}_f, \widetilde{\star})$.*

2. *Ο ομομορφισμός f επάγει έναν ισομορφισμό μονοειδών*
   $$\overline{f}:(X/\mathscr{R}_f, \widetilde{\star}) \xrightarrow{\cong} (\mathsf{Im}(f),*), \quad \overline{f}([x]_{\mathscr{R}_f}) = f(x)$$

3. *Ο ομομορφισμός f είναι σύνθεση του επιμορφισμού $\pi_{\mathscr{R}_f}: X \longrightarrow X/\mathscr{R}_f$, του ισομορφισμού $\overline{f}: X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f)$ και του μονομορφισμού $\mathsf{i}_f: \mathsf{Im}(f) \longrightarrow Y$, σχηματικά το ακόλουθο διάγραμμα είναι μεταθετικό:*



δηλαδή: $f = \mathsf{i}_f \circ \overline{f} \circ \pi_{\mathscr{R}_f}$

Απόδειξη. 1. Έστω x_1, x_2 και z_1, z_2 τυχόντα στοιχεία του X και υποθέτουμε ότι $x_1 \mathscr{R}_f z_1$ και $x_2 \mathscr{R}_f z_2$. Τότε θα έχουμε $f(x_1) = f(z_1)$ και $f(x_2) = f(z_2)$. Επειδή η απεικόνιση f είναι ομομορφισμός, έπεται ότι: $f(x_1 \star x_2) = f(x_1) * f(x_2) = f(z_1) * f(z_2) = f(z_1 \star z_2)$ και επομένως $(x_1 \star x_2)\ \mathscr{R}_f\ (z_1 \star z_2)$. Η τελευταία σχέση δείχνει ότι

[15] Η συλλογή όλων των μονοειδών δεν αποτελεί σύνολο. Έτσι, όταν αναφερόμαστε σε μια σχέση ισοδυναμίας ή σε μια διαμέριση ορισμένης επί μιας κλάσης αντικειμένων η οποία δεν είναι σύνολο, εννοούμε ότι η σχέση ισοδυναμίας ή η διαμέριση έχει τις τυπικές ιδιότητες τις οποίες έχει μια σχέση ισοδυναμίας ή μια διαμέριση ορισμένη επί ενός συνόλου.

η σχέση ισοδυναμίας $\mathscr{R}_f$ είναι συμβιβαστή με την πράξη «$\star$» του μονοειδούς X, και επομένως ορίζεται το μονοειδές πηλίκο $(X/\mathscr{R}_f, \widetilde{\star})$ και ο επιμορφισμός κανονικής προβολής $\pi_{\mathscr{R}_f}\colon X \longrightarrow X/\mathscr{R}_f$.

2. Σύμφωνα με την Πρόταση 1.2.24, η f επάγει μια απεικόνιση $\widetilde{f}\colon X/\mathscr{R}_f \longrightarrow Y$, $\widetilde{f}([x]_{\mathscr{R}_f}) = f(x)$ η οποία είναι «1-1», και επιπλέον, για κάθε $[x_1]_{\mathscr{R}_f}, [x_2]_{\mathscr{R}_f} \in X/\mathscr{R}_f$:

$$\widetilde{f}([x_1]_{\mathscr{R}_f} \,\widetilde{\star}\, [x_2]_{\mathscr{R}_f}) = \widetilde{f}([x_1 \star x_2]_{\mathscr{R}_f}) = f(x_1 \star x_2) = f(x_1) * f(x_2) = \widetilde{f}([x_1]_{\mathscr{R}_f}) * \widetilde{f}([x_1]_{\mathscr{R}_f})$$

Άρα η απεικόνιση $\widetilde{f}$ είναι μονομορφισμός μονοειδών, ο οποίος προφανώς επάγει έναν ισομορφισμό μονοειδών $\overline{f}\colon (X/\mathscr{R}_f, \widetilde{\star}) \longrightarrow (\mathsf{Im}(f), *)$.

3. Από τη συζήτηση που προηγήθηκε της Παρατήρησης 1.4.27, η απεικόνιση $\pi_{\mathscr{R}_f}\colon X \longrightarrow X/\mathscr{R}_f$ είναι επιμορφισμός μονοειδών, και η απεικόνιση $\mathsf{i}_f\colon \mathsf{Im}(f) \longrightarrow Y$ είναι μονομορφισμός μονοειδών. Τέλος, από την Πρόταση 1.2.24 έπεται ότι $f = \mathsf{i}_f \circ \overline{f} \circ \pi_{\mathscr{R}_f}$. ■

Παράδειγμα 1.4.29. Θεωρούμε δύο σύνολα $X = \{e, x, y, z\}$ και $Y = \{\epsilon, a\}$ επί των οποίων έχουν οριστεί πράξεις «$\star$» και «$\cdot$» αντίστοιχα με πίνακες Cayley τους ακόλουθους:

$\star$	**e**	**x**	**y**	**z**
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

και

$\cdot$	ϵ	**a**
ϵ	ϵ	a
a	a	ϵ

Εύκολα τότε βλέπουμε ότι τα ζεύγη $(X, \star)$ και $(Y, \cdot)$ είναι (μεταθετικά) μονοειδή με ουδέτερα στοιχεία e και ϵ αντίστοιχα. Ορίζουμε απεικόνιση

$$f\colon X \longrightarrow Y, \quad f(e) = f(z) = \epsilon \quad \text{και} \quad f(x) = f(y) = a$$

Επειδή $f(e) = \epsilon$, λαμβάνοντας υπόψη ότι το μονοειδές X είναι μεταθετικό και τις ακόλουθες σχέσεις:

$$f(x\star y) = f(z) = \epsilon = a\cdot a = f(x)\cdot f(y), \quad f(x\star z) = f(y) = a = a\cdot\epsilon = f(x)\cdot f(z), \quad f(y\star z) = f(x) = a = a\cdot\epsilon = f(y)\cdot f(z)$$

έπεται ότι η απεικόνιση f είναι ομομορφισμός μονοειδών και επειδή προφανώς η f είναι απεικόνιση «επί», θα έχουμε $\mathsf{Im}(f) = Y$. Οι παραπάνω σχέσεις δείχνουν ότι $[e]_{\mathscr{R}_f} = \{e, z\}$ και $[x]_{\mathscr{R}_f} = \{x, y\}$ και άρα $X/\mathscr{R}_f = \{[e]_{\mathscr{R}_f}, [x]_{\mathscr{R}_f}\}$. Από το Θεώρημα 1.4.28 έχουμε τον ισομορφισμό μονοειδών

$$\overline{f}\colon X/\mathscr{R}_f = \{[e]_{\mathscr{R}_f},\ [x]_{\mathscr{R}_f}\} \longrightarrow Y, \quad \overline{f}([e]_{\mathscr{R}_f}) = f(e) = \epsilon, \quad \overline{f}([x]_{\mathscr{R}_f}) = f(x) = a \quad \surd$$

Παράδειγμα 1.4.30. Έστω $(X, \star)$ ένα μονοειδές με ουδέτερο στοιχείο e. Σταθεροποιούμε ένα στοιχείο $x \in X$ και θεωρούμε τον ομομορφισμό μονοειδών

$$f_x\colon (\mathbb{N}_0, +) \longrightarrow (X, \star), \quad f(n) = x^n$$

όπως στο μέρος 3 του Παραδείγματος 1.4.18. Προφανώς $\mathsf{Im}(f_x) = [x\rangle$ είναι το κυκλικό υπομονοειδές του X το οποίο παράγεται απο το στοιχείο x. Επομένως από το Θεώρημα 1.4.28 προκύπτει ένας ισομορφισμός μονοειδών

$$\overline{f}\colon \mathbb{N}_0/\mathscr{R}_{f_x} \xrightarrow{\cong} [x\rangle, \quad \overline{f}([n]_{\mathscr{R}_{f_x}}) = f(n) = x^n$$

όπου η σχέση ισοδυναμίας $\mathscr{R}_{f_x}$ η οποία επάγεται από την f_x ορίζεται ως εξής, $\forall n, m \in \mathbb{N}_0$: $n \sim_{\mathscr{R}_{f_x}} m$, αν και μόνο αν $f_x(n) = f_x(m)$, δηλαδή αν και μόνο αν $x^n = x^m$. Υπενθυμίζουμε ότι: $\mathbb{N}_0/\mathscr{R}_{f_x} = \{[n]_{\mathscr{R}_{f_x}} \subseteq \mathbb{N}_0 \mid n \in \mathbb{N}_0\}$, όπου $[n]_{\mathscr{R}_{f_x}} = \{m \in \mathbb{N}_0 \mid n \sim_{\mathscr{R}_{f_x}} m\} = \{m \in \mathbb{N}_0 \mid x^n = x^m\}$, και η επαγόμενη πράξη επί του μονοειδούς πηλίκου $\mathbb{N}_0/\mathscr{R}_{f_x}$ ορίζεται ως: $[n]_{\mathscr{R}_{f_x}} \,\widetilde{+}\, [m]_{\mathscr{R}_{f_x}} = [n+m]_{\mathscr{R}_{f_x}}$.

Θα περιγράψουμε το μονοειδές πηλίκο $\mathbb{N}_0/\mathscr{R}_{f_x}$, άρα και το κυκλικό μονοειδές $[x,\rangle$, όταν $x \in \mathsf{U}(X, \cdot)$, δηλαδή όταν το στοιχείο x είναι αντιστρέψιμο. Για την γενική περίπτωση παραπέμπουμε στην Άσκηση 1.5.31. Έτσι υποθέτουμε ότι το x είναι αντιστρέψιμο και, καθώς χρησιμοποιούμε πολλαπλασιαστικο συμβολισμό, έστω x^{-1} το αντίστροφό του. Διακρίνουμε περιπτώσεις:

1. Αν $x = e$, τότε για τυχόντες μη αρνητικούς ακέραιους n, m θα έχουμε $x^n = e^n = e = e^m = x^m$, και επομένως $n \sim_{\mathscr{R}_{f_x}} m$, $\forall n, m \in \mathbb{N}_0$. Ιδιαίτερα $[0]_{\mathscr{R}_{f_x}} = [n]_{\mathscr{R}_{f_x}}$, $\forall n \in \mathbb{N}_0$, και επομένως $\mathbb{N}_0/\mathscr{R}_{f_x} = \{[0]_{\mathscr{R}_{f_x}}\}$.

2. *Υποθέτουμε ότι $x \neq e$, και υπάρχει θετικός ακέραιος r έτσι ώστε $x^r = e$.* Τότε, αν n συμβολίζει τον μικρότερο θετικό ακέραιο r έτσι ώστε $x^r = e$, θα δείξουμε ότι υπάρχει ένας ισομορφισμός μονοειδών

$$g\colon\ \mathbb{Z}_n \xrightarrow{\cong} \mathbb{N}_0/\mathscr{R}_{f_x}, \quad g([k]_n) = [k]_{\mathscr{R}_{f_x}}$$

από το μονοειδές $\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$ των κλάσεων υπολοίπων $\bmod n$ εφοδιασμένο με την πράξη της πρόσθεσης στο μονοειδές πηλίκο $\mathbb{N}_0/\mathscr{R}_{f_x}$. Η απεικόνιση g είναι καλά ορισμένη, διότι, αν $[k]_n = [l]_n$, τότε $n \mid k-l$, και επομένως $k - l = t \cdot n$ για έναν ακέραιο t. Τότε $x^{k-l} = x^{t\cdot n} = (x^n)^t = e^t = e$ και άρα $e = x^{k-l} = x^k \cdot x^{-l} \Longrightarrow x^l = e \cdot x^l = x^k \cdot x^{-l} \cdot x^l = x^k \cdot e = x^k$. Η τελευταία σχέση δείχνει ότι $f_x(k) = f_x(l)$, δηλαδή $g([k]_n) = [k]_{\mathscr{R}_{f_x}} = [l]_{\mathscr{R}_{f_x}} = g([l]_n)$ και η g είναι καλά ορισμένη. Αν $[k]_n, [l]_n \in \mathbb{Z}_n$, τότε

$$g([k]_n + [l]_n) = g([k+l]_n) = [k+l]_{\mathscr{R}_{f_x}} = [k]_{\mathscr{R}_{f_x}} \mathbin{\widetilde{+}} [l]_{\mathscr{R}_{f_x}} = g([k]_n) \mathbin{\widetilde{+}} g([l]_n)$$

και επομένως η απεικόνιση g είναι ομομορφισμός μονοειδών. Αν $[k]_n, [l]_n \in \mathbb{Z}_n$ και $g([k]_n) = g([l]_n)$, τότε $x^k = x^l$, και επομένως $x^{k-l} = x^k \cdot x^{-l} = x^l \cdot x^{-l} = x^0 = e$. Επειδή n είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $x^n = e$ και $0 \leq k, l < n$, οπότε $0 \leq k - l < n$ έπεται ότι $k - l = 0$, και άρα $k = l$. Τότε $[k]_n = [l]_n$ και επομένως η απεικόνιση g είναι «1-1», δηλαδή μονομορφισμός. Επειδή η απεικόνιση g είναι προφανώς «επί», έπεται ότι η g είναι ισομορφισμός μονοειδών.

3. *Υποθέτουμε ότι $x \neq e$ και δεν υπάρχει θετικός ακέραιος r έτσι ώστε $x^r = e$.* Θα δείξουμε ότι η απεικόνιση κανονικής προβολής

$$\pi_{\mathscr{R}_{f_x}}\colon\ \mathbb{N}_0 \xrightarrow{\cong} \mathbb{N}_0/\mathscr{R}_{f_x}, \quad \pi_{\mathscr{R}_{f_x}}(k) = [k]_{\mathscr{R}_{f_x}}$$

είναι ένας ισομορφισμός μονοειδών. Επειδή η απεικόνιση $\pi_{\mathscr{R}_{f_x}}$ είναι πάντα επιμορφισμός μονοειδών, αρκεί να δείξουμε ότι είναι «1-1». Αν $\pi_{\mathscr{R}_{f_x}}(k) = \pi_{\mathscr{R}_{f_x}}(l)$, τότε $[k]_{\mathscr{R}_{f_x}} = [l]_{\mathscr{R}_{f_x}}$ και επομένως $x^k = f_x(k) = f_x(l) = x^l$. Τότε $x^{k-l} = e$ και άρα $k - l = 0$, διότι από την υπόθεση δεν υπάρχει θετικός ακέραιος r έτσι ώστε $x^r = e$. Άρα $k = l$ και η απεικόνιση $\pi_{\mathscr{R}_{f_x}}$ είναι «1-1» και επομένως ισομορφισμός μονοειδών.

Συνοψίζουμε: αν $x = e$, τότε $[x\rangle = \{e\}$, και αν $x \neq e$, τότε υπάρχουν ισομορφισμοί μονοειδών:

$([x\rangle, \cdot) \cong (\mathbb{Z}_n, +)$ (αν $n = \min\{r \in \mathbb{N} \mid x^r = e\} \in \mathbb{N}$) και $([x\rangle, \cdot) \cong (\mathbb{N}_0, +)$ (αν δεν υπάρχει $n \in \mathbb{N}$: $x^r = e$) $\surd$

Παρατήρηση 1.4.31. Έστω (P) μια ιδιότητα την οποία μπορεί να ικανοποιεί ή μπορεί να μην ικανοποιεί ένα μονοειδές. Η ιδιότητα (P) καλείται **δομική ιδιότητα μονοειδών** αν και μόνο αν ισχύει ότι:

ένα μονοειδές $(X, \star)$ ικανοποιεί την ιδιότητα (P) $\Longleftrightarrow$

κάθε μονοειδές $(Y, *)$ το οποίο είναι ισόμορφο με το $(X, \star)$ ικανοποιεί την ιδιότητα (P)

Για παράδειγμα, η ιδιότητα ότι «*το πλήθος των στοιχείων ενός μονοειδούς $(X, \star)$ είναι ίσο με k*» είναι προφανώς δομική ιδιότητα μονοειδών, διότι ικανοποιείται από κάθε μονοειδές στην κλάση ισομορφίας του $(X, \star)$. Η ιδιότητα ότι «*το πλήθος των αντιστρέψιμων στοιχείων ενός μονοειδούς $(X, \star)$ είναι ίσο με k*» είναι δομική ιδιότητα μονοειδών. Πράγματι, αν $(Y, *)$ είναι ένα μονοειδές στην κλάση ισομορφίας του $(X, \star)$, και $f\colon (X, \star) \longrightarrow (Y, *)$ είναι ένας ισομορφισμός μονοειδών, τότε, χρησιμοποιώντας την Πρόταση 1.4.23 και το ότι η f είναι «1-1» και «επί», έπεται ότι ο επαγόμενος ομομορφισμός μονοειδών $\mathsf{U}(f)\colon \mathsf{U}(X, \star) \longrightarrow \mathsf{U}(Y, *)$ είναι ισομορφισμός, και άρα τα μονοειδή $(X, \star)$ και $(Y, *)$ έχουν το ίδιο πλήθος αντιστρέψιμων στοιχείων. Παρόμοια βλέπουμε ότι η ιδιότητα «*υπάρχει $e \neq x \in X$: $x \star x = e$*» είναι μια δομική ιδιότητα μονοειδών.

Αντίθετα η ιδιότητα «*το στοιχείο -3 ανήκει στο μονοειδές $(\mathbb{R}, +)$*» δεν είναι δομική ιδιότητα μονοεδών διότι, όπως θα δούμε στο μέρος 5 του Παραδείγματος 1.4.33, το μονοειδές $(\mathbb{R}^+, \cdot)$ είναι ισόμορφο με το μονοειδές $(\mathbb{R}, +)$ και $-3 \notin \mathbb{R}^+$. ▲

Είναι προφανές ότι, αν υπάρχει μια δομική ιδιότητα την οποία ικανοποιεί ένα μονοειδές $(X, \star)$ και την οποία δεν ικανοποιεί ένα μονοειδές $(Y, *)$, τότε τα μονειδή $(X, \star)$ και $(Y, *)$ δεν μπορεί να είναι ισόμορφα.

Παράδειγμα 1.4.32. Θεωρούμε το μονοειδές $(\mathbb{R}^*,\cdot)$ των μη μηδενικών πραγματικών αριθμών με πράξη τη συνήθη πράξη πολλαπλασιασμού πραγματικών αριθμών και ουδέτερο στοιχείο τον αριθμό 1, και το μονοειδές $(\mathbb{R},+)$ των πραγματικών αριθμών με πράξη τη συνήθη πράξη πρόσθεσης πραγματικών αριθμών και ουδέτερο στοιχείο τον αριθμό 0. Αν $x\in\mathbb{R}^*$, τότε $x^2=x\cdot x=1$ αν και μόνο αν $x=1$ ή $x=-1$. Άρα υπάρχει $1\neq x\in\mathbb{R}^*$: $x^2=x\cdot x=1$. Αντίθετα, αν $x\in\mathbb{R}$ και $2x=x+x=0$, τότε προφανώς $x=0$. Έτσι το μόνο στοιχείο του μονοειδούς $(\mathbb{R},+)$ με την ιδιότητα $x+x=0$ είναι το ουδέτερο στοιχείο 0. Επομένως η εξίσωση $x\cdot x=1$ έχει δύο λύσεις στο μονοειδές $(\mathbb{R}^*,\cdot)$ και μία λύση στο μονοειδές $(\mathbb{R},+)$. Άρα τα μονοειδή $(\mathbb{R}^*,\cdot)$ και $(\mathbb{R},+)$ δεν μπορεί να είναι ισόμορφα. $\surd$

Παράδειγμα 1.4.33. 1. Θεωρούμε ένα σύνολο $X=\{e,x,y\}$ επί του οποίου ορίζουμε μια πράξη «$\star$» όπως στον παρακάτω πίνακα (Π_1):

(Π_1):

$\star$	**e**	**x**	**y**
e	e	x	y
x	x	y	e
y	y	e	x

και (Π_2):

$+$	$[\mathbf{0}]_\mathbf{3}$	$[\mathbf{1}]_\mathbf{3}$	$[\mathbf{2}]_\mathbf{3}$
$[\mathbf{0}]_\mathbf{3}$	$[0]_3$	$[1]_3$	$[2]_3$
$[\mathbf{1}]_\mathbf{3}$	$[1]_3$	$[2]_3$	$[0]_3$
$[\mathbf{2}]_\mathbf{3}$	$[2]_3$	$[0]_3$	$[1]_3$

Τότε εύκολα βλέπουμε ότι το ζεύγος $(X,\star)$ είναι ένα (μεταθετικό) μονοειδές με ουδέτερο στοιχείο e και πίνακα Cayley τον πίνακα (Π_1). Θεωρούμε επίσης το μονοειδές $(\mathbb{Z}_3,+)$ των κλάσεων υπολοίπων mod 3 με πράξη την πρόσθεση, βλέπε το μέρος 4 του Παραδείγματος 1.4.4, του οποίου ο πίνακας Cayley είναι ο πίνακας (Π_2). Τα μονοειδή X και $\mathbb{Z}_3$ *είναι ισόμορφα* διότι η απεικόνιση $f\colon X\longrightarrow\mathbb{Z}_3$, όπου $f(e)=[0]_3$, $f(x)=[1]_3$, και $f(y)=[2]_3$, είναι προφανώς ένας ισομορφισμός μονοειδών. Έτσι $(X,\star)\cong(Y,*)$, και, όπως βλέπουμε, οι πίνακες Cayley (Π_1) και (Π_2), αν εξαιρέσουμε τον συμβολισμό των στοιχείων και των πράξεων, είναι ταυτόσημοι.

2. Θεωρούμε ένα σύνολο $X=\{e,x,y,z\}$ επί του οποίου ορίζουμε μια πράξη «$\star$» όπως στον παρακάτω πίνακα (Π_3), και το σύνολο $Y=\{(1,1),(-1,1),(1,-1),(-1,-1)\}\subseteq\mathbb{Z}\times\mathbb{Z}$ επί του οποίου ορίζουμε πράξη όπως στον παρακάτω πίνακα (Π_4):

(Π_3):

$\star$	**e**	**x**	**y**	z
e	e	x	y	z
x	x	e	z	y
y	y	z	e	x
z	z	y	x	e

και (Π_4):

$\cdot$	$(\mathbf{1},\mathbf{1})$	$(\mathbf{-1},\mathbf{1})$	$(\mathbf{1},\mathbf{-1})$	$(\mathbf{-1},\mathbf{-1})$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(-1,1)$	$(1,-1)$	$(-1,-1)$
$(\mathbf{-1},\mathbf{1})$	$(-1,1)$	$(1,1)$	$(-1,-1)$	$(1,-1)$
$(\mathbf{1},\mathbf{-1})$	$(1,-1)$	$(-1,-1)$	$(1,1)$	$(-1,1)$
$(\mathbf{-1},\mathbf{-1})$	$(-1,-1)$	$(1,-1)$	$(-1,1)$	$(1,1)$

Τότε εύκολα βλέπουμε ότι το ζεύγος $(X,\star)$ είναι ένα (μεταθετικό) μονοειδές με ουδέτερο στοιχείο e και πίνακα Cayley τον πίνακα (Π_3). Επίσης εύκολα βλέπουμε ότι το υποσύνολο Y είναι κλειστό στην πράξη «$\cdot$» μονοειδούς ευθύ γινόμενο $(\mathbb{Z}\times\mathbb{Z},\cdot)$ και περιέχει το ουδέτερο στοιχείο του, και επομένως είναι ένα μονοειδές του οποίου ο πίνακας Cayley είναι ο πίνακας (Π_4). Τα μονοειδή X και Y *είναι ισόμορφα* διότι η απεικόνιση

$$f\colon X\longrightarrow Y,\quad \text{όπου}\quad f(e)=(1,1),\quad f(x)=(-1,1),\quad f(y)=(1,-1),\quad f(z)=(-1,-1)$$

είναι, όπως μπορούμε να δούμε εύκολα, ένας ισομορφισμός μονοειδών. Έτσι $(X,\star)\cong(Y,*)$, και, όπως βλέπουμε, οι πίνακες Cayley (Π_3) και (Π_4), αν εξαιρέσουμε τον συμβολισμό των στοιχείων και των πράξεων, είναι ταυτόσημοι.

3. Θεωρούμε το μονοειδές $(\mathbb{Z}_4,+)$ των κλάσεων υπολοίπων mod 4, του οποίου ο πίνακας Cayley είναι ο παρακάτω πίνακας (Π_5), και το υποσύνολο $C_4=\{1,-1,i,-i\}\subseteq\mathbb{C}$ επί του οποίου ορίζεται η συνήθης πράξη πολλαπλασιασμού μιγαδικών αριθμών όπως στον παρακάτω πίνακα (Π_6):

(Π_5):

$+$	$[\mathbf{0}]_\mathbf{4}$	$[\mathbf{1}]_\mathbf{4}$	$[\mathbf{2}]_\mathbf{4}$	$[\mathbf{3}]_\mathbf{4}$
$[\mathbf{0}]_\mathbf{4}$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[\mathbf{1}]_\mathbf{4}$	$[1]_4$	$[2]_3$	$[3]_4$	$[0]_4$
$[\mathbf{2}]_\mathbf{4}$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[\mathbf{3}]_\mathbf{4}$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

και (Π_6):

$\cdot$	$\mathbf{1}$	$\mathbf{-1}$	$\mathbf{i}$	$\mathbf{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\mathbf{i}$	i	$-i$	-1	1
$\mathbf{-i}$	$-i$	i	1	-1

Προφανώς το υποσύνολο C_4 είναι υπομονοειδές του μονοειδούς $(\mathbb{C}^*,\cdot)$. Τότε το μονοειδές $(\mathbb{Z}_4,+)$ *δεν είναι ισόμορφο* με το μονοειδές $(X,\star)$ ή το μονοειδές $(Y,\cdot)$. Η αιτία είναι ότι, αν και υπάρχει «1-1» και «επί» απεικόνιση μεταξύ του $\mathbb{Z}_4$ και του X ή του Y (διότι όλα αυτά τα σύνολα έχουν το ίδιο πλήθος στοιχείων ίσο με 4), δεν υπάρχει μεταξύ αυτών «1-1» και «επί» απεικόνιση η οποία να είναι και ομομορφισμός. Πράγματι, παρατηρώντας τους πίνακες Cayley (Π_5) και (Π_4) των μονοειδών $(\mathbb{Z}_4,+)$ και $(Y,\cdot)$, βλέπουμε ότι για κάθε στοιχείο $y\in Y$ ισχύει ότι $y^2=y\cdot y=(1,1)=e_Y$, αλλά το μόνο στοιχείο $[k]_4\in\mathbb{Z}_4$ με την ανάλογη ιδιότητα $2[k]_4=[k]_4+[k]_4=[0]_4=e_{\mathbb{Z}_4}$ είναι το στοιχείο $[2]_4$ διότι $2[2]_4=[2]_4+[2]_4=[4]_4=[0]_4$. Έτσι, αν υπάρχει ισομορφισμός μονοειδών $f\colon(Y,\cdot)\longrightarrow(\mathbb{Z}_4,+)$, τότε για το στοιχείο $[1]_4\in\mathbb{Z}_4$, επειδή η αντίστροφη απεικόνιση f^{-1} είναι ομομορφισμός, θα έχουμε

$$e_Y=(1,1)=f^{-1}([1]_4)\cdot f^{-1}([1]_4)=f^{-1}([1]_4+[1]_4)=f^{-1}([2]_4)\quad\Longrightarrow\quad f(e_Y)=[2]_4\neq[0]_4$$

και αυτό είναι άτοπο διότι, επειδή η απεικόνιση f είναι ομομορφισμός, θα έχουμε $f(e_Y)=e_{\mathbb{Z}_4}=[0]_4$. Επομένως[16] $(\mathbb{Z}_4,+)\ncong(X,\star)$ και $(\mathbb{Z}_4,+)\ncong(Y,*)$.

Από την άλλη πλευρά, εύκολα βλέπουμε ότι η απεικόνιση

$$f\colon C_4\longrightarrow\mathbb{Z}_4,\quad f(1)=[0]_4,\quad f(-1)=[2]_4,\quad f(i)=[1]_4,\quad f(-i)=[3]_4$$

είναι ένας ισομορφισμός μονοειδών και άρα: $(C_4,\cdot)\cong(\mathbb{Z}_4,+)$.

4. Έστω $X=\{x\}$ ένα τυχόν μονοσύνολο και $(\mathsf{F}(X),\star)$ το ελεύθερο μονοειδές επί του X με ουδέτερο στοιχείο e, όπως στο μέρος 6 του Παραδείγματος 1.4.4. Θεωρούμε επίσης και το μονοειδές $(\mathbb{N}_0,+)$. Τότε η απεικόνιση

$$f\colon\mathbb{N}_0\longrightarrow\mathsf{F}(X),\quad f(0)=e\quad\text{και}\quad f(n)=xxxxxx\cdots xxxxx\ (n\ \text{παράγοντες}),\quad\forall n\geq 1$$

είναι προφανώς ένας ισομορφισμός μονοειδών, και άρα: $(\mathbb{N}_0,+)\cong(\mathsf{F}(X),\star)$.

5. Θεωρούμε τα μονοειδή $(\mathbb{R},+)$ και $(\mathbb{R}^+,\cdot)$, όπου $\mathbb{R}^+=\{x\in\mathbb{R}\mid x>0\}$ και «+», «·» είναι οι συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών αντίστοιχα. Από το μέρος 2. του Παραδείγματος 1.4.18, η εκθετική απεικόνιση

$$f\colon(\mathbb{R},+)\longrightarrow(\mathbb{R}^+,\cdot),\quad f(x)=e^x$$

είναι ομομορφισμός μονοειδών, και επειδή η f είναι «1-1» και «επί», με αντίστροφη την απεικόνιση $g\colon\mathbb{R}^+\longrightarrow\mathbb{R}$, $g(x)=\log_e x$, έπεται ότι η απεικόνιση f είναι ένας ισομορφισμός μονοειδών και άρα: $(\mathbb{R},+)\cong(\mathbb{R}^+,\cdot)$.

Αν το μονοειδές $(\mathbb{R}^*,\cdot)$ των μη μηδενικών πραγματικών αριθμών είναι ισόμορφο με το μονοειδές $(\mathbb{R}^+,\cdot)$ των θετικών πραγματικών αριθμων, όπου και στις δύο περιπτώσεις «·» είναι η συνήθης πράξη του πολλαπλασιασμού πραγματικών αριθμών, δηλαδή έχουμε $(\mathbb{R}^*,\cdot)\cong(\mathbb{R}^+,\cdot)$, τότε, επειδή $(\mathbb{R},+)\cong(\mathbb{R}^+,\cdot)$, έπεται ότι θα έχουμε $(\mathbb{R}^*,+)\cong(\mathbb{R},+)$. Αυτό όμως είναι άτοπο, όπως προκύπτει από το Παράδειγμα 1.4.32. Άρα $(\mathbb{R}^*,\cdot)\ncong(\mathbb{R}^+,\cdot)$.

6. Έστω X ένα μη κενό σύνολο και έστω $\mathscr{P}(X)$ το δυναμοσύνολο του X. Θεωρούμε το μονοειδές $(\mathscr{P}(X),\cup)$ με ουδέτερο στοιχείο το κενό σύνολο $\emptyset$ και το μονοειδές $(\mathscr{P}(X),\cap)$ με ουδέτερο στοιχείο το σύνολο X. Τότε η απεικόνιση

$$f\colon(\mathscr{P}(X),\cup)\longrightarrow(\mathscr{P}(X),\cap),\quad f(A)=A^c=X\setminus A$$

είναι ένας ισομορφισμός μονοειδών διότι $f(\emptyset)=\emptyset^c=X$, και αν $A,B\in\mathscr{P}(X)$ είναι υποσύνολα του X, τότε: $f(A\cup B)=(A\cup B)^c=A^c\cap B^c=f(A)\cap f(B)$. Χρησιμοποιώντας ότι $f^2(A)=f(f(A))=(A^c)^c=A=\mathsf{Id}_{\mathscr{P}(X)}(A)$, $\forall A\subseteq X$, έπεται ότι $f^2=\mathsf{Id}_{\mathscr{P}(X)}$, και άρα η f είναι «1-1» και «επί» με αντίστροφη την f. Επομένως η απεικόνιση f είναι ισομορφισμός μονοειδών. $\surd$

Το ακόλουθο Πόρισμα δίνει έναν χαρακτηρισμό ισομορφισμού μονοειδών.

Πόρισμα 1.4.34. *Για μια απεικόνιση $f\colon(X,\star)\longrightarrow(Y,*)$ μεταξύ μονοειδών, τα ακόλουθα είναι ισοδύναμα:*

1. *Η απεικόνιση f είναι ισομορφισμός μονοειδών.*

[16] Η ιδιότητα $x^2=e_X$, την οποία μπορεί να ικανοποιεί ένα στοιχείο x σε ένα μονοειδές $(X,\star)$, είναι «δομική», δηλαδή ικανοποιείται από κάθε μονοειδές το οποίο ανήκει στην κλάση ισομορφίας του μονοειδούς $(X,\star)$. Επομένως, αν δύο μονοειδή έχουν διαφορετικό πλήθος στοιχείων τα οποία ικανοποιούν την ιδιότητα αυτή, τότε τα μονοειδή αυτά δεν μπορεί να είναι ισόμορφα.

2. Η f είναι ομομορφισμός μονοειδών και υπάρχει ομομορφισμός μονοειδών $g\colon Y \longrightarrow X$ έτσι ώστε:

$$f\circ g = \mathsf{Id}_Y \qquad \text{και} \qquad g\circ f = \mathsf{Id}_X$$

Αν ισχύει μια από τις ισοδύναμες συνθήκες 1. και 2., τότε η απεικόνιση g στη συνθήκη 2. είναι μοναδική και

$$g = f^{-1}$$

Απόδειξη. 1. $\Longrightarrow$ 2. Αν η f είναι ισομορφισμός μονοειδών, τότε από την Πρόταση 1.4.22 έπεται ότι η απεικόνιση $g = f^{-1}$ είναι ομομορφισμός μονοειδών και προφανώς ικανοποιεί τις συνθήκες στο μέρος 2.

2. $\Longrightarrow$ 1. Αν η απεικόνιση f είναι ομομορφισμός μονοειδών και ισχύουν οι συνθήκες στο μέρος 2., τότε η απεικόνιση f είναι αντιστρέψιμη και τότε από την Πρόταση 0.2.8, έπεται ότι η f είναι «1-1» και «επί» και επομένως η f είναι ισομορφισμός μονοειδών. ■

Αν $(X,\star)$ είναι ένα μονοειδές και $f_1,\cdots,f_n : X \longrightarrow X$ είναι απεικονίσεις, όχι απαραίτητα ομομορφισμοί μονοειδών, τότε ορίζεται η απεικόνιση

$$f_1\star f_2\star\cdots\star f_n \;:\; X\longrightarrow X,\quad (f_1\star f_2\star\cdots\star f_n)(x) = f_1(x)\star f_2(x)\star\cdots\star f_n(x)$$

Αν οι απεικονίσεις f_k, $1\le k\le n$, είναι ομομορφισμοί, τότε γενικά η απεικόνιση $f_1\star f_2\star\cdots\star f_n$ δεν είναι ομομορφισμός μονοειδών, βλέπε την Άσκηση 1.5.28.

Πρόταση 1.4.35. *Θεωρούμε το μονοειδές ευδύ γινόμενο $(\prod_{k=1}^n X_k,\star)$ των μονοειδών $(X_k,\star_k)$, με ουδέτερο στοιχείο $e_k\in X_k$ αντίστοιχα, όπου $1\le k\le n$. Τότε οι απεικονίσεις*

$$\iota_k :\; X_k \;\longrightarrow\; \prod_{k=1}^n X_k,\quad \iota_k(x) = (e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)$$

είναι «1-1» ομομορφισμοί μονοειδών και ισχύουν οι σχέσεις:

$$\forall\, k,m = 1,2,\cdots,n\colon \qquad \pi_k\circ\iota_m = \begin{cases}\mathsf{Id}_{X_k}, & \text{αν } k=m\\ \mathsf{e}_{mk}, & \text{αν } k\neq l\end{cases} \;:\; X_m \longrightarrow X_k$$

όπου π_k, $1\le k\le n$, είναι οι ομομορφισμοί κανονικής προβολής, βλέπε το μέρος 6 του Παραδείγματος 1.4.18, και όπου $\mathsf{e}_{mk}\colon X_m\longrightarrow X_k$, $\mathsf{e}_{mk}(x) = e_k$, είναι ο τετριμμένος ομομορφισμός μονοειδών, $1\le k,m\le n$. Επιπλέον

$$\mathsf{Id}_X = (\iota_1\circ\pi_1)\star(\iota_2\circ\pi_2)\star\cdots\star(\iota_n\circ\pi_n)$$

Απόδειξη. Σταθεροποιώντας έναν δείκτη $k = 1,2,\cdots,n$, και $x,y\in X_k$, θα έχουμε:

$$\iota_k(e_k) = (e_1,\cdots,e_{k-1},e_k,e_{k+1},\cdots,e_n) = e_{\prod_{k=1}^n X_k}$$

$$\iota_k(x\star_k y) = (e_1,\cdots,e_{k-1},x\star_k y,e_{k+1},\cdots,e_n) = (e_1\star_1 e_1,\cdots,e_{k-1}\star_{k-1}e_{k-1},x\star_k y,e_{k+1}\star_{k+1}e_{k+1},\cdots,e_n\star_n e_n) =$$
$$= (e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\star(e_1,\cdots,e_{k-1},y,e_{k+1},\cdots,e_n) = \iota_k(x)\star\iota_k(y)$$

Επομένως η απεικόνιση ι_k, η οποία προφανώς είναι «1-1», είναι ένας ομομορφισμός μονοειδών.

Σταθεροποιούμε δείκτες $k,m = 1,2,\cdots,n$, και έστω τυχόν στοιχείο $x\in X_m$. Τότε το ζητούμενο προκύπτει από τις ακόλουθες σχέσεις:

$$\pi_k\circ\iota_m(x) = \pi_k((e_1,\cdots,e_{m-1},x,e_{m+1},\cdots,e_n) = \begin{cases}x, & \text{αν } m=k\\ e_k, & \text{αν } m\neq k\end{cases} = \begin{cases}\mathsf{Id}_{X_k}(x), & \text{αν } m=k\\ \mathsf{e}_{mk}(x), & \text{αν } m\neq k\end{cases}$$

Τέλος, έστω $\mathsf{x} = (x_1,x_2,\cdots,x_n)\in\prod_{k=1}^n X_k$. Τότε:

$$(\iota_1\circ\pi_1)(\mathsf{x})\star(\iota_2\circ\pi_2)(\mathsf{x})\star\cdots\star(\iota_n\circ\pi_n)(\mathsf{x}) = \iota_1(\pi_1(\mathsf{x}))\star\iota_2(\pi_2(\mathsf{x})\star\cdots\star\iota_n(\pi_n(\mathsf{x})) = \iota_1(x_1)\star\iota_2(x_2)\star\cdots\star\iota_n(x_n) =$$
$$= (x_1,e_2,\cdots,e_n)\star(e_1,x_2,\cdots,e_n)\star\;\cdots\;\star(e_1,e_2,\cdots,x_n) =$$
$$= (x_1\star_1 e_1\star_1\cdots\star_1 e_1,\; e_2\star_2 x_2\star_2\cdots\star_2 e_2,\;\cdots,\; e_n\star_n e_n\star_n\cdots\star_n x_n) = (x_1,x_2,\cdots,x_n) = \mathsf{x}$$

Επομένως $\mathsf{x} = (\iota_1\circ\pi_1)(\mathsf{x})\star(\iota_2\circ\pi_2)(\mathsf{x})\star\cdots\star(\iota_n\circ\pi_n)(\mathsf{x})$, $\forall\mathsf{x}\in X$ και άρα: $\mathsf{Id}_X = (\iota_1\circ\pi_1)\star(\iota_2\circ\pi_2)\star\cdots\star(\iota_n\circ\pi_n)$. ■

Έστω $(X,\star)$ ένα μονοειδές. Θεωρούμε την αριστερή κανονική αναπαράσταση του $(X,\star)$:

$$\mathsf{L}\colon X \longrightarrow \mathsf{Map}(X),\quad x \longmapsto \mathsf{L}(x) := \mathsf{L}_x\colon X \longrightarrow X,\quad y \longmapsto \mathsf{L}_x(y) = x\star y$$

και την δεξιά κανονική αναπαράσταση του $(X,\star)$:

$$\mathsf{R}\colon X \longrightarrow \mathsf{Map}(X),\quad x \longmapsto \mathsf{R}(x) := \mathsf{R}_x\colon X \longrightarrow X,\quad y \longmapsto \mathsf{R}_x(y) = y\star x$$

όπως στο Παράδειγμα 1.4.19. Θεωρούμε τα υποσύνολα $\mathsf{Im}(\mathsf{L}) \subseteq \mathsf{Map}(X) \supseteq \mathsf{Im}(\mathsf{R})$, δηλαδή:

$$\mathsf{Im}(\mathsf{L}) = \big\{\mathsf{L}_x\colon X \longrightarrow X,\ \mathsf{L}_x(y) = x\star y \mid x\in X\big\} \qquad \text{και} \qquad \mathsf{Im}(\mathsf{R}) = \big\{\mathsf{R}_x\colon X \longrightarrow X,\ \mathsf{R}_x(y) = y\star x \mid x\in X\big\}$$

Κλείνουμε την παρούσα ενότητα με το ακόλουθο αποτέλεσμα, γνωστό ως Θεώρημα του Cayley για μονοειδή, το οποίο, με χρήση κανονικών αναπαραστάσεων μονοειδών, μας επιτρέπει να θεωρήσουμε κάθε μονοειδές ως υπομονοειδές του μονοειδούς των απεικονίσεων επί ενός κατάλληλου συνόλου.

Πρόταση 1.4.36 (Θεώρημα του Cayley για μονοειδή)**.** *Έστω $(X,\star)$ ένα μονοειδές.*

1. *Η αριστερή κανονική αναπαράσταση $\mathsf{L}\colon (X,\star) \longrightarrow (\mathsf{Map}(X),\circ)$ είναι «1-1», το υποσύνολο $\mathsf{Im}(\mathsf{L})$ είναι ένα υπομονοειδές του $(\mathsf{Map}(X),\circ)$ και η L επάγει έναν ισομορφισμό μονοειδών $(X,\star) \cong \mathsf{Im}(\mathsf{L}) \subseteq \mathsf{Map}(X)$.*

   Επιπλέον η απεικόνιση L επάγει έναν «1-1» ομομορφισμό μονοειδών $\mathsf{L}\colon \mathsf{U}(X,\star) \longrightarrow \mathsf{S}(X)$.

2. *Η δεξιά κανονική αναπαράσταση $\mathsf{R}\colon (X,\star^{\mathsf{op}}) \longrightarrow (\mathsf{Map}(X),\circ)$ είναι «1-1», το υποσύνολο $\mathsf{Im}(\mathsf{R})$ είναι ένα υπομονοειδές του $(\mathsf{Map}(X),\circ)$ και η R επάγει έναν ισομορφισμό μονοειδών $(X,\star^{\mathsf{op}}) \cong \mathsf{Im}(\mathsf{R}) \subseteq \mathsf{Map}(X)$.*

   Επιπλέον η απεικόνιση R επάγει έναν «1-1» ομομορφισμό μονοειδών $\mathsf{R}\colon \mathsf{U}(X,\star^{\mathsf{op}}) \longrightarrow \mathsf{S}(X)$.

Απόδειξη. 1. Από το Παράδειγμα 1.4.19 έπεται ότι η απεικόνιση $\mathsf{L}\colon X \longrightarrow \mathsf{Map}(X)$, $x \longmapsto \mathsf{L}(x)\colon X \longrightarrow X$, όπου $\mathsf{L}(x)(y) = x\star y$, είναι ένας ομομορφισμός μονοειδών.

Έστω x_1 και x_2 στοιχεία του μονοειδούς X έτσι ώστε: $\mathsf{L}_{x_1} = \mathsf{L}_{x_2}$. Τότε για κάθε στοιχείο y του X θα έχουμε:

$$\forall\, y\in X\colon\quad \mathsf{L}_{x_1}(y) = \mathsf{L}_{x_2}(y) \quad\Longrightarrow\quad x_1\star y = x_2\star y, \quad \text{και άρα για } y = e\colon\quad x_1\star e = x_2\star e \quad\Longrightarrow\quad x_1 = x_2$$

Επομένως, αν $\mathsf{L}(x_1) = \mathsf{L}(x_2)$, τότε $x_1 = x_2$, και επομένως η απεικόνιση L είναι «1-1». Από την Πρόταση 1.4.24, έπεται ότι το υποσύνολο $\mathsf{Im}(\mathsf{L})$ είναι ένα υπομονοειδές του Y, και προφανώς η απεικόνιση $\mathsf{L}\colon X \longrightarrow \mathsf{Im}(\mathsf{L})$ είναι ένας ισομορφισμός μονοειδών. Τέλος, επειδή $\mathsf{U}(\mathsf{Map}(X),\circ) = \mathsf{S}(X)$, από την Πρόταση 1.4.23 η απεικόνιση L επάγει έναν ομομορφισμό μονοειδών $\mathsf{L}\colon \mathsf{U}(X,\star) \longrightarrow \mathsf{S}(X)$ ο οποίος είναι προφανώς «1-1».

2. Η απόδειξη είναι παρόμοια και αφηνεται ως Άσκηση στον αναγνώστη. ■

Παρατήρηση 1.4.37. Συχνά αναφερόμαστε στο υπομονοειδές $\mathsf{Im}(\mathsf{L}) \subseteq \mathsf{Map}(X)$, αντίστοιχα $\mathsf{Im}(\mathsf{R}) \subseteq \mathsf{Map}(X)$, ως η αριστερή, αντίστοιχα δεξιά, κανονική αναπαράσταση του μονοειδούς $(X,\star)$.

Η αριστερή (ή δεξιά) κανονική αναπαράσταση ενός μονοειδούς $(X,\star)$ μας επιτρέπει να θεωρούμε τα στοιχεία του, μέσω τους ισόμορφου αντιγράφου $(\mathsf{Im}(\mathsf{L}),\circ)$, ως απεικονίσεις επί του X και ταυτόχρονα να θεωρούμε την πράξη «$\star$» ως σύνθεση απεικονίσεων. Αυτή η θεώρηση παρουσιάζει αρκετά πλεονεκτήματα, καθώς επιτρέπει να έχουμε εποπτεία επί της πράξης «$\star$» η οποία, όπως και το σύνολο X, μπορεί να έχει δοθεί με αφηρημένο τρόπο. ▲

Παράδειγμα 1.4.38. Θεωρούμε το μονοειδές $(X,\star)$, όπου $X = \{e,x,y\}$, με τον ακόλουθο πίνακα Cayley, βλέπε 1.4.33:

(Π) :

$\star$	**e**	**x**	**y**
e	e	x	y
x	x	y	e
y	y	e	x

Θα προσδιορίσουμε την αριστερή κανονική αναπαράσταση $\mathsf{Im}(\mathsf{L})$ του $(X,\star)$. Θα έχουμε

$$\mathsf{Im}(\mathsf{L}) = \{\mathsf{L}_e,\ \mathsf{L}_x,\ \mathsf{L}_y\} \subseteq \mathsf{Map}(X)$$

και άρα αρκεί να περιγράψουμε τις απεικονίσεις $\mathsf{L}_e,\ \mathsf{L}_x,\ \mathsf{L}_y : X \longrightarrow X$ και ακολούθως να σχηματίσουμε το αντίστοιχο Cayley του μονοειδούς $(\mathsf{Im}(\mathsf{L}),\circ)$. Θα έχουμε:

$$\mathsf{L}_e(e) = e\star e = e,\quad \mathsf{L}_e(x) = e\star x = x,\quad \mathsf{L}_e(y) = e\star y = y,\qquad \text{και άρα}\qquad \mathsf{L}_e = \mathsf{Id}_X$$

$$\mathsf{L}_x(e) = x\star e = x,\quad \mathsf{L}_x(x) = x\star x = y,\quad \mathsf{L}_x(y) = x\star y = e$$

$$\mathsf{L}_y(e) = y\star e = y,\quad \mathsf{L}_y(x) = y\star x = e,\quad \mathsf{L}_y(y) = y\star y = x$$

Εύκολα βλέπουμε τότε ότι το διάγραμμα Cayley του μονοειδούς $(\mathsf{Im}(\mathsf{L}),\circ)$ είναι το ακόλουθο

(Π') :

$\circ$	$\mathsf{L}_\mathbf{e}$	$\mathsf{L}_\mathbf{x}$	$\mathsf{L}_\mathbf{y}$
$\mathsf{L}_\mathbf{e}$	L_e	L_x	L_y
$\mathsf{L}_\mathbf{x}$	L_x	L_y	L_e
$\mathsf{L}_\mathbf{y}$	L_y	L_e	L_x

$\surd$

1.5 Ασκήσεις

Άσκηση 1.5.1. *Έστω $f: A \longrightarrow B$ μια απεικόνιση μεταξύ συνόλων.*

1. *Να δειχθεί ότι η f είναι «1-1» αν και μόνο αν ικανοποιεί τη συνθήκη ότι αν $g,h: X \longrightarrow A$ είναι δύο απεικονίσεις, όπου X είναι ένα σύνολο, έτσι ώστε $f\circ g = f\circ h$, τότε $g = h$, δηλαδή:*

$$X \underset{h}{\overset{g}{\rightrightarrows}} A \xrightarrow{f} B \ :\quad f\circ g = f\circ h \quad\Longrightarrow\quad g = h$$

2. *Να δειχθεί ότι η f είναι «επί» αν και μόνο αν ικανοποιεί τη συνθήκη ότι αν $g,h: B \longrightarrow Y$ είναι δύο απεικονίσεις, όπου Y είναι ένα σύνολο, έτσι ώστε $g\circ f = h\circ f$, τότε $g = h$, δηλαδή:*

$$A \xrightarrow{f} B \underset{h}{\overset{g}{\rightrightarrows}} Y \ :\quad g\circ f = h\circ f \quad\Longrightarrow\quad g = h$$

Άσκηση 1.5.2. *Να περιγραφούν όλες οι δυνατές σχέσεις ισοδυναμίας επί ενός συνόλου με τέσσερα στοιχεία.*

Άσκηση 1.5.3. *Έστω $n,m\in\mathbb{N}$ και έστω τα σύνολα πηλίκα $\mathbb{Z}_n$ και $\mathbb{Z}_m$ του $\mathbb{Z}$ ως προς τις σχέσεις ισοδυναμίας $\mathscr{R}_n$ και $\mathscr{R}_m$ αντίστοιχα, όπως στο παράδειγμα 1.2.5.*

1. *Πότε ισχύει ότι $\mathscr{R}_n \subseteq \mathscr{R}_m$ (ως υποσύνολα του $\mathbb{Z}\times\mathbb{Z}$);*
2. *Πότε ορίζοντας αντιστοιχία $f: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$, $f([x]_n) = [x]_m$, αποκτούμε μια καλά ορισμένη απεικόνιση;*
3. *Γενικότερα, αν $k\in\mathbb{Z}$, να εξεταστεί πότε ορίζοντας $f: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$, $f([x]_n) = [kx]_m$ αποκτούμε μια καλά ορισμένη απεικόνιση.*

Άσκηση 1.5.4. *Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί ενός συνόλου X και $\mathscr{T}$ μια σχέση ισοδυναμίας επί ενός συνόλου Y. Να δειχθεί ότι ορίζοντας:*

$$\forall\,(x,y),(z,w)\in X\times Y:\quad (x,y)\sim_{\mathscr{R}\times\mathscr{T}}(z,w) \iff x\sim_{\mathscr{R}} z \quad\text{και}\quad y\sim_{\mathscr{T}} w$$

αποκτούμε μια σχέση ισοδυναμίας $\mathscr{R}\times\mathscr{T}$, τη σχέση ισοδυναμίας ευθέος γινομένου, επί του $X\times Y$.

Άσκηση 1.5.5. *Έστω $\Delta = \{A_i \mid i \in I\}$ μια διαμέριση του μη κενού συνόλου X, δηλαδή: $X = \sum_{i\in I} A_i$. Έστω Y ένα σύνολο και έστω ότι $f_i \colon A_i \longrightarrow Y$ είναι απεικονίσεις, για κάθε $i \in I$. Να δειχθεί ότι υπάρχει μοναδική απεικόνιση $f \colon X \longrightarrow Y$ έτσι ώστε: $f|_{A_i} = f_i$, $\forall i \in I$.*

Υπό προϋποθέσεις μπορούν να οριστούν διάφορες πράξεις σε σχέσεις επί συνόλων. Θεωρούμε μη-κενά σύνολα X, Y, Z, και W. Έστω $\mathscr{R} \subseteq X \times Y$, $\mathscr{T} \subseteq Y \times Z$, και $\mathscr{S} \subseteq Z \times W$, σχέσεις από το X και Y, από το Y στο Z, και από το Z στο W αντίστοιχα. Η *σύνθεση* $\mathscr{R} \circ \mathscr{T}$ των σχέσεων $\mathscr{R}$ και $\mathscr{T}$ ορίζεται ως η ακόλουθη σχέση από το X στο Z:

$$\mathscr{R} \circ \mathscr{T} = \{(x, z) \in X \times Z \mid \text{υπάρχει } y \in Y : (x, y) \in \mathscr{R} \text{ και } (y, z) \in \mathscr{T}\}$$

Επίσης η *αντίστροφη* της σχέσης $\mathscr{R}$ από το X στο Y ορίζεται ως η ακόλουθη σχέση από το Y στο X:

$$\mathscr{R}^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in \mathscr{R}\}$$

Συμβολίζουμε με I_X την ακόλουθη «διαγώνια» ή ταυτοτική σχέση επί ενός συνόλου X:

$$I_X = \{(x, x) \in X \times X \mid x \in X\}$$

Άσκηση 1.5.6. *Διατηρώντας τους παραπάνω συμβολισμούς, να δείξετε τα ακόλουθα.*

1. *Αν οι σχέσεις $\mathscr{R}$ και $\mathscr{T}$ είναι απεικονίσεις, τότε η σχέση $\mathscr{T} \circ \mathscr{R}$ είναι απεικόνιση και μάλιστα είναι η σύνθεση των απεικονίσεων $\mathscr{R}$ και $\mathscr{T}$.*
2. *Δείξτε ότι: $(\mathscr{T} \circ \mathscr{R})^{-1} = \mathscr{R}^{-1} \circ \mathscr{T}^{-1}$.*
3. *Ισχύει η προσεταιριστική ιδιότητα σύνθεσης σχέσεων: $\mathscr{S} \circ (\mathscr{T} \circ \mathscr{R}) = (\mathscr{S} \circ \mathscr{T}) \circ \mathscr{R}$.*
4. *$\mathscr{R} \circ I_X = \mathscr{R} = I_Y \circ \mathscr{R}$.*
5. *Αν $X = Y$, και οι σχέσεις $\mathscr{R}$ και $\mathscr{T}$ είναι σχέσεις ισοδυναμίας, να εξεταστεί αν οι σχέσεις $\mathscr{R} \circ \mathscr{T}$ και $\mathscr{R}^{-1}$ είναι σχέσεις ισοδυναμίας.*

Στην ακόλουθη άσκηση ζητείται να χαρακτηριστούν οι σχέσεις ισοδυναμίας με βάση πράξεις επί αυτών.

Άσκηση 1.5.7. *Έστω $\mathscr{R}$ μια σχέση επί του μη κενού συνόλου Q.*

1. *Η σχέση $\mathscr{R}$ είναι ανακλαστική αν και μόνο αν $I_X \subseteq \mathscr{R}$.*
2. *Η σχέση $\mathscr{R}$ είναι συμμετρική αν και μόνο αν $\mathscr{R} = \mathscr{R}^{-1}$.*
3. *Η σχέση $\mathscr{R}$ είναι μεταβατική αν και μόνο αν $\mathscr{R} \circ \mathscr{R} \subseteq \mathscr{R}$.*
4. *Η σχέση $\mathscr{R}$ είναι σχέση ισοδυναμίας αν και μόνο αν $I_X \subseteq \mathscr{R}$ και $\mathscr{R} = \mathscr{R} \circ \mathscr{R}^{-1}$.*

Άσκηση 1.5.8. 1. *Να βρεθεί σχέση $\mathscr{R}$ επί κατάλληλου μη κενού συνόλου X η οποία είναι ανακλαστική και συμμετρική, αλλά δεν είναι μεταβατική (και άρα σχέση ισοδυναμίας επί του X).*

2. *Να βρεθεί σχέση $\mathscr{S}$ επί κατάλληλου μη κενού συνόλου Y η οποία είναι συμμετρική και μεταβατική, αλλά δεν είναι ανακλαστική (και άρα σχέση ισοδυναμίας επί του Y).*

3. *Να βρεθεί σχέση $\mathscr{T}$ επί κατάλληλου μη κενού συνόλου Z η οποία είναι ανακλαστική και μεταβατική, αλλά δεν είναι συμμετρική (και άρα σχέση ισοδυναμίας επί του Z).*

Άσκηση 1.5.9. *Έστω $\mathscr{R}$ μια σχέση ισοδυναμίας επί ενός συνόλου X το οποίο είναι εφοδιασμένο με μια πράξη «$\star$». Να δειχθεί ότι η σχέση ισοδυναμίας $\mathscr{R}$ είναι συμβιβαστή με την πράξη «$\star$» αν και μόνο αν:*

$$\forall x, y, z \in X : \quad x \sim_{\mathscr{R}} y \implies x \star z \sim_{\mathscr{R}} y \star z \quad \text{και} \quad z \star x \sim_{\mathscr{R}} z \star y$$

Άσκηση 1.5.10. *Θεωρούμε το σύνολο $\mathscr{CS}(\mathbb{Q})$ των ακολουθιών Cauchy ρητών αριθμών.*[17] *Στο σύνολο $\mathscr{CS}(\mathbb{Q})$ ορίζουμε τη σχέση $\mathscr{R} \subseteq \mathscr{CS}(\mathbb{Q}) \times \mathscr{CS}(\mathbb{Q})$ ως εξής:*

$$(r_n)_{n\in\mathbb{N}} \sim_{\mathscr{R}} (r'_n)_{n\in\mathbb{N}} \iff \eta\ (r_n - r'_n)_{n\in\mathbb{N}} \text{ είναι μια μηδενική ακολουθία: } \varinjlim(r_n - r'_n) = 0$$

1. *Να δειχθεί ότι η $\mathscr{R}$ είναι μια σχέση ισοδυναμίας επί τού $\mathscr{CS}(\mathbb{Q})$.*
2. *Να περιγραφεί το σύνολο πηλίκο $\mathscr{CS}(\mathbb{Q})/\mathscr{R}$.*

Άσκηση 1.5.11. *Θεωρούμε το σύνολο $\mathbb{R}$ των πραγματικών αριθμών και έστω $\mathbb{R}[t]$ το σύνολο των πολυωνύμων με συντελεστές από το $\mathbb{R}$. Για κάθε πολυώνυμο $H(t) \in \mathbb{R}[t]$, ορίζουμε μια σχέση $\mathscr{R}_{H(t)}$ στο σύνολο $\mathbb{R}[t]$ ως εξής:*

$$\forall\, P(t), Q(t) \in \mathbb{R}[t]:\ P(t) \sim_{\mathscr{R}_{H(t)}} Q(t) \iff H(t) \mid P(t) - Q(t) \text{ δηλαδή υπάρχει } A(t) \in \mathbb{R}[t]:\ P(t) - Q(t) = A(t)H(t)$$

1. *Να δειχθεί ότι η σχέση $\mathscr{R}_{H(t)}$ είναι μια σχέση ισοδυναμίας επί του $\mathbb{R}[t]$.*
2. *Αν $H(t) = t^2 + 1$, να δειχθεί ότι το σύνολο πηλίκο $\mathbb{R}[t]/\mathscr{R}_{H(t)}$ είναι σε «1-1» και «επί» αντιστοιχία με το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών.*

Άσκηση 1.5.12. *Έστω $(X, \star)$ μια ημιομάδα. Στο σύνολο X επισυνάπτουμε ένα νέο στοιχείο ω (η μόνη απαίτηση για το ω είναι ότι δεν ανήκει στο σύνολο X). Θεωρούμε το συνολο $X(\omega) = X \cup \{\omega\}$, επί του οποίου ορίζουμε διμελή πράξη*

$$\widetilde{\star}:\ X(\omega) \times X(\omega) \longrightarrow X(\omega),\quad x \widetilde{\star} y = x \star y \ \text{ αν } \ x, y \in X,\quad \omega \widetilde{\star} \omega = \omega = \omega,\quad \text{και } \ \forall x \in X:\quad x \widetilde{\star} \omega = x = \omega \widetilde{\star} x$$

Να δειχθεί ότι το ζεύγος $(X(\omega), \widetilde{\star})$ είναι ένα μονοειδές και η απεικόνιση

$$f: (X, \star) \longrightarrow (X(\omega), \widetilde{\star}),\quad f(x) = x$$

είναι «1-1» και ένας ομομορφισμός ημιομάδων.[18]

Άσκηση 1.5.13. *Έστω $f: (X, \star) \longrightarrow (Y, *)$ μια απεικόνιση μεταξύ μονοειδών έτσι ώστε: $f(x \star y) = f(x) * f(y)$, $\forall x, y \in X$. Να δειχθεί ότι δεν είναι απαραίτητο ότι ισχύει $f(e_X) = e_Y$, και επομένως η απεικονιση f δεν είναι απαραίτητα ομομορφισμός μονοειδών.*

Άσκηση 1.5.14. *Έστω $f: (X, \star) \longrightarrow (Y, *)$ μια απεικόνιση μεταξύ μονοειδών έτσι ώστε: $f(x \star y) = f(x) * f(y)$, $\forall x, y \in X$. Αν το στοιχείο $f(e_X) \in Y$ είναι αντιστρέψιμο, να δειχθεί ότι $f(e_X) = e_Y$ και επομένως η απεικονιση f είναι ομομορφισμός μονοειδών.*

Άσκηση 1.5.15. *Έστω $f: (X, \star) \longrightarrow (Y, *)$ μια απεικόνιση «επί» μεταξύ μονοειδών, έτσι ώστε: $f(x \star y) = f(x) * f(y)$, $\forall x, y \in X$. Να δειχθεί ότι $f(e_X) = e_Y$ και επομένως η f είναι ομομορφισμός μονοειδών.*

Άσκηση 1.5.16. *Θεωρούμε την ακόλουθη πράξη «$*$» επί του $\mathbb{Z}$:*

$$\forall n, m \in \mathbb{Z}:\quad n \star m = n + m - nm$$

Να δειχθεί ότι το ζεύγος $(\mathbb{Z}, *)$ είναι μονοειδές. Ποιο είναι το ουδέτερο στοιχείο του; Ποια είναι η σχέση του μονοειδούς $(\mathbb{Z}, *)$ με το μονοειδές $(\mathbb{Z}, \cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός ακεραίων;

[17] Υπενθυμίζουμε ότι μια ακολουθία $(r_n)_{n\in\mathbb{N}}$, $r_n \in \mathbb{Q}$, $\forall n \in \mathbb{N}$, ρητών αριθμών καλείται **ακολουθία Cauchy** αν:

$$\forall \epsilon \in \mathbb{Q},\ \epsilon > 0,\ \exists n_0 \in \mathbb{N}:\ \forall m, n \geq n_0 \implies |r_n - r_m| < \epsilon$$

[18] Σύμφωνα με την παραπάνω Άσκηση κάθε ημιομάδα «εμφυτεύεται» σε ένα μονοειδές.

Άσκηση 1.5.17. *Έστω $f\colon (X,\star)\longrightarrow (Y,*)$ ένας ομομορφισμός μονοειδών.*

1. *Αν S είναι ένα υπομονοειδές του X, να δειχθεί ότι το υποσύνολο $f(S)$ είναι ένα υπομονοειδές του Y.*
2. *Αν T είναι ένα υπομονοειδές του Y, να δειχθεί ότι το υποσύνολο $f^{-1}(T)$ είναι ένα υπομονοειδές του X.*

Άσκηση 1.5.18. *Να υπολογιστεί η αριστερή κανονική αναπαράσταση $(\mathsf{Im}(\mathsf{L}),\circ)$ του προσθετικού μονοειδούς $(\mathbb{Z}_4,+)$ και του μονοειδούς ευθέος γινομένου $(\mathbb{Z}_2,+)\times(\mathbb{Z}_2,+)$.*

Άσκηση 1.5.19. *Έστω $(X,\star)$ ένα μονοειδές και $(G,\cdot)$ ένα μονοειδές κάθε στοιχείο του οποίου είναι αντιστρέψιμο, δηλαδή ισχύει ότι $G=\mathsf{U}(G)$. Να δειχθεί ότι για κάθε ομομορφισμό μονοειδών $f\colon G\longrightarrow X$ ισχύει ότι $\mathsf{Im}(f)\subseteq\mathsf{U}(X)$, και άρα ορίζεται η απεικόνιση $f'\colon G\longrightarrow\mathsf{U}(X)$, $f'(a)=f(a)$ η οποία είναι ομομορφισμός μονοειδών. Επιπλέον η απεικόνιση*

$$\Phi\colon \mathsf{Hom}_{\mathrm{Mon}}(G,X)\longrightarrow \mathsf{Hom}_{\mathrm{Mon}}(G,\mathsf{U}(X)),\quad \Phi(f)=f'$$

είναι «1-1» και «επί».

Άσκηση 1.5.20. *Να δειχθεί ότι υπάρχουν n^{n^2} διαφορετικές (διμελείς) πράξεις επί ενός συνόλου X με πλήθος στοιχείων ίσο με n. Πόσες από αυτές τις πράξεις είναι μεταθετικές;*

Να δειχθεί ότι υπάρχουν ακριβώς 7 διαφορετικά μονοειδή με πλήθος στοιχείων ίσο με 3.

Άσκηση 1.5.21. *Θεωρούμε το μονοειδές $(\mathsf{Map}(X),\circ)$ των απεικονίσεων επί ενός συνόλου X με πεπερασμένο πλήθος στοιχείων, και έστω $A\subseteq X$. Να δειχθεί ότι το υποσύνολο*

$$\mathsf{Map}_A(X)=\{f\in\mathsf{Map}(X)\mid f(A)\subseteq A\}$$

είναι κλειστό στην πράξη της σύνθεσης απεικονίσεων και επομένως το ζεύγος $(\mathsf{Map}_A(X),\circ)$ είναι ένα μονοειδές.

Άσκηση 1.5.22. *Θεωρούμε το μονοειδές $(\mathsf{Map}(X),\circ)$ των απεικονίσεων επί ενός συνόλου X με πεπερασμένο πλήθος στοιχείων, και έστω $A\subseteq X$. Να δειχθεί ότι το υποσύνολο*

$$\mathsf{S}_A(X)=\{f\in\mathsf{S}(X)\mid f(A)\subseteq A\}$$

του μονοειδούς $\mathsf{S}(X)$, και επομένως το ζεύγος $(\mathsf{S}_A(X),\circ)$ είναι ένα μονοειδές με την ιδιότητα ότι κάθε στοιχείο του είναι αντιστρέψιμο.

Άσκηση 1.5.23. *Στο σύνολο $X=\mathbb{Z}\times\mathbb{Z}$, ορίζουμε διμελή πράξη:*

$$\star\ :\ X\times X\longrightarrow X,\quad (x_1,y_1)\star(x_2,y_2)=(x_1x_2+2y_1y_2,\,x_1y_2+x_2y_1)$$

Να δειχθεί ότι το ζεύγος $(X,\star)$ είναι ένα μεταθετικό μονοειδές. Να περιγραφεί το υπομονοειδές $\mathsf{U}(X,\star)$ των αντιστρέψιμων στοιχείων του $(X,\star)$, και να δειχθεί ότι οι Νόμοι Διαγραφής, όπως περιγράφονται στην Πρόταση 1.4.12, ισχύουν για όλα τα στοιχεία του $(X,\star)$ εκτός από το στοιχείο $(0,0)$.

Άσκηση 1.5.24. *Στο σύνολο των ακεραίων $\mathbb{Z}$ ορίζουμε διμελή πράξη «$\star$» ως εξής:*

$$\star\ :\ \mathbb{Z}\times\mathbb{Z}\longrightarrow\mathbb{Z},\quad x\star y=x+y-xy$$

Να δειχθεί ότι το ζεύγος $(\mathbb{Z},\star)$ είναι μονοειδές το οποίο είναι ισόμορφο με το μονοειδές $(\mathbb{Z},\cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός ακεραίων.

Άσκηση 1.5.25. *Θεωρούμε το σύνολο* $\mathsf{A}(\mathbb{K})$ *των ακολουθιών με στοιχεία από το σύνολο* $\mathbb{K}$*, όπου* $\mathbb{K}$ *είναι ένα εκ των* $\mathbb{Z}$*,* $\mathbb{Q}$*,* $\mathbb{R}$*,* $\mathbb{C}$*. Υποθέτουμε ότι το σύνολο* $\mathsf{A}(\mathbb{K})$ *είναι εφοδιασμένο με τις πράξεις πρόσθεσης «*$+$*» και πολλαπλασιασμού «*$\cdot$*» ακολουθιών, βλέπε μέρος 10 του Παραδείγματος 1.3.8.*

1. *Να δειχθεί ότι τα ζεύγη* $(\mathsf{A}(\mathbb{K}),+)$ *και* $(\mathsf{A}(\mathbb{K}),\cdot)$ *είναι μεταθετικά μονοειδή.*
2. *Να δειχθεί ότι:*

$$\mathsf{U}(\mathsf{A}(\mathbb{K}),+)=\mathsf{A}(\mathbb{K}) \quad \text{και} \quad \mathsf{U}(\mathsf{A}(\mathbb{K}),\cdot)=\left\{\mathsf{a}=(a_n)_{n\geq 0} \mid a_0\in \mathsf{U}(\mathbb{K},\cdot) \text{ και } a_n=0, \forall\, n\geq 1\right\}$$

Άσκηση 1.5.26. *Θεωρούμε μονοειδή* $(X_1,\star_1)$*,* $(X_2,\star_2)$*,* $\cdots$*,* $(X_n,\star_n)$ *με ουδέτερο στοιχείο* e_i *αντίστοιχα, όπου* $1\leq i\leq n$*, και έστω* $(X,\star)$ *το μονοειδές ευθύ γινόμενο, βλέπε την Πρόταση 1.4.35. Να προσδιοριστεί το μονοειδές* $\mathsf{U}(X,\star)$ *των αντιστρέψιμων στοιχείων του* $(X,\star)$*.*

Άσκηση 1.5.27. *Έστω* $(X,\star)$ *ένα μονοειδές με ουδέτερο στοιχείο* e*. Ένα στοιχείο* $x\in X$ *καλείται ταυτοδύναμο αν* $x^2=x\star x=e$*. Να δειχθεί ότι, αν το μονοειδές* X *είναι μεταθετικό, τότε το σύνολο των ταυτοδύναμων στοιχείων του* X *αποτελεί ένα υπομονοειδές του* X*. Να δοθεί παράδειγμα μη μεταθετικού μονοειδούς στο οποίο το σύνολο των ταυτοδύναμων στοιχείων του δεν είναι υπομονοειδές.*

Άσκηση 1.5.28. *Αν* $(X,\star)$ *είναι ένα μεταθετικό μονοειδές και* $f_1,\cdots,f_n: X\longrightarrow X$ *είναι ομομορφισμοί μονοειδών, τότε να δειχθεί ότι η απεικόνιση*

$$f_1\star f_2\star\cdots\star f_n\ :\ X\longrightarrow X,\quad (f_1\star f_2\star\cdots\star f_n)(x)=f_1(x)\star f_2(x)\star\cdots\star f_n(x)$$

είναι ένας ομομορφισμός μονοειδών. Ισχύει το συμπέρασμα αν το μονοειδές $(X,\star)$ *δεν είναι μεταθετικό;*

Άσκηση 1.5.29. *Έστω ότι* $(X_1,\star_1)$ *και* $(X_2,\star_2)$ *είναι δύο μονοειδή και έστω* $(X,\star)$ *το μονοειδές ευθύ γινόμενο των* $(X_i,\star_i)$*,* $i=1,2$*. Να δειχθεί ότι υπάρχουν ισομορφισμοί μονοειδών*

$$X_1/\mathscr{R}\xrightarrow{\cong} X_2 \quad \text{και} \quad X_2/\mathscr{T}\xrightarrow{\cong} X_1$$

όπου $\mathscr{R}$ *και* $\mathscr{T}$ *είναι κατάλληλες σχέσεις ισοδυναμίας επί των* X_1 *και* X_2 *αντίστοιχα.*

Άσκηση 1.5.30. *Θεωρούμε μονοειδή* $(X,*)$ *και* $(X_k,\star_k)$*,* $1\leq k\leq n$*. Υποθέτουμε ότι για κάθε* $k=1,2,\cdots,n$*, υπάρχουν ομομορφισμοί μονοειδών*

$$\widetilde{\iota}_k: X_k\longrightarrow X \quad \text{και} \quad \widetilde{\pi}_k: X\longrightarrow X_k$$

έτσι ώστε, $\forall\, k,m=1,2,\cdots,n$*:*

$$\pi_k\circ\iota_m=\begin{cases}\mathsf{Id}_{X_k}, & \text{αν } k=m\\ \mathsf{e}_{mk}, & \text{αν } k\neq l\end{cases}\ :\ X_m\longrightarrow X_k \quad \text{και} \quad \mathsf{Id}_X=(\iota_1\circ\pi_1)\star(\iota_2\circ\pi_2)\star\cdots\star(\iota_n\circ\pi_n)$$

Να δειχθεί ότι υπάρχει μοναδικός ισομορφισμός μονοειδών

$$f:(X,*)\xrightarrow{\cong}(\prod_{k=1}^{n}X_k,\star) \qquad \text{έτσι ώστε:} \quad \pi_k\circ f=\widetilde{\pi}_k \quad \text{και} \quad f\circ\widetilde{\iota}_k=\iota_k,\quad 1\leq k\leq n$$

όπου οι απεικονίσεις π_k*,* e_{mk}*, και* ι_k*,* $1\leq k,m\leq n$*, είναι οι ομομορφισμοί μονοειδών της Πρότασης 1.4.35.*

Άσκηση 1.5.31. *Έστω* $(X,\star)$ *ένα μονοειδές και* $x\in X$ *ένα στοιχείο του. Θεωρούμε το κυκλικό μονοειδές* $[x\rangle$ *το οποίο παράγεται από το* x*, βλέπε το Παράδειγμα 1.4.30.*

1. *Αν το σύνολο* $[x\rangle$ *είναι άπειρο, τότε να δειχθεί ότι το μονοειδές* $[x\rangle$ *ειναι ισόμορφο με το μονοειδές* $(\mathbb{N}_0,+)$*.*
2. *Αν το σύνολο είναι πεπερασμένο, τότε υπάρχουν μη αρνητικοί ακέραιοι* n *και* k*, όπου* $k\geq 1$*, έτσι ώστε:*

$$[x\rangle=\left\{e,\,x,\,x^2,\cdots,x^{n+k-1}\mid x^{n+k}=x^n\right\}$$

Κεφάλαιο 2

Ομάδες: Βασικές Ιδιότητες, Παραδείγματα, και Κατασκευές

Στο παρόν Κεφάλαιο θα μελετήσουμε αναλυτικά την έννοια της ομάδας. Εν συντομία, μια ομάδα είναι ένα μονοειδές κάθε στοιχείο του οποίου είναι αντιστρέψιμο. Έτσι η έννοια της ομάδας αποτελεί ειδική περίπτωση της έννοιας του μονοειδούς. Η θεωρία ομάδων είναι πολύ πιο πλούσια από τη θεωρία μονοειδών και αποτελεί έναν από τους δομικούς λίθους της σύγχρονης άλγεβρας. Από την άλλη πλευρά, η θεωρία ομάδων διαδραματίζει σπουδαίο ρόλο σε πολλές περιοχές των Μαθηματικών, καθώς και άλλων επιστημών, καθώς αποτελεί το κατάλληλο εννοιολογικό πλαίσιο μελέτης φαινομένων συμμετρίας. Για τους παραπάνω λόγους, η θεωρία ομάδων αξίζει να μελετηθεί διεξοδικότερα και ανεξάρτητα από τη θεωρία μονοειδών. Έτσι στην παρούσα ενότητα θα αναλύσουμε τις βασικές ιδιότητες ομάδων, θα δώσουμε παραδείγματα και κατασκευές ομάδων, ανεξάρτητα από την εκτεθείσα θεωρία μονοειδών στις υποενότητες 1.4 και 1.4.2 του Κεφαλαίου 1.

2.1 Η Έννοια της Ομάδας και Βασικές Ιδιότητες

Στην παρούσα ενότητα εισάγουμε την έννοια της ομάδας, αναπτύσσουμε τις βασικές ιδιότητες οι οποίες απορρέουν από τα αξιώματα, και δίνουμε διάφορους χαρακτηρισμούς ομάδων οι οποίοι θα μας είναι χρήσιμοι στη συνέχεια. Στην επόμενη υποενότητα θα δοθεί πληθώρα παραδειγμάτων ομάδων.

Σημειώνουμε ότι από τώρα και στο εξής θεωρούμε γνωστές τις βασικές ιδιότητες διμελών πράξεων επί συνόλων οι οποίες αναπτύχθηκαν στο προηγούμενο Κεφάλαιο.

2.1.1 Η Έννοια της Ομάδας

Εν συντομία μια ομάδα είναι ένα μονοειδές, με την έννοια του Ορισμού 1.4.1, κάθε στοιχείο του οποίου έχει αντίστροφο. Αναλυτικότερα:

Ορισμός 2.1.1. *Μια* **ομάδα** *είναι ένα ζεύγος $(G, \star)$, όπου G είναι ένα σύνολο, και*

$$\star : G \times G \longrightarrow G, \quad \star(x, y) = x \star y$$

είναι μια διμελής πράξη επί του συνόλου G, για την οποία ικανοποιούνται τα ακόλουθα αξιώματα:

1. *Η πράξη «$\star$» είναι* **προσεταιριστική**, *δηλαδή ισχύει ότι:*

$$\forall x, y, z \in G: \quad x \star (y \star z) = (x \star y) \star z \tag{2.1}$$

2. *Υπάρχει ένα στοιχείο $e \in G$, το οποίο καλείται* **ουδέτερο** *ή* **ταυτοτικό στοιχείο** *της G, έτσι ώστε:*

$$\forall x \in G: \quad x \star e = x = e \star x \tag{2.2}$$

3. *Για κάθε στοιχείο $x \in G$, υπάρχει ένα στοιχείο $x' \in G$, το οποίο καλείται* **αντίστροφο** *ή* **αντίθετο στοιχείο** *του x, έτσι ώστε να ισχύει:*
$$\forall x \in G,\ \exists x' \in G: \quad x \star x' = e = x' \star x \tag{2.3}$$

Μια ομάδα $(G, \star)$ καλείται **αβελιανή**[1] *ή* **μεταθετική** *αν επιπλέον:*

4. *Η πράξη «$\star$» είναι* **μεταθετική**, *δηλαδή ισχύει:*
$$\forall x, y \in G: \quad x \star y = y \star x \tag{2.4}$$

Η ακόλουθη βοηθητική πρόταση πιστοποιεί ότι το ουδέτερο στοιχείο e μιας ομάδας $(G, \star)$ είναι μοναδικό, και επίσης το αντίστροφο στοιχείο x' κάθε στοιχείου $x \in G$ είναι επίσης μοναδικό.

Λήμμα 2.1.2. *Έστω $(G, \star)$ μια ομάδα.*

1. *Αν e και e' είναι δύο ουδέτερα στοιχεία της G, δηλαδή τα στοιχεία τα οποία ικανοποιούν το Αξίωμα (2.2) του Ορισμού 2.1.1, τότε $e = e'$.*

2. *Αν $x \in G$, και x' και x'' είναι δύο αντίστροφα ή αντίθετα στοιχεία της G, δηλαδή στοιχεία του συνόλου G τα οποία ικανοποιούν το Αξίωμα 2.3 του Ορισμού 2.1.1, τότε $x = x'$.*

Απόδειξη. 1. Επειδή το στοιχείο e είναι ουδέτερο στοιχείο της G, θα έχουμε $e \star e' = e' = e' \star e$. Επειδή το στοιχείο e' είναι επίσης ουδέτερο στοιχείο της G, θα έχουμε και $e' \star e = e = e \star e'$. Επομένως $e = e'$.

2. Θα έχουμε τις σχέσεις: $x \star x' = e = x' \star x$ και $x \star x'' = e = x'' \star x$. Τότε:
$$x'' \star (x \star x') = x'' \star e \implies (x'' \star x) \star x' = x'' \implies e \star x' = x'' \implies x' = x''$$ ■

Υπενθυμίζουμε ότι αν «$\star$» είναι μια προσεταιριστική πράξη επί ενός συνόλου X για την οποία υπάρχει ουδέτερο στοιχείο $e \in X$, τότε ορίζεται η n-οστή δύναμη $\star^n x$ κάθε στοιχείου $x \in X$, αν $n \geq 0$ ή αν $n < 0$ και το στοιχείο x είναι αντιστρέψιμο με αντίστροφο το στοιχείο x', ως εξής (βλέπε τον Ορισμό 1.3.16):
$$\star^n x := \begin{cases} \underbrace{x \star x \star \cdots \star x}_{n-\text{παράγοντες}}, & \text{αν } n > 0 \\ e, & \text{αν } n = 0 \\ \underbrace{x' \star x' \star \cdots \star x'}_{n-\text{παράγοντες}}, & \text{αν } n < 0 \end{cases} \tag{2.5}$$

Για την περαιτέρω ανάπτυξη των βασικών ιδιοτήτων της γενικής θεωρίας ομάδων, είναι χρήσιμο να απλοποιήσουμε τον συμβολισμό μας.

Συμβολισμός 2.1.3. Όπως και στην γενική θεωρία διμελών πράξεων επί συνόλων, στη θεωρία ομάδων οι επικρατέστεροι συμβολισμοί πράξεων είναι ο πολλαπλασιαστικός και ο προσθετικός συμβολισμός:

• (Πολλαπλασιαστικός Συμβολισμός) Αν ο συμβολισμός της διμελούς πράξης σε μια ομάδα G είναι «πολλαπλασιαστικός», δηλαδή προσομοιάζει με την συνήθη πράξη πολλαπλασιασμού σε ένα σύνολο αριθμών, οπότε χρησιμοποιούμε ως σύμβολο της διμελούς πράξης το σύμβολο «$\cdot$», τότε για κάθε στοιχείο x σε μια ομάδα $(G, \cdot)$, και για κάθε ακέραιο $n \in \mathbb{Z}$, θα γράφουμε $\cdot^n x := x^n$. Το στοιχείο x^n καλείται η n-**οστή δύναμη** (φυσική ή ακέραια) του x ως προς την πράξη «$\cdot$» της ομάδας G. Σημειώνουμε ότι στον πολλαπλασιαστικό

[1] Η ορολογία «αβελιανή», στα αγγλικά «abelian», προέρχεται από το επώνυμο του Nield Henrik Abel 1802-1829 [http://en.wikipedia.org/wiki/Niels_Henrik_Abel], ο οποίος υπήρξε σημαντικός Νορβηγός μαθηματικός με πρωτοπόρα συμβολή στη Θεωρία Ομάδων, στη Θεωρία Συναρτήσεων, και στη Θεωρία (αλγεβρικών) Εξισώσεων.

συμβολισμό, συνήθως το ουδέτερο στοιχείο e συμβολίζεται με 1, και το αντίστροφο x' ενός στοιχείου $x \in G$ συμβολίζεται με $x^{-1} \in X$, και οι σχέσεις (2.5) παίρνουν την ακόλουθη μορφή:

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \cdots \cdot x}_{n-\text{παράγοντες}}, & \text{αν } n > 0 \\ e, & \text{αν } n = 0 \\ \underbrace{x^{-1} \cdot x^{-1} \cdot \cdots \cdot x^{-1}}_{(-n)-\text{παράγοντες}}, & \text{αν } n < 0 \end{cases}$$

• (Προσθετικός Συμβολισμός) Αν ο συμβολισμός της διμελούς πράξης σε μια ομάδα G είναι «προσθετικός», δηλαδή προσομοιάζει με την συνήθη πράξη πρόσθεσης σε ένα σύνολο αριθμών, οπότε χρησιμοποιούμε ως σύμβολο της διμελούς πράξης το σύμβολο «+», τότε για κάθε στοιχείο x σε μια ομάδα $(G,+)$, και για κάθε ακέραιο $n \in \mathbb{Z}$, θα γράφουμε $\cdot^n x := nx$. Το στοιχείο nx καλείται η n-**οστό πολλαπλάσιο** (φυσικό ή ακέραιο) του x ως προς την πράξη «+» της ομάδας G. Σημειώνουμε ότι, στον προσθετικό συμβολισμό, συνήθως το ουδέτερο στοιχείο e συμβολίζεται με 0, και το αντίστροφο x' ενός στοιχείου $x \in G$ συμβολίζεται με $-x \in X$, και οι σχέσεις (2.5) παίρνουν την ακόλουθη μορφή:

$$nx := \begin{cases} \underbrace{x + x + \cdots + x}_{n-\text{παράγοντες}}, & \text{αν } n > 0 \\ e, & \text{αν } n = 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{(-n)-\text{παράγοντες}}, & \text{αν } n < 0 \end{cases}$$

Σημειώνουμε ότι παραδοσιακά ο προσθετικός συμβολισμός για μια πράξη χρησιμοποιείται συνήθως (αλλά όχι πάντα) όταν η πράξη είναι μεταθετική. ▲

Σύμβαση: Από τώρα και στο εξής, στην ανάπτυξη των βασικών στοιχείων της γενικής θεωρίας ομάδων θα χρησιμοποιούμε τον πολλαπλασιστικό συμβολισμό «·» για την πράξη μιας ομάδας. Έτσι μια ομάδα θα είναι ένα ζεύγος $(G,\cdot)$, ή απλά G όταν η πράξη «·» υπονοείται και δεν υπάρχει κίνδυνος σύγχυσης, έτσι ώστε να ικανοποιούνται τα αξιώματα του ορισμού 2.1.1. Επιπλέον, και χάριν απλότητας, για μια ομάδα $(G,\cdot)$, αρκετές φορές θα γράφουμε:

1. xy για το αποτέλεσμα της πράξης $x \cdot y$ στην ομάδα G.
2. e_G ή e ή 1 για το ουδέτερο στοιχείο της ομάδας G.
3. x^{-1} για το αντίστροφο του στοιχείου x στην ομάδα G.
4. x^n, όπου $n \in \mathbb{Z}$, για την φυσική ή ακέραια δύναμη του στοιχείου x μιας ομάδας G.

Παράλληλα, όπου κρίνουμε σκόπιμο, θα διατυπώνουμε στοιχεία της θεωρίας ομάδων χρησιμοποιώντας τον προσθετικό συμβολισμό, ο οποίος κατά κανόνα, αλλά όχι πάντα, θα είναι σε ισχύ όταν η ομάδα είναι αβελιανή.

Τέλος, αν και τυπικά μια ομάδα είναι ένα ζεύγος $(G,\cdot)$ όπου G είναι ένα μη κενό σύνολο και «·» είναι μια διμελής πράξη $\cdot : G \times G \longrightarrow G$ επί του G έτσι ώστε να ικανοποιούνται τα αξιώματα (2.1), (2.2), (2.3) του ορισμού 2.1.1, χάριν απλότητας, και αν δεν υπάρχει κίνδυνος σύγχυσης, πολλές φορές θα αναφερόμαστε στην ομάδα G, καθώς η πράξη «·» θα υπονοείται. ▲

Παρατήρηση 2.1.4. Με βάση την Σύμβαση του Συμβολισμού 2.1.3, αν $(G,\cdot)$ είναι μια ομάδα και $x, y \in G$, τότε θα γράφουμε

$$x \cdot y' = x \cdot y^{-1} \quad \text{ή απλά} \quad xy^{-1}$$

για το αποτέλεσμα της πράξης του στοιχείου x με το αντίστροφο του στοιχείου y. Στην περίπτωση προσθετικού συμβολισμού θα γράφουμε:

$$x \cdot y' = x + (-y) := x - y \quad ▲$$

Για τις δυνάμεις και αντιστοίχως τα πολλαπλάσια στοιχείων μιας ομάδας ισχύουν κανόνες ανάλογοι των κανόνων που ισχύουν για τις ακέραιες δυνάμεις και τα ακέραια πολλαπλάσια των γνωστών μας αριθμών. Η απόδειξη της ακόλουθης Πρότασης είναι ταυτόσημη με την απόδειξη της Πρότασης 1.3.18 και του Πορίσματος 1.3.19.

Πρόταση 2.1.5. *Έστω $(G,\cdot)$ μια ομάδα. Τότε για τυχόν στοιχείο $x \in G$ θα έχουμε:*

$$\forall n,m \in \mathbb{Z}: \quad x^{n+m} = x^n \cdot x^m \tag{2.6}$$

$$\forall n,m \in \mathbb{Z}: \quad (x^n)^m = x^{nm} \tag{2.7}$$

$$\forall n \in \mathbb{Z}: \quad (x^n)^{-1} = x^{-n} = (x^{-1})^n \tag{2.8}$$

Τέλος, αν $x,y \in G$ και ισχύει ότι: $x\cdot y = y\cdot x$, τότε:

$$\forall n \in \mathbb{Z}: \quad (x\cdot y)^n = x^n \cdot y^n \tag{2.9}$$

Παρατήρηση 2.1.6. Λαμβάνοντας υπόψη την Σύμβαση του Συμβολισμού 2.1.3, χρησιμοποιώντας προσθετικό συμβολισμό «+» για την πράξη μιας ομάδας $(G,+)$, η Πρόταση 2.1.5 παίρνει την ακόλουθη μορφή. Έστω $x \in G$ ένα στοιχείο της G. Τότε:

1. $\forall n,m \in \mathbb{Z}$: $(n+m)x = nx + mx$.
2. $\forall n,m \in \mathbb{Z}$: $n(mx) = (nm)x$.
3. $\forall n \in \mathbb{Z}$: $-(nx) = (-n)x = n(-x)$.
4. Αν $x+y = y+x$, τότε,[2] $\forall n \in \mathbb{Z}$: $n(x+y) = nx + ny$. ▲

2.1.2 Στοιχειώδεις Ιδιότητες Ομάδων

Στην παρούσα υποενότητα θα αναλύσουμε τις βασικές ιδιότητες τις οποίες έχει μια ομάδα και οι οποίες θα μας είναι χρήσιμες στη συνέχεια. Επιπλέον θα δώσουμε διάφορους χαρακτηρισμούς για το πότε ένα σύνολο εφοδιασμένο με μια διμελή πράξη είναι ομάδα.

Η ακόλουθη Πρόταση δείχνει ότι σε μια ομάδα ισχύουν οικεία αποτελέσματα που αφορούν γνωστές πράξεις μεταξύ αριθμών, όπως οι νόμοι διαγραφής και η επίλυση πρωτοβάθμιων γραμμικών εξισώσεων.

Πρόταση 2.1.7. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα.*

1. *(Υπαρξη και Μοναδικοτητα Λυσεων Γραμμικων Εξισωσεων σε Ομαδες). Αν $a,b \in G$, τότε η εξίσωση*

$$a\cdot x = b \quad (\text{αντίστοιχα} \quad y\cdot a = b)$$

έχει μοναδική λύση την ακόλουθη:

$$x = a^{-1}\cdot b \quad (\text{αντίστοιχα} \quad y = b\cdot a^{-1})$$

2. *(Νομοι Διαγραφης σε Ομαδες). Αν $a,b,c \in G$, τότε:*

$$a\cdot b = a\cdot c \implies b = c \quad \text{και} \quad b\cdot a = c\cdot a \implies b = c$$

[2] Προσοχή: η προσθετική εκδοχή της σχέσης (2.9) **δεν είναι** η σχέση $(x+y)^n = x^n + y^n$ η οποία γενικά δεν είναι αληθής.

Απόδειξη. 1. Για την εξίσωση $a \cdot x = b$, υποθέτουμε ότι υπάρχει λύση x, δηλαδή στοιχείο $x \in G$ έτσι ώστε $a \cdot x = b$. Χρησιμοποιώντας τα αξιώματα ομάδας του Ορισμού 2.1.1, θα έχουμε:

$$a \cdot x = b \implies a^{-1} \cdot (a \cdot x) = a^{-1} \cdot b \implies (a^{-1} \cdot a) \cdot x = a^{-1} \cdot b \implies e \cdot x = a^{-1} \cdot b \implies x = a^{-1} \cdot b$$

Αντίστροφα το στοιχείο $a^{-1} \cdot b$ ικανοποιεί την εξίσωση $a \cdot x = b$, διότι: $a \cdot (a^{-1} \cdot b) = (a \cdot a^{-1}) \cdot b = e \cdot b = b$. Άρα το στοιχείο $x = a^{-1} \cdot b$ είναι η μοναδική λύση στην ομάδα G της εξίσωσης $ax = b$.

Εργαζόμενοι παρόμοια, εύκολα βλέπουμε ότι το στοιχείο $y = b \cdot a^{-1}$ είναι η μοναδική λύση στην ομάδα G της εξίσωσης $y \cdot a = b$.

2. Υποθέτουμε ότι $a \cdot b = a \cdot c$. Τότε:

$$a \cdot b = a \cdot c \implies a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c) \implies (a \cdot a^{-1}) \cdot b = (a \cdot a^{-1}) \cdot c \implies e \cdot b = e \cdot c \implies b = c$$

Εργαζόμενοι παρόμοια, εύκολα βλέπουμε ότι αν $b \cdot a = c \cdot a$, τότε $b = c$. ■

Το ακόλουθο χρήσιμο αποτέλεσμα θα διευκολύνει πολύ την περαιτέρω ανάπτυξη της θεωρίας ομάδων.

Πρόταση 2.1.8. *Έστω ότι $(G, \cdot)$ είναι μια ομάδα.*

1. *Αν $a, b \in G$, τότε:*
$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \qquad \text{και} \qquad (a^{-1})^{-1} = a$$
Γενικότερα αν $a_1, a_2, \cdots, a_n \in G$, τότε:
$$(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1} \tag{2.10}$$

2. *Αν $a, b \in G$, τότε:*
   - *(α΄)* $a \cdot b = e \implies a = b^{-1}$ και $b = a^{-1}$.
   - *(β΄)* $a^2 = a \implies a = e$.
   - *(γ΄)* $a \cdot b = a \implies b = e$.
   - *(δ΄)* $a \cdot b = b \implies a = e$.

Απόδειξη. 1. Θεωρώντας το στοιχείο $b^{-1} \cdot a^{-1} \in G$, και χρησιμοποιώντας τα αξιώματα ομάδας, θα έχουμε:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot (b^{-1}) \cdot a^{-1}) = a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) = a \cdot (e \cdot a^{-1}) = a \cdot a^{-1} = e$$

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot (a \cdot b)) = b^{-1} \cdot ((a^{-1} \cdot a) \cdot b) = b^{-1} \cdot (e \cdot b) = b^{-1} \cdot b = e$$

Επομένως το στοιχείο ικανοποιεί το αξίωμα (2.3) του Ορισμού 2.1.1 περί ύπαρξης αντίστροφου στοιχείου για το στοιχείο $a \cdot b \in G$. Από την μοναδικότητα του αντίστροφου στοιχείου, βλέπε το Λήμμα 2.1.2, έπεται ότι: $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.

Για το τυχόν στοιχείο $a \in G$, το αξίωμα (2.3) πιστοποιεί την ύπαρξη του αντιστρόφου στοιχείου a^{-1} του a έτσι ώστε εξ ορισμού:

$$a^{-1} \cdot a = e \qquad \text{και} \qquad a \cdot a^{-1} = e$$

Ερμηνεύοντας την παραπάνω σχέση, ξεκινώντας από το στοιχείο a^{-1}, έπεται ότι το στοιχείο a ικανοποιεί την ιδιότητα του αντιστρόφου του στοιχείου a^{-1}. Επομένως, λόγω μοναδικότητας του αντίστροφου στοιχείου όπως πιστοποιείται από το Λήμμα 2.1.2, θα έχουμε: $(a^{-1})^{-1} = a$.

Θα δείξουμε με χρήση της Αρχής Μαθηματικής Επαγωγής ότι ισχύει η σχέση (2.10). Όπως δείχνει η παραπάνω ανάλυση, η σχέση (2.10) είναι αληθής αν $n = 1$ ή $n = 2$. Υποθέτουμε ότι η σχέση (2.10), για n το πλήθος στοιχεία $a_1, a_2, \cdots, a_n$. Τότε, θεωρώντας $n+1$ το πλήθος στοιχεία $a_1, a_2, \cdots, a_n, a_{n+1}$ και χρησιμοποιώντας διαδοχικά την επαγωγική υπόθεση και την προσεταιριστική ιδιότητα, θα έχουμε:

$$(a_1 \cdot a_2 \cdots a_n \cdot a_{n+1})^{-1} = [(a_1 \cdot a_2 \cdots a_n) \cdot a_{n+1})^{-1} = a_{n+1}^{-1} \cdot (a_1 \cdot a_2 \cdots a_n)^{-1} =$$

$$= a_{n+1}^{-1} \cdot (a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1}) = a_{n+1}^{-1} \cdot a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1}$$

Άρα η σχέση (2.10) ισχύει για $n+1$ το πλήθος στοιχεία, και επομένως από την Αρχή Μαθηματικής Επαγωγής, έπεται ότι η σχέση (2.10) ισχύει για κάθε φυσικό αριθμό $n \in \mathbb{N}$.

2. Έστω $a, b \in G$:

   (α') Αν $a \cdot b = e$, τότε θα έχουμε:

   $$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot e \implies (a^{-1} \cdot a) \cdot b = a^{-1} \implies e \cdot b = a^{-1} \implies b = a^{-1}$$

   $$(a \cdot b) \cdot b^{-1} = e \cdot b^{-1} \implies a \cdot (b \cdot b^{-1}) = b^{-1} \implies a \cdot e = b^{-1} \implies a = b^{-1}$$

   (β') Αν $a^2 = a$, δηλαδή $a \cdot a = a$, τότε:

   $$a^{-1} \cdot (a \cdot a) = a^{-1} \cdot a \implies (a^{-1} \cdot a) \cdot a = e \implies e \cdot a = e \implies a = e$$

   (γ') Αν $ab = a$, τότε:

   $$a \cdot b = a \implies a^{-1} \cdot (a \cdot b) = a^{-1} \cdot a \implies (a^{-1} \cdot a) \cdot b = e \implies e \cdot b = e \implies b = e$$

   (δ') Αν $a \cdot b = b$, τότε:

   $$a \cdot b = b \implies (a \cdot b) \cdot b^{-1} = b \cdot b^{-1} \implies a \cdot (b \cdot b^{-1}) = e \implies a \cdot e = e \implies a = e$$ ■

Η ακόλουθη Πρόταση δείχνει ότι τα αξιώματα (2.2) και (2.3) στον ορισμό ομάδας, μπορούν να απλοποιηθούν περαιτέρω.

Πρόταση 2.1.9. *Έστω $(G, \cdot)$ ένα ζεύγος το οποίο αποτελείται από ένα σύνολο G και μια προσεταιριστική πράξη επί του G έτσι ώστε να ικανοποιούνται τα εξής:*

1. *(Ύπαρξη αριστερού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $e \cdot a = a$, $\forall\, a \in G$.*
2. *(Ύπαρξη αριστερού αντίστροφου στοιχείου). Για κάθε στοιχείο $a \in G$, υπάρχει ένα στοιχείο $a' \in G$ έτσι ώστε: $a' \cdot a = e$.*

Τότε το ζεύγος $(G, \cdot)$ είναι ομάδα με ουδέτερο στοιχείο το e.

Απόδειξη. Για τυχόν στοιχείο $a \in G$, σύμφωνα με την συνθήκη 2., υπάρχει στοιχείο $a' \in G$ έτσι ώστε: $a' \cdot a = e$. Παρόμοια, για το στοιχείο $a' \in G$, σύμφωνα με την συνθήκη 2., υπάρχει στοιχείο $a'' \in G$ έτσι ώστε: $a'' \cdot a' = e$. Τότε, χρησιμοποιώντας τις παραπάνω σχέσεις και την προσεταιριστική ιδιότητα, θα έχουμε:

$$a \cdot a' = e \cdot (a \cdot a') = (a'' \cdot a') \cdot (a \cdot a') = a'' \cdot ((a' \cdot a) \cdot a') = a'' \cdot (e \cdot a') = a'' \cdot a' = e$$

Επομένως, για το τυχόν στοιχείο $a \in G$, υπάρχει στοιχείο $a' \in G$ έτσι ώστε: $a \cdot a' = e = a \cdot a'$, δηλαδή ισχύει το αξίωμα (2.3).

Τέλος, για το τυχόν στοιχείο $a \in G$, χρησιμοποιώντας τηη προσεταιριστική ιδιότητα της πράξης «$\cdot$» και τις παραπάνω σχέσεις, θα έχουμε:

$$a = e \cdot a = (a \cdot a') \cdot a = a \cdot (a' \cdot a) = a \cdot e$$

Άρα, για το τυχόν στοιχείο $a \in G$, θα έχουμε: $a \cdot e = a = e \cdot a$, δηλαδή ισχύει το αξίωμα (2.2). Συνοψίζοντας, δείξαμε ότι ικανοποιοιούνται τα αξιώματα (2.1), (2.2), και (2.3) του ορισμού 2.1.1, και άρα το ζεύγος $(G, \cdot)$ είναι ομάδα. ■

Παρατήρηση 2.1.10. Η Πρόταση 2.1.9 πιστοποιεί ότι ένα ζεύγος $(G, \cdot)$ είναι ομάδα, αν η πράξη «$\cdot$» είναι προσεταιριστική, αν υπάρχει αριστερό ουδέτερο στοιχείο για την πράξη «$\cdot$», και αν για κάθε στοιχείο του συνόλου G, υπάρχει αριστερό αντίστροφο στοιχείο ως προς την πράξη «$\cdot$».

Ακριβώς ανάλογα, αν $(G, \cdot)$ είναι ένα ζεύγος το οποίο αποτελείται από ένα σύνολο G και μια προσεταιριστική πράξη επί του G έτσι ώστε να ικανοποιούνται τα εξής:

1. (Ύπαρξη δεξιού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $a \cdot e = a$, $\forall\, a \in G$.

2. (Ύπαρξη δεξιού αντίστροφου στοιχείου). Για κάθε στοιχείο $a \in G$, υπάρχει ένα στοιχείο $a' \in G$ έτσι ώστε: $a \cdot a' = e$.

τότε το ζεύγος $(G, \cdot)$ είναι ομάδα.

Από την άλλη πλευρά, υπάρχουν παραδείγματα ζευγών $(G, \cdot)$, όπου «·» είναι μια προσεταιριστική πράξη επί του συνόλου G έτσι ώστε :

1. (Ύπαρξη δεξιού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $a \cdot e = a$, $\forall a \in G$.

2. (Ύπαρξη αριστερού αντίστροφου στοιχείου). Για κάθε στοιχείο $a \in G$, υπάρχει ένα στοιχείο $a' \in G$ έτσι ώστε: $a' \cdot a = e$.

ή

1. (Ύπαρξη αριστερού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $e \cdot a = a$, $\forall a \in G$.

2. (Ύπαρξη δεξιού αντίστροφου στοιχείου). Για κάθε στοιχείο $a \in G$, υπάρχει ένα στοιχείο $a' \in G$ έτσι ώστε: $a \cdot a' = e$.

και το ζεύγος $(G, \cdot)$ **δεν είναι** ομάδα.[3]

Αναφέρουμε για μελλοντική χρήση τον ακόλουθο βασικό ορισμό ο οποίος ταξινομεί την κλάση των ομάδων με βάση το πλήθος των στοιχείων τους.

Ορισμός 2.1.11. *Μια ομάδα $(G, \cdot)$ καλείται* **πεπερασμένη ομάδα** *αν το πλήθος των στοιχείων της είναι πεπερασμένο: $|G| < \infty$, διαφορετικά η G καλείται* **άπειρη ομάδα**.

Η **τάξη** *της ομάδας G ορίζεται να είναι το πλήθος $|G|$ των στοιχείων του συνόλου G όταν η ομάδα είναι πεπερασμένη, διαφορετικά το σύμβολο ∞ αν η ομάδα G είναι άπειρη, και τότε θα γράφουμε $|G| = \infty$.*

Η έννοια της τάξης ομάδας, και της συνοδού έννοιας της τάξης στοιχείου ομάδας, αναλύεται εκτενέστερα στο Κεφάλαιο 3 στο οποίο και παραπέμπουμε για περισσότερες λεπτομέρειες.

Παρατήρηση 2.1.12. Όταν μια ομάδα $(G, \cdot)$ είναι άπειρη, ο συμβολισμός $|G| = \infty$ σημαίνει ότι η ομάδα G έχει άπειρο πλήθος στοιχείων χωρίς να υπονοεί ότι το πλήθος των στοιχείων της $|G|$ είναι συγκεκριμένος άπειρος πληθάριθμος. Για παράδειγμα, οι προσθετικές ομάδες $(\mathbb{Z}, +)$ και $(\mathbb{R}, +)$ είναι και οι δύο άπειρες, αλλά το πλήθος των στοιχείων της $\mathbb{Z}$ είναι αριθμήσιμο, και άρα γνήσια μικρότερο από το πλήθος των στοιχείων της $\mathbb{R}$ το οποίο είναι μη αριθμήσιμο. Παρεπέμπουμε στην επόμενη υποενότητα για παραδείγματα σχετικά με την τάξη ομάδων. ▲

2.2 Παραδείγματα Ομάδων

Στην παρούσα ενότητα, παραθέτουμε και αναλύουμε εν συντομία βασικά παραδείγματα ομάδων, πολλά από τα οποία θα μας απασχολήσουν και στη συνέχεια.

Παράδειγμα 2.2.1. Έστω $G = \{\epsilon\}$ ένα μονοσύνολο (η φύση του στοιχείου ϵ μας είναι αδιάφορη), επί του οποίου ορίζουμε μια πράξη «·» θέτοντας $\epsilon \cdot \epsilon = \epsilon$. Τότε το ζεύγος $(G, \cdot)$ είναι κατά προφανή τρόπο μια αβελιανή ομάδα με ουδέτερο στοιχείο ϵ και $\epsilon^{-1} = \epsilon$, η οποία καλείται η **τετριμμένη ομάδα**. Αντίστροφα, αν $(G, \cdot)$ είναι μια ομάδα με ουδέτερο στοιχείο e, τότε το μονοσύνολο $\{e\}$ είναι κλειστό στην πράξη «·» και άρα το ζεύγος $(\{e\}, \cdot)$ αποτελεί ομάδα. Όπως θα δούμε αργότερα τετριμμένες ομάδες είναι δομικά ίδιες και γι' αυτό τον λόγο θα τις ταυτίζουμε. √

[3] Τέτοια παραδείγματα αναλύθηκαν διεξοδικά για πρώτη φορά στις εργασίες των A.H. Clifford: *A system arising from a weakened set of group postulates*, Annals of Mathematics **34** (1933), 865-871, και H. B. Mann: *On certain systems which are almost groups*, Bull. Amer. Math. Soc. **50** (1944), 879–881.

Παράδειγμα 2.2.2. Στην πλειονότητα των παρακάτω παραδειγμάτων ομάδων η επαλήθευση των αξιωμάτων είναι πολύ εύκολη, και σε κάθε περίπτωση έχει συζητηθεί στο Κεφάλαιο 1.

1. Τα ζεύγη $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, όπου «+» είναι η συνήθης πράξη πρόσθεσης αριθμών αποτελούν αβελιανές ομάδες. Αν $\mathbb{K}$ είναι ένα εκ των συνόλων $\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$, τότε η αβελιανή ομάδα $(\mathbb{K},+)$ καλείται η **προσθετική ομάδα του** $\mathbb{K}$.

   Αντίθετα τα ζεύγη $(\mathbb{N},+)$ και $(\mathbb{N}_0,+)$ δεν αποτελούν ομάδες (για την πράξη «+» δεν υπάρχει ουδέτερο στοιχείο στο σύνολο $\mathbb{N}$, και για έναν θετικό ακέραιο n δεν υπάρχει αντίστροφο (ή αντίθετο) στοιχείο στο σύνολο $\mathbb{N}_0$). Υπενθυμίζουμε ότι $\mathbb{N}_0=\mathbb{N}\cup\{0\}$.

2. Τα ζεύγη $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, όπου «·» είναι η συνήθης πράξη πολλαπλασιασμού αριθμών αποτελούν αβελιανές ομάδες. Υπενθυμίζουμε ότι $\mathbb{K}^*=\mathbb{K}\setminus\{0\}$. Αν $\mathbb{K}$ είναι ένα εκ των συνόλων $\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$, η αβελιανή ομάδα $(\mathbb{K}^*,\cdot)$ καλείται η **πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων του** $\mathbb{K}$.

   Αντίθετα, τα ζεύγη $(\mathbb{N},\cdot)$, $(\mathbb{N}_0,\cdot)$, $(\mathbb{Z},\cdot)$ και $(\mathbb{N},\cdot)$ και $(\mathbb{Z},\cdot)$ δεν αποτελούν ομάδα, καθώς, αν και μονοειδή, κανένα στοιχείο $n\neq\pm1$ σε ένα εκ των παραπάνω συνόλων δεν έχει αντίστροφο.

3. Γενικότερα, έστω $(\mathcal{V},+,\cdot)$ ένας $\mathbb{K}$-διανυσματικός χώρος υπεράνω ενός «σώματος» $\mathbb{K}\in\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$, με την έννοια της Γραμμικής Άλγεβρας.[4] Τότε το ζεύγος $(\mathcal{V},+)$ είναι μια αβελιανή ομάδα η οποία καλείται η **προσθετική ομάδα του διανυσματικού χώρου** $\mathcal{V}$. Για παράδειγμα, έχουμε:

   (α′) την προσθετική αβελιανή ομάδα $(\mathbb{K}[t],+)$ των πολυωνύμων υπεράνω ενός σώματος $\mathbb{K}$,

   (β′) την προσθετική αβελιανή ομάδα $(\mathsf{A}(\mathbb{K}),+)$ των ακολουθιών με στοιχεία από ένα σώμα $\mathbb{K}$,

   (γ′) την προσθετική αβελιανή ομάδα $(\mathscr{F}(S,\mathcal{V}),+)$ των συναρτήσεων $f\colon S\longrightarrow\mathcal{V}$ από ένα μη-κενό σύνολο S σε έναν $\mathbb{K}$-διανυσματικό χώρο $\mathcal{V}$, για παράδειγμα $\mathcal{V}=\mathbb{K}$, κτλ.

   Κάποιες από τις παραπάνω ομάδες θα αναλυθούν λεπτομερέστερα στη συνέχεια.

4. Έστω $\mathsf{M}_{m\times n}(\mathbb{R})$ το σύνολο όλων των $m\times n$ πινάκων A με στοιχεία πραγματικούς αριθμούς:

$$\mathsf{M}_{m\times n}(\mathbb{R})=\big\{A=(a_{ij})\mid a_{ij}\in\mathbb{R},\ 1\leq i\leq m,\ 1\leq j\leq n\big\},\quad \text{όπου}\quad A=(a_{ij})=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\ a_{21}&a_{22}&\cdots&a_{2n}\\ \vdots&\vdots&\ddots&\vdots\\ a_{m1}&a_{m2}&\cdots&a_{mn}\end{pmatrix}$$

   Στο σύνολο $\mathsf{M}_{m\times n}(\mathbb{R})$ θεωρούμε την συνήθη πράξη πρόσθεσης πινάκων: αν $A=(a_{ij})$ και $B=(b_{ij})$, τότε $A+B=(c_{ij})$, όπου $c_{ij}=a_{ij}+b_{ij}$, $1\leq i\leq m$, $1\leq j\leq n$. Η πράξη «+» επί του συνόλου $\mathsf{M}_{m\times n}(\mathbb{R})$ είναι προσεταιριστική, μεταθετική, ο *μηδενικός πίνακας* $\mathsf{O}=(x_{ij})$, όπου $x_{ij}=0$, $1\leq i\leq m$, $1\leq j\leq n$, είναι το ουδέτερο στοιχείο, και για το σύνολο των αντιθέτων στοιχείων ως προς την πράξη «+» έχουμε προφανώς $\mathsf{U}(\mathsf{M}_{m\times n}(\mathbb{R}),+)=\mathsf{M}_{m\times n}(\mathbb{R})$, διότι για κάθε πίνακα $A=(a_{ij})$, υπάρχει ο πίνακας $-A:=(-a_{ij})$ έτσι ώστε $A+(-A)=\mathsf{O}=(-A)+A$.

   Η παραπάνω ανάλυση δείχνει ότι το ζεύγος $(\mathsf{M}_{m\times n}(\mathbb{R}),+)$ είναι μια αβελιανή ομάδα. Παρόμοιο συμπέρασμα προκύπτει αν στη θέση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών είναι ένα εκ των συνόλων $\mathbb{Z}$,

[4] Υπενθυμίζουμε ότι, αν $\mathbb{K}\in\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$, τότε ένας $\mathbb{K}$-**διανυσματικός χώρος**, ή *διανυσματικός χώρος υπεράνω του* $\mathbb{K}$, είναι μια τριάδα $(\mathcal{V},+,\cdot)$, όπου το ζεύγος $(\mathcal{V},+)$ είναι μια αβελιανή ομάδα, τα στοιχεία της οποίας καλούμε διανύσματα και τα συμβολίζουμε με $\vec{x}$, $\vec{y}$, $\vec{z}$, κλπ., και

$$\cdot\colon\mathbb{K}\times\mathcal{V}\longrightarrow\mathcal{V},\quad (k,\vec{x})\longmapsto k\cdot\vec{x}$$

είναι μια εξωτερική πράξη του $\mathbb{K}$ επί του $\mathcal{V}$ έτσι ώστε να ικανοποιούνται οι ακόλουθες ιδιότητες, $\forall k,l\in\mathbb{K}$, $\forall\vec{x},\vec{y}\in\mathcal{V}$:

(α′) $(k+l)\cdot\vec{x}=k\cdot\vec{x}+l\cdot\vec{x}$.

(β′) $k\cdot(\vec{x}+\vec{y})=k\cdot\vec{x}+k\cdot\vec{y}$.

(γ′) $(kl)\cdot\vec{x}=k\cdot(l\cdot\vec{x})$.

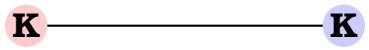
(δ′) $1\cdot\vec{x}=\vec{x}$.

Τα σύνολα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι *σώματα* με την έννοια του Κεφαλαίου 7, όπου και παραπέμπουμε για περισσότερες λεπτομέρειες. Η έννοια του διανυσματικού χώρου υπεράνω του $\mathbb{K}$ ορίζεται ακριβώς όπως παραπάνω όταν γενικότερα το σύνολο $\mathbb{K}$ είναι σώμα.

$\mathbb{Q}$, και $\mathbb{C}$, και έτσι αποκτούμε τις αβελιανές ομάδες: $(\mathsf{M}_{m\times n}(\mathbb{Z}),+)$, $(\mathsf{M}_{m\times n}(\mathbb{Q}),+)$, και $(\mathsf{M}_{m\times n}(\mathbb{C}),+)$ των $m\times n$ πινάκων A με στοιχεία ακέραιους, ρητούς, και μιγαδικούς αριθμούς αντίστοιχα. $\surd$

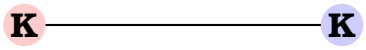
Το επόμενο παράδειγμα παρουσιάζει ένα «μη συμβατικό» παράδειγμα ομάδας.

Παράδειγμα 2.2.3. Στο ακόλουθο «Παιχνίδι με δύο Κέρματα» δύο κέρματα A και B, χρωματισμένα παρακάτω το ένα με μπλέ χρώμα (το κέρμα A) και το άλλο με κόκκινο χρώμα (το κέρμα B), βρίσκονται σε ένα τραπέζι, και στην αρχική τους θέση δείχνουν και τα δύο κορώνα (Κ):

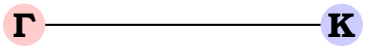


Μπορούμε να μετακινήσουμε τα κέρματα κατά τη διάρκεια του παιχνιδιού. Οι επιτρεπτές κινήσεις στα κέρματα είναι οι εξής:

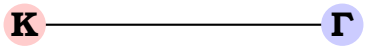
1. $I \longmapsto$ *καμία κίνηση*:



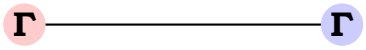
2. $M_1 \longmapsto$ *στρέφουμε το κέρμα* A:



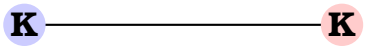
3. $M_2 \longmapsto$ *στρέφουμε το κέρμα* B:



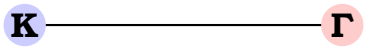
4. $M_3 \longmapsto$ *στρέφουμε τα κέρματα* A *και* B:



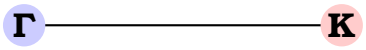
5. $M_4 \longmapsto$ *εναλλάσσουμε τις θέσεις των κερμάτων* A *και* B:



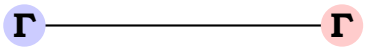
6. $M_5 \longmapsto$ *στρέφουμε το κέρμα* A *και ακολούθως εναλλάσσουμε τις θέσεις των κερμάτων* A *και* B:



7. $M_6 \longmapsto$ *στρέφουμε το κέρμα* B *και ακολούθως εναλλάσσουμε τις θέσεις των κερμάτων* A *και* B:



8. $M_7 \longmapsto$ *στρέφουμε τα κέρματα* A *και* B *και ακολούθως εναλλάσσουμε τις θέσεις των κερμάτων* A *και* B:



Θεωρούμε το σύνολο των επιτρεπτών κινήσεων του «Παιχνιδιού με δύο Κέρματα»

$$G = \{I,\ M_1,\ M_2,\ M_3,\ M_4,\ M_5,\ M_6,\ M_7\}$$

το οποίο εφοδιάζουμε με πράξη $\star\colon G\times G \longrightarrow G,\ (x,y)\longmapsto x\star y$, το αποτέλεσμα της οποίας είναι η εκτέλεση των διαδοχικών κινήσεων: πρώτα η κίνηση y ακολουθούμενη από την κίνηση x. Για παράδειγμα:

$$M_4\star M_3 = M_7 = M_3\star M_4, \qquad M_4\star M_1 = M_5 = M_2\star M_4 \quad \text{και} \quad M_1\star M_4 = M_6 \quad \text{και} \quad M_i^2 = I, \quad 1\le i\le 4$$

Η πράξη «$\star$» επί του συνόλου G δεν είναι μεταθετική διότι, για παράδειγμα:

$$M_4\star M_1 = M_5 \neq M_6 = M_1\star M_4$$

Δεν είναι δύσκολο να δείξει κανείς ότι η πράξη «$\star$» επί του συνόλου G είναι προσεταιριστική. Προφανώς το στοιχείο I είναι ουδέτερο στοιχείο για την πράξη «$\cdot$», και, όπως μπορούμε να δούμε εύκολα, κάθε στοιχείο του συνόλου G έχει αντίστροφο ως προς την πράξη «$\star$» (για παράδειγμα, $M_i^{-1} = M_i$, αν $1\le i\le 4$, και $M_5^{-1} = M_5^3 = M_6$ κλπ.). Για λεπτομέρειες, παραπέμπουμε στην Άσκηση 2.10.13, όπου ζητείται να αποδειχθεί ότι το σύνολο $(G,\star)$ είναι μια μη αβελιανή ομάδα με 8 στοιχεία (η ομάδα G αποτελεί παράδειγμα «διεδρικής» ομάδας - την κλάση των διεδρικών ομάδων θα τη συναντήσουμε και σε μεταγενέστερη ενότητα). $\surd$

Μια μεγάλη κλάση παραδειγμάτων ομάδων προκύπτει από την ακόλουθη πρόταση η οποία πιστοποιεί ότι το σύνολο των αντιστρέψιμων στοιχείων ενός μονοειδούς αποτελεί ομάδα (βλέπε το Παράδειγμα 1.3.30).

Πρόταση 2.2.4. *Έστω $(M,\cdot)$ ένα μονοειδές με ουδέτερο στοιχείο e.*

1. *Το ζεύγος $(\mathsf{U}(M,\cdot),\cdot)$ αποτελεί ομάδα, όπου*

$$\mathsf{U}(M,\cdot) = \{a\in M \mid \exists a^{-1}\in M\colon\ a\cdot a^{-1} = e = a^{-1}\cdot a\}$$

   είναι το σύνολο των αντιστρέψιμων στοιχείων του μονοειδούς $(M,\cdot)$. Επιπρόσθετα, αν το μονοειδές $(M,\cdot)$ είναι μεταθετικό, τότε η ομάδα $(\mathsf{U}(M,\cdot),\cdot)$ είναι αβελιανή.

2. *Το μονοειδές $(M,\cdot)$ είναι ομάδα αν και μόνο αν $M = \mathsf{U}(M,\cdot)$ (δηλαδή κάθε στοιχείο του μονοειδούς M είναι αντιστρέψιμο).*

Απόδειξη. 1. Δείχνουμε πρώτα ότι το σύνολο $\mathsf{U}(M,\cdot)$ είναι κλειστό στην πράξη «$\cdot$» του μονοειδούς $(M,\cdot)$. Πράγματι, αν $a,b\in\mathsf{U}(M,\cdot)$, τότε τα στοιχεία a,b διαθέτουν αντίστροφα στοιχεία $a^{-1},b^{-1}\in M$, και θα έχουμε: $a\cdot a^{-1} = e = a^{-1}\cdot a$ και $b\cdot b^{-1} = e = b^{-1}\cdot b$. Τότε:

$$(a\cdot b)\cdot(b^{-1}\cdot a^{-1}) = a\cdot(b\cdot(b^{-1}\cdot a^{-1})) = a\cdot((b\cdot b^{-1})\cdot a^{-1}) = a\cdot(e\cdot a^{-1}) = a\cdot a^{-1} = e$$

$$(b^{-1}\cdot a^{-1})\cdot(a\cdot b) = ((b^{-1}\cdot a^{-1})\cdot a)\cdot b = (b^{-1}\cdot(a^{-1})\cdot a)\cdot b = (b^{-1}\cdot e)\cdot b = b^{-1}\cdot b = e$$

Οι παραπάνω σχέσεις δείχνουν ότι το στοιχείο $a\cdot b\in M$ είναι αντιστρέψιμο, δηλαδή ανήκει στο υποσύνολο $\mathsf{U}(M,\cdot)$, και μάλιστα: $(a\cdot b)^{-1} = b^{-1}\cdot a^{-1}$. Ιδιαίτερα έπεται ότι το υποσύνολο $\mathsf{U}(M,\cdot)$ είναι κλειστό στην πράξη «$\cdot$» του μονοειδούς $(M,\cdot)$. Επειδή $e\cdot e = e$, έπεται ότι $e\in\mathsf{U}(M,\cdot)$ και τότε το στοιχείο e είναι ουδέτερο στοιχείο για την πράξη «$\cdot$» του υποσυνόλου $\mathsf{U}(M,\cdot)$. Επομένως το ζεύγος $(\mathsf{U}(M,\cdot),\cdot)$ είναι ένα υπομονοειδές του $(M,\cdot)$.

Ιδιαίτερα για το ζεύγος $(\mathsf{U}(M,\cdot),\cdot)$ ικανοποιούνται τα αξιώματα (2.1) και (2.2) του Ορισμού 2.1.1, και μένει να δείξουμε το αξίωμα (2.3), δηλαδή ότι κάθε στοιχείο $a\in\mathsf{U}(M,\cdot)$ είναι αντιστρέψιμο. Αυτό προκύπτει άμεσα, διότι το στοιχείο a^{-1} είναι προφανώς το αντίστροφο του a και ανήκει στο υπομονοειδές $\mathsf{U}(M,\cdot)$. Επομένως το ζεύγος $(\mathsf{U}(M,\cdot),\cdot)$ είναι ομάδα, η οποία είναι προφανώς αβελιανή αν το μονοειδές $(M,\cdot)$ είναι μεταθετικό.

2. Επειδή από το μέρος 1., το ζεύγος $(\mathsf{U}(M,\cdot),\cdot)$ είναι ομάδα, αν $M = \mathsf{U}(M,\cdot)$, τότε το μονοειδές $(M,\cdot)$ είναι ομάδα. Αντίστροφα, αν το μονοειδές $(M,\cdot)$ αποτελεί ομάδα, τότε κάθε στοιχείο του M είναι αντιστρέψιμο και άρα: $M = \mathsf{U}(M,\cdot)$. ■

Ως εφαρμογή της Πρότασης 2.2.4 αποκτούμε τα ακόλουθα παραδείγματα ομάδων.

Παράδειγμα 2.2.5. (Ομάδες Κλάσεων Υπολοίπων mod n). Θεωρούμε τα μεταθετικά μονοειδή $(\mathbb{Z}_n,+)$ και $(\mathbb{Z}_n,\cdot)$, όπου

$$\mathbb{Z}_n=\{[0]_n,\ [1]_n,\ \cdots,\ [n-1]_n\}$$

είναι το σύνολο των κλάσεων υπολοίπων mod n και «+», «·» οι πράξεις οι οποίες ορίστηκαν στο Παράδειγμα 1.3.40. Από την Πρόταση 2.2.4 έπεται ότι τα ζεύγη $(\mathsf{U}(\mathbb{Z}_n),+)$ και $(\mathsf{U}(\mathbb{Z}_n),\cdot)$ των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$ ως προς τις πράξεις και «+», «·» είναι αβελιανές ομάδες. Επειδή κάθε στοιχείο $[k]_n\in\mathbb{Z}_n$ είναι αντιστρέψιμο ως προς την πράξη «+» με αντίστροφο την κλάση υπολοίπων $[-k]_n$ (πράγματι: $[k]_n+[-k]_n=[k-k]_n=[0]_n=[-k]_n+[k]_n$), έπεται ότι $(\mathsf{U}(\mathbb{Z}_n),+)=(\mathbb{Z}_n,+)$ και άρα το ζεύγος $(\mathbb{Z}_n),+)$ είναι αβελιανή ομάδα.

Από την άλλη πλευρά ισχύει ότι:

$$\mathsf{U}(\mathbb{Z}_n,\cdot)=\{[k]_n\in\mathbb{Z}_n\mid (k,n)=1\} \tag{2.11}$$

Απόδειξη: Έστω ότι $[k]_n\in\mathsf{U}(\mathbb{Z}_n,\cdot)$. Τότε υπάρχει κλάση ισοτιμίας $[l]_n$ έτσι ώστε: $[k]_n\cdot[l]_n=[1]_n$ δηλαδή $[k\cdot l]_n=[1]_n$. Τότε θα έχουμε $n\mid 1-k\cdot l$ και άρα υπάρχει ακέραιος m έτσι ώστε $1-k\cdot l=n\cdot m$ δηλαδή $1=k\cdot l+n\cdot m$. Η τελευταία σχέση είναι ισοδύναμη με τη σχέση $(k,n)=1$. Αντίστροφα, αν $(k,n)=1$, τότε από γνωστές ιδιότητες του μέγιστου κοινού διαιρέτη ακεραίων αριθμών έπεται ότι υπάρχουν ακέραιοι l,m έτσι ώστε: $1=k\cdot l+n\cdot m$. Τότε, θεωρώντας κλάσεις ισοτιμίας mod n, θα έχουμε $[1]_n=[k\cdot l+n\cdot m]_n=[k\cdot l]_n+[n\cdot m]_n=[k]_n\cdot[l]_n+[n]_n\cdot[m]_n$ και επομένως $[1]_n=[k]_n\cdot[l]_n$ διότι $[n]_n=[0]_n$. Επειδή ο πολλαπλασιασμός κλάσεων ισοτιμίας είναι μεταθετική πράξη έπεται ότι η κλάση ισοτιμίας $[k]_n$ είναι αντιστρέψιμο στοιχείο του μονοειδούς $(\mathbb{Z}_n,\cdot)$ με αντίστροφη την κλάση ισοτιμίας $[l]_n$, δηλαδή $[k]_n\in\mathsf{U}(\mathbb{Z}_n,\cdot)$. Άρα πράγματι έχουμε την ισότητα (2.11): $\mathsf{U}(\mathbb{Z}_n,\cdot)=\{[k]_n\in\mathbb{Z}_n\mid (k,n)=1\}$.

Η αβελιανή ομάδα $(\mathbb{Z}_n,+)$ καλείται η **προσθετική ομάδα των κλάσεων υπολοίπων** mod n, και η αβελιανή ομάδα $\mathsf{U}(\mathbb{Z}_n,\cdot)$ καλείται η **πολλαπλασιαστική ομάδα των αντιστρέψιμων κλάσεων υπολοίπων** mod n. $\surd$

Ομάδες Μεταθέσεων και Συμμετρικές Ομάδες

Παράδειγμα 2.2.6. (Ομάδες Μεταθέσεων - Συμμετρικές Ομάδες). Για κάθε μη κενό σύνολο X, θεωρούμε το μονοειδές $(\mathsf{Map}(X),\circ)$, όπου $\mathsf{Map}(X)=\{f\colon X\longrightarrow X\mid f:\text{απεικόνιση}\}$ είναι το σύνολο των απεικονίσεων επί ενός μη-κενού συνόλου X, και «$\circ$» είναι η πράξη της σύνθεσης απεικονίσεων:

$$\circ\colon \mathsf{Map}(X)\times\mathsf{Map}(X)\longrightarrow \mathsf{Map}(X),\quad (f,g)\longmapsto f\circ g$$

Από την Πρόταση 0.2.8, για το σύνολο των αντιστρέψιμων στοιχείων, έχουμε:

$$\mathsf{U}(\mathsf{Map}(X),\circ)=\{f\colon X\longrightarrow X\mid f:\text{απεικόνιση «1-1» και «επί»}\}=\mathsf{S}(X)$$

και άρα αποκτούμε την ομάδα $(\mathsf{S}(X),\circ)$ η οποία καλείται η **ομάδα των μεταθέσεων** του συνόλου X.

Σημειώνουμε ότι, αν το πλήθος των στοιχείων του συνόλου X είναι $|X|=n$, τότε σύμφωνα με την Πρόταση 1.3.23, το πλήθος των στοιχείων της ομάδας $\mathsf{S}(X)$ είναι $n!$. Υπενθυμίζουμε ότι, αν $X=\{1,2,\cdots,n\}$, τότε συμβολίζουμε $\mathsf{S}(X)=S_n$ και η ομάδα $(S_n,\circ)$ καλείται η n-**οστή συμμετρική ομάδα**. $\surd$

Όπως πιστοποιεί η παρακάτω Πρόταση, η ομάδα μεταθέσεων ενός μη-κενού συνόλου σπάνια είναι αβελιανή.

Πρόταση 2.2.7. *Για την ομάδα μεταθέσεων $(\mathsf{S}(X),\circ)$ ενός συνόλου $X\neq\emptyset$, τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα $(\mathsf{S}(X),\circ)$ είναι αβελιανή.*
2. *$|X|\leq 2$.*

Απόδειξη. «2. $\Longrightarrow$ 1.» Αν το σύνολο X έχει ένα στοιχείο: $X=\{a\}$, τότε προφανώς η ομάδα μεταθέσεων $\mathsf{S}(X)$ αποτελείται μόνο από την ταυτοτική μετάθεση $\mathsf{Id}_X\colon X\longrightarrow X$, $\mathsf{Id}_X(a)=a$. Επομένως $\mathsf{S}(X)=\{\mathsf{Id}_X\}$ είναι η τετριμμένη ομάδα η οποία κατά προφανή τρόπο είναι αβελιανή. Υποθέτουμε ότι το σύνολο X έχει δύο

στοιχεία: $X=\{a,b\}$. Τότε το σύνολο $\mathsf{Map}(X)$ όλων των απεικονίσεων : $X\longrightarrow X$ αποτελείται από τις ακόλουθες τέσσερις απεικονίσεις

$$\mathsf{Id}_X:\begin{cases}a\longmapsto a\\ b\longmapsto b\end{cases}\quad,\quad f:\begin{cases}a\longmapsto b\\ b\longmapsto a\end{cases}\quad,\quad g:\begin{cases}a\longmapsto a\\ b\longmapsto a\end{cases}\quad,\quad h:\begin{cases}a\longmapsto b\\ b\longmapsto b\end{cases}$$

Από τις παραπάνω απεικονίσεις, αυτές οι οποίες είναι μεταθέσεις του X, δηλαδή είναι απεικονίσεις «1-1» και «επί», είναι προφανώς οι Id_X και f. Άρα

$$\mathsf{S}(X)=\{\mathsf{Id}_X,\ f\}$$

Επειδή $\mathsf{Id}_X\circ f=f=\mathsf{Id}_X\circ f$, $\mathsf{Id}_X\circ\mathsf{Id}_X=\mathsf{Id}_X=\mathsf{Id}_X\circ\mathsf{Id}_X$, και επειδή, όπως μπορούμε να υπολογίσουμε εύκολα $f^2=f\circ f=\mathsf{Id}_X$, έπεται ότι η ομάδα $(\mathsf{S}(X),\circ)$ είναι αβελιανή. Άρα αν $|X|\le 2$, η ομάδα $(\mathsf{S}(X),\circ)$ είναι αβελιανή.

«1. $\Longrightarrow$ 2.» Έστω ότι η ομάδα $(\mathsf{S}(X),\circ)$ είναι αβελιανή. Υποθέτοντας ότι $|X|\ge 3$, θα καταλήξουμε σε άτοπο. Επειδή $|X|\ge 3$, υπάρχουν στο σύνολο X τουλάχιστον τρία διακεκριμένα στοιχεία, έστω τα a,b,c. Ορίζουμε τις ακόλουθες απεικονίσεις:

$$f:\begin{cases}a\longmapsto b\\ b\longmapsto a\\ x\longmapsto x,\ \text{αν } x\in X\setminus\{a,b\}\end{cases}\qquad\text{και}\qquad g:\begin{cases}a\longmapsto b\\ b\longmapsto c\\ c\longmapsto a\\ x\longmapsto x,\ \text{αν } x\in X\setminus\{a,b,c\}\end{cases}$$

Εκ κατασκευής ποι απεικονίσεις f και g είναι «1-1» και «επί», και άρα $f,g\in\mathsf{S}(X)$. Επειδή

$$(f\circ g)(a)=f(g(a))=f(b)=a\neq c=g(b)=g(f(a))=(g\circ f)(a),\qquad\text{έπεται ότι:}\quad f\circ g\neq g\circ f$$

και επομένως η ομάδα $\mathsf{S}(X),\circ)$ δεν είναι αβελιανή, το οποίο είναι άτοπο από την υπόθεση. Στο άτοπο καταλήξαμε υποθέτοντας ότι $|X|\ge 3$. Άρα $|X|\le 2$. ■

Θεωρούμε την n-οστή συμμετρική ομάδα $(\mathsf{S}_n,\circ)$, $n\ge 1$. Υπενθυμίζουμε, βλέπε την υποενότητα 1.3.27 και την Πρόταση 1.3.23, ότι $|\mathsf{S}_n|=n!$, και τα στοιχεία της S_n, δηλαδή οι «1-1» και «επί» απεικόνισεις

$$\sigma:\ \{1,2,\cdots,n\}\ \longrightarrow\ \{1,2,\cdots,n\},\quad i\longmapsto\sigma(i)$$

παρίστανται, χάριν εποπτείας, με έναν $2\times n$ πίνακα

$$\sigma=\begin{pmatrix}1&2&\cdots&i&\cdots&n-1&n\\ \sigma(1)&\sigma(2)&\cdots&\sigma(i)&\cdots&\sigma(n-1)&\sigma(n)\end{pmatrix}$$

του οποίου η πρώτη γραμμή περιέχει τα στοιχεία του συνόλου $\mathbb{N}_n$ και η δεύτερη γραμμή περιέχει τις εικόνες των στοιχείων αυτών μέσω της μετάθεσης σ. Αν $\sigma,\tau\in\mathsf{S}_n$, τότε για το γινόμενο $\sigma\cdot\tau$ των μεταθέσεων σ και τ, δηλαδή για τη σύνθεση των απεικονίσεων σ και τ, όπου πρώτα εφαρμόζουμε τη συνάρτηση τ, θα έχουμε

$$\sigma\tau=\begin{pmatrix}1&2&\cdots&n-1&n\\ \sigma(1)&\sigma(2)&\cdots&\sigma(n-1)&\sigma(n)\end{pmatrix}\begin{pmatrix}1&2&\cdots&n-1&n\\ \tau(1)&\tau(2)&\cdots&\tau(n-1)&\tau(n)\end{pmatrix}=$$

$$=\begin{pmatrix}1&2&\cdots&n-1&n\\ \sigma(\tau(1))&\sigma(\tau(2))&\cdots&\sigma(\tau(n-1))&\sigma(\tau(n))\end{pmatrix}$$

Η ταυτοτική μετάθεση, δηλαδή η ταυτοτική απεικόνιση $\mathrm{Id}_{\mathbb{N}_n}$, συμβολίζεται συνήθως με ι και είναι

$$\iota=\begin{pmatrix}1&2&\cdots&n-1&n\\ 1&2&\cdots&n-1&n\end{pmatrix}$$

Για λόγους αναφοράς περιγράφουμε τα στοιχεία των συμμετρικών ομάδων S_n, όταν $n\le 3$.

1. Αν $n=1$, τότε προφανώς η μόνη μετάθεση του συνόλου $\mathbb{N}_1=\{1\}$ είναι η ταυτοτική μετάθεση ι:
$$\mathsf{S}_1=\left\{\iota=\begin{pmatrix}1\\1\end{pmatrix}\right\}$$

2. Αν $n=2$, τότε θα έχουμε:
$$\mathsf{S}_2=\left\{\iota=\begin{pmatrix}1&2\\1&2\end{pmatrix},\ \ \sigma=\begin{pmatrix}1&2\\2&1\end{pmatrix}\right\}$$
Πράγματι γνωρίζουμε ότι το πλήθος των στοιχείων της S_2 είναι $2!=2$. Επειδή, όπως προκύπτει εύκολα, οι απεικονίσεις ι, και σ είναι «1-1» και «επί» απεικονίσεις $\mathbb{N}_2\longrightarrow\mathbb{N}_2$, δηλαδή είναι μεταθέσεις του συνόλου $\mathbb{N}_2=\{1,2\}$, έπεται ότι αυτές οι μεταθέσεις είναι ακριβώς όλα τα στοιχεία της ομάδας S_2.

3. Αν $n=3$, τότε θα έχουμε:
$$\mathsf{S}_3=\{\iota,\ \mu_1,\ \mu_2,\ \mu_3,\ \rho_1,\ \rho_2\}$$
όπου:
$$\rho_0=\iota=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \mu_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \mu_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \mu_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$\rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \rho_2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$
Πράγματι, γνωρίζουμε ότι το πλήθος των στοιχείων της S_3 είναι $3!=6$. Επειδή, όπως προκύπτει εύκολα, οι απεικονίσεις ι, μ_1, μ_2, μ_3, ρ_1, και ρ_2 είναι «1-1» και «επί» απεικονίσεις $\mathbb{N}_3\longrightarrow\mathbb{N}_3$, δηλαδή είναι μεταθέσεις του συνόλου $\mathbb{N}_3=\{1,2,3\}$, έπεται ότι αυτές οι μεταθέσεις είναι ακριβώς όλα τα στοιχεία της ομάδας S_3.

Θα μελετήσουμε τις συμμετρικές ομάδες αναλυτικότερα σε μεταγενέστερο εδάφιο.

Υπενθυμίζοντας τον κυκλικό συμβολισμό μεταθέσεων, βλέπε τον συμβολισμό 1.3.27 στο Κεφάλαιο 1, θα γράφουμε έναν k-κύκλο σ στα στοιχεία $a_1,a_2,\cdots,a_k$ (με αυτή τη σειρά) του συνόλου $\{1,2,\cdots,n\}$ ως
$$\sigma=(a_1\ \ a_2\ \ \cdots\ \ a_{n-1}\ \ a_n)$$
δηλαδή σ είναι η μετάθεση η οποία μεταθέτει κυκλικά τα στοιχεία $a_1,a_2,\cdots,a_k$ και διατηρεί σταθερά τα υπόλοιπα:
$$\sigma(a_k)=\begin{cases}a_{k+1}, & \text{αν}\ \ 1\le k\le n-1\\ a_1, & \text{αν}\ \ k=n\end{cases}\qquad\text{και}\qquad \sigma(x)=x,\quad \text{αν}\ \ x\in\{1,2,\cdots,n\}\setminus\{a_1,a_2,\cdots,a_k\}$$
Η ταυτοτική μετάθεση $\iota\in\mathsf{S}_n$ είναι ένας 1-κύκλος, και άρα διατηρεί όλα τα στοιχεία του συνόλου $\{1,2,\cdots,n\}$ σταθερά και συμβολίζεται συνήθως με $\iota=(1)$.

Για λόγους αναφοράς περιγράφουμε τα στοιχεία των συμμετρικών ομάδων S_n ως κύκλους στοιχείων του συνόλου $\mathbb{N}_n$, όταν $n\le 3$.

1. Αν $n=1$, τότε προφανώς η μόνη μετάθεση του συνόλου $\mathbb{N}_1=\{1\}$ είναι η ταυτοτική μετάθεση ι:
$$\mathsf{S}_1=\{\iota=(1)\}$$

2. Αν $n=2$, τότε θα έχουμε:
$$\mathsf{S}_2=\{\iota=(1),\quad \sigma=(1\ 2)\}$$

3. Αν $n=3$, τότε θα έχουμε:
$$\mathsf{S}_3=\{\iota=(1),\quad \mu_1=(2\ 3),\quad \mu_2=(1\ 3),\quad \mu_3=(1\ 2),\quad \rho_1=(1\ 2\ 3),\quad \rho_2=(1\ 3\ 2)\}$$

Η Γενική Γραμμική Ομάδα

Παράδειγμα 2.2.8. (Η Γενική Γραμμική Ομάδα). Υπενθυμίζουμε ότι για κάθε θετικό ακέραιο n μπορούμε να ορίσουμε στο σύνολο $\mathsf{M}_n(\mathbb{R}) := \mathsf{M}_{n\times n}(\mathbb{R})$ των $n\times n$ πινάκων με στοιχεία πραγματικούς αριθμούς μια νέα πράξη, την πράξη «$\cdot$» του πολλαπλασιασμού πινάκων ως εξής:

$$\text{Αν}\quad A=(a_{ij})\quad\text{και}\quad B=(b_{ij}),\quad\text{τότε:}\quad A\cdot B=((A\cdot B)_{ij})=(c_{ij}),\quad\text{όπου}\quad c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\quad 1\le i,j\le n$$

Όπως προκύπτει από το μέρος 6 του Παραδείγματος 1.3.8, η πράξη «$\cdot$» πολλαπλασιασμού πινάκων είναι προσεταιριστική, αλλά γενικά όχι μεταθετική, και ο μοναδιαίος $n\times n$ πίνακας I_n αποτελεί ουδέτερο στοιχείο για την πράξη «$\cdot$». Επομένως το ζεύγος $(\mathsf{M}_n(\mathbb{R}),\cdot)$ είναι ένα μονοειδές. Το σύνολο $\mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot)$ των αντιστρέψιμων στοιχείων του μονοειδούς $(\mathsf{M}_n(\mathbb{R}),\cdot)$ συμπίπτει με το σύνολο $\mathsf{GL}(n,\mathbb{R})$ των αντιστρέψιμων $n\times n$ πινάκων πραγματικών αριθμών:

$$\mathsf{U}(\mathsf{M}_n(\mathbb{R}),\cdot):=\mathsf{GL}(n,\mathbb{R})=\{A\in\mathsf{M}_n(\mathbb{R})\mid A:\ \text{αντιστρέψιμος}\}$$

Σημειώνουμε ότι, όπως γνωρίζουμε από την Γραμμική Άλγεβρα, ισχύει ότι $\mathsf{GL}(n,\mathbb{R})=\{A\in\mathsf{M}_n(\mathbb{R})\mid \mathsf{Det}(A)\neq 0\}$. Η παραπάνω ανάλυση δείχνει ότι το ζεύγος $(\mathsf{GL}(n,\mathbb{R}),\cdot)$ είναι ομάδα, η οποία καλείται η **γενική γραμμική ομάδα** υπεράνω του $\mathbb{R}$. Παρόμοιο συμπέρασμα προκύπτει αν στη θέση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, και $\mathbb{C}$, και έτσι αποκτούμε τις γενικές γραμμικές ομάδες: $(\mathsf{GL}(n,\mathbb{Z}),\cdot)$, $(\mathsf{GL}(n,\mathbb{Q}),\cdot)$, και $(\mathsf{GL}(n,\mathbb{C}),\cdot)$ των $n\times n$ αντιστρέψιμων πινάκων με στοιχεία ακέραιους, ρητούς, και μιγαδικούς αριθμούς αντίστοιχα. $\surd$

Όπως πιστοποιεί η παρακάτω Πρόταση, η γενική γραμμική ομάδα σπάνια είναι αβελιανή.

Πρόταση 2.2.9. *Για την γενική γραμμική ομάδα* $\mathsf{GL}(n,\mathbb{K})$, *όπου* $\mathbb{K}\in\{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$, *τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα* $\mathsf{GL}(n,\mathbb{K})$ *είναι αβελιανή.*
2. $n=1$, *και τότε* $\mathsf{GL}(n,\mathbb{K})=\mathbb{K}^*$.

Απόδειξη. «1. $\Longleftarrow$ 2.» Αν $n=1$, τότε επειδή προφανώς οι αντιστρέψιμοι 1×1 πίνακες είναι τα μη μηδενικά στοιχεία του $\mathbb{K}$, έχουμε ότι $\mathsf{GL}(n,\mathbb{K})=\mathbb{K}^*$, και άρα η ομάδα $\mathsf{GL}(n,\mathbb{K})$ είναι αβελιανή διότι η ομάδα $\mathbb{K}^*$ είναι αβελιανή (η πράξη πολλαπλασιασμού στο σύνολο $\mathbb{K}$ είναι μεταθετική).

«2. $\Longrightarrow$ 1.» Για να δείξουμε ότι, αν η γενική γραμμική ομάδα $\mathsf{GL}(n,\mathbb{K})$ είναι αβελιανή, τότε $n=1$, αρκεί να δείξουμε ότι, αν $n\ge 2$, τότε η $\mathsf{GL}(n,\mathbb{K})$ δεν είναι αβελιανή. Θεωρούμε τους 2×2 πίνακες

$$K=\begin{pmatrix}1&1\\0&1\end{pmatrix}\quad\text{και}\quad L=\begin{pmatrix}1&0\\1&1\end{pmatrix}$$

Όπως βλέπουμε εύκολα οι πίνακες K και L είναι αντιστρέψιμοι και

$$K\cdot L=\begin{pmatrix}2&1\\1&1\end{pmatrix}\neq\begin{pmatrix}1&1\\1&2\end{pmatrix}=L\cdot K$$

Έτσι $K,L\in\mathsf{GL}(2,\mathbb{K})$ και $K\cdot L\neq L\cdot K$, δηλαδή η ομάδα $\mathsf{GL}(2,\mathbb{K})$ δεν είναι αβελιανή.

Αν $n>2$, τότε θεωρούμε τον μοναδιαίο $(n-2)\times(n-2)$-πίνακα I_{n-2} και τα ευθέα αθροίσματα[5] $K\oplus I_{n-2}$

[5] Υπενθυμίζουμε ότι, αν $A=(a_{ij})$ είναι ένας $n\times n$ πίνακας και $B=(b_{ij})$ είναι ένας $m\times m$ πίνακας αριθμών, τότε το **ευθύ άθροισμα** των πινάκων A και B ορίζεται να είναι ο $(n+m)\times(n+m)$ πίνακας

$$A\oplus B=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}&0&0&\cdots&0\\a_{21}&a_{22}&\cdots&a_{2n}&0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\a_{n1}&a_{n2}&\cdots&a_{nn}&0&0&\cdots&0\\0&0&\cdots&0&b_{11}&b_{12}&\cdots&b_{1m}\\0&0&\cdots&0&b_{21}&b_{22}&\cdots&b_{2m}\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0&b_{m1}&b_{m2}&\cdots&b_{mm}\end{pmatrix}.$$

του K και του I_{n-2}, και $L \oplus I_{n-2}$ του L και του I_{n-2}:

$$A = K \oplus I_{n-2} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \quad \text{και} \quad B = L \oplus I_{n-2} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

Εύκολα βλέπουμε ότι οι πίνακες A και B είναι αντιστρέψιμοι, άρα είναι στοιχεία της γενικής γραμμικής ομάδας $\mathsf{GL}(n,\mathbb{K})$, και $A \cdot B \neq B \cdot A$. Επομένως η $\mathsf{GL}(n,\mathbb{K})$ δεν είναι αβελιανή, αν $n > 1$. ■

Η Διεδρική Ομάδα

Θεωρούμε το επίπεδο $\mathbb{R}^2 = \{(x,y) \in \mathbb{R}^2 \mid x, y \in \mathbb{R}\}$, επί του οποίου ορίζουμε απεικονίσεις

$$T : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad T(x,y) = (-x, y)$$

$$R : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad R(x,y) = \begin{pmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} = \left(x\cos(\frac{2\pi}{n}) - y\sin(\frac{2\pi}{n}),\ x\sin(\frac{2\pi}{n}) + y\cos(\frac{2\pi}{n}) \right)$$

Υπολογίζουμε εύκολα ότι:

$$T^2 = \mathsf{Id}_{\mathbb{R}^2} = R^n \quad \text{και} \quad T \circ R = R^{-1} \circ T = R^{n-1} \circ T \tag{2.12}$$

Ιδιαίτερα οι παραπάνω σχέσεις δείχνουν ότι οι απεικονίσεις T και R είναι «1-1» και «επί», και άρα είναι στοιχεία της ομάδας μεταθέσεων $(\mathsf{S}(\mathbb{R}^2), \circ)$. Επιπλέον $T^{-1} = T$ και $R^{-1} = R^{n-1}$. Θέτουμε

$$\mathsf{D}_n = \{T^i \circ R^j \in \mathsf{S}(\mathbb{R}^2) \mid i, j \in \mathbb{Z}\}$$

Λαμβάνοντας υπόψη τις σχέσεις (2.12), βλέπουμε εύκολα ότι:

$$\mathsf{D}_n = \{\mathsf{Id}_{\mathbb{R}^2},\ R,\ R^2,\ \cdots,\ R^{n-1}, T,\ T \circ R,\ T \circ R^2,\ \cdots,\ T \circ R^{n-1}\}$$

και το σύνολο D_n είναι κλειστό στην πράξη της σύνθεσης απεικονίσεων, περιέχει την ταυτοτική απεικόνιση του $\mathbb{R}^2$, και επίσης περιέχει την αντίστροφη απεικόνιση κάθε στοιχείου του. Επομένως το ζεύγος $(\mathsf{D}_n, \circ)$ αποτελεί ομάδα με πλήθος στοιχείων $2n$, η οποία αποτελεί μοντέλο της n-**οστής διεδρικής ομάδας**. Γεωμετρικά η απεικόνιση ϕ παριστά ανάκλαση ως προς τον άξονα $\{(0,y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}$ των $y'y$ του επιπέδου $\mathbb{R}^2$, και η απεικόνιση ψ παριστά στροφή επιπέδου κατά γωνία $\theta_n = \frac{2\pi}{n}$ γύρω από την αρχή των αξόνων με φορά αντίθετη της φοράς των δεικτών του ρολογιού.

Οι παραπάνω απεικονίσεις, καθώς και οι ακέραιες δυνάμεις τους όταν εφαρμοστούν στα σημεία ενός κανονικού n-γώνου Δ_n, $n \geq 3$, εγγεγραμμένου στον μοναδιαίο κύκλο ακτίνας 1 στο επίπεδο $\mathbb{R}^2$, έτσι ώστε το κέντρο του Δ_n να βρίσκεται στην αρχή των αξόνων, αποτελούν συμμετρίες του κανονικού n-γώνου διότι το αφήνουν αναλλοίωτο ως γεωμετρικό σχήμα. Προφανώς η απεικόνιση R^k παριστάνει στροφή του επιπέδου κατά γωνία $\frac{2k\pi}{n}$ με κέντρο την αρχή των αξόνων, και όπως μπορούμε να δούμε εύκολα, βλέπε την Άσκηση 2.10.31, ικανοποιούνται οι ακόλουθες σχέσεις:

$$R^n = T^2 = (R \circ T)^2 = \mathsf{Id}_{\mathbb{R}^2} \quad \text{και} \quad R^k \neq \mathsf{Id}_{\mathbb{R}^2}, \ \text{αν} \ 1 < k < n$$

Ας προσδιορίσουμε την διεδρική ομάδα D_n για μικρές τιμές του n:

1. Αν $n = 1$, τότε η απεικόνιση R είναι στροφή επιπέδου κατά γωνία 2π και άρα είναι η ταυτοτική απεικόνιση. Επομένως $\mathsf{D}_1 = \{\mathsf{Id}_{\mathbb{R}^2}, T\}$.

   Γεωμετρικά η D_1 παριστάνει την ομάδα συμμετρίας ενός κανονικού 1-γώνου, δηλαδή ενός ευθύγραμμου τμήματος Δ_1 το οποίο είναι παράλληλο με τον άξονα $\{(x,0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$, του οποίου το μέσον βρίσκεται στην αρχή των αξόνων (ή ισοδύναμα την ομάδα συμμετρίας ενός ισοσκελούς μη ισόπλευρου τριγώνου).

2. Αν $n=2$, τότε η απεικόνιση R είναι στροφή επιπέδου κατά γωνία π και άρα θα έχουμε $R(x,y)=(-x,-y)$. Επομένως $\mathsf{D}_2=\{\mathsf{Id}_{\mathbb{R}^2}, R, T, R\circ T\}$.

   Γεωμετρικά η D_2 παριστάνει την ομάδα συμμετρίας ενός παραλληλογράμμου το οποίο δεν είναι τετράγωνο, και του οποίου οι πλευρές είναι παράλληλες με τους άξονες και το κέντρο συμμετρίας του, δηλαδή η τομή των διαγωνίων του, βρίσκεται στην αρχή των αξόνων.

3. Αν $n=3$, τότε η απεικόνιση R είναι στροφή επιπέδου κατά γωνία $\frac{2\pi}{3}$ και άρα θα έχουμε $R(x,y)=(-\frac{x}{2}-\frac{\sqrt{3}y}{2}, \frac{\sqrt{3}x}{2}-\frac{y}{2})$. Επομένως $\mathsf{D}_3=\{\mathsf{Id}_{\mathbb{R}^2}, R, R^2, T, T\circ R, T\circ R^2\}$.

   Γεωμετρικά η D_3 παριστάνει την ομάδα συμμετρίας ενός ισόπλευρου τριγώνου του οποίου το κέντρο συμμετρίας του, δηλαδή η τομή των διαγωνίων του, βρίσκεται στην αρχή των αξόνων.

4. Αν $n=4$, τότε η απεικόνιση R είναι στροφή επιπέδου κατά γωνία $\frac{\pi}{2}$ και άρα θα έχουμε $R(x,y)=(-y,x)$. Επομένως $\mathsf{D}_4=\{\mathsf{Id}_{\mathbb{R}^2}, R, R^2, R^3, T, T\circ R, T\circ R^2, T\circ R^3\}$.

   Γεωμετρικά η D_4 παριστάνει την ομάδα συμμετρίας ενός τετραγώνου του οποίου το κέντρο συμμετρίας του, δηλαδή η τομή των διαγωνίων του, βρίσκεται στην αρχή των αξόνων.

Παράδειγμα 2.2.10. Κλείνουμε την παρούσα υποενότητα με μια σειρά ενδεικτικών παραδειγμάτων ομάδων, οι οποίες προκύπτουν ως ομάδες αντιστρέψιμων στοιχείων μονοειδών με χρήση της Πρότασης 2.2.4.

1. Θεωρούμε το μεταθετικό μονοειδές $(M,+)$, όπου M είναι ένα εκ των συνόλων αριθμών $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, και «$+$» είναι η συνήθης πράξη πρόσθεσης αριθμών. Για τα σύνολα των αντίθετων (ή αντιστρέψιμων) στοιχείων του μονοειδούς $(M,+)$, έχουμε:

$$\mathsf{U}(\mathbb{N}_0,+)=\{0\},\quad \mathsf{U}(\mathbb{Z},+)=\mathbb{Z},\quad \mathsf{U}(\mathbb{Q},+)=\mathbb{Q},\quad \mathsf{U}(\mathbb{R},+)=\mathbb{R},\quad \mathsf{U}(\mathbb{C},+)=\mathbb{C}$$

   και έτσι αποκτούμε την τετριμμένη ομάδα $\{0\}$, και τις αβελιανές ομάδες $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, του Παραδείγματος 2.2.2.

2. Θεωρούμε το μεταθετικό μονοειδές $(M,\cdot)$, όπου M είναι ένα εκ των συνόλων αριθμών $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, και «$\cdot$» είναι η συνήθης πράξη πολλαπλασιασμού αριθμών. Για τα σύνολα των αντιστρέψιμων στοιχείων του μονοειδούς $(M,\cdot)$, έχουμε:

$$\mathsf{U}(\mathbb{N},\cdot)=\{1\},\quad \mathsf{U}(\mathbb{Z},\cdot)=\{1,-1\},\quad \mathsf{U}(\mathbb{Q},\cdot)=\mathbb{Q}^*,\quad \mathsf{U}(\mathbb{R},\cdot)=\mathbb{R}^*,\quad \mathsf{U}(\mathbb{C},\cdot)=\mathbb{C}^*,$$

   και έτσι αποκτούμε την τετριμμένη ομάδα $\{1\}$, την αβελιανή ομάδα $(\{1,-1\},\cdot)$ και τις αβελιανές ομάδες $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, του Παραδείγματος 2.2.2.

3. (Ομάδες Υποσυνόλων). Έστω A ένα μη κενό σύνολο, και έστω $\mathscr{P}(A)$ το δυναμοσύνολο του A. Θεωρούμε το σύνολο $\mathscr{P}(A)$ εφοδιασμένο με την πράξη «*συμμετρικής διαφοράς*» υποσυνόλων του A:

$$\Delta\colon \mathscr{P}(A)\times\mathscr{P}(A)\longrightarrow \mathscr{P}(A),\quad (X,Y)\longmapsto X\Delta Y=(X\cup Y)\setminus(X\cap Y)$$

   Όπως προκύπτει από το μέρος 8 του Παραδείγματος 1.3.8, η πράξη «Δ» είναι προσεταιριστική και μεταθετική. Επιπλέον υπάρχει ουδέτερο στοιχείο, το κενό σύνολο $\emptyset$, για την πράξη «Δ», και άρα το ζεύγος $(\mathscr{P}(A),\Delta)$ είναι ένα μεταθετικό μονοειδές. Για το σύνολο $\mathsf{U}\big(\mathscr{P}(A),\Delta\big)$ των αντιστρέψιμων στοιχείων του $\mathscr{P}(A)$ ως προς την πράξη «Δ» έχουμε: $\mathsf{U}\big(\mathscr{P}(A),\Delta\big)=\mathscr{P}(A)$, διότι για κάθε $X\in\mathscr{P}(A)$ έχουμε: $X\Delta X=\emptyset$, δηλαδή το αντίστροφο ως προς την πράξη Δ του X υπάρχει και συμπίπτει με το X. Επομένως το ζεύγος $(\mathscr{P}(A),\Delta)$ αποτελεί αβελιανή ομάδα.

4. (Ομάδες Συναρτήσεων). Έστω $\mathscr{F}(X,\mathbb{R})=\{f\colon X\longrightarrow\mathbb{R}\mid f:\text{απεικόνιση}\}$ το σύνολο όλων των πραγματικών απεικονίσεων οι οποίες είναι ορισμένες επί ενός υποσυνόλου X της πραγματικής ευθείας. Το σύνολο $\mathscr{F}(X,\mathbb{R})$ είναι εφοδιασμένο με τις εξής πράξεις πρόσθεσης και πολλαπλασιασμού συναρτήσεων, $\forall f,g\colon X\longrightarrow\mathbb{R}$:

$$f+g,\ f\cdot g\colon X\longrightarrow\mathbb{R},\quad \text{όπου}\quad (f+g)(x)=f(x)+g(x),\quad (f\cdot g)(x)=f(x)\cdot g(x)$$

Όπως προκύπτει από το μέρος 9 του Παραδείγματος 1.3.8, τα ζεύγη $(\mathscr{F}(X,\mathbb{R}),+)$ και $\mathscr{F}(X,\mathbb{R}),\cdot)$ είναι μεταθετικά μονοειδή με ουδέτερα στοιχεία τις σταθερές απεικονίσεις 0 και 1 αντίστοιχα, όπου:

$$0\colon X\longrightarrow\mathbb{R},\ \ 0(x)=0 \qquad \text{και} \qquad 1\colon X\longrightarrow\mathbb{R},\ \ 1(x)=1$$

Επειδή κάθε $f\in\mathscr{F}(X,\mathbb{R})$ έχει αντίστροφο στοιχείο ως προς την πράξη «+» την απεικόνιση $-f\colon X\longrightarrow\mathbb{R}$, $(-f)(x)=-f(x)$, έπεται ότι το ζεύγος $\mathsf{U}(\mathscr{F}(X,\mathbb{R}),+)=(\mathscr{F}(X,\mathbb{R}),+)$ είναι αβελιανή ομάδα. Από την άλλη πλευρά, μια απεικόνιση $f\in\mathscr{F}(X,\mathbb{R})$ είναι αντιστρέψιμη ως προς την πράξη «$\cdot$», αν και μόνο αν $f(x)\neq 0$, $\forall x\in X$. Πράγματι, αν η f είναι αντιστρέψιμη, τότε υπάρχει συνάρτηση $g\colon X\longrightarrow\mathbb{R}$, έτσι ώστε $f\cdot g=1$, και τότε για κάθε $x\in\mathbb{R}$ θα έχουμε $(f\cdot g)(x)=f(x)\cdot g(x)=1(x)=1$, και ιδιαίτερα $f(x)\neq 0$, $\forall x\in X$. Αντίστροφα, αν η τελευταία σχέση ισχύει, τότε μπορούμε να ορίσουμε την απεικόνιση $g\colon X\longrightarrow\mathbb{R}$, $g(x)=\frac{1}{f(x)}$ η οποία ανήκει στο σύνολο $\mathscr{F}(X,\mathbb{R})$ και θα έχουμε, για κάθε $x\in X$: $(f\cdot g)(x)=f(x)\cdot g(x)=f(x)\cdot\frac{1}{f(x)}=1=1(x)$, δηλαδή $f\cdot g=1$ και, επειδή η πράξη «$\cdot$» είναι μεταθετική, θα έχουμε και $g\cdot f=1$. Επομένως θα έχουμε την αβελιανή ομάδα $\mathsf{U}(\mathscr{F}(X,\mathbb{R}),\cdot)$, όπου:

$$\mathsf{U}(\mathscr{F}(X,\mathbb{R}),\cdot)=\big\{f\colon X\longrightarrow\mathbb{R}\mid f(x)\neq 0,\ \forall x\in X\big\}$$

Παρόμοιο συμπέρασμα προκύπτει αν στη θέση του συνόλου $\mathbb{R}$ των πραγματικών αριθμών είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, και $\mathbb{C}$, και έτσι αποκτούμε τις αβελιανές ομάδες: $(\mathscr{F}(X,\mathbb{Z}),+)$, $(\mathscr{F}(X,\mathbb{Q}),+)$, $(\mathscr{F}(X,\mathbb{C}),+)$, των συναρτήσεων $:X\longrightarrow\mathbb{K}$, όπου $\mathbb{K}=\mathbb{Z},\mathbb{Q},\mathbb{C}$ αντίστοιχα. Κατά τον ίδιο τρόπο επίσης αποκτούμε τις ομάδες $\mathsf{U}(\mathscr{F}(X,\mathbb{K}),\cdot)$, όταν $\mathbb{K}=\mathbb{Z},\mathbb{R},\mathbb{Q},\mathbb{C}$.

5. (Ομάδες Ακολουθιών). Έστω ότι $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, καθένα εκ των οποίων θεωρείται εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού. Θεωρούμε το σύνολο

$$\mathsf{A}(\mathbb{K})=\big\{\mathsf{a}=(a_n)_{n\geq 0}\mid a_n\in\mathbb{K},\ \forall n\geq 0\big\}$$

των ακολουθιών με στοιχεία από το σύνολο $\mathbb{K}$. Υπενθυμίζουμε ότι, όπως στο μέρος 10 του Παραδείγματος 1.3.8, επί του $\mathsf{A}(\mathbb{K})$ ορίζονται πράξεις πρόσθεσης «+» και πολλαπλασιασμού «$\cdot$» ως εξής: Αν $\mathsf{a}=(a_n)_{n\geq 0}$ και $\mathsf{b}=(b_n)_{n\geq 0}$ είναι στοιχεία του $\mathsf{A}(\mathbb{K})$, τότε:

$$+\ :\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad \mathsf{a}+\mathsf{b}=\mathsf{c}=(c_n)_{n\geq 0},\quad \text{όπου}\quad c_n=a_n+b_n,\ \ \forall n\geq 0$$

$$\cdot\ :\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad \mathsf{a}\cdot\mathsf{b}=\mathsf{d}=(d_n)_{n\geq 0},\quad \text{όπου}\quad d_n=\sum_{k=0}^{n}a_kb_{n-k},\ \ \forall n\geq 0$$

Όπως προκύπτει εύκολα, βλέπε την Άσκηση 1.5.25, τα ζεύγη $(\mathsf{A}(\mathbb{K}),+)$ και $(\mathsf{A}(\mathbb{K}),\cdot)$, είναι μεταθετικά μονοειδή, όπου το ουδέτερο στοιχείο του μονοειδούς $(\mathsf{A}(\mathbb{K}),+)$ είναι η μηδενική ακολουθία $0=(a_n)_{n\geq 0}$, όπου $a_n=0$, $\forall n\geq 0$, και το ουδέτερο στοιχείο του μονοειδούς $(\mathsf{A}(\mathbb{K}),\cdot)$, είναι η ακολουθία $1=(a_n)_{n\geq 0}$, όπου $a_0=1$ και $a_n=0$, $\forall n\geq 1$. Επειδή κάθε ακολουθία $\mathsf{a}\in\mathsf{A}(\mathbb{K})$ έχει αντίστροφο στοιχείο ως προς την πράξη «+» την ακολουθία $-\mathsf{a}$, όπου $-\mathsf{a}=(-a_n)_{n\geq 0}$, έπεται ότι θα έχουμε την αβελιανή ομάδα:

$$\mathsf{U}(\mathsf{A}(\mathbb{K}),+)=(\mathsf{A}(\mathbb{K}),+)$$

Από την άλλη πλευρά, επειδή, όπως προκύπτει εύκολα (βλέπε την Άσκηση 1.5.25), η ακολουθία $\mathsf{a}=(a_n)_{m\geq 0}$ είναι αντιστρέψιμη ως προς την πράξη «$\cdot$» αν και μόνο αν $a_0\in\mathsf{U}(\mathbb{K},\cdot)$ και $a_n=0$, $\forall n\geq 1$, αποκτούμε την αβελιανή ομάδα

$$\mathsf{U}(\mathsf{A}(\mathbb{K}),\cdot)=\big\{\mathsf{a}=(a_n)_{n\geq 0}\mid a_0\in\mathsf{U}(\mathbb{K},\cdot)\ \text{και}\ a_n=0,\forall n\geq 1\big\}$$

6. (Ομάδες Αριθμητικών Συναρτήσεων). Έστω $\mathscr{A}=\{f\colon\mathbb{N}\longrightarrow\mathbb{C}\mid f:\ \text{συνάρτηση}\}$ το σύνολο των αριθμητικών συναρτήσεων εφοδιασμένο με την πράξη του ενελικτικού γινομένου

$$\forall f,g\in\mathscr{A}:\quad f\star g\colon\mathbb{N}\longrightarrow\mathbb{C},\quad (f\star g)(n)=\sum_{d|n}f(d)g(\frac{n}{d})$$

Από το μέρος 11 του Παραδείγματος 1.3.8 γνωρίζουμε ότι το ζεύγος $(\mathscr{A}, \star)$ είναι ένα μεταθετικό μονοειδές, δηλαδή η πράξη «$\star$» είναι προσεταιριστική, μεταθετική, και έχει ουδέτερο στοιχείο την αριθμητική συνάρτηση $\varepsilon\colon \mathbb{N} \longrightarrow \mathbb{C}$, όπου $\varepsilon(1) = 1$ και $\varepsilon(n) = 0$, $\forall n \geq 2$. Επομένως από την Πρόταση 2.2.4 αποκτούμε την αβελιανή **ομάδα των ενελικτικά αντιστρεπτών αριθμητικών συναρτήσεων**

$$\mathsf{U}(\mathscr{A}, *) = \left\{ f\colon \mathbb{N} \longrightarrow \mathbb{C} \mid \exists\, g\colon \mathbb{N} \longrightarrow \mathbb{C},\ \text{έτσι ώστε}\colon f * g = \varepsilon \right\}$$

Από τη Θεωρία Αριθμών γνωρίζουμε[6] ότι η f είναι ενελικτικά αντιστρεπτή αν και μόνο αν $f(1) \neq 0$, και άρα:

$$\mathsf{U}(\mathscr{A}, *) = \left\{ f\colon \mathbb{N} \longrightarrow \mathbb{C} \mid f(1) \neq 0 \right\} \quad \surd$$

2.3 Ο Πίνακας Cayley μιας Ομάδας

Έστω $(G, \cdot)$ μια ομάδα. Αν το σύνολο G έχει πεπερασμένο πλήθος στοιχείων, τότε ο πίνακας Cayley της G είναι ο πίνακας Cayley της πράξης «$\cdot$» όπως στον Ορισμό 1.3.9. Όπως θα δούμε, στην περίπτωση των ομάδων, ο πίνακας Cayley ικανοποιεί επιπρόσθετες ιδιότητες και επιπλέον όλες οι βασικές πληροφορίες οι οποίες αφορούν μια ομάδα εμπεριέχονται στον πίνακα Cayley της ομάδας. Περισσότερο αναλυτικά, θεωρούμε μια ομάδα με πεπερασμένο πλήθος στοιχείων, έστω $(G, \cdot)$, όπου:

$$G = \left\{ a_1 = e, a_2, \cdots, a_n \right\} \qquad \text{και} \qquad \cdot\colon G \times G \longrightarrow G, \quad (a_i, a_j) \longmapsto a_i \cdot a_j$$

Υπενθυμίζουμε πρώτα ότι, αν $A = (a_{ij})$ είναι ένας $n \times n$ πίνακας με στοιχεία από ένα τυχόν σύνολο, τότε το στοιχείο a_{ij} βρίσκεται στην τομή της i-γραμμής και της j-στήλης του πίνακα A.

Ορισμός 2.3.1. *Ο τετραγωνικός $n \times n$ πίνακας $\mathsf{C}(G, \cdot) = (a_{ij})$ στοιχείων της G, όπου:*

$$a_{ij} := a_i \cdot a_j, \quad 1 \leq i, j \leq n$$

*καλείται **πίνακας Cayley** της ομάδας $(G, \cdot)$, και παριστάται όπως στο παρακάτω σχήμα :*

$\cdot$	$\mathbf{a_1}$	$\mathbf{a_2}$	$\cdots$	$\mathbf{a_i}$	$\cdots$	$\mathbf{a_j}$	$\cdots$	$\mathbf{a_n}$
$\mathbf{a_1}$	$a_1 \cdot a_1$	$a_1 \cdot a_2$	$\ldots$	$a_1 \cdot a_i$	$\ldots$	$a_1 \cdot a_j$	$\ldots$	$a_1 \cdot a_n$
$\mathbf{a_2}$	$a_2 \cdot a_1$	$a_2 \cdot a_2$	$\ldots$	$a_2 \cdot a_i$	$\ldots$	$a_2 \cdot a_j$	$\ldots$	$a_2 \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{a_i}$	$a_i \cdot a_1$	$a_i \cdot a_2$	$\cdots$	$a_i \cdot a_i$	$\cdots$	$a_i \cdot a_j$	$\cdots$	$a_i \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$
$\mathbf{a_j}$	$a_j \cdot a_1$	$a_j \cdot a_2$	$\cdots$	$a_j \cdot a_i$	$\cdots$	$a_j \cdot a_j$	$\cdots$	$a_j \cdot a_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$\mathbf{a_n}$	$a_n \cdot a_1$	$a_n \cdot a_2$	$\cdots$	$a_n \cdot a_i$	$\cdots$	$a_n \cdot a_j$	$\cdots$	$a_n \cdot a_n$

Σχήμα 2.1: Ο πίνακας Cayley της ομάδας $(G, \cdot)$, όπου $G = \left\{ a_1, a_2, \cdots, a_n \right\}$.

Παρατήρηση 2.3.2. **Ιδιότητες Πίνακα Cayley μιας Ομάδας** $(G, \cdot)$ Έστω όπως και παραπάνω $(G, \cdot)$ μια ομάδα με πεπερασμένο πλήθος στοιχείων $G = \left\{ a_1, a_2, \cdots, a_n \right\}$. Θεωρούμε τον πίνακα Cayley $\mathsf{C}(G, \cdot)$ της ομάδας όπως στο Σχήμα 2.1.

[6] Βλέπε το βιβλίο [28].

1. Όταν είναι γνωστός ο πίνακας Cayley $\mathsf{C}(G,\cdot)$ μιας ομάδας $(G,\cdot)$, τότε μπορεί να διαπιστωθεί άμεσα αν η πράξη η ομάδα G είναι αβελιανή ή όχι. Πράγματι, είναι αρκετό να παρατηρήσει κανείς ότι για κάθε i,j με $1 \le i,j, \le n$, τα στοιχεία $a_{ij} = a_i \cdot a_j$ και $a_{ji} = a_j \cdot a_i$, βρίσκονται συμμετρικά ως προς την κύρια διαγώνιο του πίνακα η οποία αποτελείται από τα στοιχεία $a_{ii} = a_i \cdot a_i$, $1 \le i \le n$. Συνεπώς η πράξη $\cdot$ είναι μεταθετική, και άρα η ομάδα G είναι αβελιανή, αν και μόνο αν τα στοιχεία του πίνακα Cayley $\mathsf{C}(G,\cdot)$ που κείνται συμμετρικά ως προς την κύρια διαγώνιό του είναι ίσα.

   Ισοδύναμα η ομάδα $(G,\cdot)$ είναι αβελιανή αν και μόνο αν ο πίνακας Cayley $\mathsf{C}(G,\cdot)$ είναι συμμετρικός[7]: $\mathsf{C}(G,\cdot) = {}^t\mathsf{C}(G,\cdot)$.

2. Χωρίς βλάβη της γενικότητας, αναδιατάσσοντας αν είναι ανάγκη τα στοιχεία της ομάδας G, μπορούμε να υποθέσουμε ότι το ουδέτερο στοιχείο της ομάδας είναι το στοιχείο $e = a_1$. Τότε θα έχουμε $a_1 \cdot a_k = a_k = a_k \cdot a_1$, $1 \le k \le n$, και επομένως η πρώτη γραμμή $a_{1k} = a_1 \cdot a_k$, $1 \le k \le n$, και η πρώτη στήλη $a_{k1} = a_k \cdot a_1$, $1 \le k \le n$, του πίνακα Cayley στο Σχήμα 2.1 αποτελείται από τα στοιχεία $a_1, a_2, \cdots, a_n$ της G με την ίδια σειρά αναγραφής.

   Με άλλα λόγια, η ύπαρξη ουδέτερου στοιχείου $e \in G$ δείχνει ότι ακριβώς μια γραμμή και μια στήλη του πίνακα Cayley της G συμπίπτει με τα στοιχεία της ομάδας χωρίς να αλλάξει η σειρά αναγραφής τους.

3. Επειδή από την Πρόταση 2.1.8, οι εξισώσεις $a \cdot x = b$ και $y \cdot a = b$, για κάθε $a, b \in G$, έχουν μοναδική λύση στην G, έπεται ότι κάθε στοιχείο της G εμφανίζεται ακριβώς μια φορά σε κάθε γραμμή και σε κάθε στήλη του πίνακα Cayley.

   Με άλλα λόγια, αν a_k είναι ένα τυχόν στοιχείο της G, τότε για κάθε στήλη j και για κάθε γραμμή i, υπάρχουν μοναδικά στοιχεία a_m και a_l της ομάδας G έτσι ώστε: $a_i \cdot a_l = a_k$ και $a_m \cdot a_j = a_k$. ▲

Παρατήρηση 2.3.3. Ο ακόλουθος ισχυρισμός είναι πολύ χρήσιμος στον σχηματισμό του πίνακα Cayley μιας ομάδας, όπως θα δούμε στην συνέχεια.

- Ισχυρισμός: *Έστω $(G,\cdot)$ ένα ζεύγος το οποίο αποτελείται από ένα πεπερασμένο σύνολο G και μια προσεταιριστική πράξη «$\cdot$» επί του G. Έστω ότι για τον πίνακα Cayley $\mathsf{C}(G,\cdot)$ της πράξης «$\cdot$» ισχύουν τα εξής:*

  1. *Υπάρχει τουλάχιστον μια γραμμή (αντίστοιχα στήλη) του πίνακα Cayley $\mathsf{C}(G,\cdot)$ η οποία συμπίπτει με τα στοιχεία του συνόλου G χωρίς να αλλάξει η σειρά αναγραφής τους.*

  2. *Σε κάθε στήλη (αντίστοιχα γραμμή) του πίνακα Cayley $\mathsf{C}(G,\cdot)$, κάθε στοιχείο του συνόλου G εμφανίζεται ακριβώς μια φορά.*

Τότε το ζεύγος $(G,\cdot)$ είναι ομάδα.

Απόδειξη. Έστω $G = \{a_1, a_2, \cdots, a_n\}$, και αναγράφουμε τα στοιχεία της G στον πίνακα Cayley $\mathsf{C}(G,\cdot)$ με την ίδια σειρά αναγραφής: $a_1, a_2, \cdots, a_n$, βλέπε Σχήμα 2.1. Υποθέτουμε ότι η k-οστή γραμμή του πίνακα Cayley $\mathsf{C}(G,\cdot)$, δηλαδή η γραμμή $(a_k \cdot a_1, a_k \cdot a_2, \cdots, a_k \cdot a_n)$, συμπίπτει με την γραμμή $(a_1, a_2, \cdots, a_n)$ των στοιχείων της G. Τότε θα έχουμε:

$$a_k \cdot a_1 = a_1, \quad a_k \cdot a_2 = a_2, \quad \cdots, \quad a_k \cdot a_n = a_n$$

Οι παραπάνω σχέσεις δείχνουν ότι το στοιχείο a_k του συνόλου G είναι αριστερό ουδέτερο στοιχείο για την πράξη «$\cdot$». Από την άλλη πλευρά, επειδή κάθε στοιχείο a του συνόλου G εμφανίζεται ακριβώς μια φορά σε κάθε στήλη του πίνακα $\mathsf{C}(G,\cdot)$, έπεται ότι κάθε στήλη του πίνακα Cayley περιέχει τα στοιχεία του συνόλου G, ενδεχομένως με διαφορετικής σειρά αναγραφής. Έτσι, αν a, b είναι δύο τυχόντα στοιχεία του συνόλου G, τότε τα στοιχεία $a_1 \cdot a$, $a_2 \cdot a$, $\cdots$, $a_n \cdot a$ είναι τα στοιχεία a_1, a_2, $\cdots$, a_n του συνόλου G, ενδεχομένως με διαφορετική σειρά. Αν $b = a_j$, για κάποιο $1 \le j \le n$, τότε θα έχουμε ότι υπάρχει $k \in \{1, 2, \cdots, n\}$, έτσι ώστε: $a_k \cdot a = a_j = b$. Αυτό δείχνει ότι η εξίσωση $y \cdot a = b$ έχει λύση στο σύνολο G. Ιδιαίτερα, επιλέγοντας $a \in G$ να

[7] Υπενθυμίζουμε ότι ο *ανάστροφος* πίνακας ${}^tA$ ενός πίνακα $A = (a_{ij})$, είναι ο πίνακας ${}^tA = (a_{ji})$, δηλαδή στην τομή της i-γραμμής και της j-στήλης βρίσκεται το στοιχείο a_{ji} του πίνακα A. Εξ ορισμού ο πίνακας A είναι *συμμετρικός* αν συμπίπτει με τον ανάστροφό του: $A = {}^tA$.

είναι ένα τυχόν στοιχείο της G και $b = e$ ένα αριστερό ουδέτερο στοιχείο για την πράξη «$\cdot$», έπεται ότι υπάρχει στοιχείο $a' \in G$, έτσι ώστε: $a' \cdot a = e$. Επομένως για κάθε στοιχείο a της G υπάρχει αριστερό αντίστροφο στο σύνολο G ως προς την πράξη «$\cdot$». Τότε από την Πρόταση 2.1.9, έπεται ότι το ζεύγος $(G, \cdot)$ είναι ομάδα.

Η παρενθετική εκδοχή του παραπάνω ισχυρισμού αποδεικνύεται παρόμοια. $\surd$

Πίνακες Cayley ομάδων με πλήθος στοιχείων ≤ 4

Θα περιγράψουμε όλες τις ομάδες οι οποίες έχουν το πολύ τέσσερα στοιχεία, μέσω των αντίστοιχων πινάκων Cayley, και θα δούμε διακεκριμένα μοντέλα αυτών των ομάδων. Έστω $(G, \cdot)$ μια ομάδα.

1. Αν $|G| = 1$, δηλαδή η G είναι η τετριμμένη ομάδα, τότε η G αποτελείται μόνο από το ουδέτερο στοιχείο της
$$G = \{e\}$$
Προφανώς $e^2 = e$, και ο πίνακας Cayley της G είναι:

$\cdot$	**e**
e	e

Αναγκαστικά λοιπόν υπάρχει ένας πίνακας Cayley για μια ομάδα με πλήθος στοιχείων ίσο με ένα. Αντίστροφα ο παραπάνω πίνακας Cayley της πράξης «$\cdot$» προφανώς ορίζει μοναδικά μια δομή ομάδας στο μονοσύνολο $G = \{e\}$.

Μοντέλο ομάδας με ένα στοιχείο αποτελεί το μονοσύνολο $\{0\} \subseteq \mathbb{Z}$ εφοδιασμένο με την σύνηθη πράξη της πρόσθεσης «+», καθώς έχουμε $0 + 0 = 0$, και το μονοσύνολο $\{1\} \subseteq \mathbb{Z}$ εφοδιασμένο με την σύνηθη πράξη του πολλαπλασιασμού «$\cdot$», καθώς έχουμε $1 \cdot 1 = 1$.

2. Αν $|G| = 2$, τότε η G αποτελείται από το ουδέτερο στοιχείο της e και ένα επιπλέον στοιχείο, έστω a:
$$G = \{e, a\}$$
Σύμφωνα με την Παρατήρηση 2.3.2 περί ιδιοτήτων του πίνακα Cayley μιας ομάδας, επειδή e είναι το ουδέτερο στοιχείο της G, η πρώτη γραμμή και η πρώτη στήλη του πίνακα είναι τα στοιχεία της G με την ίδια σειρά παράθεσης. Για το στοιχείο στη θέση $(2,2)$, θα έχουμε αναγκαστικά $a^2 = e$, διότι η μόνη άλλη επιλογή $a^2 = a$ σύμφωνα με την Πρόταση 2.1.8, μας οδηγεί στο άτοπο $a = e$ (εναλλακτικά, διότι διαφορετικά θα είχαμε το a δύο φορές στην δεύτερη στήλη του πίνακα).

Έτσι ο πίνακας Cayley της G είναι:

$\cdot$	**e**	**a**
e	e	a
a	e	e

Αναγκαστικά λοιπόν υπάρχει μόνο ένας πίνακας Cayley για μια ομάδα με πλήθος στοιχείων ίσο με δύο. Αντίστροφα, εύκολα βλέπουμε, με χρήση της Παρατήρησης 2.3.3, ότι ο παραπάνω πίνακας Cayley της πράξης «$\cdot$» ορίζει μοναδικά μια δομή ομάδας στο σύνολο $G = \{e, a\}$.

Μοντέλα ομάδας με πλήθος στοιχείων ίσο με δύο αποτελούν τα ζεύγη:
$$(\mathbb{Z}_2, +) \qquad \text{και} \qquad (\mathsf{U}_2 = \{1, -1\}, \cdot)$$

3. Αν $|G| = 3$, τότε η G αποτελείται από το ουδέτερο στοιχείο e και δύο επιπλέον στοιχεία, έστω a και b:
$$G = \{e, a, b\}$$
Σύμφωνα με την Παρατήρηση 2.3.2 περί ιδιοτήτων του πίνακα Cayley μιας ομάδας, επειδή e είναι το ουδέτερο στοιχείο της G, η πρώτη γραμμή και η πρώτη στήλη του πίνακα $\mathsf{C}(G, \cdot)$ είναι τα στοιχεία της G με την ίδια σειρά παράθεσης.

Για το στοιχείο στη θέση (2,2), δηλαδή για το στοιχείο a^2: αυτό δεν μπορεί να είναι το a, διότι το a υπάρχει στην ίδια γραμμή και στήλη. Αν $a^2 = e$, τότε το στοιχείο στη θέση (2,3), δηλαδή το στοιχείο $a \cdot b$ θα πρέπει αναγκαστικά να είναι το b, διότι η δεύτερη γραμμή θα πρέπει να περιέχει όλα τα στοιχεία της G ακριβώς μια φορά. Όμως αυτό είναι άτοπο διότι το b υπάρχει ήδη στην τρίτη στήλη. Επομένως η υπόθεση $a^2 = e$ μας οδήγησε σε άτοπο και άρα αναγκαστικά θα έχουμε $a^2 = e$, και τότε στη θέση (2,3) θα έχουμε $a \cdot b = e$. Χρησιμοποιώντας ότι κάθε γραμμή και στήλη θα πρέπει να περιέχει όλα τα στοιχεία της G ακριβώς μια φορά, βλέπουμε ότι $b \cdot a = e$ και $b^2 = a$.

Έτσι ο πίνακας Cayley της G είναι:

$\cdot$	**e**	**a**	**b**
e	e	a	b
a	a	b	e
b	b	e	a

Αναγκαστικά λοιπόν υπάρχει μόνο ένας πίνακας Cayley για μια ομάδα με πλήθος στοιχείων ίσο με τρία. Αντίστροφα, εύκολα βλέπουμε, με χρήση της Παρατήρησης 2.3.3, ότι ο παραπάνω πίνακας Cayley της πράξης «$\cdot$» ορίζει μοναδικά μια δομή ομάδας στο σύνολο $G = \{e, a, b\}$.

Μοντέλα ομάδας με πλήθος στοιχείων ίσο με τρία αποτελούν τα εξής ζεύγη:

$$(\mathbb{Z}_3, +) \quad \text{και} \quad (\mathsf{U}_3 = \{1, \omega, \omega^2\}, \cdot), \quad \text{όπου} \quad \omega = \frac{-1+\sqrt{3}}{2} \quad \text{και} \quad \omega^2 = \frac{-1-\sqrt{3}}{2}$$

4. Έστω $|G| = 4$. Για την ανάλυση ομάδων με πλήθος στοιχείων ίσο με τέσσερα παραπέμπουμε στην Άσκηση 2.10.12, όπου ζητείται να αποδειχθεί ότι υπάρχουν ακριβώς δύο «διαφορετικές» ομάδες με πλήθος στοιχείων ίσο με 4. Αυτές οι ομάδες είναι και οι δύο αβελιανές και έχουν πίνακες Cayley:

Πίνακας Α′ :

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Πίνακας Β′:

$*$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Η ομάδα που έχει ως πίνακα πράξης τον Πίνακα Α′ καλείται **η ομάδα $\mathcal{V}_4$ των τεσσάρων στοιχείων του Klein**[8] και συνήθως συμβολίζεται με $\mathcal{V}_4$.[9]. Παρατηρούμε ότι στην ομάδα αυτή, για κάθε στοιχείο $x \in G$ ισχύει: $x^2 = e$, κάτι το οποίο δεν ισχύει στην ομάδα με πίνακα Cayley τον Πίνακα Β′, διότι για παράδειγμα $c^2 = b^2 = a \neq e$. Από τον πίνακα Cayley Β′ παρατηρούμε η ομάδα G είναι της μορφής $G = \{e, b, b^2, b^3\} = \{e, c, c^2, c^3\}$.

Μοντέλο της ομάδας $\mathcal{V}_4$ του Klein είναι η ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, όπου

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{([0]_2, [0]_2), \ ([0]_2, [1]_2), \ ([1]_2, [0]_2), \ ([1]_2, [1]_2)\}$$

και πράξη: $([x]_2, [y]_2) + ([x']_2, [y']_2) = ([x + x']_2, [y + y']_2)$, και η οποία έχει πίνακα Cayley:

$+$	$([\mathbf{0}]_2, [\mathbf{0}]_2)$	$([\mathbf{1}]_2, [\mathbf{0}]_2)$	$([\mathbf{0}]_2, [\mathbf{1}]_2)$	$([\mathbf{1}]_2, [\mathbf{1}]_2)$
$([\mathbf{0}]_2, [\mathbf{0}]_2)$	$([0]_2, [0]_2)$	$([1]_2, [0]_2)$	$([0]_2, [1]_2)$	$([1]_2, [1]_2)$
$([\mathbf{1}]_2, [\mathbf{0}]_2)$	$([1]_2, [0]_2)$	$([0]_2, [0]_2)$	$([1]_2, [1]_2)$	$([0]_2, [1]_2)$
$([\mathbf{0}]_2, [\mathbf{1}]_2)$	$([0]_2, [1]_2)$	$([1]_2, [1]_2)$	$([0]_2, [0]_2)$	$([1]_2, [0]_2)$
$([\mathbf{1}]_2, [\mathbf{1}]_2)$	$([1]_2, [1]_2)$	$([0]_2, [1]_2)$	$([1]_2, [0]_2)$	$([0]_2, [0]_2)$

[8] Felix Klein (1849-1925) [http://en.wikipedia.org/wiki/Felix_Klein]: Γερμανός μαθηματικός με σημαντική συμβολή στη Θεωρία Ομάδων, στη Μιγαδική Ανάλυση, και στη μη Ευκλείδεια Γεωμετρία. Το έργο του αναφορικά με την σχέση μεταξύ Θεωρίας Ομάδων και Γεωμετρίας είχε εξαιρετικά μεγάλη επίδραση στα σύγχρονα Μαθηματικά. Ο Felix Klein είναι ευρύτερα γνωστός για το Πρόγραμμα του Erlangen, το οποίο διατύπωσε το 1872, στο οποίο πρότεινε την ταξινόμηση Γεωμετριών διαφόρων τύπων με βάση ομάδες συμμετρίας.

[9] Από τον γερμανικό όρο Vierergruppe: η ομάδα τεσσάρων στοιχείων.

Η αντιστοιχία μεταξύ της ομάδας $\mathcal{V}_4$ με πίνακα Cayley τον Πίνακα Α′ και της ομάδας $\mathbb{Z}_2 \times \mathbb{Z}_2$ με πίνακα Cayley τον παραπάνω, είναι η εξής:

$$e \longleftrightarrow ([0]_2, [0]_2), \quad a \longleftrightarrow ([1]_2, [0]_2), \quad b \longleftrightarrow ([0]_2, [1]_2), \quad c \longleftrightarrow ([1]_2, [1]_2)$$

Στην δεύτερη ομάδα, το μόνο στοιχείο x, εκτός του ουδετέρου έτσι ώστε $x^2 = e$ είναι το $x = a$. Η ομάδα με πίνακα Cayley τον πίνακα Β′ αποτελεί το πρότυπο **κυκλικής ομάδας τάξης 4** (Η γενική θεωρία κυκλικών ομάδων θα αναπτυχθεί στο Κεφάλαιο 4), και συνήθως θα την συμβολίζουμε με C_4. Μοντέλο αυτής της ομάδας είναι η ομάδα $(\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}, +)$, και η ομάδα $(\{1, -1, i, -i\}, \cdot)$, όπου $i \in \mathbb{C}$ είναι η φανταστική μονάδα, και «$\cdot$» είναι ο συνήθης πολλαπλασιασμός μιγαδικών αριθμών, με αντίστοιχους πίνακες Cayley τους εξής:

$+$	$[\mathbf{0}]_4$	$[\mathbf{1}]_4$	$[\mathbf{2}]_4$	$[\mathbf{3}]_4$
$[\mathbf{0}]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[\mathbf{1}]_4$	$[1]_4$	$[2]_3$	$[3]_4$	$[0]_4$
$[\mathbf{2}]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[\mathbf{3}]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

και

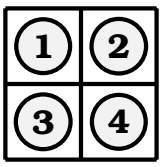
$\cdot$	$\mathbf{1}$	$\mathbf{-1}$	$\mathbf{i}$	$\mathbf{-i}$
$\mathbf{1}$	1	-1	i	$-i$
$\mathbf{-1}$	-1	1	$-i$	i
$\mathbf{i}$	i	$-i$	-1	1
$\mathbf{-i}$	$-i$	i	1	-1

Η αντιστοιχία μεταξύ της ομάδας G με πίνακα Cayley τον πίνακα Β′ και της ομάδας $\mathbb{Z}_4$ με πίνακα Cayley τον παραπάνω πίνακα είναι η εξής:

$$e \longleftrightarrow [0]_4, \quad a \longleftrightarrow [2]_4, \quad b \longleftrightarrow [1]_4, \quad c \longleftrightarrow [3]_4$$

Παρατηρούμε ότι όλες οι ομάδες με πλήθος στοιχείων το πολύ τέσσερα είναι αβελιανές διότι ο πίνακας Cayley αυτών των ομάδων είναι συμμετρικός ως προς την κύρια διαγώνιο.

Παράδειγμα 2.3.4. Στο ακόλουθο «Μικρό Σκάκι» έχουμε ένα μικρό σκάκι με μόνο 4 τετράγωνα:



μπορούμε να κινηθούμε κατά τους εξής τρόπους:

1. O: οριζόντια: $1 \longrightarrow 2$, $2 \longrightarrow 1$, $3 \longrightarrow 4$, $4 \longrightarrow 3$.
2. K: κάθετα: $1 \longrightarrow 3$, $3 \longrightarrow 1$, $2 \longrightarrow 4$, $4 \longrightarrow 2$.
3. Δ: διαγώνια: $1 \longrightarrow 4$, $4 \longrightarrow 1$, $2 \longrightarrow 3$, $3 \longrightarrow 2$.
4. I: καμμία κίνηση: $1 \longrightarrow 1$, $2 \longrightarrow 2$, $3 \longrightarrow 3$, $4 \longrightarrow 4$.

Στο σύνολο των επιτρεπτών κίνησεων

$$G = \{I, O, K, \Delta\}$$

ορίζουμε μια πράξη $\star$: $G \times G \longrightarrow G$, ως εξής: $\forall x, y \in G$, το αποτέλεσμα $x \star y$ της πράξης «$\star$» στις επιτρεπτές κινήσεις x, y είναι η εκτέλεση της κίνησης y ακολουθούμενη από την κίνηση x.

Για παράδειγμα, αν κινηθούμε πρώτα κάθετα και μετά οριζόντια, τότε το αποτέλεσμα είναι να κινηθούμε διαγώνια: $O \star K = \Delta$. Αν κινηθούμε αρχικά οριζόντια και ακολούθως πάλι οριζόντια, θα καταλήξουμε στην αρχική θέση: $O \star O = I$, και παρόμοια $K \star K = I$, και $\Delta \star \Delta = I$.

Εύκολα μπορούμε να δούμε ότι το ζεύγος $(G, \star)$ είναι μια ομάδα με πίνακα Cayley

$\star$	**I**	**O**	**K**	**Δ**
I	I	O	K	Δ
O	O	I	Δ	K
K	K	Δ	I	O
Δ	Δ	K	O	I

Παρατηρούμε ότι ο παραπάνω πίνακας Cayley συμπίπτει με τον πίνακα Cayley της ομάδας του Klein $\mathcal{V}_4$, μέσω της αντιστοιχίας

$$I \longleftrightarrow e, \quad K \longleftrightarrow a, \quad O \longleftrightarrow b, \quad \Delta \longleftrightarrow c$$

και άρα οι ομάδες G και $\mathcal{V}_4$ είναι δομικά ίδιες διότι έχουν τον ίδιο ππίνακα Cayley.

Κλείνουμε την παρούσα υποενότητα σχηματίζοντας το διάγραμμα Cayley των συμμετρικών ομάδων S_n μικρής τάξης.

Παράδειγμα 2.3.5. (Πίνακες Cayley συμμετρικών ομάδων S_n, όπου $n \leq 3$).

– Αν $n = 1$, τότε η συμμετρική ομάδα $\mathsf{S}_1 = \{\iota\}$ είναι η τετριμμένη και άρα ο πίνακας Cayley της S_1 είναι ο εξής:

$\circ$	$\boldsymbol{\iota}$
$\boldsymbol{\iota}$	ι

– Αν $n = 2$, τότε η συμμετρική ομάδα $\mathsf{S}_2 = \{\iota, \mu\}$, όπου $\mu = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = (1\ 2)$, έχει δύο στοιχεία, και προφανώς ο πίνακας Cayley της S_2 είναι ο εξής:

$\circ$	$\boldsymbol{\iota}$	$\boldsymbol{\mu}$
$\boldsymbol{\iota}$	ι	μ
$\boldsymbol{\mu}$	μ	ι

– Αν $n = 3$, θεωρούμε τη συμμετρική ομάδα $(\mathsf{S}_3, \circ)$. Υπενθυμίζουμε ότι $\mathsf{S}_3 = \{\iota,\ \mu_1,\ \mu_2,\ \mu_3,\ \rho_1,\ \rho_2\}$, όπου:

$$\rho_0 = \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\ 3), \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3), \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2),$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ ,3), \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Τότε εύκολα υπολογίζουμε ότι ο πίνακας Cayley της S_3 είναι ο εξής:

$\circ$	$\boldsymbol{\iota}$	$\boldsymbol{\mu}_1$	$\boldsymbol{\mu}_2$	$\boldsymbol{\mu}_3$	$\boldsymbol{\rho}_1$	$\boldsymbol{\rho}_2$
$\boldsymbol{\iota}$	ι	μ_1	μ_2	μ_3	ρ_1	ρ_2
$\boldsymbol{\mu}_1$	μ_1	ι	ρ_1	ρ_2	μ_2	μ_3
$\boldsymbol{\mu}_2$	μ_2	ρ_2	ι	ρ_1	μ_3	μ_1
$\boldsymbol{\mu}_3$	μ_3	ρ_1	ρ_2	ι	μ_1	μ_2
$\boldsymbol{\rho}_1$	ρ_1	μ_3	μ_1	μ_2	ρ_2	ι
$\boldsymbol{\rho}_2$	ρ_2	μ_2	μ_3	μ_1	ι	ρ_1

Χρησιμοποιώντας τον κυκλικό συμβολισμό μεταθέσεων ο πίνακας Cayley της S_3 είναι ο εξής:

$\circ$	**(1)**	**(23)**	**(13)**	**(12)**	**(123)**	**(132)**
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(23)	(23)	(1)	(132)	(123)	(13)	(12)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(12)	(12)	(132)	(123)	(1)	(23)	(13)
(123)	(123)	(12)	(23)	(13)	(132)	(1)
(132)	(132)	(13)	(12)	(23)	(1)	(123)

Παράδειγμα 2.3.6. Κλείνουμε την παρούσα ενότητα με τον πίνακα Cayley της ομάδας $(\mathbb{Z}_6, +)$ των κλάσεων υπολοίπων mod 6, όπου $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$:

$+$	$\mathbf{[0]_6}$	$\mathbf{[1]_6}$	$\mathbf{[2]_6}$	$\mathbf{[3]_6}$	$\mathbf{[4]_6}$	$\mathbf{[5]_6}$
$\mathbf{[0]_6}$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$\mathbf{[1]_6}$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$\mathbf{[2]_6}$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$\mathbf{[3]_6}$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$\mathbf{[4]_6}$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$\mathbf{[5]_6}$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

2.4 Υποομάδες

Υποομάδες είναι υποσύνολα μιας ομάδας τα οποία κληρονομούν τη δομή ομάδας μέσω της επαγόμενης πράξης. Στην παρούσα ενότητα θα ορίσουμε την έννοια της υποομάδας μια ομάδας, θα αναπτύξουμε τη βασική θεωρία τους, και θα αναλύσουμε μια σειρά παραδειγμάτων και κατασκευών υποομάδων.

2.4.1 Υποομάδες και οι βασικές τους ιδιότητες

Έστω ότι $(G, \cdot)$ είναι μια ομάδα.

Υπενθυμίζουμε ότι ένα υποσύνολο $H \subseteq G$ είναι ***κλειστό ως προς την πράξη*** $\cdot : G \times G \longrightarrow G$ της ομάδας G, αν:

$$\forall a, b \in H: \quad a \cdot b \in H$$

Όταν το υποσύνολο H είναι κλειστό ως προς την πράξη «$\cdot$» τής G, τότε, όπως γνωρίζουμε, η απεικόνιση «$\cdot$» επάγει μια πράξη

$$\cdot : H \times H \longrightarrow H$$

επί της H. Προφανώς η επαγόμενη πράξη «$\cdot$» είναι προσεταιριστική. Είναι σημαντικό να γνωρίζουμε ποια υποσύνολα μιας ομάδας κληρονομούν την ιδιότητα της ομάδας, και έτσι οδηγούμαστε στον ακόλουθο ορισμό.

Ορισμός 2.4.1. *Έστω $(G, \cdot)$ μια ομάδα και $H \subseteq G$ ένα υποσύνολο της G. Το H καλείται **υποομάδα** της G αν:*

1. *Το υποσύνολο H είναι κλειστό στην πράξη «$\cdot$» της ομάδας G.*
2. *Το ζεύγος $(H, \cdot)$ αποτελεί ομάδα.*

Συμβολισμός 2.4.2. Συνήθως, δηλώνουμε ότι ένα υποσύνολο H μιας ομάδας $(G, \cdot)$ είναι μια υποομάδα της G γράφοντας

$$H \leq G$$

Μια υποομάδα H της G καλείται **γνήσια** αν $H \neq G$. Θα δηλώνουμε ότι ένα υποσύνολο H μιας ομάδας $(G, \cdot)$ είναι μια γνήσια υποομάδα τής G γράφοντας

$$H < G \quad \surd$$

Παρατήρηση 2.4.3. Όπως προκύπτει από τον ορισμό, κάθε ομάδα G έχει πάντα δύο υποομάδες (οι οποίες μπορεί να συμπίπτουν όταν $G = \{e\}$): την ίδια την ομάδα G, δηλαδή την **μη γνήσια υποομάδα** G, και το υποσύνολο $\{e\}$, δηλαδή την **τετριμμένη υποομάδα** $\{e\}$. Θα δούμε αργότερα ποιες ομάδες έχουν μόνο δύο υποομάδες (οι οποίες αναγκαστικά θα είναι η τετριμμένη και η μη γνήσια υποομάδα). ▲

Συνεπώς, όταν το σύνολο H είναι μια υποομάδα τής $(G,\cdot)$, τότε το σύνολο H είναι κλειστό ως προς την πράξη «$\cdot$» της G και με την επαγόμενη πράξη αποτελεί ομάδα. Επομένως η H διαθέτει ουδέτερο στοιχείο, το οποίο προσωρινά συμβολίζουμε με e_H, και επομένως ισχύει ότι:

$$\forall a \in H: \quad a \cdot e_H = a = e_H \cdot a$$

Επιπλέον για κάθε στοιχείο $a \in H$, υπάρχει το αντίστροφό του στην ομάδα H, το οποίο προσωρινά συμβολίζουμε με $a_H^{-1} \in H$, και επομένως ισχύει ότι:

$$a \cdot a_H^{-1} = e_H = a_H^{-1} \cdot a$$

Η επόμενη βοηθητική πρόταση μας εξασφαλίζει ότι τα ουδέτερα στοιχεία μιας ομάδας και μιας υποομάδας συμπίπτουν, και επίσης το αντίστροφο ενός στοιχείου σε μια υποομάδα συμπίπτει με το αντίστροφο στοιχείο στην ομάδα:

Λήμμα 2.4.4. *Έστω $(G,\cdot)$ μια ομάδα με ουδέτερο στοιχείο e, και έστω $H \leq G$ μια υποομάδα της.*

1. *Το ουδέτερο στοιχείο e_H της ομάδας H συμπίπτει με το ουδέτερο στοιχείο e της ομάδας G.*
2. *Για κάθε $a \in H$, το αντίστροφό του a_H^{-1} στην ομάδα H συμπίπτει με το αντίστροφό του a^{-1} στην G.*

Απόδειξη. 1. Επειδή το στοιχείο e_H είναι ουδέτερο στοιχείο της ομάδας H, έπεται ότι θα έχουμε $e_H \cdot e_H = e_H$. Επειδή το στοιχείο e είναι ουδέτερο στοιχείο της ομάδας G, έπεται ότι θα έχουμε $e_H \cdot e = e_H$. Άρα θα έχουμε στην ομάδα G ότι: $e_H \cdot e_H = e_H \cdot e$. Από τον Νόμο Διαγραφής στην ομάδα G, βλέπε την Πρόταση 2.1.8, έπεται τότε ότι: $e_H = e$.

2. Επειδή από το μέρος 1. ισχύει ότι $e_H = e$, έπεται ότι για το στοιχείο $a \in H$ θα έχουμε: $a \cdot a_H^{-1} = e_H = e$ (ύπαρξη αντιστρόφου του a στην ομάδα H) και $a \cdot a^{-1} = e$ (ύπαρξη αντιστρόφου του a στην ομάδα G). Άρα θα έχουμε στην ομάδα G ότι: $a \cdot a_H^{-1} = e = a \cdot a^{-1}$. Από τον Νόμο Διαγραφής στην ομάδα G, βλέπε την Πρόταση 2.1.8, έπεται τότε ότι: $a_H^{-1} = a^{-1}$. ■

Η ακόλουθη πρόταση δίνει ένα χρήσιμο κριτήριο για το πότε ένα υποσύνολο μιας ομάδας είναι υποομάδα.

Πρόταση 2.4.5. *Αν $(G,\cdot)$ είναι μια ομάδα με ουδέτερο στοιχείο e, και H είναι ένα υποσύνολό της, τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Το H είναι μια υποομάδα της $(G,\cdot)$.*
2. *(α΄) Το υποσύνολο H είναι κλειστό στην πράξη «$\cdot$» της G.*
   (β΄) $e \in H$.
   (γ΄) $\forall a \in H: \ a^{-1} \in H$.
3. *(α΄) $H \neq \emptyset$.*
   (β΄) $\forall a, b \in H: \ a \cdot b^{-1} \in H$.

Απόδειξη. 1. $\Longrightarrow$ 2. Έστω ότι το υποσύνολο H είναι μια υποομάδα της G. Τότε, σύμφωνα με τον ορισμό της υποομάδας 2.4.1, το υποσύνολο H είναι κλειστό στην πράξη «$\cdot$» της ομάδας, και είναι προφανώς ένα μη κενό σύνολο (διότι το H ως ομάδα περιέχει τουλάχιστον ένα στοιχείο, το ουδέτερο στοιχείο της). Απο το Λήμμα 2.4.4, έπεται ότι η υποομάδα H περιέχει το ταυτοτικό στοιχείο e της G και επίσης το αντίστροφο a^{-1} κάθε στοιχείου $a \in H$.

2. $\Longrightarrow$ 3. Επειδή από την υπόθεση $e \in H$, έπεται ότι $H \neq \emptyset$. Έστω $a, b \in H$ δύο στοιχεία της H. Τότε από την υπόθεση, επειδή $b \in H$, έπεται ότι $b^{-1} \in H$. Τέλος, επειδή το υποσύνολο H είναι κλειστό στην πράξη «$\cdot$» της ομάδας G και $a, b^{-1} \in H$, έπεται ότι $a \cdot b^{-1} \in H$.

3. $\Longrightarrow$ 1. Επειδή $H \neq \emptyset$, έπεται ότι υπάρχει ένα στοιχείο $a \in G$ το οποίο ανήκει στο υποσύνολο H: $a \in H$. Τότε από το μέρος (β′) της υπόθεσης 3. έπεται ότι: $a \cdot a^{-1} = e \in H$. Άρα το ουδέτερο στοιχείο της G ανήκει στο υποσύνολο H. Επιπλέον για κάθε στοιχείο $a \in H$ τα στοιχεία e, a είναι στοιχεία του H και γι′ αυτό, σύμφωνα με το μέρος (β′) της υπόθεσης 3., το στοιχείο $e \cdot a^{-1} = a^{-1}$ είναι στοιχείο του υποσυνόλου H.

Θα δείξουμε τώρα ότι ο περιορισμός της πράξης «$\cdot$» στο υποσύνολο H ορίζει μια πράξη $\cdot : H \times H \longrightarrow H$, δηλαδή αν $(a,b) \in H \times H$, τότε το στοιχείο $a \cdot b$ της G ανήκει στο υποσύνολο H. Πράγματι, αν $(a,b) \in H \times H$, τότε $b \in H$ και, όπως είδαμε παραπάνω, θα έχουμε $b^{-1} \in H$. Συνεπώς, το ζεύγος (a, b^{-1}) ανήκει στο $H \times H$ και γι′ αυτό, εφαρμόζοντας και πάλι το μέρος (b') της υπόθεσης 3., θα έχουμε ότι το στοιχείο $a \cdot (b^{-1})^{-1}$ ανήκει στο H. Επειδή $(b^{-1})^{-1} = b$, έπεται ότι το στοιχείο $a \cdot b$ είναι στοιχείο του υποσυνόλου H.

Τέλος, επειδή η πράξη «$\cdot$» επί της G είναι προσεταιριστική, είναι φανερό ότι παραμένει προσεταιριστική και περιορισμένη επί του υποσυνόλου H. Επόμενως το ζεύγος $(H, \cdot)$ είναι ομάδα, διότι η πράξη «$\cdot$» επί του H είναι προσεταιριστική, υπάρχει ουδέτερο στοιχείο $e \in H$, και κάθε στοιχείο $a \in H$, έχει αντίστροφο στοιχείο $a^{-1} \in H$. Άρα το υποσύνολο H είναι μια υποομάδα της G. ■

Παρατήρηση 2.4.6. Ακολουθώντας προσθετικό συμβολισμό, έστω $(G,+)$ μια ομάδα με ουδέτερο στοιχείο e. Αν H είναι ένα υποσύνολο της G, τότε η Πρόταση 2.4.5 λαμβάνει την ακόλουθη μορφή:

1. Το H είναι μια υποομάδα της $(G,+)$.
2. Το υποσύνολο H είναι κλειστό στην πράξη «$\cdot$» της G, $e \in H$, και $\forall a \in H$: $-a \in H$.
3. $H \neq \emptyset$, και $\forall a, b \in H$: $a - b \in H$. ▲

Παρατήρηση 2.4.7. Έστω K, H δύο υποσύνολα μιας ομάδας $(G, \cdot)$, έτσι ώστε $K \subseteq H$.

1. Αν το υποσύνολο H είναι υποομάδα της ομάδας G και το υποσύνολο K είναι υποσύνολο της ομάδας H, τότε το υποσύνολο K είναι υποομάδα της ομάδας G:
$$H \leq G \quad \text{και} \quad K \leq H \quad \Longrightarrow \quad K \leq G$$
2. Αν τα υποσύνολα H και K είναι υποομάδες της ομάδας G, τότε το υποσύνολο K είναι υποομάδα της ομάδας H:
$$K, H \leq G \quad \Longrightarrow \quad K \leq H$$

Η απόδειξη των παραπάνω ισχυρισμών είναι άμεση εφαρμογή του κριτηρίου 2.4.5. ▲

Σε μερικές περιπτώσεις ο έλεγχος αν ένα υποσύνολο μιας ομάδας αποτελεί υποομάδα, είναι εξαιρετικά απλός, όπως δείχνει η ακόλουθη πολύ χρήσιμη Πρόταση:

Πρόταση 2.4.8. *Έστω $(G, \cdot)$ μια ομάδα και H ένα μη κενό υποσύνολό της το οποίο έχει πεπερασμένο πλήθος στοιχείων: $|H| < \infty$. Αν το H είναι κλειστό ως προς την πράξη «$\cdot$» της G, τότε το H είναι υποομάδα της G.*

Απόδειξη. Επειδή το σύνολο H είναι κλειστό ως προς την πράξη «$\cdot$» της G, έπεται ότι, για τυχόντα στοιχεία $a, b \in H$, το στοιχείο $a \cdot b$ ανήκει επίσης στην H και επομένως ορίζεται η επαγόμενη πράξη επί της H:
$$\cdot : H \times H \longrightarrow H, \qquad (a,b) \longmapsto a \cdot b$$
Σύμφωνα με την Πρόταση 2.4.5, για να είναι το υποσύνολο H υποομάδα τής G, πρέπει το ουδέτερο στοιχείο e της G να ανήκει στο H και για κάθε στοιχείο $a \in H$, το αντίστροφό του a^{-1} στην G να ανήκει επίσης στο H.

Επειδή το σύνολο H είναι πεπερασμένο, μπορούμε να υποθέσουμε ότι $H = \{a_1, a_2, \ldots, a_n\}$, όπου $n \in \mathbb{N}$. Έστω a ένα οποιοδήποτε αλλά συγκεκριμένο στοιχείο της H.

1. Θεωρούμε την απεικόνιση
$$\ell_a : H \longrightarrow H, \quad \ell_a(a_k) = a \cdot a_k$$
Η απεικόνιση ℓ_a είναι «1-1», διότι, αν a_i, a_j είναι στοιχεία της H έτσι ώστε $\ell_a(a_i) = \ell_a(a_j)$, τότε $a \cdot a_i = a \cdot a_j$ και επομένως από τον νόμο διαγραφής στην ομάδα G, βλέπε την Πρόταση 2.1.8, θα έχουμε $a_i = a_j$. Επειδή το σύνολο H είναι πεπερασμένο και η απεικόνιση $\ell_a : H \longrightarrow H$ είναι «1-1», έπεται ότι η ℓ_a είναι απεικόνιση «επί». Επομένως υπάρχει κάποιο στοιχείο $a_j \in H$ έτσι ώστε $a = \ell_a(a_j)$, δηλαδή $a = a \cdot a_j$. Τότε $a \cdot e = a \cdot a_j$ και πάλι από τον νόμο διαγραφής στην ομάδα G έπεται ότι $a_j = e$. Άρα $e \in H$ διότι $a_j \in H$.

2. Τέλος, για το τυχόν στοιχείο $a \in H$, επειδή η ℓ_a είναι «επί», έπεται ότι υπάρχει στοιχείο $a_k \in H$ έτσι ώστε: $\ell_a(a_k) = e$, δηλαδή $a \cdot a_k = e$. Τότε στην ομάδα G θα έχουμε $a^{-1} = a_k \in H$, δηλαδή το αντίστροφο, στην ομάδα G, κάθε στοιχείου του υποσυνόλου H ανήκει στην H. Επομένως σύμφωνα με την Πρόταση 2.4.5, το υποσύνολο H είναι υποομάδα της G. ■

Παράδειγμα 2.4.9. Στην προσθετική ομάδα $(\mathbb{Z}, +)$ των ακεραίων, θεωρούμε το (μη κενό) υποσύνολο $\mathbb{N}_0$, το οποίο έχει άπειρο πλήθος στοιχείων και προφανώς είναι κλειστό στην πράξη «+» της ομάδας $\mathbb{Z}$. Όμως το υποσύνολο $\mathbb{N}_0$ δεν είναι υποομάδα της ομάδας $\mathbb{Z}$ διότι, για παράδειγμα, το αντίθετο του στοιχείου $1 \in \mathbb{N}_0$ στην ομάδα $\mathbb{Z}$, δηλαδή το -1, δεν ανήκει στο υποσύνολο $\mathbb{N}_0$. Σύμφωνα με την Πρόταση 2.4.8, ο λόγος για τον οποίο συμβαίνει αυτό είναι ότι το υποσύνολο $\mathbb{N}_0$ έχει άπειρο πλήθος στοιχείων. √

2.4.2 Παραδείγματα Υποομάδων

Στην παρούσα ενότητα θα αναλύσουμε μια πληθώρα παραδειγμάτων υποομάδων μιας ομάδας. Έτσι θα εφοδιαστούμε με αρκετά νέα παραδείγματα ομάδων τα οποία θα μας είναι χρήσιμα και στην συνέχεια.

Παράδειγμα 2.4.10. (Ομάδες και Υποομάδες προερχόμενες από την ομάδα $(\mathbb{Z}, +)$ των ακεραίων). Θεωρούμε την προσθετική ομάδα $(\mathbb{Z}, +)$ των ακεραίων. Η ομάδα $(\mathbb{Z}, +)$ είναι μια αβελιανή ομάδα με άπειρο πλήθος στοιχείων.

Για κάθε $n \geq 1$, το σύνολο
$$n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}$$
των ακέραιων πολλαπλασίων του n είναι μια υποομάδα του $\mathbb{Z}$. Πράγματι $n\mathbb{Z} \neq \emptyset$ διότι $0 = n \cdot 0$, και αν $a = n \cdot k_1$ και $b = n \cdot k_2$ είναι δύο στοιχεία του υποσυνόλου $n\mathbb{Z}$, όπου $k_1, k_2 \in \mathbb{Z}$, τότε $a - b = n \cdot k_1 - n \cdot k_2 = n \cdot (k_1 - k_2) \in n\mathbb{Z}$. Επομένως από την Παρατήρηση 2.4.6 έπεται ότι $n\mathbb{Z} \leq \mathbb{Z}$. Έτσι η προσθετική ομάδα $\mathbb{Z}$ των ακεραίων περιέχει τις υποομάδες:
$$\{0\} = 0\mathbb{Z}, \quad \mathbb{Z} = 1\mathbb{Z}, \quad 2\mathbb{Z}, \quad 3\mathbb{Z}, \quad \cdots, \quad n\mathbb{Z}, \quad \cdots$$
οι οποίες προφανώς είναι ανά δύο διακεκριμένες, και εκτός της τετριμμένης υποομάδας $\{0\}$, όλες έχουν άπειρο πλήθος στοιχείων. Θα δούμε σε επόμενη ενότητα ότι οι παραπάνω ομάδες είναι όλες οι υποομάδες της $\mathbb{Z}$. √

Παράδειγμα 2.4.11. (Η Ομάδα του Κύκλου). Θεωρούμε την ομάδα $(\mathbb{C}^*, \cdot)$ των μη-μηδενικών μιγαδικών αριθμών, όπου «·» είναι ο συνήθης πολλαπλασιασμός μιγαδικών αριθμών.

Θεωρούμε το υποσύνολο
$$\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\}$$
του $\mathbb{C}$, όπου $|z|$ συμβολίζει το μέτρο του μιγαδικού αριθμού z. Έτσι, αν $z = x + iy$, όπου $x, y \in \mathbb{R}$, τότε $|z| = \sqrt{x^2 + y^2}$ και $|z|^2 = x^2 + y^2 = z \cdot \overline{z}$, όπου $\overline{z} = x - iy$ είναι ο συζυγής του z. Προφανώς $\mathsf{T} \subseteq \mathbb{C}^*$ και $\mathsf{T} \neq \emptyset$ διότι $1 \in \mathsf{T}$. Έστω $z, w \in \mathsf{T}$, δηλαδή θα έχουμε $|z| = 1 = |w|$. Τότε, χρησιμοποιώντας στοιχειώδεις ιδιότητες του μέτρου μιγαδικών αριθμών, βλέπε την υποενότητα 0.4, θα έχουμε:
$$|z \cdot w^{-1}| = |z| \cdot |w^{-1}| = |z| \cdot |w|^{-1} = 1 \cdot 1^{-1} = 1 \quad \Longrightarrow \quad z \cdot w^{-1} \in \mathsf{T}$$
Από την Πρόταση 2.4.5, έπεται ότι το υποσύνολο T είναι μια υποομάδα της $(\mathbb{C}^*, \cdot)$.

Επειδή τα στοιχεία της ομάδας T είναι όλοι οι μιγαδικοί αριθμοί $z = x+iy$ έτσι ώστε $|z| = 1$ ή ισοδύναμα όλοι οι μιγαδικοί αριθμοί $z = x+iy$ έτσι ώστε $|z|^2 = x^2+y^2 = 1$, γεωμετρικά το σύνολο T είναι περιφέρεια κύκλου με ακτίνα 1 στο επίπεδο $\mathbb{R}^2$. Γι' αυτόν τον λόγο η ομάδα T καλείται η **ομάδα του κύκλου**. $\surd$

Παράδειγμα 2.4.12. (Η Ομάδα των n-οστών Ριζών της Μονάδας). Για κάθε θετικό ακέραιο n, θεωρούμε το υποσύνολο

$$\mathsf{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$$

του $\mathbb{C}$. Προφανώς $\mathsf{U}_n \neq \emptyset$, διότι $1 \in \mathsf{U}_n$, και $\mathsf{U}_n \subseteq \mathbb{C}^*$. Θεωρούμε τυχόντα στοιχεία $z_1, z_2 \in \mathsf{U}_n$, δηλαδή $z_1^n = 1 = z_2^n$. Τότε:

$$(z_1 \cdot z_2^{-1})^n = z_1^n \cdot (z_2^n)^{-1} = 1 \cdot 1^{-1} = 1 \quad \Longrightarrow \quad z_1 \cdot z_2^{-1} \in \mathsf{U}_n$$

Επομένως, σύμφωνα με την Πρόταση 2.4.5, έπεται ότι το υποσύνολο U_n είναι μια υποομάδα της $(\mathbb{C}^*, \cdot)$ η οποία καλείται η **ομάδα των n-οστών ριζών της μονάδας**.

Θα περιγράψουμε αναλυτικότερα τα στοιχεία της ομάδας U_n. Υπενθυμίζουμε ότι κάθε μιγαδικός αριθμός $z = a+bi$ μπορεί να γραφεί στην *πολική μορφή* του: $z = r(\cos(\theta) + i\sin(\theta)) = re^{i\theta}$, όπου $r = |z| \in \mathbb{R}$ είναι το μέτρο του z, και θ είναι το *όρισμα* του z. Έστω $z \in \mathsf{U}_n$, και άρα $z^n = 1$, και έστω $z = r(\cos(\theta) + i\sin(\theta)) = re^{i\theta}$ η πολική μορφή του z. Τότε θα έχουμε:

$$z^n = 1 \quad \Longrightarrow \quad |z^n| = 1 \quad \Longrightarrow \quad |z|^n = 1 \quad \Longrightarrow \quad |z| = r = 1 \quad \Longrightarrow \quad z = \cos(\theta) + i\sin(\theta) = e^{i\theta}$$

Ιδιαίτερα βλέπουμε ότι $\mathsf{U}_n \subseteq \mathbb{C}^*$. Επομένως θα έχουμε:

$$\mathsf{U}_n \leq \mathsf{T} \leq \mathbb{C}^*$$

Χρησιμοποιώντας βασικές ιδιότητες μιγαδικών αριθμών στην πολική τους μορφή (τύπος του De Moivre, δηλαδή η τρίτη ισότητα στην παρακάτω σχέση), βλέπε την υποενότητα 0.4, θα έχουμε:

$$1 = z^n = (\cos(\theta) + i\sin(\theta)^n = \cos(n\theta) + i\sin(n\theta) \quad \Longrightarrow \quad \cos(n\theta) = 1 \quad \text{και} \quad \sin(n\theta) = 0 \quad \Longrightarrow$$

$$\Longrightarrow \quad n\theta = 2k\pi, \;\; k \in \mathbb{Z} \quad \Longrightarrow \quad \theta = \frac{2k\pi}{n}, \quad k \in \mathbb{Z}$$

Από την άλλη πλευρά, η τιμή του $z = \cos(\theta) + i\sin(\theta)$, όπου $\theta = \frac{2k\pi}{n}$, εξαρτάται μόνο από την κλάση ισοτιμίας mod n του ακέραιου k. Πράγματι, έστω αν k, l είναι ακέραιοι έτσι ώστε $[k]_n = [l]_n$, τότε $n \mid k-l$, και άρα μπορούμε να γράψουμε ότι $k - l = r \cdot n$, ή ισοδύναμα $k = l + r \cdot n$, για κάποιον ακέραιο r. Τότε

$$\cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) = \cos(\frac{2(l+r\cdot n)\pi}{n}) + i\sin(\frac{2(l+r\cdot n)\pi}{n}) = \cos(\frac{2l\pi}{n} + 2r\pi) + i\sin(\frac{2l\pi}{n} + 2r\pi) = \cos(\frac{2l\pi}{n}) + i\sin(\frac{2l\pi}{n})$$

Αντίστροφα, αν για κάποιους ακέραιους k, l ισχύει ότι $\cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) = \cos(\frac{2l\pi}{n}) + i\sin(\frac{2l\pi}{n})$, τότε θα έχουμε $\cos(\frac{2k\pi}{n}) = \cos(\frac{2l\pi}{n})$ και $\sin(\frac{2k\pi}{n}) = \sin(\frac{2l\pi}{n})$, και επομένως υπάρχει ακέραιος r έτσι ώστε:

$$\frac{2k\pi}{n} - \frac{2l\pi}{n} = 2r\cdot\pi \quad \Longrightarrow \quad (k-l)\cdot\pi = r\cdot n\pi \quad \Longrightarrow \quad k - l = r\cdot n \quad \Longrightarrow \quad n \mid k-l \quad \Longrightarrow \quad [k]_n = [l]_n$$

Επειδή το πλήθος των διακεκριμένων κλάσεων ισοτιμίας mod n είναι n, έπεται ότι το πλήθος των διακεκριμένων στοιχείων της μορφής $z = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n})$ είναι n και επομένως θα έχουμε:

$$\mathsf{U}_n = \left\{ e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) \in \mathbb{C} \;\middle|\; 0 \leq k \leq n-1 \right\}$$

Από τον τύπο του De Moivre έπεται ότι $e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) = [\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})]^k = (e^{\frac{2\pi i}{n}})^k$, $\forall k \geq 1$. Έτσι, θέτοντας

$$\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}), \qquad \text{θα έχουμε:} \quad \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) = \zeta_n^k$$

και επομένως

$$\mathsf{U}_n = \{1,\ \zeta_n,\ \zeta_n^2,\ \cdots,\ \zeta_n^{n-1}\}$$

και άρα η ομάδα U_n των n-οστών ριζών της μονάδας έχει ακριβώς n στοιχεία. Γεωμετρικά τα στοιχεία της ομάδας U_n είναι κορυφές κανονικού n-γώνου εγγεγραμμένου σε κύκλο ακτίνας 1 στο επίπεδο $\mathbb{R}^2$. Ιδιαίτερα βλέπουμε ότι $\mathsf{U}_n \subseteq \mathsf{T}$, όπου T είναι η ομάδα του κύκλου, τα σημεία της οποίας όπως είδαμε συμπίπτουν με τα σημεία του κύκλου ακτίνας 1 στο επίπεδο $\mathbb{R}^2$. Περιγράφουμε τα στοιχεία της U_n για μικρές τιμές του n:

$$\mathsf{U}_1 = \{1\}, \qquad \mathsf{U}_2 = \{1,-1\}, \qquad \mathsf{U}_3 = \left\{1,\ \frac{-1+i\sqrt{3}}{2},\ \frac{-1-i\sqrt{3}}{2}\right\}, \qquad \mathsf{U}_4 = \{1,i,-1,-i\} \quad \surd$$

Παράδειγμα 2.4.13. (Η Ειδική Γραμμική Ομάδα). Υπενθυμίζουμε ότι το σύνολο

$$\mathsf{GL}(n,\mathbb{K}) = \{A \in \mathsf{M}_n(\mathbb{K}) \ \mid \ A\colon \text{αντιστρέψιμος}\}$$

των $n \times n$ αντιστρέψιμων πινάκων με στοιχεία από το σύνολο $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένα εκ των συνόλων αριθμών $\mathbb{Q},\mathbb{R},\mathbb{C}$, εφοδιασμένο με την πράξη «$\cdot$» του πολλαπλασιασμού πινάκων αποτελεί μια ομάδα. Σημειώνουμε ότι $\mathsf{GL}(n,\mathbb{K}) = \{A \in \mathsf{M}_n(\mathbb{K}) \mid |A| \neq 0\}$, όπου $|A| = \det(A)$ είναι η ορίζουσα του πίνακα A.

Θεωρούμε το υποσύνολο

$$\mathsf{SL}(n,\mathbb{K}) = \{A \in \mathsf{GL}(n,\mathbb{K}) \ \mid \ \det(A) = 1\}$$

της ομάδας $\mathsf{GL}(n,\mathbb{K})$. Θα εφαρμόσουμε την Πρόταση 2.4.5 για να αποδείξουμε ότι το υποσύνολο $\mathsf{SL}(n,\mathbb{K})$ είναι υποομάδα της $\mathsf{GL}(n,\mathbb{K})$. Παρατηρούμε πρώτα ότι το υποσύνολο $\mathsf{SL}(n,\mathbb{K}) \neq \emptyset$, διότι ο μοναδιαίος $n \times n$ πίνακας I_n είναι στοιχείο του συνόλου $\mathsf{SL}(n,\mathbb{K})$. Επιπλέον, αν $A,B \in \mathsf{SL}(n,\mathbb{K})$, δηλαδή $|A| = 1 = |B|$, τότε χρησιμοποιώντας βασικές ιδιότητες οριζουσών θα έχουμε:

$$|A \cdot B^{-1}| = |A| \cdot |B^{-1}| = |A| \cdot |B|^{-1} = 1 \cdot 1^{-1} = 1 \quad \Longrightarrow \quad A \cdot B \in \mathsf{SL}(n,\mathbb{K})$$

Σύμφωνα με την Πρόταση 2.4.5, το υποσύνολο $\mathsf{SL}(n,\mathbb{K})$ είναι υποομάδα της $\mathsf{GL}(n,\mathbb{K})$, η οποία καλείται η ***n*-οστή ειδική γραμμική ομάδα** υπεράνω του $\mathbb{K}$. $\surd$

Παράδειγμα 2.4.14. (Η Ορθογώνια Ομάδα και η Ομάδα Περιστροφών του $\mathbb{R}^n$). Υπενθυμίζουμε ότι ένας πίνακας $A \in \mathsf{M}_n(\mathbb{R})$ καλείται *ορθογώνιος*, αν: $A \cdot {}^tA = I_n = {}^tA \cdot A$, όπου I_n είναι ο μοναδιαίος $n \times n$ πραγματικών αριθμών και ${}^tA$ είναι ο ανάστροφος του πίνακα A. Η παραπάνω σχέση δείχνει ότι ο πίνακας A είναι αντιστρέψιμος, άρα $A \in \mathsf{GL}(n,\mathbb{R})$, και ο αντίστροφός του είναι $A^{-1} = {}^tA$. Θεωρούμε το ακόλουθο σύνολο όλων των ορθογώνιων πινάκων

$$\mathsf{O}(n) = \{A \in \mathsf{M}_n(\mathbb{R}) \mid A\colon \text{ορθογώνιος}\}$$

Προφανώς $\mathsf{O}(n) \neq \emptyset$, διότι $I_n \in \mathsf{O}(n)$, και όπως είδαμε: $\mathsf{O}(n) \subseteq \mathsf{GL}(n,\mathbb{R})$. Αν $A,B \in \mathsf{O}(n)$, δηλαδή $A \cdot {}^tA = I_n = {}^tA \cdot A$ και $B \cdot {}^tB = I_n = {}^tB \cdot B$, ή ισοδύναμα $A^{-1} = {}^tA$ και $B^{-1} = {}^tB$, τότε θα έχουμε

$$(A \cdot B^{-1}) \cdot {}^t(A \cdot B^{-1}) = (A \cdot {}^tB) \cdot {}^t(A \cdot {}^tB) = (A \cdot {}^tB) \cdot ({}^t({}^tB) \cdot {}^tA) = (A \cdot {}^tB) \cdot (B \cdot {}^tA) = A \cdot ({}^tB \cdot B) \cdot {}^tA = A \cdot I_n \cdot {}^tA = A \cdot {}^tA = I_n$$

$${}^t(A \cdot B^{-1}) \cdot (A \cdot B^{-1}) = {}^t(A \cdot {}^tB) \cdot (A \cdot {}^tB) = ({}^t({}^tB) \cdot {}^tA) \cdot (A \cdot {}^tB) = (B \cdot {}^tA) \cdot (A \cdot {}^tB) = B \cdot ({}^tA \cdot A) \cdot {}^tB = B \cdot I_n \cdot {}^tB = B \cdot {}^tB = I_n$$

Οι παραπάνω σχέσεις δείχνουν ότι ο πίνακας $A \cdot B^{-1}$ είναι ορθογώνιος: $A \cdot B^{-1} \in \mathsf{O}(n)$. Επομένως, σύμφωνα με την Πρόταση 2.4.5, το υποσύνολο $\mathsf{O}(n)$ των ορθογωνίων πινάκων είναι υποομάδα της $\mathsf{GL}(n,\mathbb{R})$, η οποία καλείται η ***n*-οστή ορθογώνια ομάδα**.

Αν ο πίνακας A είναι ορθογώνιος, τότε, θεωρώντας ορίζουσες στη σχέση $A \cdot {}^tA = I_n$ και χρησιμοποιώντας οτι η ορίζουσα ενός πίνακα συμπίπτει με την ορίζουσα του αναστρόφου του, θα έχουμε:

$$|A \cdot {}^tA| = |I_n| \quad \Longrightarrow \quad |A| \cdot |{}^tA| = 1 \quad \Longrightarrow \quad |A| \cdot |A| = 1 \quad \Longrightarrow \quad |A|^2 = 1 \quad \Longrightarrow \quad |A| = \pm 1$$

Θεωρούμε το ακόλουθο υποσύνολο της ορθογώνιας ομάδας $\mathsf{O}(n)$:

$$\mathsf{SO}(n) = \{A \in \mathsf{O}(n) \mid |A| = 1\}$$

Τότε προφανώς $I_n \in \mathsf{SO}(n)$, και αν $A, B \in \mathsf{SO}(n)$, τότε θα έχουμε

$$|A \cdot B^{-1}| = |A| \cdot |B^{-1}| = |A| \cdot |B|^{-1} = 1 \cdot 1^{-1} = 1 \quad \Longrightarrow \quad A \cdot B^{-1} \in \mathsf{SO}(n)$$

Επομένως από την Πρόταση 2.4.5, έπεται ότι το υποσύνολο $\mathsf{SO}(n)$ των ορθογωνίων πινάκων με ορίζουσα 1 είναι υποομάδα της ορθογώνιας ομάδας $\mathsf{O}(n)$, η οποία καλείται η **ειδική n-οστή ορθογώνια ομάδα** ή **ομάδα περιστροφών** του $\mathbb{R}^n$. $\surd$

Παράδειγμα 2.4.15. (Η Μοναδιαία Ομάδα). Υπενθυμίζουμε ότι ένας πίνακας $A \in \mathsf{M}_n(\mathbb{C})$ καλείται *μοναδιαίος*, αν: $A \cdot A^* = I_n = A^* \cdot A$, όπου I_n είναι ο μοναδιαίος $n \times n$ μιγαδικών αριθμών και A^* είναι ο ανάστροφος-συζυγής[10] του πίνακα A. Η παραπάνω σχέση δείχνει ότι ο πίνακας A είναι αντιστρέψιμος, άρα $A \in \mathsf{GL}(n, \mathbb{C})$, και ο αντίστροφός του είναι $A^{-1} = A^*$. Θεωρούμε το ακόλουθο σύνολο όλων των μοναδιαίων πινάκων

$$\mathsf{U}(n) = \left\{ A \in \mathsf{M}_n(\mathbb{C}) \mid A\text{: μοναδιαίος} \right\}$$

Προφανώς $\mathsf{U}(n) \neq \emptyset$, διότι $I_n \in \mathsf{U}(n)$, και όπως είδαμε: $\mathsf{U}(n) \subseteq \mathsf{GL}(n, \mathbb{C})$. Αν $A, B \in \mathsf{U}(n)$, δηλαδή $A \cdot A^* = I_n = A^* \cdot A$ και $B \cdot B^* = I_n = B^* \cdot B$, ή ισοδύναμα $A^{-1} = A^*$ και $B^{-1} = B^*$, τότε θα έχουμε

$$(A \cdot B^{-1}) \cdot (A \cdot B^{-1})^* = (A \cdot B^*) \cdot (A \cdot B^*)^* = (A \cdot B^*) \cdot ((B^*)^* \cdot A^*) = (A \cdot B^*) \cdot (B \cdot A^*) = A \cdot (B^* \cdot B) \cdot A^* = A \cdot I_n \cdot A^* = A \cdot A^* = I_n$$

$$(A \cdot B^{-1})^* \cdot (A \cdot B^{-1}) = (A \cdot B^*)^* \cdot (A \cdot B^*) = ((B^*)^* \cdot A^*) \cdot (A \cdot B^*) = (B \cdot A^*) \cdot (A \cdot B^*) = B \cdot (A^* \cdot A) \cdot B^* = B \cdot I_n \cdot B^* = B \cdot B^* = I_n$$

Οι παραπάνω σχέσεις δείχνουν ότι ο πίνακας $A \cdot B^{-1}$ είναι μοναδιαίος: $A \cdot B^{-1} \in \mathsf{U}(n)$. Επομένως, σύμφωνα με την Πρόταση 2.4.5, το υποσύνολο $\mathsf{U}(n)$ των μοναδιαίων πινάκων είναι υποομάδα της $\mathsf{GL}(n, \mathbb{R})$, η οποία καλείται η **$n$-οστή μοναδιαία ομάδα**.

Αν ο πίνακας μιγαδικών αριθμών A είναι μοναδιαίος, τότε, θεωρώντας ορίζουσες στη σχέση $A \cdot A^* = I_n$ και χρησιμοποιώντας οτι η ορίζουσα του αναστρόφου-συζυγή ενός πίνακα συμπίπτει με τον συζυγή της ορίζουσας του πίνακα, θα έχουμε (στη συνέχεια συμβολίζουμε την ορίζουσα ενός πίνακα A και ως $|A| = \mathsf{Det}(A)$, για να μη δημιουργείται σύγχυση με το μέτρο του μιγαδικού αριθμού $\mathsf{Det}(A)$):

$$|A \cdot A^*| = |I_n| \quad \Longrightarrow \quad |A| \cdot |A^*| = 1 \quad \Longrightarrow \quad |A| \cdot \overline{|A|} = 1 \quad \Longrightarrow \quad |\mathsf{Det}(A)| = 1$$

δηλαδή το μέτρο της ορίζουσας ενός μοναδιαίου πίνακα είναι ίσο με 1. Με βάση αυτή την παρατήρηση, θεωρούμε το ακόλουθο υποσύνολο της διαγώνιας ομάδας $\mathsf{U}(n)$:

$$\mathsf{SU}(n) = \left\{ A \in \mathsf{U}(n) \mid |\mathsf{Det}(A)| = 1 \right\}$$

Τότε προφανώς $I_n \in \mathsf{SU}(n)$, και αν $A, B \in \mathsf{SU}(n)$, τότε θα έχουμε

$$|\mathsf{Det}(A \cdot B^{-1})| = |\mathsf{Det}(A)| \cdot |\mathsf{Det}(B^{-1})| = |\mathsf{Det}(A)| \cdot |\mathsf{Det}(B)^{-1}| = |\mathsf{Det}(A)| \cdot |\mathsf{Det}(B)|^{-1} = 1 \cdot 1^{-1} = 1 \quad \Longrightarrow \quad A \cdot B^{-1} \in \mathsf{SU}(n)$$

Επομένως από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο $\mathsf{SU}(n)$ των μοναδιαίων πινάκων των οποίων η ορίζουσα έχει μέτρο ίσο με 1, είναι υποομάδα της μοναδιαίας ομάδας $\mathsf{U}(n)$, η οποία καλείται η **ειδική n-οστή μοναδιαία ομάδα**. $\surd$

Παρατήρηση 2.4.16. Οι (υπο)ομάδες

$$\mathsf{GL}(n, \mathbb{R}), \quad \mathsf{GL}(n, \mathbb{C}), \quad \mathsf{SL}(n, \mathbb{R}), \quad \mathsf{SL}(n, \mathbb{C}), \quad \mathsf{O}(n), \quad \mathsf{SO}(n), \quad \mathsf{U}(n), \quad \mathsf{SU}(n)$$

αποτελούν μέρος μιας σημαντικής κλάσης ομάδων, των *κλασικών ομάδων πινάκων*. Οι ομάδες αυτές διαδραματίζουν σημαντικό ρόλο στα Μαθηματικά και στη Φυσική, και η θεωρία τους παρουσιάζει εξαιρετικό ενδιαφέρον. Εδώ θα παρουσιάσουμε κάποιες σχέσεις μεταξύ αυτών των ομάδων για μικρές τιμές του $n \in \mathbb{N}$.

[10] Ο ανάστροφος-συζυγής ενός πίνακα $A = (a_{ij})$ μιγαδικών αριθμών ορίζεται να είναι ο πίνακας $A^* = (\overline{a_{ji}})$, δηλαδή το στοιχείο στην (i, j) θέση του A^* είναι ο συζυγής $\overline{a_{ji}}$ του στοιχείου στην (j, i)-θέση του πίνακα A. Είναι γνωστό, και εύκολο να δειχθεί, ότι για τον ανάστροφο-συζυγή πινάκων μιγαδικών αριθμών ισχύουν οι εξής σχέσεις:

$$(A \cdot B)^* = B^* \cdot A^* \quad \text{και} \quad (A^*)^* = A \quad \text{και} \quad |A^*| = \overline{|A|}$$

1. Προφανώς: $\mathsf{GL}(1,\mathbb{R}) = \mathbb{R}^*$, και επομένως $\mathsf{SL}(1,\mathbb{R}) = \{1\}$. Παρόμοια $\mathsf{GL}(1,\mathbb{C}) = \mathbb{C}^*$, και επομένως $\mathsf{SL}(1,\mathbb{C}) = \{1\}$.

2. Προφανώς $\mathsf{O}(1) = \{x \in \mathbb{R} \mid x^2 = 1\} = \{1,-1\}$, και επομένως $\mathsf{SO}(1) = \{1\}$.

3. Θα έχουμε $\mathsf{U}(1) = \{z \in \mathbb{C} \mid z \cdot \overline{z} = 1\} = \{z \in \mathbb{C} \mid |z| = 1\}$, και προφανώς $\mathsf{SU}(1) = \{z \in \mathsf{U}(1) \mid z = 1\} = \{1\}$.

Αργότερα, έχοντας εισάγαγει την έννοια του ισομορφισμού ομάδων, θα δούμε και άλλες σχέσεις μεταξύ των παραπάνω ομάδων, για μικρές τιμές του $n \in \mathbb{N}$. Επιπρόσθετα θα αναλύσουμε κάποιες ενδιαφέρουσες γεωμετρικές ερμηνείες αυτών των ομάδων, όταν $n = 2,3$. ▲

Θα δούμε τώρα μια σειρά παραδειγμάτων υποομάδων τα οποία προκύπτουν με αφαρμογή της Πρότασης 2.4.8. Ιδιαίτερα στα επόμενα τρία παραδείγματα θα προσδιορίσουμε όλες τις υποομάδες μιας ομάδας με πλήθος στοιχείων το πολύ τέσσερα.

Παράδειγμα 2.4.17. Έστω $(G,\cdot)$ μια ομάδα με πλήθος στοιχείων $|G| \leq 3$.

1. Αν $|G| = 1$, τότε $G = \{e\}$ είναι η τετριμμένη ομάδα, και η μόνη υποομάδα της G είναι η ίδια η G.

2. Αν $|G| = 2$, τότε $G = \{e,a\}$, όπου $a^2 = e$, βλέπε το μέρος 2 στην υποενότητα 2.3. Επειδή προφανώς η μόνη υποομάδα της G με πλήθος στοιχείων ίσο με 2 είναι η ίδια η G, θα έχουμε ότι οι υποομάδες της G είναι οι $\{e\}$ και G.

3. Αν $|G| = 3$, τότε η G είναι της μορφής $G = \{e,a,a^2\}$, όπου $a^3 = e$, βλέπε το μέρος 3 στην υποενότητα 2.3. Αν H είναι μια υποομάδα της G με δύο στοιχεία, τότε το σύνολο H αναγκαστικά θα είναι ένα εκ των $\{e,a\}$, $\{e,a^2\}$. Επειδή $a^2 = a \cdot a \notin \{e,a\}$ και $a^2 \cdot a^2 = a^4 = a^3 \cdot a = e \cdot a = a \notin \{e,a^2\}$, τα σύνολα αυτά δεν είναι κλειστά στην πράξη της ομάδας και άρα δεν είναι υποομάδες. Έτσι δεν υπάρχει υποπομάδα της G με πλήθος στοιχείων ίσο με 2. Επειδή προφανώς η μόνη υποομάδα της G με πλήθος στοιχείων ίσο με 3 είναι η ίδια η G, θα έχουμε ότι οι υποομάδες της G είναι οι $\{e\}$ και G. √

Παράδειγμα 2.4.18. Έστω $(\mathcal{V}_4,\cdot)$ η ομάδα των τεσσάρων στοιχείων του Klein, όπου $\mathcal{V}_4 = \{e,a,b,c\}$, της οποίας ο πίνακας Cayley δίνεται από τον Πίνακα Α′ του μέρους 4 της υποενότητας 2.3. Ιδιαίτερα θα έχουμε ότι $a^2 = b^2 = c^2 = e$. Οι σχέσεις αυτές δείχνουν ότι τα υποσύνολα

$$H_1 = \{e,\ a\}, \qquad H_2 = \{e,\ b\}, \qquad H_3 = \{e,\ c\}$$

είναι κλειστά στην πράξη «$\cdot$» της $\mathcal{V}_4$, και επομένως, σύμφωνα με την Πρόταση 2.4.8, είναι υποομάδες της ομάδας $\mathcal{V}_4$. Θα δείξουμε ότι οι υποομάδες H_i, όπου $i = 1,2,3$, μαζί με την τετριμμένη υποομάδα $H_0 = \{e\}$, και την $\mathcal{V}_4$, είναι όλες οι διακεκριμένες υποομάδες της $\mathcal{V}_4$. Η μοναδική υποομάδα της $\mathcal{V}_4$ με ένα στοιχείο είναι προφανώς η τετριμμένη H_0. Αν K είναι μια υποομάδα της $\mathcal{V}_4$ με δύο στοιχεία, τότε η K θα περιέχει αναγκαστικά το ουδέτερο στοιχείο e της $\mathcal{V}_4$, και επίσης ένα εκ των υπόλοιπων στοιχείων a,b,c της $\mathcal{V}_4$. Έτσι αναγκαστικά η K θα είναι μια εκ των H_i, όπου $i = 1,2,3$. Αν K είναι μια υποομάδα της $\mathcal{V}_4$ με τρία στοιχεία, τότε η K θα περιέχει αναγκαστικά το ουδέτερο στοιχείο e της $\mathcal{V}_4$, και δύο εκ των υπόλοιπων στοιχείων a,b,c. Άρα η K θα είναι ένα εκ των εξής συνόλων: $K_1 = \{e,a,b\}$, $K_2 = \{e,a,c\}$, $K_3 = \{e,b,c\}$. Επειδή $a \cdot b = c \notin K_1$, $a \cdot c = b \notin K_2$, και $b \cdot c = a \notin K_3$, έπεται ότι κανένα από τα σύνολα K_i δεν είναι κλειστό στην πράξη της $\mathcal{V}_4$ και άρα δεν είναι υποομάδα της $\mathcal{V}_4$. Επομένως δεν υπάρχουν υποομάδες της $\mathcal{V}_4$ με τρία στοιχεία. Προφανώς η μόνη υποομάδα της ομάδας $\mathcal{V}_4$, με τέσσερα στοιχεία είναι η ίδια η $\mathcal{V}_4$. Συνοψίζοντας, δείξαμε ότι οι διακεκριμένες υποομάδες της ομάδας $\mathcal{V}_4$ του Klein είναι οι εξής:

$$\{e\}, \quad \{e,\ a\}, \quad \{e,\ b\}, \quad \{e,\ c\}, \quad \mathcal{V}_4 = \{e,\ a,\ b,\ c\} \quad \surd$$

Παράδειγμα 2.4.19. Έστω C_4 η κυκλική ομάδα τάξης 4, της οποίας ο πίνακας Cayley δίνεται από τον Πίνακα Β′ του μέρους 4 της υποενότητας 2.3. Τότε θα έχουμε $\mathsf{C}_4 = \{e,c,c^2,c^3\}$, όπου $c^4 = e \neq c^2$. Επειδή το υποσύνολο $H = \{e,c^2\} \subseteq \mathsf{C}_4$ είναι κλειστό στην πράξη «$\cdot$», έπεται ότι είναι υποομάδα της C_4. Αν K είναι μια υποομάδα της G με δύο στοιχεία, τότε το σύνολο K θα είναι ένα εκ των $\{e,c\}$, $\{e,c^2\}$, και $\{e,c^3\}$. Επειδή

$c^2 \neq \{e, c\}$ και επειδή $c^3 \cdot c^3 = c^6 = c^4 \cdot c^2 = e \cdot c^2 = c^2 \notin \{e, c^3\}$, έπεται ότι τα υποσύνολα $\{e, c\}$ και $\{e, c^3\}$ δεν είναι υποσύνολα της ομάδας C_4. Άρα η μόνη υποομάδα της C_4 με δύο στοιχεία είναι η H. Αν K είναι μια ομάδα με πλήθος στοιχείων ίσο με τρία, τότε το υποσύνολο K θα είναι ένα εκ των $\{e, c, c^2\}$, $\{e, c, c^3\}$, και $\{e, c^2, c^3\}$. Όπως παραπάνω, εύκολα βλέπουμε ότι κανένα από αυτά τα υποσύνολα δεν είναι κλειστό στην πράξη της C_4, και επομένως δεν υπάρχει υποομάδα της C_4 με πλήθος στοιχείων ίσο με 3. Προφανώς η μόνη υποομάδα της ομάδας C_4, με τέσσερα στοιχεία είναι η ίδια η C_4. Συνοψίζοντας, δείξαμε ότι οι διακεκριμένες υποομάδες της ομάδας C_4 είναι οι εξής:

$$\{e\}, \quad \{e,\ c^2\}, \quad \mathsf{C}_4 = \{e,\ c,\ c^2,\ c^3\} \quad \surd$$

Παράδειγμα 2.4.20. (Η ομάδα των τετρανίων (quaternions) του Hamilton[11]). Ένα χαρακτηριστικό παράδειγμα υποομάδας, η οποία, όπως θα δούμε αργότερα, έχει ενδιαφέρουσες ιδιότητες, είναι η ομάδα των τετρανίων (*quaternion group*) του Hamilton. Η ομάδα ορίζεται να είναι το ακόλουθο σύνολο οκτώ 2×2 πινάκων μιγαδικών αριθμών:

$$Q = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \ \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} \right\} \subseteq \mathsf{M}_2(\mathbb{C})$$

Επειδή όλοι οι πίνακες του συνόλου Q είναι αντιστρέψιμοι, έπεται ότι $Q \subseteq \mathsf{GL}(2, \mathbb{C})$, και επιπλέον το σύνολο Q περιέχει το ουδέτερο στοιχείο $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ της ομάδας $\mathsf{GL}(2, \mathbb{C})$. Θέτοντας:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

θα έχουμε ότι:

$$Q = \left\{ \pm I_2, \ \pm I, \ \pm J, \ \pm K \right\}$$

Υπολογίζουμε εύκολα ότι μεταξύ των πινάκων του συνόλου Q ισχύουν οι ακόλουθες σχέσεις:

$$I^2 = J^2 = K^2 = -I_2$$

$$I \cdot J = K \quad \text{και} \quad J \cdot I = -K$$

$$J \cdot K = I \quad \text{και} \quad K \cdot J = -I$$

$$K \cdot I = J \quad \text{και} \quad I \cdot K = -J$$

Με βάση τις παραπάνω σχέσεις, προκύπτει άμεσα ότι το σύνολο Q είναι κλειστό στην πράξη πολλαπλασιασμού πινάκων, και επομένως σύμφωνα με την Πρόταση 2.4.8 το σύνολο Q είναι μια υποομάδα της ομάδας $\mathsf{GL}(2, \mathbb{C})$ των αντιστρέψιμων 2×2 πινάκων με στοιχεία μιγαδικούς αριθμούς. Δηλαδή $Q \leq \mathsf{GL}_2(\mathbb{C})$. Επειδή, όπως βλέπουμε εύκολα, η ορίζουσα πίνακα κάθε στοιχείου της ομάδας Q είναι ίση με 1, έπεται ότι η ομάδα Q είναι υποομάδα της ειδικής γραμμικής ομάδας $\mathsf{SL}(2, \mathbb{C})$, και έτσι έχουμε τις ακόλουθες σχέσεις υπομάδων:

$$Q \ \leq \mathsf{SL}(2, \mathbb{C}) \ \leq \ \mathsf{GL}(2, \mathbb{C})$$

Η ομάδα $(Q, \cdot)$ καλείται η **ομάδα των τετρανίων του Hamilton**, και, όπως θα δούμε και αργότερα, έχει αξιοσημείωτες ιδιότητες. $\surd$

[11] William Rowan Hamilton (1805-1865) [https://en.wikipedia.org/wiki/William_Rowan_Hamilton]: Διακεκριμένος Ιρλανδός μαθηματικός και αστρονόμος με σημαντική συμβολή στην Κλασική Μηχανική, στην Άλγεβρα και στην Οπτική. Είναι γνωστός για την ανακάλυψη των τετρανίων που φέρουν το όνομά του, καθώς και για την επαναδιατύπωση της Νευτώνειας Μηχανικής, γνωστής ως Μηχανικής του Hamilton.

Παράδειγμα 2.4.21. Έστω Q η ομάδα των τετρανίων του Hamilton, όπως στο Παράδειγμα 2.4.20, και θεωρούμε τα ακόλουθα υποσύνολά της:

$$K = \{\pm I_2\}, \quad H_1 = \{\pm I_2, \pm I\}, \quad H_2 = \{\pm I_2, \pm J\}, \quad H_3 = \{\pm I_2, \pm K\}$$

Από την ανάλυση του Παραδείγματος 2.4.20, βλέπουμε εύκολα ότι καθένα από τα παραπάνω υποσύνολα της ομάδας Q είναι κλειστό στην πράξη «$\cdot$» της Q, και επομένως από την Πρόταση 2.4.8, τα υποσύνολα K, H_i, $i = 1,2,3$, είναι υποομάδες της Q. Επειδή οι υποομάδες H_i περιέχουν την υποομάδα K από την Παρατήρηση 2.4.7 έπεται ότι η K είναι υποομάδα της H_i, όπου $i = 1,2,3$. Έτσι θα έχουμε τις ακόλουθες σχέσεις υποομάδων της Q:

$$\forall i = 1,2,3: \qquad K \leq H_i \leq Q$$

Στο επόμενο Κεφάλαιο, θα δούμε ότι οι υποομάδες K, H_i, όπου $i = 1,2,3$, μαζί με την τετριμμένη υποομάδα $\{I_2\}$, και την Q, είναι όλες οι διακεκριμένες υποομάδες της Q. $\surd$

Παράδειγμα 2.4.22. Θεωρούμε τη συμμετρική ομάδα $(\mathsf{S}_3, \circ)$. Υπενθυμίζουμε ότι $\mathsf{S}_3 = \{\iota, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$, όπου:

$$\rho_0 = \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Θεωρούμε τα υποσύνολα

$$H_1 = \{\iota, \mu_1\}, \qquad H_2 = \{\iota, \mu_2\}, \qquad H_3 = \{\iota, \mu_3\}, \qquad H_4 = \{\iota, \rho_1, \rho_2\}$$

Λαμβάνοντας υπόψη τον πίνακα Cayley της S_3 ο οποίος κατασκευάστηκε στο Παράδειγμα 2.3.5, βλέπουμε ότι τα παραπάνω υποσύνολα είναι κλειστά στην πράξη της ομάδας S_3, και επομένως, σύμφωνα με την Πρόταση 2.4.8, τα σύνολα H_i, όπου $1 \leq i \leq 4$, είναι υποομάδες της S_3. Στο επόμενο Κεφάλαιο, θα δούμε ότι οι υποομάδες H_i, όπου $1 \leq i \leq 4$, μαζί με την τετριμμένη υποομάδα $\{\iota\}$, και την S_3, είναι όλες οι διακεκριμένες υποομάδες της S_3. $\surd$

Κλείνουμε την παρούσα ενότητα, με τα ακόλουθα παραδείγματα υποομάδων, κάποια εκ των οποίων συνοψίζουν προγενέστερα παραδείγματα, και στην πλειονότητα των υπολοίπων η επαλήθευση των αξιωμάτων υποομάδας είναι πολύ εύκολη.

Παράδειγμα 2.4.23. (Παραδείγματα υποομάδων).

1. Θεωρούμε την προσθετική ομάδα $(\mathbb{C}, +)$. Τότε έχουμε την ακολουθία υποομάδων:

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

2. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{C}^*, \cdot)$. Τότε έχουμε την ακολουθία υποομάδων:

$$\{-1, 1\} \leq \mathbb{Q}^* \leq \mathbb{R}^* \leq \mathbb{C}^*$$

3. Αν $n \geq 1$, θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{C}, \cdot)$. Τότε έχουμε την ακολουθία υποομάδων:

$$\mathsf{U}_n \leq \mathsf{T} \leq \mathbb{C}^*$$

4. Θεωρούμε την προσθετική ομάδα $(\mathsf{M}_{n\times n}(\mathbb{K}), +)$. Αν $\mathsf{AT}_n(\mathbb{K})$ είναι το σύνολο των άνω τριγωνικών $n \times n$-πινάκων υπεράνω του $\mathbb{K}$, και $\mathsf{D}_n(\mathbb{K})$ είναι το σύνολο των διαγωνίων $n \times n$-πινάκων υπεράνω του $\mathbb{K}$, τότε έχουμε την ακολουθία υποομάδων:

$$\mathsf{D}_n(\mathbb{K}) \leq \mathsf{AT}_n(\mathbb{K}) \leq \mathsf{M}_{n\times n}(\mathbb{K})$$

5. Θεωρούμε τη γενική γραμμική ομάδα $(\mathsf{GL}(n,\mathbb{R}),\cdot)$ υπεράνω του $\mathbb{R}$, και την γενική γραμμική ομάδα $(\mathsf{GL}(n,\mathbb{C}),\cdot)$ υπεράνω του $\mathbb{C}$. Τότε έχουμε τις ακόλουθες σειρές υποομάδων:

$$\mathsf{SL}_n(\mathbb{R}) \leq \mathsf{GL}_n(\mathbb{R}) \qquad \text{και} \qquad \mathsf{SL}_n(\mathbb{C}) \leq \mathsf{GL}_n(\mathbb{C})$$

$$\mathsf{SO}(n,\mathbb{R}) \leq \mathsf{O}(n,\mathbb{R}) \leq \mathsf{GL}_n(\mathbb{R}) \qquad \text{και} \qquad \mathsf{SU}(n,\mathbb{C}) \leq \mathsf{U}(n,\mathbb{C}) \leq \mathsf{GL}_n(\mathbb{C})$$

6. Έστω $(\mathcal{V},+)$ η προσθετική ομάδα ενός $\mathbb{K}$-διανυσματικού χώρου $\mathcal{V}$ υπεράνω ενός σώματος $\mathbb{K} \in \{\mathbb{Q},\mathbb{R},\mathbb{C}\}$. Τότε για κάθε υπόχωρο $\mathcal{W}$ του $\mathcal{V}$, έχουμε ότι $\mathcal{W} \leq \mathcal{V}$.

   Ιδιαίτερα, θεωρώντας το σύνολο $\mathbb{K}[t]$ των πολυωνύμων υπεράνω του $\mathbb{K}$ ως το υποσύνολο της προσθετικής ομάδας $(\mathsf{A}(\mathbb{K}),+)$ των ακολουθιών με στοιχεία από το $\mathbb{K}$ το οποίο αποτελείται από τις ακολουθίες όλοι οι όροι των οποίων είναι ίσοι με μηδέν μετά από κάποιον δείκτη, έπεται ότι θα έχουμε $\mathbb{K}[t] \leq \mathsf{A}(\mathbb{K})$.

7. Έστω $I = (a,b) \subseteq \mathbb{R}$ ένα διάστημα της πραγματικής ευθείας, και θεωρούμε την προσθετική ομάδα $\mathscr{F}(I,\mathbb{R})$ των συναρτήσεων $f\colon I \longrightarrow \mathbb{R}$. Αν $\mathscr{C}(I,\mathbb{R})$ είναι το υποσύνολο του $\mathscr{F}(I,\mathbb{R})$ το οποίο αποτελείται από όλες τις συνεχείς συναρτήσεις $f\colon I \longrightarrow \mathbb{R}$, τότε, επειδή κάθε σταθερή συνάρτηση είναι συνεχής, επειδή το άθροισμα συνεχών συναρτήσεων είναι συνεχής συνάρτηση, και επειδή η αντίθετη $-f$ μιας συνεχούς συνάρτησης f είναι συνεχής συνάρτηση, από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο $\mathscr{C}(I,\mathbb{R})$ είναι υποομάδα της ομάδας $\mathscr{F}(I,\mathbb{R})$:

$$\mathscr{C}(I,\mathbb{R}) \leq \mathscr{F}(I,\mathbb{R})$$

8. Θεωρούμε την ομάδα $(\mathsf{U}(\mathscr{A}),\star)$ των ενελικτικά αντιστρέψιμων αριθμητικών συναρτήσεων με πράξη το ενελικτικό γινόμενο «$\star$», όπως στο μέρος 6 του Παραδείγματος 2.2.10. Υπενθυμίζουμε ότι μια αριθμητική συνάρτηση f καλείται *πολλαπλασιαστική*, αν $f \neq 0$ και ισχύει ότι $f(mn) = f(m)f(n)$, όταν $(n,m) = 1$. Έστω $\mathscr{M}$ το υποσύνολο του συνόλου $\mathscr{A}$ των αριθμητικών συναρτήσεων το οποίο αποτελείται από όλες τις πολλαπλασιαστικές αριθμητικές συναρτήσεις. Επειδή για μια πολλαπλασιαστική συνάρτηση f προφανώς ισχύει ότι $f(1) = 1 \neq 0$, έπεται ότι $\mathscr{M} \subseteq \mathsf{U}(\mathscr{A})$. Αποδεικνύεται στην στοιχειώδη Θεωρία Αριθμών[12] ότι το ενελικτικό γινόμενο δύο πολλαπλασιαστικών συναρτήσεων f και g είναι πολλαπλασιαστική συνάρτηση, δηλαδή $f,g \in \mathscr{M} \implies f \star g \in \mathscr{M}$. Έτσι το υποσύνολο $\mathscr{M}$ είναι κλειστό στην πραξη «$\star$» της ομάδας $\mathsf{U}(\mathscr{A})$, και επομένως από την Πρόταση 2.4.8 το υποσύνολο $\mathscr{M}$ είναι μια υποομάδα της $\mathsf{U}(\mathscr{A})$:

$$\mathscr{M} \leq \mathsf{U}(\mathscr{A})$$

9. Έστω $\mathcal{V}$ ένας $\mathbb{K}$-διανυσματικός χώρος υπεράνω του $\mathbb{K} \in \{\mathbb{Q},\mathbb{R},\mathbb{C}\}$. Έστω

$$\mathsf{GL}(\mathcal{V}) = \{f\colon \mathcal{V} \longrightarrow \mathcal{V} \mid f\colon \text{ισομορφισμός}\}$$

   το σύνολο όλων των ισομορφισμών $\mathbb{K}$-διανυσματικών χώρων, δηλαδή των «1-1» και «επί» γραμμικών απεικονίσεων, από τον $\mathcal{V}$ στον $\mathcal{V}$. Επειδή κάθε ισομορφισμός $f\colon \mathcal{V} \longrightarrow \mathcal{V}$ είναι μια μετάθεση του συνόλου $\mathcal{V}$, έπεται ότι $\mathsf{GL}(\mathcal{V}) \subseteq \mathsf{S}(\mathcal{V})$. Το υποσύνολο $\mathsf{GL}(\mathcal{V}) \neq \emptyset$, διότι προφανώς $\mathsf{Id}_{\mathcal{V}} \in \mathsf{GL}(\mathcal{V})$. Από την άλλη πλευρά, επειδή η σύνθεση «1-1» και «επί» γραμμικών απεικονίσεων $f,g\colon \mathcal{V} \longrightarrow \mathcal{V}$ είναι επίσης «1-1» και «επί» γραμμική απεικόνιση, έπεται ότι το υποσύνολο $\mathsf{GL}(\mathcal{V})$ είναι κλειστό στην πράξη «$\circ$», δηλαδή της σύνθεσης απεικονίσεων, της ομάδας μεταθέσεων $\mathsf{S}(\mathcal{V})$. Τέλος, επειδή η αντίστροφη απεικόνιση μιας «1-1» και «επί» γραμμικής απεικονίσης είναι επίσης γραμμική και «1-1» και «επί», από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο $\mathsf{GL}(\mathcal{V})$ είναι υποομάδα της ομάδας μεταθέσεων $\mathsf{S}(\mathcal{V})$:

$$\mathsf{GL}(\mathcal{V}) \leq \mathsf{S}(\mathcal{V})$$

   Η ομάδα $\mathsf{GL}(\mathcal{V})$ αποτελεί το ανάλογο της ομάδας $\mathsf{GL}(n,\mathbb{K})$ σε χώρους άπειρης διάστασης. Όταν $\dim_{\mathbb{K}} \mathcal{V} = n$, τότε οι ομάδες $\mathsf{GL}(\mathcal{V})$ και $\mathsf{GL}(n,\mathbb{K})$ είναι ισόμορφες, δηλαδή είναι δομικά ίδιες. $\surd$

[12] Βλέπε το βιβλίο [28].

2.4.3 Το Διάγραμμα Hasse των Υποομάδων μιας Ομάδας

Έστω ότι $(G,\cdot)$ είναι μια ομάδα. Θεωρούμε το σύνολο $\mathsf{Sub}(G)$ των υποομάδων της ομάδας $(G,\cdot)$:

$$\mathsf{Sub}(G) = \{H \subseteq G \mid H : \text{ υποομάδα της } G\}$$

Υπενθυμίζουμε ότι, αν H είναι μια υποομάδα της G, τότε γράφουμε $H \leq G$, και αν H και K είναι υποομάδες της G έτσι ώστε $K \subseteq H$, τότε $K \leq H$, δηλαδή η υποομάδα K είναι υποομάδα της H. Επίσης γράφουμε $K \lneqq H$ αν $K \leq H$ και $H \neq K$. Έτσι ορίζεται μια σχέση «$\leq$» επί του συνόλου $\mathsf{Sub}(G)$ των υποομάδων της ομάδας G.

Λήμμα 2.4.24. *Το ζεύγος* $(\mathsf{Sub}(G), \leq)$ *είναι ένα μερικώς διατεταγμένο σύνολο.*

Απόδειξη. Προφανώς $H \leq H$, για κάθε υποομάδα H της G. Αν H και K είναι υποομάδες της G, έτσι ώστε $H \leq K$ και $K \leq H$, τότε προφανώς $H = K$. Τέλος, αν H, K και L είναι υποομάδες της G, έτσι ώστε $H \leq K$ και $K \leq L$, τότε $H \leq L$. Επομένως η σχέση «$\leq$» είναι μια σχέση μερικής διάταξης επί του συνόλου $\mathsf{Sub}(G)$. ■

Υπενθυμίζουμε από την υποενότητα 1.1.2 ότι, αν $(X, \preccurlyeq)$ είναι ένα μερικώς διατεταγμένο σύνολο, τότε το **διάγραμμα Hasse** του $(X, \preccurlyeq)$ έχει ως κορυφές σημεία τα οποία είναι σε «1-1» και «επί» αντιστοιχία με τα στοιχεία του συνόλου X. Δύο κορυφές του διαγράμματος, οι οποίες αναπαριστούν τα στοιχεία x, y του X, ενώνονται με μια ακμή, αν το y είναι κάλυψη του x, δηλαδή $x \prec y$ και δεν υπάρχει στοιχείο $z \in X$ έτσι ώστε $x \prec z \prec y$, και τότε τοποθετούμε την κορυφή y υπεράνω της κορυφής x. Υπενθυμίζουμε επίσης ότι $x \prec y$ σημαίνει ότι $x \preccurlyeq y$ και $x \neq y$.

Ορισμός 2.4.25. *Αν* $(G,\cdot)$ *είναι μια ομάδα, τότε το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου* $(\mathsf{Sub}(G), \leq)$ *καλείται το* **διάγραμμα Hasse των υποομάδων της** G.

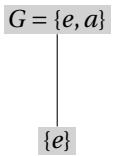
Επομένως το διάγραμμα Hasse των υποομάδων της G έχει ως κορυφές σημεία τα οποία είναι σε «1-1» και «επί» αντιστοιχία με τις διακεκριμένες υποομάδες της G. Χάριν απλότητας, από τώρα και στο εξής, ταυτίζουμε τις κορυφές του διαγράμματος με τις υποομάδες της G. Δύο κορυφές του διαγράμματος οι οποίες αναπαριστούν υποομάδες H, K της G ενώνονται με μια ακμή

αν $K \lneqq H$ και δεν υπάρχει υποομάδα L της G με $K \lneqq L \lneqq H$, και τότε τοποθετούμε την υποομάδα H υπεράνω της υποομάδας K.

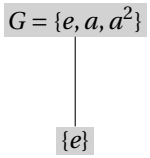
Παράδειγμα 2.4.26. (Το Διάγραμμα Hasse των υποομάδων μιας ομάδας G με $|G| \leq 4$.). Θεωρούμε μια ομάδα $(G,\cdot)$ με ουδέτερο στοιχείο e, και πλήθος στοιχείων ≤ 4.

1. Αν $|G| = 1$, τότε η ομάδα G είναι η τετριμμένη ομάδα $G = \{e\}$ και η μόνη υποομάδα της G είναι η ίδια η ομάδα G. Επομένως το διάγραμμα Hasse των υποομάδων της G αποτελείται από μια κορυφή, η οποία αντιστοιχεί στην G, και δεν υπάρχει καμία ακμή.

2. Αν $|G| = 2$, τότε η ομάδα G θα είναι της μορφής $G = \{e, a\}$. Προφανώς οι μόνες υποομάδες της G είναι η τετριμμένη υποομάδα $\{e\}$ και η ίδια η ομάδα G. Έτσι το διάγραμμα Hasse των υποομάδων της G αποτελείται από δύο κορυφές, οι οποίες αντιστοιχούν στις υποομάδες $\{e\}$ και G, και μια ακμή η οποία τις συνδέει:

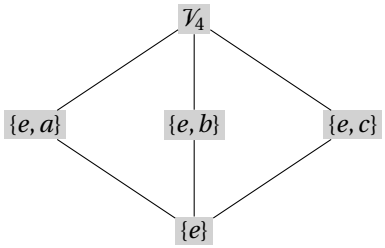


3. Αν $|G| = 3$, τότε η ομάδα G είναι της μορφής $G = \{e, a, a^2\}$, βλέπε το Παράδειγμα 2.4.17, από όπου έπεται ότι οι μόνες υποομάδες της G είναι οι $\{e\}$ και G, Άρα το διάγραμμα Hasse των υποομάδων της ομάδας G είναι το εξής:

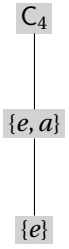


4. Αν $|G| = 4$, τότε από την υποενότητα 4 γνωρίζουμε ότι υπάρχουν ακριβώς δύο ομάδες με πλήθος στοιχείων ίσο με 4: η ομάδα $\mathcal{V}_4$ των τεσσάρων στοιχείων του Klein, και η κυκλική ομάδα τάξης 4. Η ομάδα του Klein είναι αβελιανή και είναι της μορφής $\mathcal{V}_4 = \{e, a, b, c\}$, όπου $a^2 = b^2 = c^2 = e$. Η κυκλική ομάδα τάξης 4 είναι αβελιανή και είναι της μορφής $G = \{e, c, c^2, c^3\}$, όπου $c^4 = e$.

   (α') Για το διάγραμμα Hasse των υποομάδων της ομάδας του Klein: από το Παράδειγμα 2.4.18 γνωρίζουμε ότι οι υποομάδες της $\mathcal{V}_4$ είναι οι εξής: $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, και $\mathcal{V}_4$. Επειδή για τις υποομάδες με δύο στοιχεία δεν υφίσταται σχέση υποομαδας μεταξύ τους, προφανώς θα έχουμε ότι το διάγραμμα Hasse των υποομάδων της ομάδας του Klein είναι το εξής:



   (β') Για το διάγραμμα Hasse των υποομάδων της κυκλικής ομάδας τάξης 4: από το Παράδειγμα 2.4.19 γνωρίζουμε ότι οι υποομάδες της C_4 είναι οι εξής: $\{e\}$, $\{e, c^2\}$, και C_4. Προφανώς τότε το το διάγραμμα Hasse των υποομάδων της κυκλικής ομάδας τάξης 4 είναι το εξής:



Παρατηρούμε ότι το διάγραμμα Hasse μιας ομάδας με δύο στοιχεία και μιας ομάδας με τρία στοιχεία συμπίπτει. Επομένως, αν και το διάγραμμα Hasse καταγράφει σημαντικές δομικές ιδιότητες μιας ομάδας, δεν καθορίζει μοναδικά την ομάδα. √

Θα δούμε αργότερα παραδείγματα διαγραμμάτων Hasse υποομάδων μιας ομάδας, όταν θα έχουμε αναπτύξει αποτελεσματικότερες μεθόδους για τον προσδιορισμό όλων των υποομάδων μιας ομάδας, καθώς και των σχέσεων μεταξύ αυτών.

2.4.4 Τομή Υποομάδων και Υποομάδες Παραγόμενες από Υποσύνολα - Κυκλικές Υποομάδες

Υπάρχουν διάφοροι τρόποι μέσω των οποίων μπορούμε να αποκτήσουμε νέα παραδείγματα (υπο)ομάδων από ήδη γνωστές (υπο)ομάδες. Στην παρούσα υποενότητα θα αναλύσουμε τις πλέον βασικές μεθόδους κατασκευής υποομάδων.

Υπεθυμίζουμε ότι μια υποομάδα μιας ομάδας είναι ένα (μη κενό) υποσύνολο το οποίο ικανοποιεί επιπρόσθετες ιδιότητες. Έτσι τίθεται φυσιολογικά το ερώτημα αν βασικές συνολοθεωρητικές κατασκευές, όπως η τομή και η ένωση, μεταφέρονται και στο πλαίσιο των υποομάδων. Στην ανάλυση αυτού του ερωτήματος σημείο εκκίνησης αποτελεί η επόμενη Πρόταση, σύμφωνα με την οποία η τομή τυχούσας οικογένειας υποομάδων μιας ομάδων είναι υποομάδα.

Πρόταση 2.4.27. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα, και $\mathscr{H} = \{H_i \mid H_i \leq G\}_{i\in I}$ μια οικογένεια υποομάδων της G. Τότε η τομή*

$$H = \bigcap \mathscr{H} = \bigcap_{i\in I} H_i$$

είναι μια υποομάδα της G.

Απόδειξη. Επειδή, για κάθε $i \in I$, το υποσύνολο H_i είναι υποομάδα της G, έπεται ότι περιέχει το ουδέτερο στοιχείο e της ομάδας G, και άρα $e \in H_i$, $\forall i \in I$. Τότε $e \in H = \bigcap_{i\in I} H_i$. Ιδιαίτερα βλέπουμε ότι: $H \neq \emptyset$. Θεωρούμε τυχόντα στοιχεία $a, b \in H$. Τότε προφανώς θα έχουμε ότι $a, b \in H_i$, $\forall i \in I$. Επειδή $H_i \leq G$, $\forall i \in I$, από την Πρόταση 2.4.5 έπεται ότι $a \cdot b^{-1} \in H_i$, $\forall i \in I$, και επομένως $a \cdot b^{-1} \in H = \bigcap_{i\in I} H_i$. Άρα πάλι με εφαρμογή της Πρότασης 2.4.5, έπεται ότι η τομή $H = \bigcap_{i\in I} H_i$ είναι υποομάδα της G. ■

Το ακόλουθο παράδειγμα δείχνει ότι, αντίθετα με την τομή υποομάδων, η ένωση υποομάδων μιας ομάδας, δεν είναι γενικά υποοομάδα.

Παράδειγμα 2.4.28. (Παράδειγμα ομάδας G και υποομάδων $H, K \leq G$ έτσι ώστε: $H \cup K \nleq G$).

1. Έστω $\mathcal{V}_4 = \{e, a, b, c\}$ η ομάδα των τεσσάρων στοιχείων του Klein. Από το Παράδειγμα 2.4.18 γνωρίζουμε ότι οι υποομάδες της $\mathcal{V}_4$ είναι οι εξής: $\{e\}$, $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, και $\mathcal{V}_4$. Αν $H_1 = \{e, a\}$ και $H_2 = \{e, b\}$, τότε η ένωση $H_1 \cup H_2 = \{e, a, b\}$ δεν είναι υποομάδα της $\mathcal{V}_4$ διότι, αν και $a, b \in H_1 \cup H_2$, το στοιχείο $a \cdot b = c \notin H_1 \cup H_2$.

2. Θεωρούμε την προσθετική ομάδα $(\mathbb{R}^2, +)$, όπου η πράξη της πρόσθεσης «+» ορίζεται ως εξής: $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$. Θέτοντας $H_1 = \{(x, 0) \in \mathbb{R}^2 \mid x \in \mathbb{R}\}$ και $H_2 = \{(0, y) \in \mathbb{R}^2 \mid y \in \mathbb{R}\}$, εύκολα βλέπουμε ότι τα υποσύνολα H_1 και H_2 είναι υποομάδες της $\mathbb{R}^2$. Η ένωση $H_1 \cup H_2$ αποτελείται από τα στοιχεία του $\mathbb{R}^2$ τα οποία βρίσκονται είτε στον άξονα των x, δηλαδή στην υποομάδα H_1, είτε στον άξονα των y, δηλαδή στην υποομάδα H_2. Επειδή $(1, 0) \in H_1$ και $(0, 1) \in H_2$, θα έχουμε $(1, 0), (0, 1) \in H_1 \cup H_2$, και επομένως, αν η ένωση $H_1 \cup H_2$ ήταν υποομάδα, θα έπρεπε $(1, 1) = (1, 0) + (0, 1) \in H_1 \cup H_2$ το οποίο από την παραπάνω περιγραφή δεν ισχύει. Άρα η ένωση $H_1 \cup H_2$ δεν είναι υποομάδα της $\mathbb{R}^2$. √

Επειδή, σύμφωνα με το Παράδειγμα 2.4.28, γενικά η ένωση υποομάδων μιας ομάδας δεν είναι υποομάδα, τίθεται φυσιολογικά το ερώτημα: «*Ποια είναι η μικρότερη υποομάδα της ομάδας η οποία περιέχει την ένωση δύο υποομάδων*»; Γενικότερα τίθεται φυσιολογικά το ακόλουθο ενδιαφέρον ερώτημα:

«αν $(G,\cdot)$ είναι μια ομάδα, και $S \subseteq G$ είναι ένα υποσύνολο της G, ποια είναι, αν υπάρχει, η μικρότερη υποομάδα της G η οποία περιέχει το υποσύνολο S;»

Θα ξεκινήσουμε την ανάλυση του γενικότερου ερωτήματος, εξετάζοντας πρώτα την περίπτωση κατά την οποία το υποσύνολο S αποτελείται από ένα στοιχείο.

Πρόταση 2.4.29. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και $a \in G$ ένα στοιχείο της. Το υποσύνολο*

$$\langle a \rangle := \{a^n \in G \mid n \in \mathbb{Z}\}$$

είναι μια υποομάδα της G. Επιπλέον ισχύει ότι

$$\langle a \rangle = \langle a^{-1} \rangle$$

και η $\langle a \rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει το στοιχείο a:

$$\langle a \rangle = \bigcap_{a\in H\leq G} H$$

Απόδειξη. Παρατηρούμε ότι το υποσύνολο $\langle a\rangle$ της G δεν είναι το κενό σύνολο διότι π.χ. $e = a^0 \in \langle a\rangle \ni a^1 = a$. Έστω $x, y \in \langle a\rangle$ δύο στοιχεία του υποσυνόλου $\langle a\rangle$. Τότε υπάρχουν ακέραιοι $n, m \in \mathbb{Z}$ έτσι ώστε $x = a^n$ και $y = a^m$, και θα έχουμε:

$$x \cdot y^{-1} = a^n \cdot (a^m)^{-1} = a^n \cdot a^{-m} = a^{n-m} \in \langle a\rangle$$

Επομένως από την Πρόταση 2.4.5 θα έχουμε ότι το υποσύνολο $\langle a\rangle$ είναι μια υποομάδα της G.

Προφανώς θα έχουμε:

$$\langle a\rangle = \{a^n \in G \mid n \in \mathbb{Z}\} = \{a^{-n} \in G \mid n \in \mathbb{Z}\} = \{(a^{-1})^n \in G \mid n \in \mathbb{Z}\} = \langle a^{-1}\rangle$$

Η υποομάδα $\langle a\rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει το στοιχείο a, διότι, αν H είναι μια υποομάδα της G η οποία περιέχει το στοιχείο a, τότε η H ως υποομάδα θα περιέχει το στοιχείο a^{-1}, καθώς και όλες τις ακέραιες δυνάμεις του a, δηλαδή θα περιέχει τα στοιχεία της υποομάδας $\langle a\rangle$ και άρα: $\langle a\rangle \subseteq H$. Έτσι, αν $\mathscr{H}(a)$ είναι η οικογένεια των υποομάδων της G οι οποίες περιέχουν το στοιχείο a, τότε $\langle a\rangle \subseteq H$, $\forall H \in \mathscr{H}(a)$, και επομένως θα έχουμε $\langle a\rangle \subseteq \bigcap_{H\in\mathscr{H}(a)} H$. Από την άλλη πλευρά, επειδή η υποομάδα $\langle a\rangle$ είναι μια από τις υποομάδες της οικογένειας $\mathscr{H}(a)$, θα έχουμε ότι $\bigcap_{H\in\mathscr{H}(a)} H \subseteq \langle a\rangle$. Επομένως καταλήγουμε ότι: $\bigcap_{H\in\mathscr{H}(a)} H = \langle a\rangle$. ■

Υποομάδες της μορφής $\langle a\rangle \leq G$, όπου $a \in G$, είναι σημαντικές διότι, όπως προκύπτει από την Πρόταση 2.4.29, η περιγραφή των στοιχείων τους, καθώς και η δομή τους, είναι πολύ απλή. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι ομάδες G για τις οποίες ισχύει ότι $G = \langle a\rangle$, για κάποιο στοιχείο $a \in G$. Έτσι προκύπτει φυσιολογικά, η έννοια της κυκλικής (υπο)ομάδας.

Ορισμός 2.4.30. *Έστω $(G,\cdot)$ μια ομάδα και $a \in G$ ένα στοιχείο της. Η υποομάδα $\langle a\rangle$ της G καλείται* **η κυκλική υποομάδα της** G **η οποία παράγεται από το στοιχείο** a.

Η ομάδα G καλείται ***κυκλική ομάδα****, αν υπάρχει στοιχείο $a \in G$ έτσι ώστε: $G = \langle a\rangle$. Κάθε στοιχείο a μιας ομάδας G έτσι ώστε: $G = \langle a\rangle$ καλείται* **γεννήτορας** *της κυκλικής ομάδας G.*

Παρατήρηση 2.4.31. Χρησιμοποιώντας προσθετικό συμβολισμό, η Πρόταση 2.4.29 και ο Ορισμός 2.4.30 παίρνουν την ακόλουθη μορφή. Έστω $(G,+)$ μια προσθετική ομάδα και $a \in G$. Τότε η *κυκλική υποομάδα $\langle a\rangle$ της G η οποία παράγεται από το a* ορίζεται ως:

$$\langle a\rangle = \{na \in G \mid n \in \mathbb{Z}\}$$

και είναι η μικρότερη υποομάδα της G η οποία περιέχει το στοιχείο a. ▲

Η γενική θεωρία κυκλικών ομάδων, καθώς και η ταξινόμισή τους, θα αναπτυχθεί στο Κεφάλαιο 4. Προς το παρόν παραθέτουμε βασικά παραδείγματα κυκλικών ομάδων για μεταγενέστερη χρήση.

Παράδειγμα 2.4.32. (Παραδείγματα κυκλικών (υπο)ομάδων).

1. Αν $(G,\cdot)$ είναι μια ομάδα με τάξη $|G| \leq 3$, τότε η G είναι κυκλική:

   – Αν $|G| = 1$, τότε προφανώς $G = \{e\} = \langle e\rangle$ και η G είναι κυκλική με γεννήτορα το ουδέτερο στοιχείο e.

   – Αν $|G| = 2$, τότε, όπως γνωρίζουμε, $G = \{e, a\}$, όπου $a^2 = e$. Τότε προφανώς $G = \langle a\rangle$ και η G είναι κυκλική με γεννήτορα το στοιχείο a.

   – Αν $|G| = 3$, τότε, όπως γνωρίζουμε, $G = \{e, a, b\}$, όπου $b = a^2$ και $a^3 = e$. Τότε προφανώς θα έχουμε ότι $G = \langle a\rangle$ και η G είναι κυκλική με γεννήτορα το στοιχείο a.

2. Η ομάδα των τεσσάρων στοιχείων $V_4 = \{e, a, b, c\}$ του Klein *δεν είναι κυκλική*, διότι: $a^2 = b^2 = c^2 = e$, και άρα κανένα στοιχείο της V_4 δεν μπορεί να είναι γεννήτοράς της.

3. Θεωρούμε την προσθετική ομάδα $(\mathbb{Z},+)$ των ακεραίων. Τότε:

   $$\langle 1\rangle = \{n \cdot 1 \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

   Επομένως η ομάδα $\mathbb{Z}$ είναι κυκλική με γεννήτορα τον αριθμό 1. Επειδή $\langle -1\rangle = \{n \cdot (-1) \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \{-n \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \mathbb{Z}$, συμπεραίνουμε ότι και ο αριθμός -1 είναι γεννήτορας της $\mathbb{Z}$.

4. Θεωρούμε την προσθετική ομάδα $(\mathbb{Z}_n, +)$ των κλάσεων υπολοίπων mod n, όπου n είναι ένας θετικός ακέραιος. Αν k είναι ένας θετικός ακέραιος, τότε από την Ευκλείδεια Διαίρεση του k με το n θα έχουμε: $k = nq + r$, όπου $q, r \in \mathbb{Z}$ και $0 \leq r_k < n$. Τότε $k[1]_n = [k]_n = [nq_k + r_k]_n = [nq_k]_n + [r_k]_n = [r]_n$, και άρα για $k = 1, 2, \cdots, n-1$, έχουμε $\{k[1]_n \in \mathbb{Z}_n \mid 0 \leq k < n\} = \mathbb{Z}_n$. Επομένως

$$\langle [1]_n \rangle = \{[k]_n \in \mathbb{Z}_n \mid k \in \mathbb{Z}\} = \{k[1]_n \in \mathbb{Z}_n \mid 0 \leq k < n\} = \mathbb{Z}_n$$

Επομένως η ομάδα $\mathbb{Z}_n$ είναι κυκλική με γεννήτορα την κλάση ισοτιμίας $[1]_n$.

5. Έστω $\mathsf{U}_n = \{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}\}$ η πολλαπλασιαστική ομάδα των n-οστών ριζών της μονάδας, όπου $\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$, όπως στο Παράδειγμα 2.4.12. Επειδή $(e^{\frac{2\pi i}{n}})^k = [\cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})]^k = \cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) = e^{\frac{2k\pi i}{n}}$, από την περιγραφή της ομάδας U_n στο Παράδειγμα 2.4.12, έπεται ότι:

$$\mathsf{U}_n = \{\zeta_n^k \in \mathsf{U}_n \mid k \in \mathbb{Z}\} = \langle \zeta_n \rangle$$

Άρα η ομάδα U_n είναι κυκλική με γεννήτορα την n-οστή ρίζα της μονάδας $\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$.

Εξ ορισμού μια **πρωταρχική n-οστή ρίζα της μονάδας** είναι ένας γεννήτορας της κυκλικής ομάδας U_n. Έτσι το στοιχείο ζ_n είναι μια πρωταρχική n-οστή ρίζα της μονάδας. Θα προσδιορίσουμε αργότερα όλες τις πρωταρχικές n-οστές ρίζες της μονάδας.

6. Θεωρούμε την ομάδα $(\mathsf{GL}(2, \mathbb{Q}), \cdot)$ των αντιστρέψιμων 2×2 πινάκων ρητών αριθμών, και θεωρούμε τον πίνακα $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ο οποίος είναι αντιστρέψιμος με αντίστροφο τον πίνακα $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, και επομένως $A \in \mathsf{GL}(2, \mathbb{Q})$. Επειδή, όπως μπορούμε να δουμε εύκολα: $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, $\forall n \in \mathbb{Z}$, έπεται ότι η κυκλική υποομάδα $\langle A \rangle$ της $\mathsf{GL}(n, \mathbb{Q})$ η οποία παράγεται από τον πίνακα A είναι η εξής:

$$\langle A \rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathsf{GL}(2, \mathbb{Q}) \mid n \in \mathbb{Z} \right\}$$

7. Θεωρούμε την ομάδα $(\mathsf{GL}(\mathbb{R}^n), \circ)$ των ισομορφισμών του διανυσματικού χώρου $\mathbb{R}^n$, δηλαδή των «1-1» και «επί» γραμμικών απεικονίσεων : $\mathbb{R}^n \longrightarrow \mathbb{R}^n$ με πράξη την σύνθεση «$\circ$» απεικονίσεων, όπως στο μέρος 9 του Παραδείγματος 2.4.23. Θεωρούμε την γραμμική απεικόνιση

$$f : \mathbb{R}^n \longrightarrow \mathbb{R}^n, \quad f(x_1, x_2, \cdots, x_{n-1}, x_n) = (x_2, x_3, \cdots, x_{n-1}, x_1)$$

Τότε εύκολα βλέπουμε ότι η f είναι ισομορφισμός και άρα $f \in \mathsf{GL}(\mathbb{R}^n)$. Η κυκλική υποομάδα της $\mathsf{GL}(\mathbb{R}^n)$ η οποία παράγεται από την f έχει n το πλήθος στοιχεία, διότι εύκολα βλέπουμε ότι $f^n = f \circ f \circ \cdots \circ f = \mathsf{Id}_{\mathbb{R}^n}$ (n-παράγοντες). Άρα

$$\langle f \rangle = \{\mathsf{Id}_{\mathbb{R}^n}, f, f^2, f^3, \cdots, f^{n-1}\} \quad \surd$$

Επιστρέφοντας στην αρχική ερώτηση 2.4.4 αναφορικά με την ύπαρξη και περιγραφή υποομάδας η οποία παράγεται από ένα υποσύνολο, είμαστε έτοιμοι να αποδείξουμε την ακόλουθη Πρόταση.

Πρόταση 2.4.33. *Έστω $(G, \cdot)$ μια ομάδα, και $S \subseteq G$ ένα τυχόν μη κενό υποσύνολο της G. Τότε η τομή*

$$\langle S \rangle = \bigcap_{H \in \mathscr{H}(S)} H = \bigcap_{S \subseteq H \leq G} H$$

της οικογένειας $\mathscr{H}(S) = \{H \leq G \mid S \subseteq H\}$ όλων των υποομάδων της G οι οποίες περιέχουν το σύνολο S είναι η μικρότερη υποομάδα της G η οποία περιέχει το S, και έχει την ακόλουθη περιγραφή:

$$\langle S \rangle = \left\{ s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} \in G \mid k \in \mathbb{N},\ n_i \in \mathbb{Z},\ \textit{και}\ s_i \in S,\ \textit{όπου}\ 1 \leq i \leq k \right\}$$

Απόδειξη. Παρατηρούμε ότι η οικογένεια υποομάδων $\mathscr{H}(S)$ δεν είναι κενή διότι προφανώς $G \in \mathscr{H}(S)$. Σύμφωνα με την Πρόταση 2.4.27, το υποσύνολο $\langle S\rangle$ είναι υποομάδα της G ως τομή υποομάδων της G, και προφανώς $S \subseteq \langle S\rangle$. Έστω $K \in \mathscr{H}(S)$ μια υποομάδα της G η οποία περιέχει το S, δηλαδή $S \subseteq K \leq G$. Τότε προφανώς $\bigcap_{S\subseteq H\leq G} H \subseteq K$ και άρα $\langle S\rangle \subseteq K$, δηλαδή η υποομάδα $\langle S\rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει το S.

Θέτουμε

$$K = \left\{s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} \in G \mid n_i \in \mathbb{Z} \text{ και } s_i \in S \ \ 1 \leq i \leq k\right\}$$

Έστω $x \in K$. Τότε το x είναι ένα στοιχείο της G της μορφής $x = s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k}$, όπου $n_i \in \mathbb{Z}$, και $s_i \in S$, $1 \leq i \leq k$. Επειδή τα στοιχεία s_i ανήκουν στο S, έπεται ότι τα στοιχεία $s_1, s_2, \cdots, s_k$ ανήκουν στο $\langle S\rangle$, και επειδή το σύνολο αυτό είναι υποομάδα της G, έπεται ότι το στοιχείο $x = s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k}$ ανήκει στο $\langle S\rangle$, δηλαδή $K \subseteq \langle S\rangle$. Αντίστροφα, αν $x \in \langle S\rangle$, τότε το x ανήκει σε κάθε υποομάδα της G η οποία περιέχει το S. Επομένως, για να δείξουμε ότι το x ανήκει στο υποσύνολο K, αρκεί να δείξουμε ότι το K είναι υποομάδα της G η οποία περιέχει το S.

Πράγματι, έστω $s \in S$. Τότε $e = s^0 \in K$. Αν $x, y \in K$, τότε $x = s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k}$ και $y = t_1^{m_1} t_2^{m_2} \cdots s_l^{m_l}$, όπου $s_i, t_j \in S$, $n_i, m_j \in \mathbb{Z}$, $1 \leq i \leq k$, $1 \leq j \leq l$. Θα έχουμε $x \cdot y = s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} t_1^{m_1} t_2^{m_2} \cdots s_l^{m_l} \in K$. Τέλος $x^{-1} = (s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k})^{-1} = s_k^{-n_k} \cdots s_2^{-n_2} s_1^{-n_1} \in K$. Άρα, σύμφωνα με την Πρόταση 2.4.5, το υποσύνολο K είναι μια υποομάδα της G η οποία περιέχει το S διότι $\forall s \in S$: $s = s^1 \in K$. Επομένως, σύμφωνα με την παραπάνω ανάλυση, θα έχουμε ότι, επειδή το x ανήκει σε κάθε υποομάδα της G η οποία περιέχει το S και το υποσύνολο K είναι μια υποομάδα της G η οποία περιέχει το S, θα έχουμε $x \in K$ και άρα $\langle S\rangle \subseteq K$. Επομένως $\langle S\rangle = K$. ■

Μπορούμε να αποκτήσουμε μια απλούστερη περιγραφή της υποομάδας $\langle S\rangle$ η οποία παράγεται από ένα μη κενό υποσύνολο $S \subseteq G$, ως εξής. Για ένα υποσύνολο $S \subseteq G$, συμβολίζουμε με S^{-1} το σύνολο

$$S^{-1} = \left\{s^{-1} \in G \mid s \in S\right\}$$

Πόρισμα 2.4.34. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα, και $S \subseteq G$ είναι ένα μη-κενό υποσύνολο της G. Τότε:*

$$\langle S\rangle = \left\{x_1 \cdot x_2 \cdots x_n \in G \mid x_k \in S \cup S^{-1},\ 1 \leq k \leq n,\ n \in \mathbb{N}_0\right\} = \left\{s_1^{\pm 1} \cdot s_2^{\pm 1} \cdots s_n^{\pm 1} \in G \mid s_k \in S,\ 1 \leq k \leq n,\ n \in \mathbb{N}_0\right\}$$

Απόδειξη. Από την Πρόταση 2.4.33, έπεται άμεσα ότι το σύνολο $H = \left\{x_1 \cdot x_2 \cdots x_n \in G \mid x_k \in S \cup S^{-1},\ 1 \leq k \leq n,\ n \in \mathbb{N}_0\right\}$ περιέχεται στην $\langle S\rangle$, έτσι $H \subseteq \langle S\rangle$. Αντίστροφα, γνωρίζουμε ότι κάθε στοιχείο $x \in \langle S\rangle$ είναι της μορφής $x = s_1^{n_1} s_2^{n_2} \cdots s_m^{n_m}$, όπου $s_k \in S$ και $n_k \in \mathbb{Z}$, $1 \leq k \leq m$. Θεωρούμε το στοιχείο $s_k^{n_k}$. Αν $n_k > 0$, τότε $s_k^{n_k} = s_k \cdot s_k \cdots s_k$ (n_k-παράγοντες), και αν $n_k < 0$, τότε $s_k^{n_k} = s_k^{-1} \cdot s_k^{-1} \cdots s_k^{-1}$ ($-n_k$-παράγοντες). Έτσι σε κάθε περίπτωση το στοιχείο $s_k^{n_k}$, $1 \leq k \leq n$, ανήκει στο υποσύνολο H, και και άρα θα γράφεται στην μορφή $s_k^{n_k} = x_{k1}^{\pm 1} \cdot x_{k2}^{\pm 1} \cdots x_{kr_k}^{\pm 1}$, $1 \leq k \leq m$, και επομένως το ίδιο συμβαίνει και για το στοιχείο $x = s_1^{n_1} s_2^{n_2} \cdots s_k^{n_k} = (x_{11}^{\pm 1} \cdot x_{12}^{\pm 1} \cdots x_{1r_1}^{\pm 1}) \cdots (x_{m1}^{\pm 1} \cdot x_{m2}^{\pm 1} \cdots x_{mr_m}^{\pm 1})$. Άρα $x \in H$ και επομένως $\langle S\rangle \subseteq H$. Συνοψίζοντας, δείξαμε ότι $\langle S\rangle = H$. ■

Ορισμός 2.4.35. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα, και $S \subseteq G$ είναι ένα τυχόν μη-κενό υποσύνολο της G.*

1. *Η υποομάδα $\langle S\rangle$ της Πρότασης 2.4.33 καλείται* **η υποομάδα της G η οποία παράγεται από το υποσύνολο** S.
2. *Το υποσύνολο $S \subseteq G$ καλείται* **σύνολο γεννητόρων** *της G, και τα στοιχεία $s \in S$ καλούνται* **γεννήτορες της** G, *αν $G = \langle S\rangle$.*
3. *Η ομάδα $(G,\cdot)$ καλείται* **πεπερασμένα παραγόμενη**, *αν η G έχει ένα πεπερασμένο σύνολο γεννητόρων, δηλαδή υπάρχει ένα πεπερασμένο υποσύνολο $S \subseteq G$, έτσι ώστε: $G = \langle S\rangle$.*

Επομένως, αν $H, K \leq G$ είναι υποομάδες μιας ομάδας $(G,\cdot)$, τότε η μικρότερη δυνατή υποομάδα της G η οποία περιέχει την ένωση $H \cup K$ είναι η υποομάδα $\langle H \cup K\rangle$ η οποία παράγεται από την ένωση των συνόλων H και K. Γενικότερα, από το Πόρισμα 2.4.34 προκύπτει το ακόλουθο:

Πόρισμα 2.4.36. *Έστω $\{H_i\}_{i\in I}$ μια οικογένεια υποομάδων μιας ομάδας $(G,\cdot)$. Τότε η ομάδα $\langle \bigcup_{i\in I} H_i\rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει κάθε υποομάδα H_i, $i\in I$, και έχει την ακόλουθη περιγραφή:*

$$\left\langle \bigcup_{i\in I} H_i \right\rangle = \left\{ x_{i_1}\cdot x_{i_2}\cdots x_{i_n} \in G \mid x_{i_k}\in H_{i_k},\ \text{όπου}\ i_k\in I,\ \ 1\le k\le n,\ n\in\mathbb{N}_0 \right\}$$

Παρατήρηση 2.4.37. Όπως είδαμε, η υποομάδα της G η οποία παράγεται από το υποσύνολο S έχει την ακόλουθη περιγραφή:

$$\langle S\rangle = \left\{ s_1^{n_1}s_2^{n_2}\cdots s_k^{n_k} \in G \mid n_i\in\mathbb{Z} \ \text{ και } \ s_i\in S,\ \ 1\le i\le k,\ \ k\ge 1 \right\}$$

Αν η ομάδα G είναι προσθετική, τότε:

$$\langle S\rangle = \left\{ n_1s_1+n_2s_2+\cdots+n_ks_k \in G \mid n_i\in\mathbb{Z} \ \text{ και } \ s_i\in S,\ \ 1\le i\le k,\ \ k\ge 1 \right\}$$

Παράδειγμα 2.4.38.

1. Κάθε ομάδα $(G,\cdot)$ έχει τουλάχιστον ένα σύνολο γεννητόρων, το σύνολο G: $\langle G\rangle = G$. Πράγματι κάθε στοιχείο $a\in G$ είναι της μορφής $a=a^1\in\langle G\rangle$.
2. Κάθε πεπερασμένη ομάδα $(G,\cdot)$ είναι πεπερασμένα παραγόμενη, διότι μπορούμε να επιλέξουμε ως σύνολο γεννητόρων το σύνολο G, το οποίο στην περίπτωσή μας είναι πεπερασμένο.
3. Κάθε κυκλική ομάδα είναι πεπερασμένα παραγόμενη, διότι έχει ένα σύνολο γεννητόρων το οποίο αποτελείται από ένα στοιχείο (τον γεννήτορά της).
4. Υπάρχουν άπειρες ομάδες οι οποίες είναι πεπερασμένα παραγόμενες. Για παράδειγμα, η προσθετική ομάδα $(\mathbb{Z},+)$ είναι άπειρη, και είναι πεπερασμένα παραγόμενη ως κυκλική: $\mathbb{Z}=\langle 1\rangle$.

Παράδειγμα 2.4.39. Θεωρούμε την ομάδα $Q=\{\pm I_2,\pm I,\pm J,\pm K\}\le \mathsf{GL}(2,\mathbb{C})$ των τετρανίων του Hamilton. Έστω $S=\{I,J\}$, $T=\{J,K\}$, $R=\{K,I\}$. Τότε εύκολα βλέπουμε, με χρήση της ανάλυσης του Παραδείγματος 2.4.20, ότι: $\langle S\rangle = Q$. Για παράδειγμα, αν $S=\{I,J\}$, τότε $I, I^2=-I_2, I^3=-I=I^{-1}, I^4=I, J, J^2=-I_2, J^3=-J=J^{-1}, J^4=I\in\langle S\rangle$ και παρόμοια $I\cdot J=K, I^{-1}\cdot J=-I\cdot J=-K\in\langle S\rangle$. Έτσι βλέπουμε ότι $Q\subseteq\langle S\rangle$, και άρα $Q=\langle S\rangle$. Επομένως τα σύνολα $S=\{I,J\}$, $T=\{J,K\}$, $R=\{K,I\}$ είναι σύνολα γεννητόρων της Q.

Έστω

$$T=\left\{\begin{pmatrix}\zeta_{2n} & 0\\ 0 & \overline{\zeta}_{2n}\end{pmatrix},\ \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}\subseteq \mathsf{SL}_2(\mathbb{C})$$

όπου $n\ge 1$, και ζ_{2n} είναι μια πρωταρχική $2n$-οστή ρίζα της μονάδας, π.χ. μπορούμε να πάρουμε $\zeta_{2n}=e^{\frac{\pi i}{n}}$.

Η υποομάδα

$$Q_n=\langle T\rangle=\left\{\begin{pmatrix}\zeta_{2n} & 0\\ 0 & \overline{\zeta}_{2n}\end{pmatrix},\ \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\}$$

της $\mathsf{SL}_2(\mathbb{C})$ η οποία παράγεται από το σύνολο T καλείται η ***n*-οστή γενικευμένη ομάδα των τετρανίων του Hamilton**, και έχει την ιδιότητα ότι είναι μια μη αβελιανή ομάδα τάξης $4n$, όπου $n>1$, και κάθε αβελιανή υποομάδα της είναι κυκλική, βλέπε την Άσκηση 2.10.30. Για $n=2$, εύκολα βλέπουμε ότι $Q_2=Q$ η ομάδα των τετρανίων του Hamilton. Αν $n=1$, τότε, επειδή $\zeta_2=-1$, εύκολα βλέπουμε ότι η ομάδα Q_1 είναι κυκλική τάξης 4 και:

$$Q_1=\left\langle\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\right\rangle \quad \surd$$

Παρατήρηση 2.4.40. Γενικά μια ομάδα έχει πολλά σύνολα γεννητόρων. Συνήθως, όταν η ομάδα G είναι πεπερασμένα παραγόμενη, τότε, για προφανείς λόγους, ενδιαφερόμαστε για **ελάχιστα σύνολα γεννητόρων**, δηλαδή συνόλων γεννητόρων S της G με την ιδιότητα ότι κάθε γνήσιο υποσύνολο $T\subseteq S$ παράγει μια γνήσια υποομάδα της G: $\langle T\rangle\lneq G$. Φυσικά η ύπαρξη και μοναδικότητα για ελάχιστα σύνολα γεννητόρων δεν εξασφαλίζεται, με την έννοια ότι μια ομάδα μπορεί να μην διαθέτει ελάχιστο σύνολο γεννητόρων, και επίσης

μπορεί να διαθέτει πολλά διαφορετικά ελάχιστα σύνολα γεννητόρων. Σημειώνουμε ότι πεπερασμένα σύνολα γεννητόρων με τον μικρότερο δυνατό πλήθος στοιχείων είναι ελάχιστα σύνολα γεννητόρων, αλλά το αντίστροφο δεν ισχύει. Στο επόμενο παράδειγμα θα δούμε δύο ελάχιστα σύνολα γεννητόρων της συμμετρικής ομάδας S_3. ▲

Παράδειγμα 2.4.41. Θεωρούμε τη συμμετρική ομάδα $\mathsf{S}_3 = \{\iota,\ \mu_1,\ \mu_2,\ \mu_3,\ \rho_1,\ \rho_2\}$, όπου:

$$\rho_0 = \iota = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\quad \mu_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\quad \mu_2 = \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \mu_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\rho_1 = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \rho_2 = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

Τότε:

$$\mathsf{S}_3 = \langle \mu_2, \mu_3\rangle = \langle \mu_1, \rho_1\rangle$$

Πράγματι, χρησιμοποιώντας τον πίνακα Cayley της S_3, όπως στο Παράδειγμα 2.3.5, θα έχουμε:

$$\mu_2^2 = \mu_1\cdot\mu_2 = \iota,\quad \mu_2\cdot\mu_3 = \rho_1,\quad \mu_3\cdot\mu_2 = \rho_2,\quad \mu_2\cdot\mu_3\cdot\mu_2 = \mu_2\cdot\rho_2 = \mu_1 \quad\Longrightarrow\quad \mathsf{S}_3 = \langle \mu_2, \mu_3\rangle$$

$$\mu_1^2 = \mu_1\cdot\mu_1 = \iota,\quad \rho_1^2 = \rho_1\cdot\rho_1 = \rho_2,\quad \mu_1\cdot\rho_1 = \mu_2,\quad \rho_1\mu_1 = \mu_3 \quad\Longrightarrow\quad \mathsf{S}_3 = \langle \mu_1, \rho_1\rangle$$

Από την άλλη πλευρά, η ομάδα S_3 δεν είναι κυκλική. Πράγματι, όπως προκύπτει από τον πίνακα Cayley της S_3, κανένα στοιχείο της δεν μπορεί να είναι γεννήτοράς της, διότι $\mu_1^2 = \mu_2^2 = \mu_3^2 = \rho_1^3 = \rho_2^3 = \iota$. Έτσι δεν υπάρχει σύνολο γεννητόρων της S_3 με ένα στοιχείο, και επομένως τα σύνολα $\{\mu_2, \mu_3\}$ και $\{\mu_1, \rho_1\}$ είναι ελάχιστα σύνολα γεννητόρων. √

Παράδειγμα 2.4.42. Έστω $\mathbb{K}$ ένα εκ των συνόλων $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$. Συμβολίζουμε με E_{ij} τον πίνακα ο οποίος έχει στην (i,j)-θέση την μονάδα και παντού αλλού μηδέν, $1 \le i, j, \le n$. Ένας τετραγωνικός πίνακας E με στοιχεία από το σύνολο $\mathbb{K}$ καλείται **στοιχειώδης πίνακας**, αν είναι της μορφής

$$E = I_n + aE_{ij},\ \text{για κάποιο } a \in \mathbb{K},\ \text{όπου } 1 \le i \ne j \le n.$$

Συμβολίζουμε με $\mathscr{E}(n)$ το σύνολο όλων των στοιχειωδών $n\times n$ πινάκων με στοιχεία από το $\mathbb{K}$, και έστω $\mathscr{D}(n)$ το σύνολο όλων των διαγωνίων $n\times n$ πινάκων με μη μηδενικά διαγώνια στοιχεία. Αποδεικνύεται στην Γραμμική Άλγεβρα ότι κάθε στοιχειώδης πίνακας είναι αντιστρέψιμος, και επιπλέον ένας τετραγωνικός πίνακας A είναι αντιστρέψιμος αν και μόνο αν είναι γινόμενο πεπερασμένου πλήθους στοιχειωδών πινάκων και διαγώνιων αντιστρέψιμων πινάκων. Επομένως θα έχουμε ότι:

$$\mathsf{GL}(n,\mathbb{K}) = \langle \mathscr{E}(n) \cup \mathscr{D}(n)\rangle$$

Παρόμοια για την ειδική γραμμική ομάδα $\mathsf{SL}(n,\mathbb{K}) \le \mathsf{GL}(n,\mathbb{K})$, θα έχουμε:

$$\mathsf{SL}(n,\mathbb{K}) = \langle \mathscr{E}(n)\rangle \quad √$$

Έστω $(G,\cdot)$ μια ομάδα. Τότε το σύνολο $\mathsf{Sub}(G) = \{H \subseteq G \mid H \le G\}$ όλων των υποομάδων της G είναι ένα μερικώς διατεταγμένο σύνολο όταν εφοδιαστεί με την σχέση έγκλεισης «$\subseteq$» ή ισοδύναμα με την σχέση υποομάδας «$\le$». Παρατηρούμε ότι το μερικώς διατεταγμένο σύνολο $(\mathsf{Sub}(G), \subseteq)$ έχει ελάχιστο στοιχείο, την τετριμμένη υποομάδα $\{e\}$, και μέγιστο στοιχείο, την υποομάδα G. Επιπλέον η παρακάτω Πρόταση δείχνει ότι το μερικώς διατεταγμένο σύνολο $(\mathsf{Sub}(G), \le)$ είναι πλήρης σύνδεσμος, με την έννοια του Ορισμού 1.1.4.

Πόρισμα 2.4.43. *Έστω $(G,\cdot)$ μια ομάδα. Τότε το μερικώς διατεταγμένο σύνολο $(\mathsf{Sub}(G), \le)$ των υποομάδων της G είναι ένας πλήρης σύνδεσμος με ελάχιστο στοιχείο την τετριμμένη υποομάδα $\{e\}$ και μέγιστο στοιχείο την ομάδα G. Για κάθε μη κενό υποσύνολο $\mathscr{H} \subseteq \mathsf{Sub}(G)$ υποομάδων της G, έχουμε ότι:*

$$\bigvee \mathscr{H} = \langle \mathscr{H}\rangle \quad \text{και} \quad \bigwedge \mathscr{H} = \bigcap_{H\in\mathscr{H}} H$$

Απόδειξη. Η υποομάδα $\langle \mathscr{H} \rangle$ η οποία παράγεται από το σύνολο $\bigcup_{H \in \mathscr{H}} H$ υποομάδων είναι μια υποομάδα της G η οποία περιέχει κάθε υποομάδα $H \in \mathscr{H}$ και είναι η μικρότερη υποομάδα με αυτή την ιδιότητα. Επομένως η υποομάδα $\langle \mathscr{H} \rangle$ είναι το ελάχιστο άνω φράγμα του συνόλου υποομάδων $\mathscr{H}$, δηλαδή $\bigvee \mathscr{H} = \langle \mathscr{H} \rangle$. Από την άλλη πλευρά, η τομή $\bigcap_{H \in \mathscr{H}} H$ όλων των υποομάδων $H \in \mathscr{H}$ είναι προφανώς η μεγαλύτερη υποομάδα της G η οποία περιέχεται σε κάθε υποομάδα $H \in \mathscr{H}$. Επομένως, η υποομάδα $\bigcap_{H \in \mathscr{H}} H$ είναι το μέγιστο κάτω φράγμα του συνόλου υποομάδων $\mathscr{H}$, δηλαδή $\bigwedge \mathscr{H} = \bigcap_{H \in \mathscr{H}} H$. ■

2.5 Χαρακτηριστικές Υποομάδες μιας Ομάδας

Κάθε ομάδα διαθέτει κάποιες χαρακτηριστικές υποομάδες, η δομή των οποίων μας επιτρέπει να εξάγουμε σημαντικές πληροφορίες για την ομάδα. Στην παρούσα υποενότητα θα δούμε κάποιες από αυτές τις χαρακτηριστικές υποομάδες.

2.5.1 Κεντροποιητής, Κανονικοποιητής, και Κέντρο - Συζυγείς Υποομάδες

Από τώρα και στο εξής, σταθεροποιούμε μια (πολλαπλασιαστική) ομάδα $(G, \cdot)$, και ένα τυχόν μη κενό υποσύνολο $S \subseteq G$.

Λήμμα 2.5.1. *Το υποσύνολο*

$$\mathsf{C}_G(S) = \{x \in G \mid x \cdot s = s \cdot x,\ \forall s \in S\}$$

είναι μια υποομάδα της G.

Απόδειξη. Θα έχουμε $e \cdot s = s = s \cdot e$, $\forall s \in S$, και άρα $e \in \mathsf{C}_G(S)$. Ιδιαίτερα $\mathsf{C}_G(S) \neq \emptyset$. Έστω $x, y \in \mathsf{C}_G(S)$, και άρα θα έχουμε $x \cdot s = s \cdot x$ και $y \cdot s = s \cdot y$, $\forall s \in S$. Από την τελευταία σχέση έπεται ότι, για κάθε $s \in S$, θα έχουμε: $y^{-1} \cdot y \cdot s = y^{-1} \cdot s \cdot y$ και άρα $s = y^{-1} \cdot s \cdot y$. Τότε $s \cdot y^{-1} = y^{-1} \cdot s \cdot y \cdot y^{-1} = y^{-1} \cdot s$, και θα έχουμε, $\forall s \in S$:

$$(x \cdot y^{-1}) \cdot s = x \cdot (y^{-1} \cdot s) = x \cdot (s \cdot y^{-1}) = (x \cdot s) \cdot y^{-1} = (s \cdot x) \cdot y^{-1} = s \cdot (x \cdot y^{-1}) \quad \Longrightarrow \quad x \cdot y^{-1} \in \mathsf{C}_G(S)$$

Επομένως από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο $\mathsf{C}_G(S)$ είναι μια υποομάδα της G. ■

Άμεση συνέπεια του Λήμματος 2.5.1 είναι το ακόλουθο Πόρισμα.

Πόρισμα 2.5.2. *Αν $(G, \cdot)$ είναι μια ομάδα, τότε το υποσύνολο*

$$\mathsf{Z}(G) = \{x \in G \mid x \cdot a = a \cdot x\}$$

είναι μια αβελιανή υποομάδα της G. Επιπρόσθετα η ομάδα G είναι αβελιανή αν και μόνο αν $G = \mathsf{Z}(G)$.

Απόδειξη. Παρατηρούμε ότι:

$$\mathsf{Z}(G) = \mathsf{C}_G(G)$$

και άρα, από το Λήμμα 2.5.1, το υποσύνολο το υποσύνολο $\mathsf{Z}(G)$ είναι μια υποομάδα της G. Προφανώς, αν $x, y \in \mathsf{Z}(G)$, τότε $x \cdot y = y \cdot x$, και επομένως η ομάδα $\mathsf{Z}(G)$ είναι αβελιανή. Έτσι, αν $G = \mathsf{Z}(G)$, τότε η ομάδα G είναι αβελιανή. Αντίστροφα, αν η G είναι αβελιανή και $x \in G$, τότε για κάθε στοιχείο $a \in G$ έχουμε: $x \cdot a = a \cdot x$, και επομένως $x \in \mathsf{Z}(G)$. Δηλαδή $G = \mathsf{Z}(G)$. ■

Αν το υποσύνολο $S \subseteq G$ είναι μονοσύνολο: $S = \{s\}$, τότε για την υποομάδα $\mathsf{C}_G(S)$ θα γράφουμε $\mathsf{C}_G(s)$. Παρατηρούμε τότε ότι γενικά θα έχουμε:

$$\mathsf{C}_G(S) = \bigcap_{s \in S} \mathsf{C}_G(s) \tag{2.13}$$

και αν S, T είναι υποσύνολα της G, τότε:

$$S \subseteq T \quad \Longrightarrow \quad \mathsf{C}_G(T) \leq \mathsf{C}_G(S) \qquad \text{και ιδιαίτερα} \qquad \forall S \subseteq G\colon \ \mathsf{Z}(G) \leq \mathsf{C}_G(S) \tag{2.14}$$

Ορισμός 2.5.3. *Αν $(G,\cdot)$ είναι μια ομάδα, και $S\subseteq G$, τότε η υποομάδα $\mathsf{C}_G(S)$ καλείται ο* **κεντροποιητής** *του συνόλου S στην ομάδα G.*

Η υποομάδα $\mathsf{Z}(G)$ καλείται το **κέντρο** *της ομάδας G.*

Με βάση τους παραπάνω ορισμούς, ο κεντροποιητής $\mathsf{C}_G(S)$ ενός υποσυνόλου $S\subseteq G$ δίνει ένα μέτρο του πόσο απέχει το υποσύνολο S από το να περιέχεται στο κέντρο της ομάδας G, και το κέντρο $\mathsf{Z}(G)$ της ομάδας G δίνει ένα μέτρο του πόσο απέχει η ομάδα G από το να είναι αβελιανή.

Παράδειγμα 2.5.4. Θεωρούμε τη συμμετρική ομάδα S_3 και την μετάθεση $\mu_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$. Από τον πίνακα Cayley της S_3 βλέπουμε άμεσα ότι $\mathsf{C}_{\mathsf{S}_3}(\mu_3)=\{\iota,\mu_3\}$. Παρόμοια από τον πίνακα Cayley της S_3, έπεται ότι για την μετάθεση $\rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, θα έχουμε: $\mathsf{C}_{\mathsf{S}_3}(\rho_1)=\{\iota,\rho_1,\rho_2\}$, βλέπε το Παράδειγμα 2.3.5.

Έστω $S=\{\mu_3,\rho_1\}$. Τότε από την σχέση (2.13), θα έχουμε

$$\mathsf{C}_{\mathsf{S}_3}(S)=\mathsf{C}_{\mathsf{S}_3}(\{\mu_3,\rho_1\})=\mathsf{C}_{\mathsf{S}_3}(\mu_3)\bigcap\mathsf{C}_{\mathsf{S}_3}(\rho_1)=\{\iota,\mu_3\}\bigcap\{\iota,\rho_1,\rho_2\}=\{\iota\}$$

Επομένως, με χρήση της σχέσης (2.14), επειδή $S=\{\mu_3,\rho_1\}\subseteq\mathsf{S}_3$, θα έχουμε ότι $\mathsf{Z}(\mathsf{S}_3)\subseteq\mathsf{C}_{\mathsf{S}_3}(S)=\{\iota\}$. Άρα το κέντρο της συμμετρικής ομάδας S_3 είναι η τετριμμένη υποομάδα:

$$\mathsf{Z}(\mathsf{S}_3)=\{\iota\}$$

Αργότερα θα δούμε ότι το κέντρο κάθε συμμετρικής ομάδας είναι η τετριμμένη υποομάδα. $\surd$

Στη συνέχεια είναι αναγκαίο να εισαγάγουμε συμβολισμό ο οποίος αφορά την επέκταση της πράξης «$\cdot$» μεταξύ στοιχείων της ομάδας G σε πράξη μεταξύ τυχαίων υποσυνόλων της G.

Συμβολισμός 2.5.5. (Πράξεις μεταξύ Υποσυνόλων). Έστω $(G,\cdot)$ μια ομάδα, και S,T δύο μη κενά υποσύνολα της G. Τότε θα συμβολίζουμε:

$$S\cdot T=\{s\cdot t\in G\mid s\in S\text{ και }t\in T\}$$

Ιδιαίτερα, αν $S=\{s\}$ ή $T=\{t\}$, θα γράφουμε:

$$sT=\{s\}\cdot T=\{s\cdot t\in G\mid t\in T\}\qquad\text{ή αντίστοιχα}\qquad S\cdot t=S\cdot\{t\}=\{s\cdot t\in G\mid s\in S\}$$

Επίσης θα συμβολίζουμε:

$$S^{-1}=\{s^{-1}\in G\mid s\in S\}$$

Έτσι, για παράδειγμα, αν x,y είναι στοιχεία της G, τότε:

$$xSy^{-1}=\{x\cdot s\cdot y^{-1}\in G\mid s\in S\}$$

Γενικότερα, αν $S_1,\ S_2,\ \cdots,\ S_n$ είναι μη κενά υποσύνολα της ομάδας G, τότε:

$$S_1\cdot S_2\cdots S_n=\{s_1\cdot s_2\cdots s_n\in G\mid s_i\in S_i,\ 1\le i\le n\}$$

Αν για την πράξη της ομάδας G χρησιμοποιούμε προσθετικό συμβολισμό «+», τότε οι παραπάνω συμβολισμοί παίρνουν την ακόλουθη μορφή, όπου $T,S_1,\cdots,S_n\subseteq G$, και $s\in G$:

$$s+T=\{s+t\in G\mid t\in G\},\quad T+s=\{t+s\in G\mid t\in G\},\quad -T=\{-t\in G\mid t\in T\}$$

$$S_1+S_2+\cdots+S_n=\{s_1+s_2+\cdots+s_n\in G\mid s_i\in S_i,\ 1\le i\le n\}\quad\blacktriangle$$

Με βάση τους παραπάνω συμβολισμούς, έχουμε την πρακάτω βοηθητική Πρόταση η οποία περιγράφει βασικές ιδιότητες της πράξεων

$$\cdot:\ \mathscr{P}(G)^*\times\mathscr{P}(G)^*\longrightarrow\mathscr{P}(G)^*,\quad(S,T)\longmapsto S\cdot T\qquad\qquad\cdot:\ \mathscr{P}(G)^*\longrightarrow\mathscr{P}(G)^*,\quad S\longmapsto S^{-1}$$

όπως ορίστηκαν παραπάνω, όπου $\mathscr{P}(G)^*=\mathscr{P}(G)\setminus\{\emptyset\}$ είναι το σύνολο όλων των μη κενών υποσυνόλων της ομάδας G.

Λήμμα 2.5.6. *Έστω S, T, R μη κενά υποσύνολα μιας ομάδας $(G.\cdot)$. Τότε ισχύουν οι ακόλουθες σχέσεις:*

$$S\cdot(T\cdot R) = (S\cdot T)\cdot R, \qquad (S\cdot T)^{-1} = T^{-1}\cdot S^{-1}, \qquad S\cdot\{e\} = S = \{e\}\cdot S$$

Απόδειξη. Θα έχουμε:

$$S\cdot(T\cdot R) = \{s\cdot(t\cdot r)\in G \mid s\in S,\ t\in T,\ r\in R\} = \{(s\cdot t)\cdot r\in G \mid s\in S,\ t\in T,\ r\in R\} = (S\cdot T)\cdot R$$

Επίσης

$$(S\cdot T)^{-1} = \{(s\cdot t)^{-1}\in G \mid s\in S,\ t\in T\} = \{t^{-1}\cdot s^{-1}\in G \mid s\in S,\ t\in T\} = T^{-1}\cdot S^{-1}$$

Τέλος

$$S\cdot\{e\} = \{s\cdot e\in G\ s\in S\} = \{s\in G \mid s\in G\} = S = \{s\in G \mid s\in G\} = \{e\cdot s\in G\ s\in S\} = \{e\}\cdot S$$ ■

Παρατήρηση 2.5.7. Έστω $S, T\subseteq G$ δύο μη-κενά υποσύνολα μιας ομάδας $(G,\cdot)$.

1. Για κάθε στοιχείο $z\in G$, έχουμε:

$$S = z^{-1}Tz \iff zSz^{-1} = T$$

Πράγματι, θα έχουμε: $zSz^{-1} = T \Longrightarrow z^{-1}zSz^{-1} = z^{-1}T \Longrightarrow Sz^{-1} = eSz^{-1} = z^{-1}T \Longrightarrow Sz^{-1}\cdot z = z^{-1}Tz$ $\Longrightarrow S = Se = z^{-1}Tz$. Παρόμοια βλέπουμε ότι $S = z^{-1}Tz \Longrightarrow zSz^{-1} = T$. Άρα $S = z^{-1}Tz \Longleftrightarrow zSz^{-1} = T$.

2. Ισχύουν οι εξής σχέσεις:

$$\exists x\in G\colon\ xSx^{-1} = T \iff \exists x\in G\colon\ x^{-1}Tx = S \iff \exists x\in G\colon\ x^{-1}Sx = T \iff \exists x\in G\colon\ xTx^{-1} = S$$

Από το μέρος 1., θα έχουμε ότι ισχύει η πρώτη και η τρίτη ισοδυναμία. Για την δεύτερη ισοδυναμία, έστω $x\in G$ έτσι ώστε: $x^{-1}Tx = S$. Τότε, όπως στο μέρος 1., θα έχουμε: $T = xSx^{-1} = (x^{-1})^{-1}Sx^{-1}$, δηλαδή υπάρχει στοιχείο $y\in G$, στοιχείο $y = x^{-1}$, έτσι ώστε: $ySy^{-1} = T$. Παρόμοια, αν υπάρχει $x\in G$ έτσι ώστε $xSx^{-1} = T$, τότε υπάρχει στοιχείο $y\in G$, το στοιχείο $y = x^{-1}$, έτσι ώστε: $y^{-1}SyT$. Έτσι δείξαμε ότι ισχύει και η δεύτερη ισοδυναμία. ▲

Πρόταση 2.5.8. *Έστω $(G,\cdot)$ μια ομάδα.*

1. *Για κάθε στοιχείο $x\in G$ και για κάθε μη-κενό υποσύνολο $S\subseteq G$, το υποσύνολο*

$$\mathsf{N}_G(S) = \{x\in G \mid xSx^{-1} = S\} = \{x\in G \mid x^{-1}Sx = S\}$$

είναι μια υποομάδα της G.

2. *Για κάθε στοιχείο $x\in G$ και για κάθε υποομάδα $H\leq G$, τα υποσύνολα*

$$xHx^{-1} = \{x\cdot h\cdot h^{-1}\in G \mid h\in H\} \quad \text{και} \quad x^{-1}Hx = \{x^{-1}\cdot h\cdot x\in G \mid h\in H\}$$

είναι υποομάδες της G και

$$|xHx^{-1}| = |H| = |x^{-1}Hx|$$

Απόδειξη. 1. Παρατηρούμε ότι $eSe^{-1} = eSe = S$ και επομένως $e\in\mathsf{N}_G(S)$. Ιδιαίτερα $\mathsf{N}_G(S)\neq\emptyset$.

Έστω $x, y\in\mathsf{N}_G(S)$. Τότε θα έχουμε: $xSx^{-1} = S$ και $ySy^{-1} = S$. Λαμβάνοντας υπόψη το Λήμμα 2.5.6 και την Παρατήρηση 2.5.7, θα έχουμε:

$$(x\cdot y^{-1})S(x\cdot y^{-1})^{-1} = (x\cdot y^{-1})S((y^{-1})^{-1}\cdot x^{-1}) = (xy^{-1})S(y\cdot x^{-1}) = x(y^{-1}Sy)x^{-1} = xSx^{-1} = S$$

Άρα $x\cdot y^{-1}\in\mathsf{N}_G(S)$, και επομένως από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο $\mathsf{N}_G(S)$ είναι μια υποομάδα της G.

2. Παρατηρούμε ότι, επειδή το υποσύνολο H είναι υποομάδα της G, θα έχουμε $e \in H$ και άρα $e = x \cdot x^{-1} = x \cdot e \cdot x^{-1} \in xHx^{-1}$. Ιδιαίτερα $xHx^{-1} \neq \emptyset$. Έστω $a, b \in xHx^{-1}$. Τότε $a = xh_1x^{-1}$ και $b = xh_2x^{-1}$, για κάποια στοιχεία $h_1, h_2 \in H$. Τότε, επειδή το υποσύνολο H είναι υποομάδα της G, θα έχουμε ότι $h_1 \cdot h_2^{-1} \in H$ και επομένως:

$$a \cdot b^{-1} = (x \cdot h_1 \cdot x^{-1}) \cdot (x \cdot h_2 \cdot x^{-1})^{-1} = (x \cdot h_1 \cdot x^{-1}) \cdot ((x^{-1})^{-1} \cdot h_2^{-1} \cdot x^{-1}) = (x \cdot h_1 \cdot x^{-1}) \cdot (x \cdot h_2^{-1} \cdot x^{-1}) =$$

$$= x \cdot h_1 \cdot x^{-1} \cdot x \cdot h_2^{-1} \cdot x^{-1} = x \cdot h_1 \cdot e \cdot h_2^{-1} \cdot x^{-1} = x \cdot (h_1 \cdot h_2^{-1}) \cdot x^{-1} \ \in \ xHx^{-1}$$

Επομένως από την Πρόταση 2.4.5 έπεται ότι το υποσύνολο xHx^{-1} είναι μια υποομάδα της G.

Θεωρούμε την απεικόνιση

$$f : H \longrightarrow xHx^{-1}, \quad f(h) = x \cdot h \cdot x^{-1}$$

Η απεικόνιση είναι προφανώς «επί», και επιπλέον η f είναι «1-1», διότι, χρησιμοποιώντας τον Νόμο Διαγραφής σε ομάδες, θα έχουμε:

$$f(h_1) = f(h_2) \quad \Longrightarrow \quad x \cdot h_1 \cdot x^{-1} = x \cdot h_2 \cdot x^{-1} \quad \Longrightarrow \quad h_1 = h_2$$

Επομένως η f είναι «1-1» και «επί», και άρα: $|xHx^{-1}| = |H|$, επειδή $x^{-1}Hx = x^{-1}H(x^{-1})^{-1}$, θα έχουμε και $|x^{-1}Hx| = |H|$. ■

Ορισμός 2.5.9. *Αν $(G, \cdot)$ είναι μια ομάδα, και $S \subseteq G$, τότε η υποομάδα $\mathsf{N}_G(S)$ καλείται ο* **κανονικοποιητής** *του συνόλου S στην ομάδα G.*

Δύο υποσύνολα $S, T \subseteq G$ της G καλούνται **συζυγή υποσύνολα**, *αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $xSx^{-1} = T$. Τότε συνήθως τα υποσύνολα S και T καλούνται x-συζυγή υποσύνολα.*

Ιδιαίτερα δύο υποομάδες $H, K \leq G$ καλούνται **συζυγείς υποομάδες**, *αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $xHx^{-1} = K$. Τότε συνήθως οι υποομάδες H και K καλούνται x-συζυγείς υποομάδες.*

Τέλος, δύο στοιχεία $a, b \in G$ καλούνται **συζυγή στοιχεία** *αν τα υποσύνολα $\{a\}$ και $\{b\}$ είναι συζυγή, δηλαδή αν υπάρχει στοιχείο $x \in G$: $x \cdot a \cdot x^{-1} = b$.*

Από την Παρατήρηση 2.5.7 έπεται ότι δύο υποσύνολα, αντίστοιχα υποομάδες, H, K της G είναι συζυγή υποσύνολα, αντίστοιχα συζυγείς υποομάδες, αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $xHx^{-1} = K$ αν και μόνο αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $x^{-1}Hx = K$ αν και μόνο αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $x^{-1}Kx = H$ αν και μόνο αν υπάρχει στοιχείο $x \in G$ έτσι ώστε: $xKx^{-1} = H$ (το στοιχείο x δεν είναι απαραίτητο να είναι το ίδιο σε όλες τις περιπτώσεις). Παρόμοια, τα στοιχεία $a, b \in G$ είναι συζυγή αν και μόνο αν υπάρχει στοιχείο $x \in G$: $x \cdot a \cdot x^{-1} = b$ αν και μόνο αν υπάρχει στοιχείο $x \in G$: $x^{-1} \cdot a \cdot x = b$ αν και μόνο αν υπάρχει στοιχείο $x \in G$: $a = x^{-1} \cdot b \cdot x$ αν και μόνο αν υπάρχει στοιχείο $x \in G$: $a = x \cdot b \cdot x^{-1}$ (πάλι το στοιχείο x δεν είναι απαραίτητο να είναι το ίδιο σε όλες τις περιπτώσεις).

Από τα παραπάνω έπεται ότι, για κάθε στοιχείο $x \in G$ και υποομάδα $H \leq G$, οι υποομάδες xHx^{-1} και H (ισοδύναμα οι υποομάδες $x^{-1}Hx$ και H είναι συζυγείς, και καλούνται **οι συζυγείς υποομάδες της υποομάδας** H). Όπως θα δούμε και αργότερα, υποομάδες οι οποίες συμπίπτουν με κάθε συζυγή υποομάδα τους διαθέτουν σημαντικές ιδιότητες.

Η ακόλουθη Πρόταση δείχνει ότι κάθε υποομάδα μιας ομάδας η οποία περιέχεται στο κέντρο της συμπίπτει με κάθε συζυγή υποομάδα της.

Πόρισμα 2.5.10. *Έστω $(G, \cdot)$ μια ομάδα και $H \leq G$ μια υποομάδα της G έτσι ώστε: $H \subseteq \mathsf{Z}(G)$. Τότε:*

$$\forall x \in G: \qquad xHx^{-1} = H$$

δηλαδή η H συμπίπτει με κάθε συζυγή υποομάδα της.

Απόδειξη. Έστω $a \in xHx^{-1}$. Τότε $a = x \cdot h \cdot x^{-1}$, για κάποιο στοιχείο $h \in H$. Επειδή το στοιχείο $h \in H \subseteq \mathsf{Z}(G)$, θα έχουμε $x \cdot h = h \cdot x$, και άρα $a = x \cdot h \cdot x^{-1} = h \cdot x \cdot h^{-1} = h \in H$. Επομένως $xHx^{-1} \subseteq H$. Αντίστροφα, αν $h \in H$, τότε, επειδή το στοιχείο h ανήκει στο κέντρο της G, θα έχουμε: $h = h \cdot e = h \cdot x \cdot x^{-1} = x \cdot h \cdot x^{-1} \in xHx^{-1}$, και άρα $H \subseteq xHx^{-1}$. Επομένως θα έχουμε: $H = xHx^{-1}$. ■

2.5.2 Η Μεταθέτρια Υποομάδα

Έστω $(G,\cdot)$ μια ομάδα. Αν $a,b\in G$ είναι στοιχεία της G, τότε το στοιχείο

$$[a,b]=a\cdot b\cdot a^{-1}\cdot b^{-1}$$

καλείται ο **μεταθέτης** των στοιχείων a,b, και δίνει ένα μέτρο για το πόσο απέχουν τα στοιχεία a,b από το να μετατίθενται:

$$[a,b]=e \iff a\cdot b\cdot a^{-1}\cdot b^{-1}=e \iff a\cdot b\cdot a^{-1}=e\cdot b=b \iff a\cdot b=b\cdot a$$

Για την μελέτη μεταθετών στοιχείων μιας ομάδας, θεωρούμε το σύνολο $M=\{[a,b]\in G \mid a,b\in G\}$ όλων των μεταθετών της ομάδας G. Το σύνολο M περιέχει το ουδέτερο στοιχείο e της G διότι προφανώς $e=[e,e]$, και επίσης περιέχει το αντίστροφο κάθε στοιχείου του M όπως δείχνει η ακόλουθη σχέση:

$$\forall a,b\in G:\quad [a,b]^{-1}=(a\cdot b\cdot a^{-1}\cdot b^{-1})^{-1}=(b^{-1})^{-1}\cdot(a^{-1})^{-1}\cdot b^{-1}\cdot a^{-1}=b\cdot a\cdot b^{1}\cdot a^{-1}=[b,a] \tag{2.15}$$

Δυστυχώς όμως το παραπάνω σύνολο δεν αποτελεί υποομάδα της G, και ο λόγος είναι ότι το γινόμενο δύο μεταθετών δεν είναι απαραίτητα μεταθέτης, δηλαδή το παραπάνω σύνολο δεν είναι γενικά κλειστό στην πράξη της ομάδας.[13] Έτσι οδηγούμαστε φυσιολογικά στην θεώρηση της μικρότερης υποομάδας της G η οποία περιέχει το υποσύνολο M, δηλαδή όλους τους μεταθέτες της G.

Ορισμός 2.5.11. *Αν $(G,\cdot)$ είναι μια ομάδα, τότε η* **μεταθέτρια υποομάδα** *της G ορίζεται να είναι η υποομάδα $[G,G]$ η οποία παράγεται από το σύνολο όλων των μεταθετών της G:*

$$[G,G]=\Big\langle\{[a,b]\in G \mid a,b\in G\}\Big\rangle$$

Η μεταθέτρια υποομάδα $[G,G]$ της G συμβολίζεται επίσης και ως G'.

Επειδή από τη σχέση (2.15) το αντίστροφο ενός μεταθέτη είναι μεταθέτης, από την Πρόταση 2.4.33 έπεται ότι η μεταθέτρια υποομάδα της G έχει την ακόλουθη περιγραφή:

$$[G,G]=\Big\{[a_1,b_1]\cdot[a_2,b_2]\cdots[a_n,b_n]\ \in\ G \mid a_k,b_k\in G,\ 1\le k\le n,\ n\in\mathbb{N}\Big\}$$

Προφανώς: $[G,G]=\{e\}$ αν και μόνο αν η ομάδα G είναι αβελιανή.

Από όλες τις ομάδες τις οποίες γνωρίζουμε μέχρι τώρα, η ομάδα με την μικρότερη δυνατή τάξη η οποία δεν είναι αβελιανή είναι η συμμετρική ομάδα S_3. Στο επόμενο παράδειγμα θα υπολογίσουμε την μεταθέτρια υποομάδα της.

Παράδειγμα 2.5.12. Θεωρούμε τη συμμετρική ομάδα $\mathsf{S}_3=\{\iota,\mu_1,\mu_2,\mu_3,\rho_1,\rho_2\}$. Τότε:

$$[\mathsf{S}_3,\mathsf{S}_3]=\{\iota,\ \rho_1,\ \rho_2\}=\langle\rho_1\rangle$$

Πράγματι, προφανώς $\iota\in[\mathsf{S}_3,\mathsf{S}_3]$. Χρησιμοποιώντας τον πίνακα Cayley της S_3, βλέπε το Παράδειγμα 2.3.5, θα έχουμε

$$[\mu_1,\mu_2]=\mu_1\cdot\mu_2\cdot\mu_1^{-1}\cdot\mu_2^{-1}=\mu_1\cdot\mu_2\cdot\mu_1\cdot\mu_2=\rho_1\cdot\rho_1=\rho_2 \quad\text{και}\quad [\mu_2,\mu_1]=\mu_2\cdot\mu_1\cdot\mu_2^{-1}\cdot\mu_1^{-1}=\mu_2\cdot\mu_1\cdot\mu_2\cdot\mu_1=\rho_2\cdot\rho_2=\rho_1$$

Επομένως $\langle\rho_1\rangle=\{\iota,\rho_1,\rho_2\}\subseteq[\mathsf{S}_3,\mathsf{S}_3]$. Ελέγχοντας, με χρήση του πίνακα Cayley, όλους τους δυνατούς συνδυασμούς μεταθετών στοιχείων της S_3, βλέπουμε ότι $[x,y]\in\{\iota,\rho_1,\rho_2\}$, για κάθε $x,y\in\mathsf{S}_3$, και άρα επειδή το υποσύνολο $\{\iota,\rho_1,\rho_2\}$ είναι υποομάδα της S_3, έπεται ότι πεπερασμένα γινόμενα στοιχείων της μορφής $[x,y]$, δηλαδή τυπικά στοιχεία της μεταθέτριας υποομάδας $[\mathsf{S}_3,\mathsf{S}_3]$, ανήκουν στην υποομάδα $\{\iota,\rho_1,\rho_2\}$. Επομένως $[\mathsf{S}_3,\mathsf{S}_3]=\{\iota,\rho_1,\rho_2\}$. $\surd$

[13] Παραδείγματα ομάδων G στις οποίες γινόμενο μεταθετών δεν είναι απαραίτητα μεταθέτης δεν είναι εύκολο να βρεθούν. Αποδεικνύεται ότι η τάξη της μικρότερης πεπερασμένης ομάδας στην οποία γινόμενο μεταθετών δεν είναι απαραίτητα μεταθέτης είναι 96. Επίσης αποδεικνύεται, σχετικά ευκολότερα, ότι στην ειδική γραμμική ομάδα $\mathsf{SL}(2,\mathbb{R})$, γινόμενο μεταθετών δεν είναι απαραίτητα μεταθέτης.

Κλείνουμε την παρούσα υποενότητα, καταγράφοντας μια σημαντική ιδιότητα της μεταθέτριας υποομάδας, η οποία θα μας είναι χρήσιμη στη συνέχεια.

Πρόταση 2.5.13. *Η μεταθέτρια υποομάδα $[G,G]$ της G συμπίπτει με κάθε συζυγή της υποομάδα:*

$$\forall x \in G: \quad x[G,G]x^{-1} = [G,G]$$

Απόδειξη. Θεωρούμε έναν μεταθέτη $[a,b]$ της G. Τότε για κάθε στοιχείο $x \in G$, θα έχουμε:

$$x\cdot[a,b]\cdot x^{-1} = x\cdot a\cdot b\cdot a^{-1}\cdot b^{-1}\cdot x^{-1} = x\cdot a\cdot e\cdot b\cdot e\cdot a^{-1}\cdot e\cdot b^{-1}\cdot x^{-1} = x\cdot a\cdot x^{-1}\cdot x\cdot b\cdot x^{-1}\cdot x\cdot a^{-1}\cdot x^{-1}\cdot x\cdot b^{-1}\cdot x^{-1} =$$

$$= (x\cdot a\cdot x^{-1})\cdot(x\cdot b\cdot x^{-1})\cdot(x\cdot a^{-1}\cdot x^{-1})\cdot(x\cdot b^{-1}\cdot x^{-1}) = (x\cdot a\cdot x^{-1})\cdot(x\cdot b\cdot x^{-1})\cdot(x\cdot a\cdot x^{-1})^{-1}\cdot(x\cdot b\cdot x^{-1})^{-1} = [x\cdot a\cdot x^{-1}, x\cdot b\cdot x^{-1}]$$

Επομένως το συζυγές στοιχείο ενός μεταθέτη είναι μεταθέτης των συζυγών στοιχείων:

$$\forall x,a,b \in G: \quad x\cdot[a,b]\cdot x^{-1} = [x\cdot a\cdot x^{-1}, x\cdot b\cdot x^{-1}] \tag{2.16}$$

Έστω $A = [a_1,b_1]\cdot[a_2,b_2]\cdots[a_n,b_n]$ ένα τυπικό στοιχείο της μεταθέτριας υποομάδας $[G,G]$. Τότε, χρησιμοποιώντας την παραπάνω σχέση (2.16), θα έχουμε:

$$x\cdot A\cdot x^{-1} = x\cdot[a_1,b_1]\cdot[a_2,b_2]\cdots[a_n,b_n]\cdot x^{-1} = x\cdot[a_1,b_1]\cdot e\cdot[a_2,b_2]\cdot e\cdots e\cdot[a_n,b_n]\cdot x^{-1} =$$

$$= x\cdot[a_1,b_1]\cdot x^{-1}\cdot x\cdot[a_2,b_2]\cdot x^{-1}\cdot x\cdots x\cdot[a_n,b_n]\cdot x^{-1} = (x\cdot[a_1,b_1]\cdot x^{-1})\cdot(x\cdot[a_2,b_2]\cdot x^{-1})\cdots(x\cdot[a_n,b_n]\cdot x^{-1}) =$$

$$= [x\cdot a_1\cdot x^{-1}, x\cdot b_1\cdot x^{-1}]\cdot[x\cdot a_2\cdot x^{-1}, x\cdot b_2\cdot x^{-1}]\ \cdots\ [x\cdot a_n\cdot x^{-1}, x\cdot b_n\cdot x^{-1}]\ \in\ [G,G]$$

Επομένως δείξαμε ότι $x[G,G]x^{-1} \subseteq [G,G]$, $\forall x \in G$. Αντίστροφα, έστω $[a,b]$ ένας μεταθέτης της G. Αναζητούμε στοιχείο $y \in [G,G]$ έτσι ώστε $[a,b] = x\cdot y\cdot x^{-1}$. Πολλαπλασιάζοντας την τελευταία σχέση από τα αριστερά με το x^{-1} και από τα δεξιά με το x, θα έχουμε $y = x^{-1}\cdot[a,b]\cdot x$, από όπου με χρήση της σχέσης (2.16), θα έχουμε: $y = [x^{-1}\cdot a\cdot x, x^{-1}\cdot b\cdot x] \in [G,G]$. Επομένως κάθε μεταθέτης $[a,b]$ της G ανήκει στην υποομάδα $x[G,G]x^{-1}$:

$$\forall a,b \in G: \quad [a,b] = x\cdot[x^{-1}\cdot a\cdot x, a^{-1}\cdot b\cdot x]\ \in\ [G,G]$$

Επειδή κάθε στοιχείο της μεταθέτριας ομάδας είναι πεπερασμένο γινόμενο στοιχείων της μορφής $[a,b]$ τα οποία, όπως είδαμε, ανήκουν στο υποσύνολο $x[G,G]x^{-1}$, και επειδή από την Πρόταση 2.5.8, για κάθε $x \in G$, το σύνολο $x\cdot[G,G]x^{-1}$ είναι υπομάδα της G, έπεται κάθε στοιχείο της $[G,G]$ ανήκει στην υποομάδα $x[G,G]x^{-1}$, δηλαδή $[G,G] \subseteq x[G,G]x^{-1}$. Επομένως δείξαμε ότι $[G,G] = x[G,G]x^{-1}$. ■

2.6 Κανονικές Υποομάδες

Όπως είδαμε στο Πόρισμα 2.5.10 και στην Πρόταση 2.5.13, κάθε υποομάδα μιας ομάδας η οποία περιέχεται στο κέντρο της ομάδας, καθώς και η μεταθέτρια υποομάδα μιας ομάδας, ικανοποιούν την ιδιότητα ότι συμπίπτει με κάθε συζυγή υποομάδα της. Με βάση αυτή την παρατήρηση προκύπτει ο ακόλουθος ορισμός ο οποίος ταξινομεί μια σημαντική κλάση υποομάδων μιας ομάδας.

Ορισμός 2.6.1. *Έστω $(G,\cdot)$ μια ομάδα. Μια υποομάδα $H \leq G$ της G καλείται* **κανονική**,[14] *αν η H συμπίπτει με κάθε συζυγή υποομάδα της, δηλαδή:*

$$\forall x \in G: \quad xHx^{-1} = H$$

Αν η H είναι κανονική υποομάδα της G, θα γράφουμε:

$$H \trianglelefteq G$$

[14] Ο όρος «κανονική» υποομάδα συναντάται στην βιβλιογραφία και ως: «ορθόθετη υποομάδα» ή «αναλλοίωτη υποομάδα», ή «κανονικός διαιρέτης».

Σκοπός της παρούσας υποενότητας είναι να παρουσιάσουμε βασικές ιδιότητες και χαρακτηρισμούς κανονικών υποομάδων. Σε μεταγενέστερη ενότητα θα αναπτύξουμε αναλυτικότερα τη θεωρία και τις εφαρμογές κανονικών υποομάδων.

Πρόταση 2.6.2. *Αν $(G,\cdot)$ είναι μια ομάδα και $H \leq G$ μια υποομάδα της G, τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η υποομάδα H είναι κανονική.*
2. $\mathsf{N}_G(H) = G$.
3. $\forall x \in G$: $xHx^{-1} \subseteq H$.
4. $\forall x \in G, \forall h \in H$: $x \cdot h \cdot x^{-1} \in H$.

Απόδειξη. 1. $\Longrightarrow$ 2. Αν η υποομάδα H είναι κανονική, τότε εξ ορισμού θα έχουμε ότι $\forall x \in G$: $xHx^{-1} = H$. Αυτή η σχέση σημαίνει ότι κάθε στοιχείο x της ομάδας G ανήκει στον κανονικοποιητή της H στην G, και επομένως: $G = \mathsf{N}_G(H)$.

2. $\Longrightarrow$ 3. Αν $G = \mathsf{N}_G(H)$, τότε $\forall x \in G$: $xHx^{-1} = H$, και προφανώς θα έχουμε, $\forall x \in G$: $xHx^{-1} \subseteq H$.

3. $\Longrightarrow$ 4. Αν $\forall x \in G$: $xHx^{-1} \subseteq H$, τότε προφανώς $\forall x \in G$, $\forall h \in H$: $x \cdot h \cdot x^{-1} \in H$.

4. $\Longrightarrow$ 1. Υποθέτουμε ότι $\forall x \in G$, $\forall h \in H$: $x \cdot h \cdot x^{-1} \in H$. Τότε προφανώς θα έχουμε $\forall x \in G$: $xHx^{-1} \subseteq H$, και μένει να δείξουμε ότι $H \subseteq xHx^{-1}$. Έστω $h \in H$ και $x \in G$. Θεωρούμε το στοιχείο $h' = x^{-1} \cdot h \cdot x = x^{-1} \cdot h \cdot (x^{-1})^{-1}$ το οποίο από την υπόθεση ανήκει στην υποομάδα H. Τότε θα έχουμε:

$$h' = x^{-1} \cdot h \cdot x \quad \Longrightarrow \quad h = x \cdot h' \cdot x^{-1} \in xHx^{-1}$$

και άρα $H \subseteq xHx^{-1}$. Επομένως $xHx^{-1} = H$, $\forall x \in G$, δηλαδή η H είναι κανονική υποομάδα της G. ■

Παρατήρηση 2.6.3. Έστω $(G,\cdot)$ μια ομάδα και $H \leq G$ μια υποομάδα της G. Τότε, για κάθε στοιχείο $x \in H$, ισχύει ότι: $xHx^{-1} = H$. Πράγματι, έστω $a \in xHx^{-1}$, δηλαδή $a = x \cdot h \cdot x^{-1}$, για κάποιο στοιχείο $h \in H$. Τότε, επειδή τα στοιχεία x, h, h^{-1} ανήκουν στην υποομάδα H, έπεται ότι $a = x \cdot h \cdot x^{-1} \in H$ και άρα $xHx^{-1} \subseteq H$. Αντίστροφα, αν $h \in H$, θεωρούμε το στοιχείο $h' = x^{-1} \cdot h \cdot x$, το οποίο ανήκει στην H, διότι τα στοιχεία $x^{-1}, h, x \in H$. Τότε $x \cdot h' \cdot x^{-1} \in xHx^{-1}$ και $x \cdot (x^{-1} \cdot h \cdot x) \cdot x^{-1} = (x \cdot x^{-1}) \cdot h \cdot (x \cdot x^{-1}) = e \cdot h \cdot e = h$. Επομένως $h \in xHx^{-1}$ και άρα $H \subseteq xHx^{-1}$. Συνοψίζοντας, δείξαμε ότι: $xHx^{-1} = H$, $\forall x \in H$.

Άρα, για να δείξουμε ότι μια υποομάδα $H \leq G$ είναι κανονική, αρκεί να δείξουμε οτι: $xHx^{-1} = H$, $\forall x \in G \setminus H$ ή λαμβάνοντας υπόψη την Πρόταση 2.6.2, αρκεί να δείξουμε ότι: $xHx^{-1} \subseteq H$, $\forall x \in G \setminus H$ ▲

Παράδειγμα 2.6.4. Έστω $(G,\cdot)$ μια ομάδα. Προφανώς η τετριμμένη υποομάδα $\{e\}$, καθώς και η ίδια η ομάδα G είναι κανονικές υποομάδες της G. Επιπλέον:

1. Αν $H \leq G$ είναι μια υποομάδα της G με την ιδιότητα $H \subseteq \mathsf{Z}(G)$, τότε η H είναι κανονική. Ιδιαίτερα:
   (α') Αν η G είναι αβελιανή, τότε κάθε υποομάδα της είναι κανονική.
   (β') Το κέντρο $\mathsf{Z}(G)$ της G είναι μια κανονική υποομάδα της G.
2. Η μεταθέτρια υποομάδα $[G,G]$ της G είναι κανονική.
3. Αν $H \leq G$ είναι μια υποομάδα της πεπερασμένης ομάδας G και η H είναι η μοναδική υποομάδα της G με τάξη $|H|$, τότε η H είναι κανονική.

Πράγματι, το μέρος 1. προκύπτει από το Πόρισμα 2.5.10, και το μέρος 2. προκύπτει από την Πρόταση 2.5.13. Για το μέρος 3., από την Πρόταση 2.5.8 γνωρίζουμε ότι, για κάθε στοιχείο $x \in G$, και κάθε υποομάδα $H \leq G$, το υποσύνολο xHx^{-1} είναι μια υποομάδα της G και $|xHx^{-1}| = |H|$. Επομένως, αν υπάρχει μόνο μια υποομάδα της G με τάξη $|H|$, τότε λόγω μοναδικότητας θα έχουμε $xHx^{-1} = H$, $\forall x \in G$. Δηλαδή το υποσύνολο H είναι κανονική υποομάδα της G. √

Παράδειγμα 2.6.5. Από το Παράδειγμα 2.6.4 έπεται ότι κάθε υποομάδα H μιας ομάδας G η οποία περιέχεται στο κέντρο $\mathsf{Z}(G)$ της G είναι κανονική. Θα δείξουμε ότι το αντίστροφο δεν ισχύει.

Θεωρούμε τη συμμετρική ομάδα $\mathsf{S}_3 = \{\iota, \mu_1, \mu_2, \mu_3, \rho_1, \rho_2\}$. Έστω $H = \langle \rho_1 \rangle = \{\iota, \rho_1, \rho_2\}$ η κυκλική υποομάδα της S_3 η οποία παράγεται από την μετάθεση ρ_1. Θα δείξουμε ότι $H \trianglelefteq \mathsf{S}_3$. Απο την Παρατήρηση 2.6.3, αρκεί να δείξουμε ότι $\mu_i H \mu_i^{-1} = H$ ή ισοδύναμα (επειδή $\mu_i^2 = \mu_i$): $\mu_i H \mu_i = H$, $1 \leq i \leq 3$.

Χρησιμοποιώντας τον πίνακα Cayley της S_3, όπως στο Παράδειγμα 2.3.5, θα έχουμε:

$$\mu_1 \cdot \rho_1 \cdot \mu_1 = \rho_2, \quad \mu_1 \cdot \rho_2 \cdot \mu_1 = \rho_1, \quad \mu_2 \cdot \rho_1 \cdot \mu_2 = \rho_2, \quad \mu_2 \cdot \rho_2 \cdot \mu_2 = \rho_1, \quad \mu_3 \cdot \rho_1 \cdot \mu_3 = \rho_2, \quad \mu_3 \cdot \rho_2 \cdot \mu_3 = \rho_1$$

Οι παραπάνω σχέσεις δείχνουν ότι $\mu_i H \mu_i = H$, $1 \leq i \leq 3$, και επομένως η υποομάδα H είναι κανονική υποομάδα της S_3.

Από το Παράδειγμα 2.5.4 έπεται ότι $\mathsf{Z}(\mathsf{S}_3) = \{\iota\}$. Άρα $H \trianglelefteq \mathsf{S}_3$ αλλά $H \not\subseteq \mathsf{Z}(\mathsf{S}_3)$. $\surd$

Η ακόλουθη Πρόταση παρουσιάζει κάποιες βασικές ιδιότητες των κανονικών υποομάδων.

Πρόταση 2.6.6. *Έστω $(G, \cdot)$ μια ομάδα. Τότε:*

1. *Αν $H \leq G$ είναι μια υποομάδα της G, τότε ο κανονικοποιητής $\mathsf{N}_G(H)$ της H στην G είναι η μεγαλύτερη υποομάδα της G η οποία περιέχει την H ως κανονική υποομάδα: $H \trianglelefteq K \leq G \implies K \leq \mathsf{N}_G(H)$.*
2. *Αν $\{H_i\}_{i \in I}$ είναι μια οικογένεια κανονικών υποομάδων της G, τότε η τομή $\bigcap_{i \in I} H_i$ είναι μια κανονική υποομάδα της G:*
$$\forall i \in I: \ H_i \trianglelefteq G \quad \Longrightarrow \quad \bigcap_{i \in I} H_i \trianglelefteq G$$
3. *Έστω ότι H και K είναι δύο κανονικές υποομάδες της G.*
   (α') Ισχύει ότι $HK = KH$ και το υποσύνολο $HK = KH$ είναι μια κανονική υποομάδα της G.
   (β') Η υποομάδα $H \cap K$ είναι κανονική υποομάδα της H και της K.

Απόδειξη. 1. Έστω $H \leq G$ μια υποομάδα της G. Θα δείξουμε ότι: $H \trianglelefteq \mathsf{N}_G(H)$, και αν K είναι μια υποομάδα της G με την ιδιότητα $H \trianglelefteq K$, τότε $K \subseteq \mathsf{N}_G(H)$.

Από την Πρόταση 2.5.8, έχουμε ότι το υποσύνολο $\mathsf{N}_G(H)$ είναι υποομάδα της G. Επιπλέον, από την Παρατήρηση 2.6.3 προκύπτει ότι:

$$\forall h \in H: \quad hHh^{-1} = H$$

και επομένως $H \subseteq \mathsf{N}_G(H)$. Έστω τώρα $x \in \mathsf{N}_G(H)$. Τότε εξ ορισμού $xHx^{-1} = H$ και επομένως η H είναι κανονική υποομάδα της $\mathsf{N}_G(H)$. Τέλος, έστω K μια υποομάδα της G η οποία περιέχει την H ως κανονική υποομάδα. Τότε:

$$\forall k \in K: \quad kHk^{-1} = H \quad \Longrightarrow \quad k \in \mathsf{N}_G(H)$$

και επομένως $K \subseteq \mathsf{N}_G(H)$.

2. Έστω $x \in G$ και $h \in \bigcap_{i \in I} H_i$. Θα δείξουμε ότι $x \cdot h \cdot x^{-1} \in \bigcap_{i \in I} H_i$. Επειδή $h \in H_i$, $\forall i \in I$, και επειδή κάθε υποομάδα H_i είναι κανονική υποομάδα της G, θα έχουμε:

$$\forall i \in I: \quad x \cdot h \cdot x^{-1} \in H_i \quad \Longrightarrow \quad x \cdot h \cdot x^{-1} \in \bigcap_{i \in I} H_i$$

Επομένως η τομή υποομάδων $\bigcap_{i \in I} H_i$ είναι μια κανονική υποομάδα της G.

3. Έστω ότι H και K είναι δύο κανονικές υποομάδες της G.

(α') Παρατηρούμε ότι, επειδή η H είναι κανονική υποομάδα της G, θα έχουμε $xHx^{-1} = H$, για κάθε στοιχείο $x \in G$ και ιδιαίτερα:

$$\forall k \in K: \quad kHk^{-1} = H \quad \Longrightarrow \quad kH = Hk \quad \Longrightarrow \quad KH = \{k \cdot h \in G \mid k \in K, \ h \in H\} = \{h \cdot k \in G \mid h \in H, \ k \in K\} = HK$$

Προφανώς $e \in HK$ διότι $e \in H \cap K$. Έστω $h_1 \cdot k_1, h_2 \cdot k_2 \in HK$, όπου $h_1, h_2 \in H$ και $k_1, k_2 \in K$. Τότε, χρησιμοποιώντας ότι η K είναι υποομάδα της G και ότι $HK = KH$, θα έχουμε:

$$(h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} = h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1} \in h_1 K h_2^{-1} \subseteq h_1 KH = h_1 HK = HK$$

Επομένως το υποσύνολο HK είναι μια υποομάδα της G. Επιπλέον, επειδή οι υποομάδες H και K είναι κανονικές, θα έχουμε $\forall x \in G$: $g^{-1}Hg = H$ και $g^{-1}Kg = K$, και τότε με χρήση του Λήμματος 2.5.6 έπεται ότι:

$$xHKx^{-1} = x(HeK)x^{-1} = x(H(x^{-1}\cdot x)K)x^{-1} = (xHx^{-1})(xKx^{-1}) = HK$$

και επομένως η υποομάδα HK είναι κανονική υποομάδα της G.

(β') Έστω $h \in H$. Τότε για κάθε $x \in H \cap K$, το στοιχείο $h \cdot x \cdot h^{-1}$ ανήκει στην H διότι τα στοιχεία h, x, h^{-1} ανήκουν στην υποομάδα H, και επίσης ανήκει και στην K διότι η K είναι κανονική υποομάδα της G και $x \in K$. Άρα $\forall h \in H$: $h(H \cap K)h^{-1} \subseteq H \cap K$ και τότε από την Πρόταση 2.6.2 έπεται ότι $H \cap K \trianglelefteq H$. Ακριβώς παρόμοια είναι η απόδειξη ότι η υποομάδα $H \cap K$ είναι κανονική υποομάδα της K. ■

Κλείνουμε την παρούσα υποενότητα με μια σύντομη αναφορά στην έννοια της απλής ομάδας. Μια ομάδα G περιέχει πάντα ως κανονική υποομάδα, την τετριμμένη υποομάδα $\{e\}$ και τη μη γνήσια υποομάδα G. Ομάδες οι οποίες δεν περιέχουν άλλες κανονικές υποομάδες είναι πολύ σπουδαίες:

Ορισμός 2.6.7. *Μια ομάδα G καλείται* **απλή**, *αν οι μόνες κανονικές υποομάδες της G είναι οι $\{e\}$ και G.*

Υπάρχουν πολλοί λόγοι για τους οποίους η έννοια της απλής ομάδας είναι σημαντική. Για παράδειγμα, κάθε πεπερασμένη ομάδα διαθέτει μια συνθετική σειρά, δηλαδή μια ακολουθία υποομάδων

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_{n-1} \trianglelefteq H_n = G$$

έτσι ώστε κάθε υποομάδα H_i είναι κανονική υποομάδα της H_{i+1}, $0 \le i \le n-1$, και η ομάδα πηλίκο H_{i+1}/H_i, βλέπε το Κεφάλαιο 6 για την έννοια της ομάδας πηλίκο, είναι απλή. Επομένως η γνώση όλων των πεπερασμένων απλών ομάδων συμβάλλει αποφασιστικά στη γνώση της δομής όλων των πεπερασμένων ομάδων.

Προς αυτή την κατεύθυνση, το κεντρικό πρόβλημα της θεωρίας πεπερασμένων ομάδων τον προηγούμενο αιώνα ήταν η ταξινόμηση των απλών πεπερασμένων ομάδων. Ένα από τα μεγαλύτερα επιτεύγματα των Μαθηματικών κατά τον προηγούμενο αιώνα ήταν η ταξινόμηση όλων των απλών πεπερασμένων ομάδων, η οποία για να ολοκληρωθεί χρειάστηκαν περίπου 150 χρόνια ερευνητικών προσπαθειών πάνω από 100 μαθηματικών.

Θεώρημα 2.6.8. *Κάθε πεπερασμένη απλή ομάδα είναι ισόμορφη με μία από τις ακόλουθες απλές ομάδες:*

1. *Μια κυκλική ομάδα με τάξη έναν πρώτο αριθμό.*
2. *Μια εναλλάσσουσα ομάδα A_n, όπου $n \ge 5$.*
3. *Μια απλή ομάδα τύπου Lie.*
4. *Μια από τις 26 σποραδικές ομάδες.*

Από τις παραπάνω απλές ομάδες, οι κυκλικές με τάξη έναν πρώτο αριθμό είναι οι μόνες οι οποίες είναι αβελιανές, βλέπε το Σχόλιο 3.4.12. Για τον ορισμό και τις βασικές ιδιότητες των εναλλασσουσών ομάδων A_n, παραπέμπουμε στο Κεφάλαιο 5. Οι απλές ομάδες τύπου Lie, εμφανίζονται σε 16 οικογένειες ομάδων (στις οποίες συμπεριλαμβάνονται οι κλασσικές ομάδες Lie υπεράνω πεπερασμένων σωμάτων). Η ομάδα με τη μεγαλύτερη τάξη από τις σποραδικές ομάδες είναι η ομάδα *τέρας* M με τάξη

$$|M| = 808017424794512875886459904961710757005754368000000000 =$$

$$= 2^{46}\cdot 3^{20}\cdot 5^{9}\cdot 7^{6}\cdot 11^{2}\cdot 13^{3}\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71 \approx 8\cdot 10^{53}$$

η ύπαρξη της οποίας προβλέφθηκε από τους Fischer και Griess στο διάστημα 1973-1976, και η τελικά η κατασκευή της πραγματοποιήθηκε από τον Griess το 1982.

Η απόδειξη του θεωρήματος ταξινόμησης όλων των πεπερασμένων απλών ομάδων είναι διάσπαρτη σε ερευνητικά περιοδικά και βιβλία και καλύπτει δεκάδες χιλιάδες σελίδων. Η προσπάθεια για την καταγραφή μιας ολοκληρωμένης, και όσο γίνεται απλούστερης, απόδειξης συνεχίζεται μέχρι τις μέρες μας. Για περισσότερες λεπτομέρειες, βλέπε τον ιστότοπο https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups.

2.7 Ευθέα Γινόμενα Ομάδων (Ι)

Στην παρούσα ενότητα θα μελετήσουμε μια σημαντική κατασκευή ομάδων η οποία από την μια πλευρά μας επιτρέπει να αποκτήσουμε νέα παραδείγματα ομάδων, και από την άλλη πλευρά, σε κάποιες περιπτώσεις, μας επιτρέπει την διάσπαση μιας ομάδας σε απλούστερα κομμάτια της.

2.7.1 Εξωτερικό Ευθύ Γινόμενο Ομάδων

Υποθέτουμε ότι τα ζεύγη $(G_1,\star_1)$, $(G_2,\star_2)$, $\cdots$, $(G_n,\star_n)$ είναι ομάδες με ουδέτερο στοιχείο e_k αντίστοιχα, όπου $1\le k\le n$. Η ακόλουθη Πρόταση ορίζει μια σημαντική κατασκευή μιας νέας ομάδας.

Πρόταση 2.7.1. *Με τους παραπάνω συμβολισμούς, το ζεύγος $(G,\star)$ είναι ομάδα, όπου $G=\prod_{k=1}^n G_k$, και*

$$(x_1,x_2,\cdots,x_n)\star(y_1,y_2,\cdots,y_n)=\big(x_1\star_1 y_1,\, x_2\star_2 y_2,\,\cdots,\,x_n\star_n y_n\big)$$

Επιπρόσθετα η ομάδα $(\prod_{k=1}^n G_k,\star)$ είναι αβελιανή αν και μόνο αν η ομάδα $(G_k,\star_k)$ είναι αβελιανή, $1\le k\le n$.

Απόδειξη. Έστω $\mathsf{x}=(x_1,x_2,\cdots,x_n)$, $\mathsf{y}=(y_1,y_2,\cdots,y_n)$, και $\mathsf{z}=(z_1,z_2,\cdots,z_n)\in G$. Τότε, χρησιμοποιώντας την προσεταιριστικότητα των πράξεων «$\star_i$» επί των συνόλων G_i, $1\le i\le n$, θα έχουμε:

$$\mathsf{x}\star(\mathsf{y}\star\mathsf{z})=(x_1,x_2,\cdots,x_n)\star\big((y_1,y_2,\cdots,y_n)\star(z_1,z_2,\cdots,z_n)\big)=(x_1,x_2,\cdots,x_n)\star\big(y_1\star_1 z_1,\,y_2\star_2 z_2,\cdots,y_n\star_n z_n\big)=$$

$$=\big(x_1\star_1(y_1\star_1 z_1),\;x_2\star_2(y_2\star_2 z_2),\;\cdots,\;x_n\star_n(y_n\star_n z_n)\big)=\big((x_1\star_1 y_1)\star_1 z_1,\;(x_2\star_2 y_2)\star_2 z_2,\;\cdots,\;(x_n\star_n y_n)\star_n z_n\big)=$$

$$=\big(x_1\star_1 y_1,x_2\star_2 y_2,\cdots,x_n\star_n y_n\big)\star(z_1,z_2,\cdots,z_n)=\big((x_1,x_2,\cdots,x_n)\star(y_1,y_2,\cdots,y_n)\big)\star(z_1,z_2,\cdots,z_n)=(\mathsf{x}\star\mathsf{y})\star\mathsf{z}$$

Άρα η πράξη «$\star$» επί του G είναι προσεταιριστική. Θα δείξουμε ότι το στοιχείο

$$\mathsf{e}=(e_1,e_2,\cdots,e_n)\;\in\;G$$

όπου e_i είναι το ουδέτερο στοιχείο για την πράξη «$\star_i$» επί του G_i, $1\le i\le n$, είναι το ουδέτερο στοιχείο για την πράξη «$\star$» επί του G. Πράγματι, $\forall\,\mathsf{x}=(x_1,x_2,\cdots,x_n)\in G$:

$$\mathsf{x}\star\mathsf{e}=(x_1,x_2,\cdots,x_n)\star(e_1,e_2,\cdots,e_n)=(x_1\star_1 e_1,\,x_2\star_2 e_2,\,\cdots,\,x_n\star_n e_n)=(x_1,x_2,\cdots,x_n)=\mathsf{x}$$

$$\mathsf{e}\star\mathsf{x}=(e_1,e_2,\cdots,e_n)\star(x_1,x_2,\cdots,x_n)=(e_1\star_1 x_1,\,e_2\star_2 x_2,\,\cdots,\,e_n\star_n x_n)=(x_1,x_2,\cdots,x_n)=\mathsf{x}$$

Οι παραπάνω σχέσεις δείχνουν ότι το e είναι το ουδέτερο στοιχείο για την πράξη «$\star$» επί του G. Τέλος, θα δείξουμε ότι κάθε στοιχείο $\mathsf{x}=(x_1,x_2,\cdots,x_n)\in G$ είναι αντιστρέψιμο. Έστω x_k^{-1} το αντίστροφο του στοιχείου x_k στην ομάδα G_k, $1\le k\le n$, και θέτουμε $\mathsf{x}'=(x_1,x_2,\cdots,x_n)$. Τότε θα έχουμε:

$$\mathsf{x}\star\mathsf{x}'=(x_1,x_2,\cdots,x_n)\star(x_1^{-1},x_2^{-1},\cdots,x_n^{-1})=(x_1\star_1 x_1^{-1},x_2\star_2 x_2^{-1},\;\cdots\;x_n\star_n x_n^{-1})=(e_1,e_2,\cdots,e_n)=\mathsf{e}$$

$$\mathsf{x}'\star\mathsf{x}=(x_1^{-1},x_2^{-1},\cdots,x_n^{-1})\star(x_1,x_2,\cdots,x_n)=(x_1^{-1}\star_1 x_1,x_2^{-1}\star_2 x_2,\;\cdots\;x_n^{-1}\star_n x_n)=(e_1,e_2,\cdots,e_n)=\mathsf{e}$$

Άρα το στοιχείο $\mathsf{x}=(x_1,x_2,\cdots,x_n)$ είναι αντιστρέψιμο και $\mathsf{x}^{-1}=(x_1^{-1},x_2^{-1},\cdots,x_n^{-1})$. Επομένως το ζεύγος $(G,\star)$ είναι ομάδα.

Έστω Έστω $\mathsf{x}=(x_1,x_2,\cdots,x_n)$ και $\mathsf{y}=(y_1,y_2,\cdots,y_n)$ δύο στοιχεία της G. Τότε:

$$\mathsf{x}\star\mathsf{y}=(x_1,x_2,\cdots,x_n)\star\mathsf{y}=(y_1,y_2,\cdots,y_n)=(x_1\star_1 y_1,x_2\star_2 y_2,\cdots,x_n\star_n y_n)$$

$$\mathsf{y}\star\mathsf{x}=(y_1,y_2,\cdots,y_n)\star\mathsf{x}=(x_1,x_2,\cdots,x_n)=(y_1\star_1 x_1,y_2\star_2 x_2,\cdots,y_n\star_n x_n)$$

Επομένως:

$$\mathsf{x}\star\mathsf{y}=\mathsf{y}\star\mathsf{x}\quad\Longleftrightarrow\quad x_k\star_k y_k=y_k\star_k x_k,\quad 1\le k\le n$$

Αν κάθε ομάδα $(\mathsf{G}_k,\star_k)$ είναι αβελιανή, $1\le k\le n$, τότε οι παραπάνω σχέσεις δείχνουν ότι $\mathsf{x}\star\mathsf{y}=\mathsf{y}\star\mathsf{x}$, $\forall\,\mathsf{x},\mathsf{y}\in G$, και άρα η ομάδα G είναι αβελιανή. Αντίστροφα, αν η G είναι αβελιανή, για κάθε $k=1,2,\cdots,n$, έστω $a,b\in G_k$ δύο τυχόντα στοιχεία. Τότε θα έχουμε τα στοιχεία $\mathsf{x}=(e_1,\cdots,e_{k-1},a,e_{k+1},\cdots,e_n)$ και $\mathsf{y}=(e_1,\cdots,e_{k-1},b,e_{k+1},\cdots,e_n)$, και άρα, επειδή $\mathsf{x}\star\mathsf{y}=\mathsf{y}\star\mathsf{x}$, από τις παραπάνω σχέσεις θα έχουμε: $a\star_k b=b\star_k a$. Επομένως θα έχουμε ότι ομάδα G_k είναι αβελιανή. ■

Ορισμός 2.7.2. *Έστω* $\{(G_k, \star_k)\}_{k=1}^n$ *μια πεπερασμένη οικογένεια ομάδων. Η ομάδα* $(G, \star)$*, όπου* $G = \prod_{k=1}^n G_k$*, της Πρότασης 2.7.1, καλείται η ομάδα (εξωτερικό)* **ευθύ γινόμενο** *των ομάδων* $(G_1, \star_1)$*,* $(G_2, \star_2)$*,* $\cdots$*,* $(G_n, \star_n)$*, και συμβολίζεται ως εξής:*

$$\prod_{k=1}^{n} G_k = G_1 \times G_2 \times \cdots \times G_n$$

Παράδειγμα 2.7.3. Θεωρούμε την προσθετική ομάδα $(\mathbb{K}, +)$, όπου $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ το οποίο θεωρούμε εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού. Τότε έχουμε τις αβελιανές ομάδες $(\mathbb{K}, +)$ και $(\mathbb{K}^\star, \cdot)$. Σύμφωνα με την Πρόταση 2.7.1, τα καρτεσιανά γινόμενα $\mathbb{K}^n$ και $(\mathbb{K}^*)^n$ είναι εφοδιασμένα με τις ακόλουθες πράξεις:

$$+ : \mathbb{K}^n \times \mathbb{K}^n \longrightarrow \mathbb{K}^n, \quad (x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$$

$$\cdot : (\mathbb{K}^\star)^n \times (\mathbb{K}^\star)^n \longrightarrow (\mathbb{K}^\star)^n, \quad (x_1, x_2, \cdots, x_n) \cdot (y_1, y_2, \cdots, y_n) = (x_1 y_1, x_2 y_2, \cdots, x_n y_n)$$

και τα ζεύγη $(\mathbb{K}^n, +)$ και $((\mathbb{K}^\star)^n, \cdot)$ είναι αβελιανές ομάδες. $\surd$

Επισημαίνουμε ότι ο ορισμός του ευθέος γινομένου πεπερασμένου πλήθους ομάδων επεκτείνεται ακριβώς με τον ίδιο τρόπο και για άπειρο πλήθος ομάδων.

Αναλυτικότερα, έστω $\{(G_i, \star_i)\}_{i \in I}$ μια οικογένεια ομάδων, όπου I είναι ένα, εν γένει άπειρο, σύνολο δεικτών. Στο καρτεσιανό γινόμενο σύνολων

$$\prod_{i \in I} G_i = \{(x_i)_{i \in I} \mid x_i \in G_i\}$$

με στοιχεία οικογένειες $(x_i)_{i \in I}$, ή απλούστερα (x_i), στοιχείων $x_i \in G_i$ υπεράνω του συνόλων δεικτών I, ορίζουμε διμελή πράξη ως εξής:

$$\star : \prod_{i \in I} G_i \times \prod_{i \in I} G_i \longrightarrow \prod_{i \in I} G_i, \quad (x_i)_{i \in I} \star (y_i)_{i \in I} = (x_i \star_i y_i)_{i \in I}$$

Τότε ισχύει η ακόλουθη Πρόταση, η απόδειξη της οποίας είναι παρόμοια με την απόδειξη της Πρότασης 2.7.1 και αφήνεται ως Άσκηση στον αναγνώστη.

Πρόταση 2.7.4. *Έστω* $\{(G_i, \star_i)\}_{i \in I}$ *μια οικογένεια ομάδων. Τότε το ζεύγος* $(G, \star)$ *όπου* $G = \prod_{i \in I} G_i$*, και*

$$(x_i)_{i \in I} \star (y_i)_{i \in I} = (x_i \star_i y_i)_{i \in I}$$

είναι ομάδα: η ομάδα (εξωτερικό) **ευθύ γινόμενο** *της οικογένειας* $\{(G_i, \star_i)\}_{i \in I}$*. Το ουδέτερο στοιχείο της ομάδας* $\prod_{i \in I} G_i$ *είναι το στοιχείο* $(e_i)_{i \in I}$*, και το αντίστροφο του στοιχείου* $(x_i)_{i \in I} \in \prod_{i \in I} G_i$ *είναι το στοιχείο* $(x_i^{-1})_{i \in I}$*. Τέλος, η ομάδα* $(\prod_{i \in I} G_i, \star)$ *είναι αβελιανή αν και μόνο αν η ομάδα* $(G_i, \star_i)$ *είναι αβελιανή,* $\forall\, i \in I$*.*

Στη συνέχεια θα αναλύσουμε τη δομή του ευθέος γινομένου ομάδων, καθώς και των υποομάδων τους. Σ' αυτό το σημείο είναι απαραίτητο να εισαγάγουμε συμβολισμό ο οποίος θα απλοποιήσει την ανάλυσή μας.

Σύμβαση - Συμβολισμός 2.7.5. Έστω $(G_1, \star_1)$, $(G_2, \star_2)$, $\cdots$, $(G_n, \star_n)$ ένα πεπερασμένο πλήθος ομάδων, και θεωρούμε την ομάδα εξωτερικό ευθύ γινόμενο $(\prod_{k=1}^n G_k, \star)$. Από τώρα και στο εξής, αν δεν υπάρχει κίνδυνος σύγχισης, θα συμβολίζουμε ενιαία τις εμπλεκόμενες πράξεις $((\star_k))$, $1 \leq k \leq n$, και «$\star$», με το ίδιο σύμβολο «$\cdot$», δηλαδή θα χρησιμοποιούμε τον πολλαπλασιαστικό συμβολισμό για όλες τις εμπλεκόμενες ομάδες. Έτσι θα θεωρούμε πεπερασμένο πλήθος ομάδων $(G_1, \cdot)$, $(G_2, \cdot)$, $\cdots$, $(G_n, \cdot)$, και η πράξη με την οποία η ομάδα ευθύ γινόμενο $(G, \cdot)$ δομείται σε ομάδα παίρνει την μορφή:

$$(x_1, x_2, \cdots, x_n) \cdot (y_1, y_2, \cdots, y_n) = \big(x_1 \cdot y_1, x_2 \cdot y_2, \cdots, x_n \cdot y_n\big)$$

Αντίστοιχα, όταν οι εμπλεκόμενες ομάδες δίνονται με προσθετικό συμβολισμό, τότε θα χρησιμοποιούμε το ίδιο σύμβολο «+», και άρα η ομάδα εξωτερικό ευθύ γινόμενο των ομάδων $(G_1, +)$, $(G_2, +)$, $\cdots$, $(G_n, +)$ δομείται σε ομάδα με πράξη

$$(x_1, x_2, \cdots, x_n) + (y_1, y_2, \cdots, y_n) = \big(x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n\big)$$

Ο παραπάνω συμβολισμός επεκτείνεται και σε άπειρο πλήθος ομάδων. ▲

Χάριν απλότητας, θα μελετήσουμε πρώτα την περίπτωση του ευθέος γινομένου δύο ομάδων, και έπειτα θα αναλύσουμε την γενική περίπτωση.

Έστω $(G,\cdot)$ η ομάδα ευθύ γινόμενο δύο ομάδων $(G_1,\cdot)$ και $(G_2,\cdot)$:

$$G = G_1 \times G_2 = \big\{(x_1,x_2) \mid x_1 \in G_1,\ x_2 \in G_2\big\}$$

Στην ομάδα $G = G_1 \times G_2$ θεωρούμε τα εξής υποσύνολα:

$$\widetilde{G}_1 = G_1 \times \{e_2\} = \big\{(x_1,e_2) \in G_1 \times G_2 \mid x_1 \in G_1\big\} \qquad \text{και} \qquad \widetilde{G}_2 = \{e_1\} \times G_2 = \big\{(e_1,x_2) \in G_1 \times G_2 \mid x_2 \in G_2\big\}$$

Πρόταση 2.7.6. *Τα υποσύνολα $\widetilde{G}_i \subseteq G$, $i = 1,2$, ικανοποιούν τις ακόλουθες ιδιότητες:*

1. *Τα υποσύνολα $\widetilde{G}_1$ και $\widetilde{G}_2$, είναι κανονικές υποομάδες της ομάδας G: $\widetilde{G}_i \trianglelefteq G$, $i = 1,2$.*
2. *$\widetilde{G}_1 \bigcap \widetilde{G}_2 = \big\{e_G\big\} = \big\{(e_1,e_2)\big\}$.*
3. *$G = \widetilde{G}_1 \cdot \widetilde{G}_2 = \widetilde{G}_2 \cdot \widetilde{G}_1$.*
4. *$G = \big\langle \widetilde{G}_1 \bigcup \widetilde{G}_2 \big\rangle$.*
5. *Κάθε στοιχείο a της ομάδας G γράφεται κατά μοναδικό τρόπο ως γινόμενο:*

   $$(\alpha)\ \ a = a_1 \cdot a_2, \quad \text{όπου} \quad a_i \in \widetilde{G}_i, \qquad \text{και} \qquad (\beta)\ \ a = a_2' \cdot a_1', \quad \text{όπου} \quad a_i' \in \widetilde{G}_i$$

   Δηλαδή, αν επίσης έχουμε: $a = b_1 \cdot b_2 = c_2 \cdot c_1$, όπου $b_1, c_1 \in \widetilde{G}_1$ και $b_2, c_2 \in \widetilde{G}_2$, τότε: $b_1 = a_1$ και $b_2 = a_2$, και $c_1 = a_1'$ και $c_2 = a_2'$.
6. *Η απεικόνιση*

   $$f:\ G = G_1 \times G_2 \longrightarrow \widetilde{G}_1 \times \widetilde{G}_2, \quad f(x_1,x_2) = \big((x_1,e_2),\ (e_1,x_2)\big)$$

   είναι «1-1», «επί», και διατηρεί τις πράξεις των εμπλεκόμενων ομάδων.[15]

Απόδειξη. 1. Τα υποσύνολα $\widetilde{G}_i$, $i = 1,2$, περιέχουν προφανώς το ουδέτερο στοιχείο $e_G = (e_1,e_2)$ της $G = G_1 \times G_2$, και άρα $\widetilde{G}_i \neq \emptyset$, $i = 1,2$. Έστω (x_1,e_2) και (y_1,e_2) δύο στοιχεία του υποσυνόλου $\widetilde{G}_1$. Τότε

$$(x_1,e_2) \cdot (y_1,e_2)^{-1} = (x_1,e_2) \cdot (y_1^{-1},e_2) = (x_1 \cdot y_1^{-1},e_2) \in \widetilde{G}_1$$

Επομένως το υποσύνολο $\widetilde{G}_1$ είναι μια υποομάδα της G, και παρόμοια το υποσύνολο $\widetilde{G}_2$ είναι μια υποομάδα της G.

Έστω (x_1,x_2) ένα τυχόν στοιχείο της ομάδας $G = G_1 \times G_2$ και έστω (x,e_2) ένα τυχόν στοιχείο της υποομάδας $\widetilde{G}_1$. Τότε, επειδή τα στοιχεία x, x_1 ανήκουν στην ομάδα G_1, θα έχουμε

$$(x_1,x_2) \cdot (x,e_2) \cdot (x_1,x_2)^{-1} = (x_1,x_2) \cdot (x,e_2) \cdot (x_1^{-1},x_2^{-1}) = (x_1 \cdot x \cdot x_1^{-1}, x_2 \cdot e_2 \cdot x_2^{-1}) = (x_1 \cdot x \cdot x_1^{-1}, e_2) \ \in\ G_1 \times \{e_2\} = \widetilde{G}_1$$

Επομένως, σύμφωνα με την Πρόταση 2.6.2, το υποσύνολο $\widetilde{G}_1$ είναι κανονική υποομάδα της G: $\widetilde{G}_1 \trianglelefteq G$. Παρόμοια, αν (y_1,y_2) είναι ένα τυχόν στοιχείο της ομάδας $G = G_1 \times G_2$ και (e_1,y) είναι ένα τυχόν στοιχείο της υποομάδας $\widetilde{G}_2$, τότε, επειδή τα στοιχεία y, y_2 ανήκουν στην ομάδα G_2, θα έχουμε:

$$(y_1,y_2) \cdot (e_1,y) \cdot (y_1,y_2)^{-1} = (y_1,y_2) \cdot (e_1,y) \cdot (y_1^{-1},y_2^{-1}) = (y_1 \cdot e_1 \cdot y_1^{-1}, y_2 \cdot y \cdot y_2^{-1}) = (e_1, y_2 \cdot y \cdot y_2^{-1}) \ \in\ \{e_1\} \times G_2 = \widetilde{G}_2$$

Επομένως, σύμφωνα με την Πρόταση 2.6.2, το υποσύνολο $\widetilde{G}_2$ είναι κανονική υποομάδα της G: $\widetilde{G}_2 \trianglelefteq G$.

2. Έστω $(x_1,x_2) \in \widetilde{G}_1 \bigcap \widetilde{G}_2$. Τότε $x_2 = e_2$ διότι $(x_1,x_2) \in \widetilde{G}_1 = G_1 \times \{e_2\}$, και $x_1 = e_1$ διότι $(x_1,x_2) \in \widetilde{G}_2 = \{e_1\} \times G_2$. Άρα $(x_1,x_2) = (e_1,e_2) = e_G$, και επομένως $\widetilde{G}_1 \bigcap \widetilde{G}_2 = \big\{e_G\big\} = \big\{(e_1,e_2)\big\}$.

3. Έστω (x_1,x_2) ένα τυχόν στοιχείο της ομάδας ευθύ γινόμενο G. Τότε θα έχουμε:

$$(x_1,x_2) = (x_1,e_2) \cdot (e_1,x_2) \ \in\ (G_1 \times \{e_2\}) \cdot (\{e_1\} \times G_2) = \widetilde{G}_1 \cdot \widetilde{G}_2 \qquad \Longrightarrow \qquad G = \widetilde{G}_1 \cdot \widetilde{G}_2$$

[15] Όπως θα δούμε στην επόμενη ενότητα, η απεικόνιση f, εξ ορισμού, είναι ένας ισομορφισμός ομάδων.

$$(x_1,x_2)=(e_1,x_2)\cdot(x_1,e_2)\ \in\ (\{e_1\}\times G_2)\cdot(G_1\times\{e_2\})=\widetilde{G}_2\cdot\widetilde{G}_1\quad\Longrightarrow\quad G=\widetilde{G}_2\cdot\widetilde{G}_1$$

4. Επειδή από το μέρος 3., κάθε στοιχείο a της G είναι της μορφής $a=a_1\cdot a_2$, όπου $a_1\in\widetilde{G}_1$ και $a_2\in\widetilde{G}_2$, έπεται ότι κάθε στοιχείο της G είναι γινόμενο στοιχείων του συνόλου $\widetilde{G}_1\bigcup\widetilde{G}_2$ και άρα $G=\langle\widetilde{G}_1\bigcup\widetilde{G}_2\rangle$.

5. Από το μέρος 3. έπεται ότι κάθε στοιχείο $a=(x_1,x_2)\in G$ γράφεται ως γινόμενο $a=(x_1,x_2)=(x_1,e_2)\cdot(e_1,x_2)=a_1\cdot a_2$ και $a=(x_1,x_2)=(e_1,x_2)\cdot(x_1,e_2)=a_2'\cdot a_1'$, όπου $a_1=a_1'=(x_1,e_2)\in\widetilde{G}_1$ και $a_2=a_2'=(e_2,x_2)\in\widetilde{G}_2$. Αν έχουμε $a=b_1\cdot b_2$, όπου $b_i\in\widetilde{G}_i$, $i=1,2$, τότε $a_1\cdot a_2=b_1\cdot b_2$ και επομένως $b_1^{-1}\cdot a_1=b_2\cdot a_2^{-1}$. Επειδή από το μέρος 1., τα υποσύνολα $\widetilde{G}_i$ είναι υποομάδες, θα έχουμε: $b_1^{-1}\cdot a_1\in\widetilde{G}_1$ και $b_2\cdot a_2^{-1}\in\widetilde{G}_2$, και άρα $b_1^{-1}\cdot a_1=b_2\cdot a_2^{-1}\in\widetilde{G}_1\bigcap\widetilde{G}_2$. Επειδή από το μέρος 2., έχουμε $\widetilde{G}_1\bigcap\widetilde{G}_2=\{e_G\}$, έπεται ότι $b_1^{-1}\cdot a_1=b_2\cdot a_2^{-1}=e_G$, και άρα $b_1=a_1$ και $b_2=a_2$. Δηλαδή δείξαμε ότι η γραφή ενός στοιχείου της ομάδας G ως γινόμενο ενός στοιχείου της $\widetilde{G}_1$ με ένα στοιχείο της $\widetilde{G}_2$ είναι μοναδική. Παρόμοια είναι η απόδειξη ότι γραφή ενός στοιχείου της ομάδας G ως γινόμενο ενός στοιχείου της $\widetilde{G}_2$ με ένα στοιχείο της $\widetilde{G}_1$ είναι μοναδική.

6. Η απεικόνιση f είναι «1-1» διότι αν $f(x_1,x_2)=f(y_1,y_2)$, τότε θα έχουμε

$$\big((x_1,e_2),\ (e_1,x_2)\big)=\big((y_1,e_2),\ (e_1,y_2)\big)\quad\Longrightarrow\quad(x_1,e_2)=(y_1,e_2)\quad\text{και}\quad(e_1,x_2)=(e_1,y_2)\quad\Longrightarrow\quad(x_1,x_2)=(y_1,y_2)$$

Επίσης η απεικόνιση f είναι «επί», διότι για κάθε στοιχείο $\big((x_1,e_2),\ (e_1,x_2)\big)\in\widetilde{G}_1\times\widetilde{G}_2$, έχουμε $f(x_1,x_2)=\big((x_1,e_2),\ (e_1,x_2)\big)$. Τέλος, η απεικόνιση f διατηρεί τις πράξεις των εμπλεκόμενων ομάδων, διότι:

$$f\big((x_1,x_2)\cdot(y_1,y_2)\big)=f(x_1\cdot y_1,x_2\cdot y_2)=\big((x_1\cdot y_1,e_2),\ (e_1,x_2\cdot y_2)\big)=\big((x_1,e_2)\cdot(y_1,e_2),\ (e_1,x_2)\cdot(e_1,y_2)\big)=$$

$$=\big((x_1,e_2),\ (e_1,x_2)\big)\cdot\big((y_1,e_2),\ (e_1,y_2)\big)=f(x_1,x_2)\cdot f(x_2,y_2)$$ ■

Σχόλιο 2.7.7. Έστω $(G,\cdot)=(G_1\times G_2,\cdot)$ η ομάδα ευθύ γινόμενο δύο ομάδων $(G_1,\cdot)$ και $(G_2,\cdot)$, και έστω $\widetilde{G}_1=G_1\times\{e_2\}$, και $\widetilde{G}_2=\{e_1\}\times G_2$. Σύμφωνα με την Πρόταση 2.7.6, θα έχουμε: $G=\widetilde{G}_1\cdot\widetilde{G}_2=\widetilde{G}_2\cdot\widetilde{G}_1$. Παρατηρούμε ότι ισχύει το εξής ισχυρότερο:

$$\forall a\in\widetilde{G}_1,\quad\forall b\in\widetilde{G}_2:\qquad a\cdot b=b\cdot a$$

Πράγματι, θα έχουμε $a=(x,e_2)$, για κάποιο $x\in G_1$ και $b=(e_1,y)$ για κάποιο $y\in G_2$. Τότε: $a\cdot b=(x,e_2)\cdot(e_1,y)=(x,y)=(e_1,y)\cdot(x,e_2)=b\cdot a$. $\surd$

2.7.2 Εσωτερικό Ευθύ Γινόμενο (Υπο)ομάδων

Με βάση την παραπάνω Πρόταση 2.7.6 η ομάδα ευθύ γινόμενο $G=G_1\times G_2$ καθορίζεται μοναδικά από τις κανονικές υποομάδες της $\widetilde{G}_i$, $i=1,2$, και έτσι οδηγούμαστε φυσιολογικά στον ακόλουθο ορισμό.

Ορισμός 2.7.8. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και H και K είναι δύο υποομάδες της G. Η ομάδα G καλείται η ομάδα* **εσωτερικό ευθύ γινόμενο** *των υποομάδων H και K, αν:*

1. *Οι υποομάδες H και K είναι κανονικές υποομάδες της G: $H\trianglelefteq G$ και $K\trianglelefteq G$.*
2. *$G=H\cdot K$ (ή ισοδύναμα $G=K\cdot H$).*
3. *$H\cap K=\{e\}$.*

Επομένως από την Πρόταση 2.7.6, έπεται το ακόλουθο πόρισμα.

Πόρισμα 2.7.9. *Έστω $(G,\cdot)=(G_1\times G_2,\cdot)$ η ομάδα εξωτερικό ευθύ γινόμενο δύο ομάδων $(G_1,\cdot)$ και $(G_2,\cdot)$. Τότε η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της $G_1\times\{e_2\}$ και $\{e_1\}\times G_2$.*

Παράδειγμα 2.7.10. 1. Θεωρούμε την ομάδα $\mathcal{V}_4 = \{e, a, b, c\}$ των τεσσάρων στοιχείων του Klein. Θέτουμε $H_1 = \{e, a\}$ και $H_2 = \{e, b\}$. Επειδή η $\mathcal{V}_4$ είναι αβελιανή, έπεται ότι κάθε υποομάδα της είναι κανονική. Άρα $H_i \trianglelefteq \mathcal{V}_4$, $i = 1, 2$, και προφανώς $H_1 \bigcap H_2 = \{e\}$. Τέλος, $H_1 \cdot H_2 = \{e, a\} \cdot \{e, b\} = \{e, a, b, a \cdot b\} = \{e, a, b, c\} = \mathcal{V}_4$. Επομένως η ομάδα $\mathcal{V}_4$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της H_1 και H_2.

Παρατηρούμε ότι η απεικόνιση

$$f : \mathcal{V}_4 \longrightarrow H_1 \times H_2, \quad f(e) = (e, e), \quad f(a) = (a, e), \quad f(b) = (e, b), \quad f(c) = (a, b)$$

είναι «1-1» και «επί» και διατηρεί τις πράξεις, δηλαδή: $f(x \cdot y) = f(x) \cdot f(y)$, $\forall x, y \in \mathcal{V}_4$.

2. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{C}^*, \cdot)$ των μη μηδενικών μιγαδικών αριθμών. Θεωρούμε τις υποομάδες της $\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ και $\mathbb{R}^{>0} = \{r \in \mathbb{R} \subseteq \mathbb{C} \mid r > 0\}$. Επειδή η ομάδα $\mathbb{C}^*$ είναι αβελανή, έπεται ότι κάθε υποομάδα της είναι κανονική. Άρα $\mathsf{T} \trianglelefteq \mathbb{C}^* \trianglerighteq \mathbb{R}^{>0}$. Αν $z \in \mathsf{T} \bigcap \mathbb{R}^{>0}$, τότε $z \in \mathbb{R}^{>0}$ και $|z| = z^2 = 1$, από όπου προφανώς έχουμε $z = 1$. Άρα $\mathsf{T} \bigcap \mathbb{R}^{>0} = \{1\}$. Τέλος, για κάθε μη μηδενικό μιγαδικό αριθμό z, έχουμε $z = \frac{z}{|z|} \cdot |z|$, όπου, επειδή $|\frac{z}{|z|}| = 1$, θα έχουμε $\frac{z}{|z|} \in \mathsf{T}$, και προφανώς $|z| \in \mathbb{R}^{>0}$. Επομένως $z \in \mathsf{T} \cdot \mathbb{R}^{>0}$, δηλαδή $\mathbb{C}^* = \mathsf{T} \cdot \mathbb{R}^{>0}$. Άρα η ομάδα $\mathbb{C}^*$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της T και $\mathbb{R}^{>0}$.

Παρατηρούμε ότι η απεικόνιση

$$f : \mathbb{C}^* \longrightarrow \mathsf{T} \times \mathbb{R}^{>0}, \quad f(z) = \left(\frac{z}{|z|}, |z|\right)$$

είναι «1-1» και «επί» και διατηρεί τις πράξεις, δηλαδή: $f(x \cdot y) = f(x) \cdot f(y)$, $\forall x, y \in \mathbb{C}^*$. $\surd$

Με βάση την παραπάνω ανάλυση, προκύπτει το πρόβλημα ορισμού εσωτερικού ευθέος γινομένου τριών ή περισσότερων υποομάδων μιας ομάδας. Μια πρώτη προσέγγιση θα ήταν να ορίσουμε ότι μια ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της H_1, H_2, $\cdots$, H_n, αν:

1. Κάθε υποομάδα H_i είναι κανονική, $1 \leq i \leq n$: $H_i \trianglelefteq G$.
2. $G = H_1 \cdot H_2 \cdots H_n$.
3. $H_i \cap H_j = \{e\}$, αν $1 \leq i \neq j \leq n$.

Τότε, όπως στην Πρόταση 2.7.6, θα έπρεπε κάθε στοιχείο a της ομάδας G να γράφεται μοναδικά ως γινόμενο $a_1 \cdot a_2 \cdots a_n$, όπου $a_i \in H_i$, $1 \leq i \leq n$. Το ακόλουθο παράδειγμα δείχνει ότι η παραπάνω προσέγγιση δεν είναι απολύτως σωστή:

Παράδειγμα 2.7.11. Θεωρούμε την ομάδα $\mathcal{V}_4 = \{e, a, b, c\}$ των τεσσάρων στοιχείων του Klein. Θέτουμε $H_1 = \{e, a\}$, $H_2 = \{e, b\}$, και $H_3 = \{e, c\}$. Τότε:

1. Οι υποομάδες H_i είναι κανονικές υποομάδες της $\mathcal{V}_4$, , $1 \leq i \leq 3$: $H_i \trianglelefteq \mathcal{V}_4$.

   Πράγματι αυτό προκύπτει διότι η $\mathcal{V}_4$ είναι αβελιανή και άρα κάθε υποομάδα της είναι κανονική.

2. $\mathcal{V}_4 = H_1 \cdot H_2 \cdot H_3$.

   Επειδή $a^2 = e$, $a = b \cdot c$, $b = a \cdot c$, και $c = b \cdot a$, έπεται άμεσα ότι $\mathcal{V}_4 = H_1 \cdot H_2 \cdot H_3$.

3. $H_1 \bigcap H_2 = H_1 \bigcap H_3 = H_2 \bigcap H_3 = \{e\}$.

   Προκύπτει άμεσα από την περιγραφή των υποομάδων H_i, $1 \leq i \leq 3$.

4. Υπάρχει στοιχείο της ομάδας $\mathcal{V}_4$ το οποίο δεν γράφεται μοναδικά ως γινόμενο στοιχείων των υποομάδων H_i, $1 \leq i \leq 3$.

   Πράγματι, έχουμε $e = e \cdot e \cdot e$ και $e = a \cdot b \cdot c$, και $e, a \in H_1$, $e, b \in H_2$, και $e, c \in H_2$, αλλά $a \neq e$, $b \neq e$, και $c \neq e$. Παρόμοια $a = a \cdot e \cdot e = e \cdot b \cdot c$, και $a \neq e$, $e \neq b$, και $e \neq c$.

5. Δεν υπάρχει «1-1» και «επί» απεικόνιση $V_4 \longrightarrow H_1 \times H_2 \times H_3$ (η οποία διατηρεί τις πράξεις των εμπλεκόμενων ομάδων.

   Πράγματι, $|V_4| = 4 \neq 8 = |H_1 \times H_2 \times H_3|$. $\surd$

Με βάση τις παραπάνω παρατηρήσεις, οδηγούμαστε στον ακόλουθο ορισμό εσωτερικού ευθέος γινομένου υποομάδων μιας ομάδας.

Ορισμός 2.7.12. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και H_1, H_2, $\cdots$, H_n είναι υποομάδες της G. Η ομάδα G καλείται η ομάδα* **εσωτερικό ευθύ γινόμενο** *των υποομάδων H_i, $1 \leq i \leq n$, αν:*

1. *Οι υποομάδες H_i είναι κανονικές υποομάδες της G, $1 \leq i \leq n$: $H_i \trianglelefteq G$.*
2. *$G = H_1 \cdot H_2 \cdots H_n$.*
3. *$\forall i = 1,2,\cdots,n$: $H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n\big) = \{e\}$.*

Παρατήρηση 2.7.13. Αν η ομάδα G έχει δοθεί με προσθετικό συμβολισμό: $(G,+)$, και αν το ουδέτερο στοιχείο της συμβολίζεται με 0, τότε η ομάδα G είναι το εσωτερικό γινόμενο υποομάδων της $H_1, H_2, \cdots, H_n$, αν:

1. Οι υποομάδες H_i είναι κανονικές υποομάδες της G, $1 \leq i \leq n$: $H_i \trianglelefteq G$.
2. $G = H_1 + H_2 + \cdots + H_n$.
3. $\forall i = 1,2,\cdots,n$: $H_i \bigcap \big(H_1 + H_2 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_n\big) = \{0\}$. ▲

Η ακόλουθη Πρόταση περιγράφει τις βασικές ιδιότητες ομάδων οι οποίες είναι εσωτερικά ευθέα γινόμενα πεπερασμένου πλήθους υποομάδων της.

Πρόταση 2.7.14. *Έστω ότι $(G,\cdot)$ μια ομάδα και ότι H_1, H_2, $\cdots$, H_n είναι υποομάδες της G. Αν η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H_i, $1 \leq i \leq n$, τότε:*

1. *(α′) Αν $1 \leq i \neq j \leq n$, τότε: $H_i \cap H_j = \{e\}$.*
   (β′) Αν $1 \leq i \neq j \leq n$, και $h_i \in H_i$ και $h_j \in H_j$, τότε: $h_i \cdot h_j = h_j \cdot h_i$.
   Ιδιαίτερα: $H_i \cdot H_j = H_j \cdot H_i$.
2. *Κάθε στοιχείο a της ομάδας G γράφεται κατά μοναδικό τρόπο ως γινόμενο:*

$$a = h_1 \cdot h_2 \cdots h_n, \quad \text{όπου} \quad h_i \in H_i, \ \ 1 \leq i \leq n$$

   Δηλαδή, αν επίσης έχουμε: $a = h_1' \cdot h_2' \cdots h_n'$, όπου $h_i' \in H_i$, $1 \leq i \leq n$, τότε: $h_i = h_i'$, $1 \leq i \leq n$.
   Ιδιαίτερα: $G = \langle H_1 \bigcup H_2 \bigcup \cdots \bigcup H_n \rangle$.
3. *Η απεικόνιση*

$$f : G \longrightarrow H_1 \times H_2 \times \cdots \times H_n, \quad a = h_1 \cdot h_2 \cdots h_n \longmapsto f(a) = (h_1, h_2, \cdots, h_n)$$

   είναι «1-1», «επί», και διατηρεί τις πράξεις των εμπλεκόμενων ομάδων.[16]

Απόδειξη. 1. (α′) Θεωρούμε δείκτες i και j, όπου $1 \leq i \neq j \leq n$, και έστω $x \in H_i \bigcap H_j$. Επειδή $i \neq j$, θα έχουμε ότι $H_j \subseteq H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_j \cdots H_n$, διότι κάθε στοιχείο $h_j \in H_j$ μπορεί να γραφεί ως $h_j = e \cdot e \cdots e \cdot e \cdots h_j \cdots e$. Επομένως $x \in H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_j \cdots H_n\big) = \{e\}$. Άρα $H_i \bigcap H_j = \{e\}$.

(β′) Θεωρούμε δείκτες i και j, όπου $1 \leq i \neq j \leq n$, και έστω $h_i \in H_i$ και $h_j \in H_j$. Επειδή $h_i^{-1} \in H_i$ και $h_j \in H_j$ και οι υποομάδες H_i και H_j είναι κανονικές, θα έχουμε:

$$h_j \cdot h_i^{-1} \cdot h_j^{-1} \in H_i \quad \Longrightarrow \quad h_i \cdot h_j \cdot h_i^{-1} \cdot h_j^{-1} \in H_i \quad \Longrightarrow \quad [h_i, h_j] \in H_i$$

[16] Όπως θα δούμε στην επόμενη ενότητα, η απεικόνιση f είναι ένας ισομορφισμός ομάδων.

$$h_i \cdot h_j \cdot h_i^{-1} \in H_j \implies h_i \cdot h_j \cdot h_i^{-1} \in H_j \cdot h_j^{-1} \in H_j \implies [h_i, h_j] \in H_j$$

Από τις παραπάνω σχέσεις, έχουμε: $[h_i, h_j] \in H_i \cap H_j$. Επειδή από το (α') έχουμε $H_i \cap H_j = \{e\}$, έπεται ότι $e = [h_i, h_j] = h_i \cdot h_j \cdot h_i^{-1} \cdot h_j^{-1} = (h_i \cdot h_j) \cdot (h_j \cdot h_i)^{-1}$ και επομένως $h_i \cdot h_j = h_j \cdot h_i$. Ιδιαίτερα: $H_i \cdot H_j = H_j \cdot H_i$.

2. Από το μέρος 2. του Ορισμού 2.7.12, έπεται ότι κάθε στοιχείο a της ομάδας G γράφεται ως γινόμενο $a = h_1 \cdot h_2 \cdots h_n$, όπου $h_i \in H_i$, $1 \le i \le n$. Ας υποθέσουμε ότι έχουμε και μια διαφορετική γραφή του a ως γινομένου στοιχείων από τις υποομάδες H_i: $a = h_1' \cdot h_2' \cdots h_n'$, όπου $h_i' \in H_i$, $1 \le i \le n$. Τότε για κάθε δείκτη $i = 1, 2, \cdots, n$, θα έχουμε:

$$h_1 \cdot h_2 \cdots h_n = h_1' \cdot h_2' \cdots h_n' \implies h_i \cdot (h_1 \cdot h_2 \cdots h_{i-1} \cdot h_{i+1} \cdots h_n) = h_i' \cdot (h_1' \cdot h_2' \cdots h_{i-1}' \cdot h_{i+1}' \cdots h_n') \implies$$

$$\implies (h_i')^{-1} \cdot h_i = (h_1' \cdot h_2' \cdots h_{i-1}' \cdot h_{i+1}' \cdots h_n') \cdot (h_1 \cdot h_2 \cdots h_{i-1} \cdot h_{i+1} \cdots h_n)^{-1} \implies$$

$$\implies (h_i')^{-1} \cdot h_i = (h_1' \cdot h_2' \cdots h_{i-1}' \cdot h_{i+1}' \cdots h_n') \cdot (h_n^{-1} \cdots h_{i+1}^{-1} \cdot h_{i-1}^{-1} \cdots h_2^{-1} \cdot h_1^{-1})$$

Χρησιμοποιώντας διαδοχικά ότι $h_i \cdot h_j = h_j \cdot h_i$, $1 \le i \ne j \le n$, η τελευταία σχέση γράφεται:

$$(h_i')^{-1} \cdot h_i = (h_1' \cdot h_1^{-1}) \cdot (h_2' \cdot h_2^{-1}) \cdots (h_{i-1}' \cdot h_{i-1}^{-1}) \cdot (h_{i+1}' \cdot h_{i+1}^{-1}) \cdots (h_n' \cdot h_n^{-1})$$

Στην παραπάνω ισότητα, το πρώτο μέλος ανήκει στην υποομάδα H_i και το δεύτερο μέλος στην υποομάδα $H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n$. Άρα το στοιχείο $(h_i')^{-1} \cdot h_i$ ανήκει στην υποομάδα $H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n\big)$, η οποία από το μέρος 3. του Ορισμού 2.7.12, είναι η τετριμμένη υποομάδα $\{e\}$. Έτσι $(h_i')^{-1} \cdot h_i = e$, και επομένως $h_i = h_i'$. Επειδή ο δείκτης $i = 1, 2, \cdots, n$ ήταν τυχαίος, έπεται ότι $h_i = h_i'$, $1 \le i \le n$, και επομένως η γραφή του a ως γινόμενο στοιχείων των υποομάδων H_i, $1 \le i \le n$, είναι μοναδική.

3. Επειδή από το μέρος 2., κάθε στοιχείο $a \in G$ γράφεται μοναδικά ως $a = h_1 \cdot h_2 \cdots h_n$, όπου $h_i \in H_i$, $1 \le i \le n$, ορίζεται η απεικόνιση

$$f : G \longrightarrow H_1 \times H_2 \times \cdots \times H_n, \quad a = h_1 \cdot h_2 \cdots h_n \longmapsto f(a) = (h_1, h_2, \cdots, h_n)$$

Η απεικόνιση f είναι «1-1» διότι αν $a = h_1 \cdot h_2 \cdots h_n$ και $b = h_1' \cdot h_2' \cdots h_n'$, όπου $h_i, h_i' \in H_i$, $1 \le i \le n$, και ισχύει ότι $f(a) = f(b)$, τότε θα έχουμε $(h_1, h_2, \cdots, h_n) = (h_1', h_2', \cdots, h_n')$, και άρα $h_i = h_i'$, $1 \le i \le n$, δηλαδή $a = b$. Προφανώς η f είναι «επί», διότι για κάθε στοιχείο $(h_1, h_2, \cdots, h_n) \in H_1 \times H_2 \times \cdots \times H_n$, έχουμε $f(h_1 \cdot h_2 \cdots h_n) = (h_1, h_2, \cdots, h_n)$. Τέλος, αν $b = h_1' \cdot h_2' \cdots h_n' \in G$ είναι ένα άλλο στοιχείο της G, όπου $h_i' \in H_i$, $1 \le i \le n$, τότε, χρησιμοποιώντας διαδοχικά ότι για τυχόντα στοιχεία $x_i \in H_i$ και $x_j \in H_j$, ισχύει ότι: $x_i \cdot x_j = x_j \cdot x_i$, $1 \le i \ne j \le n$, θα έχουμε:

$$f(a \cdot b) = f\big((h_1 \cdot h_2 \cdots h_n) \cdot (h_1' \cdot h_2 \cdots h_n)\big) = f\big(h_1 \cdot h_1' \cdot h_2 \cdot h_2' \cdots h_n \cdot h_n'\big) =$$

$$= \big(h_1 \cdot h_1', h_2 \cdot h_2', \cdots, h_n \cdot h_n'\big) = (h_1, \cdot h_2, \cdots h_n) \cdot (h_1', h_2', \cdots, h_n') = f(a) \cdot f(b) \qquad \blacksquare$$

Η ακόλουθη Πρόταση παρουσιάζει το αντίστροφο της Πρότασης 2.7.14.

Πρόταση 2.7.15. *Έστω $(G, \cdot)$ μια ομάδα η οποία περιέχει κανονικές υποομάδες $H_i \trianglelefteq G$, $1 \le i \le n$, έτσι ώστε κάθε στοιχείο $a \in G$ γράφεται μοναδικά ως $a = h_1 \cdot h_2 \cdots h_n$, όπου $h_i \in H_i$, $1 \le i \le n$. Τότε η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H_i, $1 \le i \le n$.*

Απόδειξη. Από την υπόθεση, βλέπουμε άμεσα ότι ικανοποιούνται οι συνθήκες 1. και 2. του Ορισμού 2.7.12, και άρα μένει να δείξουμε ότι ικανοποιείται και η συνθήκη 3., δηλαδή: $\forall i = 1, 2, \cdots, n$: $H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n\big) = \{e\}$. Έστω $x \in H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n\big)$, όπου $i \in \{1, 2, \cdots, n\}$. Τότε $x = h_1 \cdot h_2 \cdots h_{i-1} \cdot h_{i+1} \cdots h_n$, όπου $h_j \in H_j$, $1 \le j \ne i \le n$. Τότε, θέτοντας $e_j = e \in H_j$, $1 \le j \ne i \le n$, θα έχουμε:

$$x = e_1 \cdot e_2 \cdots e_{i-1} \cdot x \cdot e_{i+1} \cdots e_n = h_1 \cdot h_2 \cdots h_{i-1} \cdot e \cdot h_{i+1} \cdots h_n$$

Από την μοναδικότητα της γραφής του x ως γινομένου στοιχείων των υποομάδων H_k, $1 \le k \le n$, έπεται ότι: $x = e$ (και $h_j = e$, $1 \le j \ne i \le n$). Επομένως δείξαμε ότι για κάθε $i = 1, 2, \cdots, n$, ισχύει ότι $H_i \bigcap \big(H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n\big) = \{e\}$, και άρα η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H_i, $1 \le i \le n$. $\blacksquare$

Πρόταση 2.7.16. *Έστω ότι* $(G,\cdot)=(\prod_{k=1}^{n}G_k,\cdot)$ *είναι η ομάδα εξωτερικό ευθύ γινόμενο πεπερασμένου πλήθους ομάδων* $\{(G_k,\cdot)\}_{k=1}^{n}$, *και θέτουμε,* $\forall k=1,2,\cdots,n$*:*

$$\widetilde{G}_k=\{e_1\}\times\cdots\{e_{k-1}\}\times G_k\times\{e_{k+1}\}\times\cdots\times\{e_n\}=\{(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\ \in\ \prod_{k=1}^{n}G_k\ \mid\ x\in G_k\}$$

Τότε η ομάδα G *είναι το εσωτερικό ευθύ γινόμενο των υποομάδων* $\widetilde{G}_k$, $1\le k\le n$.

Απόδειξη. 1. Τα υποσύνολα $\widetilde{G}_k$, $i=1,2$, περιέχουν προφανώς το ουδέτερο στοιχείο $e_G=(e_1,e_2,\cdots,e_n)$ της $G=G_1\times G_2\times\cdots\times G_n)$, και άρα $\widetilde{G}_k\neq\emptyset$, $1\le k\le n$. Άν $\mathsf{x},\mathsf{y}\in\widetilde{G}_k$, τότε θα έχουμε $\mathsf{x}=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)$ και $\mathsf{y}=(e_1,\cdots,e_{k-1},y,e_{k+1},\cdots,e_n)$, όπου $x,y\in G_k$, και επομένως:

$$\mathsf{x}\cdot\mathsf{y}^{-1}=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\cdot(e_1,\cdots,e_{k-1},y^{-1},e_{k+1},\cdots,e_n)=(e_1,\cdots,e_{k-1},x\cdot y^{-1},e_{k+1},\cdots,e_n)\ \in\ \widetilde{G}_k$$

Επομένως το υποσύνολο $\widetilde{G}_k$, $1\le k\le n$, είναι μια υποομάδα της G.

Έστω $\mathsf{a}=(a_1,a_2,\cdots,a_n)\in G$ και $\mathsf{x}=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\in\widetilde{G}_k$. Τότε θα έχουμε:

$$\mathsf{a}\cdot\mathsf{x}\cdot\mathsf{a}^{-1}=(a_1,a_2,\cdots,a_n)\cdot(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\cdot(a_1^{-1},a_2^{-1},\cdots,a_n^{-1})=$$

$$=(a_1\cdot e_1\cdot a_1^{-1},\ \cdots,\ a_{k-1}\cdot e_{k-1}\cdot a_{k-1}^{-1},\ a_k\cdot x_k\cdot a_k^{-1},\ a_{k+1}\cdot e_{k+1}\cdot a_{k+1}^{-1},\ \cdots,\ a_n\cdot e_n\cdot a_n^{-1})=$$

$$=(e_1,\cdots,e_{k-1},a_k\cdot x_k\cdot a_k^{-1},e_{k+1},\cdots,e_n)\ \in\ \widetilde{G}_k$$

Επομένως από την Πρόταση 2.6.2, έπεται ότι το υποσύνολο $\widetilde{G}_k$, $1\le k\le n$, είναι μια κανονική υποομάδα της G.

2. Έστω $\mathsf{a}=(a_1,a_2,\cdots,a_n)\in G$. Τότε θέτοντας $\widetilde{\mathsf{a}}_k=(e_1,\cdots,e_{k-1},a_k,e_{k+1},\cdots,a_n)\in\widetilde{G}_k$, $1\le k\le n$, θα έχουμε

$$\mathsf{a}=(a_1,a_2,\cdots,a_n)=(a_1,e_2,\cdots,e_n)\cdot(e_1,a_2,\cdots,e_n)\cdots(e_1,e_2,\cdots,a_n)=\widetilde{\mathsf{a}}_1\cdot\widetilde{\mathsf{a}}_2\cdots\widetilde{\mathsf{a}}_n$$

Η παραπάνω σχέση δείχνει ότι $G=\widetilde{G}_1\cdot\widetilde{G}_2\cdots\widetilde{G}_n$.

3. Αν $k\in\{1,2,\cdots,n\}$, έστω $\mathsf{a}=(a_1,a_2,\cdots,a_n)\in\widetilde{G}_k\bigcap\big(\widetilde{G}_1\cdots\widetilde{G}_{k-1}\cdot\widetilde{G}_{k+1}\cdots\widetilde{G}_n\big)$. Επειδή $\mathsf{a}\in\widetilde{G}_k$, θα έχουμε $a_i=e_i$, $1\le i\neq k\le n$, και άρα $\mathsf{a}=(e_1,\cdots,e_{k-1},a_k,e_{k+1},\cdots,e_n)$. Επειδή $\mathsf{a}\in\widetilde{G}_1\cdots\widetilde{G}_{k-1}\cdot\widetilde{G}_{k+1}\cdots\widetilde{G}_n$, έπεται ότι θα έχουμε $\mathsf{a}=\mathsf{x}_1\cdots\mathsf{x}_{k-1}\cdot\mathsf{x}_{k+1}\cdots\mathsf{x}_n$, όπου $\mathsf{x}_j=(e_1,\cdots,e_{j-1},x_j,e_{j+1},\cdots,e_n)$, $1\le j\neq k\le n$, και άρα $\mathsf{x}_1\cdots\mathsf{x}_{k-1}\cdot\mathsf{x}_{k+1}\cdots\mathsf{x}_n=(x_1,\cdots,x_{k-1},e_k,x_{k+1},\cdots,x_n)$. Τότε:

$$\mathsf{a}=\mathsf{x}_1\cdots\mathsf{x}_{k-1}\cdot\mathsf{x}_{k+1}\cdots\mathsf{x}_n\ \implies\ (e_1,\cdots,e_{k-1},a_k,e_{k+1},\cdots,e_n)=(x_1,\cdots,x_{k-1},e_k,x_{k+1},\cdots,x_n)\ \implies\ a_k=e_k$$

και επομένως $\mathsf{a}=(e_1,e_2\cdots,e_n)=e$. Συνοψίζοντας, δείξαμε ότι $\widetilde{G}_k\bigcap\big(\widetilde{G}_1\cdots\widetilde{G}_{k-1}\cdot\widetilde{G}_{k+1}\cdots\widetilde{G}_n\big)=\{e\}$.

Από τα μέρη 1., 2., 3., έπεται ότι η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $\widetilde{G}_k$, $1\le k\le n$. ■

2.8 Ισομορφισμοί Ομάδων

Στην παρούσα ενότητα θα δώσουμε απάντηση στο ερώτημα: *«Πότε δύο ομάδες είναι δομικά ίδιες;»* Δηλαδή πότε δύο ομάδες έχουν τις ίδιες ιδιότητες οι οποίες απορρέουν από τα αξιώματα ομάδας, και επομένως μπορούμε να τις ταυτίζουμε ως ομάδες, μη λαμβάνοντας υπόψη τη φύση της πράξης με την οποία είναι εφοδιασμένα ή τη φύση των στοιχείων τους;

Για να απαντήσουμε στο παραπάνω ερώτημα, θα πρέπει να απαντήσουμε στο ερώτημα *«ποιος είναι ο κατάλληλος τρόπος να συγκρίνουμε δύο ομάδες* $(G_1,\star)$ *και* $(G_2,*)$*;»* Αν τα σύνολα G_1 και G_2 είναι δύο σύνολα χωρίς επιπλέον δομή, ο φυσιολογικός τρόπος με τον οποίο μπορούμε να τα συγκρίνουμε ή να τα συσχετίσουμε ή να αναλύσουμε κοινές τους ιδιότητες είναι μέσω μιας απεικόνισης $f\colon G_1\longrightarrow G_2$, και τότε μπορούμε να πούμε ότι τα G_1 και G_2 είναι «ίδια» ως σύνολα αν συνδέονται μέσω μιας «1-1» και «επί» απεικόνισης.

Ανάλογα, αν τα σύνολα G_1 και G_2 είναι εφοδιασμένα με επιπλέον αλγεβρική δομή παρόμοιου τύπου, για παράδειγμα, αν τα σύνολα G_1 και G_2 έχουν δομή ομάδας, μέσω πράξεων «$\star$» και «$*$» αντίστοιχα, τότε ο

φυσιολογικός τρόπος σύγκρισής τους ή συσχέτισής τους είναι μέσω μιας απεικόνισης $f\colon G_1 \longrightarrow G_2$ η οποία διατηρεί την κοινή αλγεβρική δομή. Τότε μπορούμε να πούμε ότι οι ομάδες G_1 και G_2 είναι «δομικά ίδιες» ως ομάδες αν υπάρχει μια «1-1» και «επί» απεικόνιση $f\colon G_1 \longrightarrow G_2$ η οποία διατηρεί την αλγεβρική δομή. Λαμβάνοντας υπόψη ότι η αλγεβρική δομή σε μια ομάδα καθορίζεται από την πράξη της ομάδας (και τα αξιώματα τα οποία αυτή ικανοποιεί), οδηγούμαστε φυσιολογικά στην έννοια του *ομομορφισμού ομάδων*, η οποία είναι η κάταλληλη έννοια σύγκρισης ή συσχέτισης ομάδων, και στην έννοια του *ισομορφισμού ομάδων*, η οποία είναι η κατάλληλη έννοια μέσω της οποίας μπορούμε να θεωρούμε ομάδες ως δομικά ίδιες.

Ορισμός 2.8.1. *Έστω $(G_1,\star)$ και $(G_2,*)$ δύο ομάδες. Μια απεικόνιση $f\colon G_1 \longrightarrow G_2$ καλείται* **ομομορφισμός ομάδων** *αν:*

$$\forall x_1, x_2 \in X: \quad f(x_1 \star x_2) = f(x_1) * f(x_2)$$

Το σύνολο όλων των ομομορφισμών ομάδων από την ομάδα $(G_1,\star)$ στην ομάδα $(G_2,*)$ συμβολίζεται με:

$$\mathsf{Hom}_{\mathrm{Grp}}(G_1,G_2) = \{f\colon G_1 \longrightarrow G_2 \mid f:\ \textit{ομομορφισμός ομάδων}\}$$

Παρατήρηση 2.8.2. Είδαμε ότι ο κατάλληλος τρόπος μέσω του οποίου μπορούμε να συσχετίσουμε ή να συγκρίνουμε δύο ομάδες είναι μέσω ενός ομομορφισμού ομάδων. Έτσι, αν μια απεικόνιση $f\colon (G_1,\star) \longrightarrow (G_2,*)$ μεταξύ ομάδων είναι ομομορφισμός, τότε μπορούμε μέσω της f να συγκρίνουμε τα σύνολα G_1 και G_2 ως ομάδες, δηλαδή λαμβάνοντας υπόψη την επιπλέον δομή με την οποία είναι εφοδιασμένα. Σ' αυτό το πλαίσιο τίθεται φυσιολογικά το ερώτημα:

Πότε δύο ομάδες είναι «δομικά ίδιες»;

δηλαδή πότε μπορούμε να ταυτίσουμε δύο ομάδες, με βάση τις ιδιότητες οι οποίες απορρέουν από τα αξιώματα ομάδας και μην λαμβάνοντας υπόψη τη φύση των στοιχείων ή της πράξης με την οποία είναι εφοδιασμένα;

Αν ο ομομορφισμός ομάδων $f\colon (G_1,\star) \longrightarrow (G_2,*)$ είναι απεικόνιση «1-1» και «επί», τότε μέσω της f τα στοιχεία των συνόλων G_1 και G_2 βρίσκονται σε αμφιμονοσήμαντη αντιστοιχία έτσι ώστε για κάθε $a,b \in G_1$, το στοιχείο $a\star b$ αντιστοιχεί μέσω της f με το στοιχείο $f(a)*f(b)$. Ως άμεση συνέπεια, έπεται ότι κάθε ιδιότητα της ομάδας $(G_1,\star)$ η οποία απορρέει από την πράξη «$\star$» και τα αξιώματα τα οποία ικανοποιεί, μεταφέρεται σε ανάλογη ιδιότητα της ομάδας $(G_2,*)$ και αντιστρόφως. Έτσι, για παράδειγμα, αν τα σύνολα G_1 και G_2 είναι πεπερασμένα, τότε οι πίνακες Cayley των ομάδων $(G_1,\star)$ και $(G_2,*)$ είναι δομικά ίδιοι, δηλαδή, αν εξαιρέσουμε την φύση των στοιχείων και της πράξης με τα οποία οι ομάδες είναι εφοδιασμένες, οι πίνακες είναι ουσιαστικά ταυτόσημοι, ενδεχομένως μετά από αναδιάταξη των στοιχείων των ομάδων. Με βάση τις παραπάνω παρατηρήσεις, οδηγούμαστε φυσιολογικά στην έννοια του ισομορφισμού ομάδων η οποία είναι η καταλληλότερη έννοια μέσω της οποίας μπορούμε να απαντήσουμε στο παραπάνω ερώτημα. ▲

Ορισμός 2.8.3. *Ένας ομομορφισμός ομάδων $f\colon (G_1,\star) \longrightarrow (G_2,*)$ καλείται* **ισομορφισμός ομάδων** *αν η απεικόνιση f είναι απεικόνιση «1-1» και «επί», και τότε θα συμβολίζουμε:*

$$f:\ (G_1,\star) \xrightarrow{\ \cong\ } (G_2,*)$$

Ένας ομομορφισμός ομάδων $f\colon (G,\cdot) \longrightarrow (G,\cdot)$ καλείται **ενδομορφισμός** *της $(G,\cdot)$. Ένας ισομορφισμός ομάδων $f\colon (G,\star) \longrightarrow (G,\star)$ καλείται* **αυτομορφισμός** *της $(G,\star)$.*

Γενικότερα ο ομομορφισμός ομάδων $f\colon (G_1,\star) \longrightarrow (G_2,*)$ καλείται:

1. **μονομορφισμός ομάδων**, αν η f είναι απεικόνιση «1-1».
2. **επιμορφισμός ομάδων**, αν η f είναι απεικόνιση «επί».

Παράδειγμα 2.8.4. 1. Για κάθε ομάδα $(G,\cdot)$ η ταυτοτική απεικόνιση $\mathsf{Id}_G\colon G \longrightarrow G$, $\mathsf{Id}_G(a) = a$ είναι προφανώς ένας ισομορφισμός ομάδων, δηλαδή ένας αυτομορφισμός της $(G,\cdot)$.

2. Αν $(G_1, \star)$ και $(G_2, *)$ είναι ομάδες με ουδέτερα στοιχεία e_1 και e_2 αντίστοιχα, τότε η απεικόνιση $f\colon G_1 \longrightarrow G_2,\ f(a) = e_2,\ \forall a \in G_1$, είναι ένας ομομορφισμός ομάδων, ο οποίος για προφανείς λόγους καλείται ο **τετριμμένος ομομορφισμός**.

3. Έστω H μια υποομάδα μιας ομάδας $(G, \cdot)$. Τότε η απεικόνιση έγκλεισης $\iota\colon H \longrightarrow G$, $\iota(a) = a$, είναι ένας μονομορφισμός ομάδων. $\surd$

Παράδειγμα 2.8.5. Θεωρούμε την προσθετική ομάδα $(\mathbb{R}, +)$ των πραγματικών αριθμών, και την πολλαπλασιαστική ομάδα $(\mathbb{R}^+, \cdot)$ των θετικών πραγματικών αριθμών, όπου $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}$ και «+», «·» είναι οι συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών αντίστοιχα. Θεωρούμε την εκθετική και λογαριθμική απεικόνιση αντίστοιχα

$$f : \mathbb{R} \longrightarrow \mathbb{R}^+, \quad f(x) = e^x \qquad \text{και} \qquad g\colon \mathbb{R}^+ \longrightarrow \mathbb{R}, \quad g(x) = \log_e(x)$$

Τότε για τυχόντες πραγματικούς αριθμούς x, y και για τυχόντες θετικούς πραγματικούς αριθμούς z, w, θα έχουμε:

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

$$g(x \cdot y) = \log_e(x \cdot y) = \log_e(x) + \log_e(y) = g(x) + g(y)$$

Επομένως οι απεικονίσεις f και g είναι ομομορφισμοί ομάδων, και επειδή η απεικόνιση f είναι «1-1» και «επί» με αντίστροφη την απεικόνιση g, έπεται ότι οι απεικονίσεις f και g είναι ισομορφισμοί ομάδων.

Παρόμοια, για κάθε πραγματικό αριθμό $a > 1$, οι απεικονίσεις

$$f_a : \mathbb{R} \longrightarrow \mathbb{R}^+, \quad f(x) = a^x \qquad \text{και} \qquad g_a\colon \mathbb{R}^+ \longrightarrow \mathbb{R}, \quad g(x) = \log_a(x)$$

είναι ισομορφισμοί ομάδων και $g_a = f_a^{-1}$ (οι ισομορφισμοί f και g προκύπτουν θέτοντας $a = e$).

Επομένως, υπάρχει άπειρο, για την ακρίβεια μη αριθμήσιμο, πλήθος (ανά δύο διαφορετικών) ισομορφισμών μεταξύ των ομάδων $(\mathbb{R}, +)$ και $(\mathbb{R}^+, \cdot)$. $\surd$

Παράδειγμα 2.8.6. Θεωρούμε μια ομάδα $(G, \cdot)$ με ουδέτερο στοιχείο e, και έστω $(\mathbb{Z}, +)$ η προσθετική ομάδα των ακεραίων. Για κάθε στοιχείο $a \in G$, η απεικόνιση

$$f_a\colon \mathbb{Z} \longrightarrow G, \quad f_a(n) = a^n$$

είναι ένας ομομορφισμός ομάδων. Πράγματι, χρησιμοποιώντας τις ιδιότητες δυνάμεων, όπως περιγράφονται στην Πρόταση 2.1.5, θα έχουμε, $\forall n, m \in \mathbb{Z}$: $f_a(n+m) = a^{n+m} = a^n \cdot a^m = f_a(n) \cdot f_a(m)$. Επομένως η απεικόνιση f_x είναι ομομορφισμός μονοειδών. Παρατηρούμε ότι μπορούμε να θεωρήσουμε την απεικόνιση f ως απεικόνιση $f'\colon \mathbb{Z} \longrightarrow \langle a \rangle$, και τότε προφανώς η απεικόνιση f' είναι επιμορφισμός ομάδων, όπου $\langle a \rangle$ είναι η κυκλική υποομάδα της G η οποία παράγεται από το στοιχείο a. $\surd$

Παράδειγμα 2.8.7. Έστω $(G, \cdot)$ μια ομάδα, $x \in G$ ένα στοιχείο της και $H \leq G$ μια υποομάδα της. Τότε η συζυγής υποομάδα xHx^{-1} της H είναι ισόμορφη με την H:

$$H \cong xHx^{-1}$$

Πράγματι, θεωρούμε την απεικόνιση

$$f : H \longrightarrow xHx^{-1}, \quad f(h) = x \cdot h \cdot x^{-1}$$

η οποία, όπως στην απόδειξη της Πρότασης 2.5.8, είναι «1-1» και «επί». Επιπλέον, αν $h_1, h_2 \in H$, θα έχουμε:

$$f(h_1 \cdot h_2) = x \cdot (h_1 \cdot h_2) \cdot x^{-1} = x \cdot h_1 \cdot e \cdot h_2 \cdot x^{-1} = x \cdot h_1 \cdot x^{-1} \cdot x \cdot h_2 \cdot x^{-1} = f(h_1) \cdot f(h_2)$$

Επομένως η f είναι ομομορφισμός και άρα είναι ισομορφισμός ομάδων. $\surd$

Η επόμενη Πρόταση περιγράφει βασικές ιδιότητες ομομορφισμών ομάδων.[17]

Πρόταση 2.8.8. *Έστω ότι $(G_1,\star)$ και $(G_2,*)$ είναι ομάδες με ουδέτερα στοιχεία e_1 και e_2 αντίστοιχα.*

1. *Έστω $f\colon G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων. Τότε:*
   - *(α΄)* $f(e_1)=e_2$.
   - *(β΄)* $\forall a\in G_1\colon\ f(a^{-1})=f(a)^{-1}$.
   - *(γ΄)* *Αν* $a_1,\cdots,a_n\in G$, $n\geq 1$, *τότε:* $f(a_1\star\cdots\star a_n)=f(a_1)*\cdots*f(a_n)$.
   - *(δ΄)* $\forall a\in G_1,\ \forall n\in\mathbb{Z}\colon\ f(a^n)=f(a)^n$.
2. *Η σύνθεση ομομορφισμών (ισομορφισμών) ομάδων ομάδων είναι (ομομορφισμός) ισομορφισμός ομάδων.*
3. *(α΄) Αν ο ομομορφισμός ομάδων $f\colon (G_1,\star)\longrightarrow(G_2,*)$ είναι ισομορφισμός, τότε η αντίστροφη απεικόνιση $f^{-1}\colon G_2\longrightarrow G_1$ είναι ισομορφισμός ομάδων.*

   (β΄) Ένας ομομορφισμός ομάδων $f\colon (G_1,\star)\longrightarrow(G_2,*)$ είναι ισομορφισμός αν και μόνο αν υπάρχει ομομορφισμός ομάδων $g\colon (G_2,*)\longrightarrow(G_1,\star)$, έτσι ώστε:

$$f\circ g=\mathsf{Id}_{G_2}\qquad \textit{και}\qquad g\circ f=\mathsf{Id}_{G_1}$$

   και τότε $g=f^{-1}$.

Απόδειξη. 1. (α΄) Χρησιμοποιώντας τον Νόμο Διαγραφής στην ομάδα $(G_2,*)$, Θα έχουμε:

$$e_2*f(e_1)=f(e_1)=f(e_1\star e_1)=f(e_1)*f(e_1)\quad\Longrightarrow\quad e_2=f(e_1)$$

(β΄) Επειδή στην ομάδα G_1 έχουμε $a\star a^{-1}=e_1=a^{-1}\star a$, και επειδή η απεικόνιση f είναι ομομορφισμός και, από το μέρος (α΄), ισχύει $f(e_1)=e_2$, θα έχουμε:

$$f(a\star a^{-1})=f(e_1)=f(a^{-1}\star a)\quad\Longrightarrow\quad f(a)*f(a^{-1})=e_2=f(a^{-1})*f(a)\quad\Longrightarrow\quad f(a)^{-1}=f(a^{-1})$$

(γ΄) Η ζητούμενη σχέση ισχύει προφανώς όταν $n=1$, και όταν $n=2$ διότι η f είναι ομομορφισμός. Υποθέτουμε ότι η ζητούμενη σχέση ισχύει για n το πλήθος στοιχεία, και έστω $a_1,a_2,\cdots,a_{n+1}\in G_1$. Χρησιμοποιώντας ότι η f είναι ομομορφισμός και την επαγωγική υπόθεση, θα έχουμε:

$$f(a_1\star\cdots\star a_n\star a_{n+1})=f(a_1\star\cdots\star a_n)*f(a_{n+1})=f(a_1)*\cdots*f(a_n)*f(a_{n+1})$$

και άρα, από την Αρχή Μαθηματικής Επαγωγής, η ζητούμενη σχέση ισχύει για κάθε $n\geq 1$.

(δ΄) Αν $n=1$, τότε η ζητούμενη σχέση προκύπτει άμεσα από το μέρος (γ΄), θέτοντας $a_1=\cdots=a_n:=a$. Αν $n=0$, τότε $a^0=e_1$ και $f(a)^0=e_2$, και η ζητούμενη σχέσην προκύπτει από το μέρος (α΄). Υποθέτουμε ότι $n<0$, και άρα $n=-m$, όπου $m\geq 1$. Τότε $a^n=a^{-m}=(a^m)^{-1}$ και θα έχουμε:

$$f(a^n)=f((a^m)^{-1})=f(a^m)^{-1}=(f(a)^m)^{-1}=f(a)^{-m}=f(a)^n$$

(ε΄) Υποθέτουμε ότι ο ομομορφισμός $f\colon G_1\longrightarrow G_2$ είναι ισομορφισμός, και άρα υπάρχει η αντίστροφη απεικόνιση $f^{-1}\colon G_2\longrightarrow G_1$, η οποία είναι «1-1» και «επί». Έστω $x,y\in G_2$. Τότε υπάρχουν μοναδικά στοιχεία $a,b\in G_1$ έτσι ώστε: $f(a)=x$ και $f(b)=y$, και $f(c)=x*y$. Τότε θα έχουμε $f^{-1}(x)=a$, $f^{-1}(y)=b$, και $f^{-1}(x*y)=c$. Επειδή η f είναι ομομορφισμός, θα έχουμε $f(a\star b)=f(a)*f(b)=x*y=f(c)$, και επειδή η f είναι «1-1», θα έχουμε $a\star b=c$, ή ισοδύναμα $f^{-1}(x)\star f^{-1}(y)=f^{-1}(x*y)$. Επομένως η f^{-1} είναι ισομορφισμός ομάδων.

[17] Αν $f\colon (G_1,\star)\longrightarrow(G_2,*)$ είναι ένας ομομορφισμός ομάδων, τότε θεωρώντας την f ως απεικόνιση μεταξύ μονοειδών, ο Ορισμός 2.8.1 δεν εξασφαλίζει ότι η f είναι ομομορφισμός μονοειδών, διότι δεν γνωρίζουμε αν η f στέλνει το ουδέτερο στοιχείο της G_1 στο ουδέτερο στοιχείο της ομάδας $(G_2,*)$. Αυτό πραγματικά συμβαίνει, όπως πιστοποιεί το μέρος 1(α΄) της Πρότασης 2.8.8.

Άρα κάθε ομομορφισμός ομάδων είναι και ομομορφισμός των υποκείμενων μονοειδών, αλλά γενικά το αντίστροφο δεν ισχύει.

2. Έστω ότι $f\colon (G_1,\star)\longrightarrow(G_2,*)$ και $g\colon (G_2,*)\longrightarrow(G_3,\cdot)$ είναι ομομορφισμοί ομάδων. Τότε για τυχόντα στοιχεία $a,b\in G_1$, θα έχουμε:

$$(g\circ f)(a\star b)=g(f(a\star b))=g(f(a)*f(b))=g(f(a))\cdot g(f(b))=(g\circ f)(a)\cdot(g\circ f)(b)$$

Επομένως η σύνθεση $g\circ f\colon (G_1,\star)\longrightarrow(G_3,\cdot)$ είναι ομομορφισμός ομάδων.

3. Αν ο ομομορφισμός f είναι ισομορφισμός, τότε μπορούμε να διαλέξουμε $g=f^{-1}$ η οποία είναι ομομορφισμός από το μέρος 3(α'). Αντίστροφα, αν υπάρχει ομομορφισμός $g\colon (G_2,*)\longrightarrow(G_1,\star)$, έτσι ώστε $f\circ g=\mathsf{Id}_{G_2}$ και $g\circ f=\mathsf{Id}_{G_1}$, τότε η f είναι «1-1» και «επί», και άρα η απεικόνιση f είναι ισομορφισμός ομάδων. ■

Ορισμός 2.8.9. *Συμβολίζουμε με* **Grp** *την κλάση*[18] *όλων των ομάδων. Στην κλάση* **Grp** *ορίζουμε μια σχέση «$\cong$» ως εξής:*

$$\text{αν } (G_1,\star),(G_2,*)\in\mathbf{Grp} \text{ τότε: } (G_1,\star)\cong(G_2,*) \iff \text{υπάρχει ισομορφισμός ομάδων } f\colon(G_1,\star)\longrightarrow(G_2,*)$$

Η σχέση «$\cong$» καλείται **σχέση ισομορφίας** *στην κλάση των ομάδων, και δύο ομάδες $(G_1,\star)$ και $(G_2,*)$ καλούνται* **ισόμορφες**, *αν:* $(G_1,\star)\cong(G_2,*)$.

Με χρήση του Παραδείγματος 2.8.5, θα έχουμε: $(\mathbb{R},+)\cong(\mathbb{R}^+,\cdot)$.

Η ακόλουθη συνέπεια της Πρότασης 2.8.8 δείχνει ότι η σχέση ισομορφίας επί της κλάσης των ομάδων είναι μια σχέση ισοδυναμίας.

Πόρισμα 2.8.10. *Η* **σχέση ισομορφίας** *«$\cong$» η οποία ορίζεται στην κλάση* **Grp** *όλων των ομάδων είναι μια σχέση ισοδυναμίας.*

Απόδειξη. Επειδή για κάθε ομάδα $(G,\star)$, η ταυτοτική απεικόνιση $\mathsf{Id}_G\colon G\longrightarrow G$ είναι ισομορφισμός ομάδων, έπεται ότι $(G,\star)\cong(G,\star)$. Αν $(G_1,\star)$ και $(G_2,*)$ είναι ομάδες και ισχύει $(G_1,\star)\cong(G_2,*)$, τότε έστω $f\colon(G_1,\star)\longrightarrow(G_2,*)$ ένας ισομορφισμός ομάδων. Από την Πρόταση 2.8.8, η αντίστροφη απεικόνιση $f^{-1}\colon(G_2,*)\longrightarrow(G_1,\star)$ είναι επίσης ισομορφισμός ομάδων, έπεται ότι $(Y,*)\cong(X,\star)$. Τέλος, έστω ότι $(G_1,\star)$, $(G_2,*)$, και $(G_3,\cdot)$ είναι ομάδες και ισχύει $(G_1,\star)\cong(G_2,*)$ και $(G_2,*)\cong(G_3,\cdot)$ τότε υπάρχουν ισομορφισμοί ομάδων $f\colon(G_1,\star)\longrightarrow(G_2,*)$ και $g\colon(G_2,*)\longrightarrow(G_3,\cdot)$. Επειδή από την Πρόταση 2.8.8, η σύνθεση ομο(ισο)μορφισμών ένας ομο(ισο)μορφισμός ομάδων, έπεται ότι η σύνθεση $g\circ f\colon(G_1,\star)\longrightarrow(G_3,\cdot)$ είναι ένας ισομορφισμός ομάδων και επομένως: $(G_1,\star)\cong(G_3,\cdot)$. Συνοψίζουμε: η σχέση ισομορφίας «$\cong$» είναι μια σχέση ισοδυναμίας στηνν κλάση **Grp** των ομάδων. ■

Η σχέση ισομορφίας «$\cong$» διαμερίζει την κλάση **Grp** όλων των ομάδων σε κλάσεις ισομορφίας και, σύμφωνα με την Παρατήρηση 2.8.2, δύο ομάδες οι οποίες ανήκουν στην ίδια κλάση ισομορφίας έχουν τις ίδιες δομικές ιδιότητες, για παράδειγμα έχουν ταυτόσημο πίνακα Cayley.

Με βάση την έννοια του ισομορφισμού ομάδων, μπορούμε να διατυπώσουμε μια αυστηρή εκδοχή για το πότε μια ιδιότητα ομάδων είναι δομική ιδιότητα.

Παρατήρηση 2.8.11. Έστω (P) μια ιδιότητα την οποία μπορεί να ικανοποιεί ή μπορεί να μην ικανοποιεί μια ομάδα. Η ιδιότητα (P) καλείται **δομική ιδιότητα ομάδων** αν και μόνο αν ισχύει ότι:

$$\textit{μια ομάδα } (G,\star) \textit{ ικανοποιεί την ιδιότητα } (P) \iff$$

$$\textit{κάθε ομάδα } (G',*) \textit{ η οποία είναι ισόμορφη με την } (G,\star) \textit{ ικανοποιεί την ιδιότητα } (P)$$

Για παράδειγμα η ιδιότητα «*η ομάδα $(G,\cdot)$ είναι αβελιανή*» είναι δομική ιδιότητα ομάδων. Πράγματι, έστω $f\colon(G_1,\cdot)\longrightarrow(G_2,*)$ ένας ισομορφισμός μεταξύ των ομάδων $(G_1,\cdot)$ και $(G_2,*)$, και υποθέτουμε ότι η ομάδα

[18] Η συλλογή όλων των ομάδων δεν αποτελεί σύνολο. Όταν αναφερόμαστε σε μια σχέση ισοδυναμίας ή σε μια διαμέριση ορισμένης επί μιας κλάσης η οποία δεν είναι σύνολο, εννοούμε ότι η σχέση ισοδυναμίας ή η διαμέριση έχει τις τυπικές ιδιότητες τις οποίες έχει μια σχέση ισοδυναμίας ή μια διαμέριση ορισμένη επί ενός συνόλου.

$(G_1,\cdot)$ είναι αβελιανή. Αν $x,y\in G_2$, τότε, επειδή η f είναι απεικόνιση «επί», υπάρχουν στοιχεία $a,b\in G_1$ έτσι ώστε: $f(a)=x$ και $f(b)=y$. Επειδή η ομάδα G_1 είναι αβελιανή, θα έχουμε $a\cdot b=b\cdot a$, και επειδή η f είναι ομομορφισμός ομάδων, θα έχουμε $f(a\cdot b)=f(b\cdot a)\implies x*y=f(a)*f(b)=f(b)*f(a)=y*x$. Επομένως η ομάδα G_2 είναι αβελιανή.

Επίσης η ιδιότητα ότι «*το πλήθος των στοιχείων μιας ομάδας* $(G,\cdot)$ *είναι ίσο με* k είναι προφανώς δομική ιδιότητα ομάδων, διότι ικανοποιείται από κάθε ομάδα $(G',*)$ στην κλάση ισομορφίας της $(G,\cdot)$: $|G|=|G'|$.

Παρόμοια, οι ιδιότητες «*υπάρχει* $e\neq a\in G$*:* $a^2=e$» ή «*το πλήθος των στοιχείων* a *έτσι ώστε:* $a^2=e$ *είναι ίσο με* k», για μια ομάδα $(G,\cdot)$ είναι δομικές ιδιότητες ομάδων. Πράγματι, αν $f:(G_1,\cdot)\longrightarrow(G_2,*)$ είναι ένας ισομορφισμός μεταξύ των ομάδων $(G_1,\cdot)$ και $(G_2,*)$ με ουδέτερα στοιχεία e_1 και e_2 αντίστοιχα, και αν $a\in G_1$, τότε, χρησιμοποιώντας ότι η f είναι ισομορφισμός, θα έχουμε: $a^2=e_1\iff f(a^2)=f(a)^2=f(e_1)=e_2$, από όπου προκύπτει το ζητούμενο.

Αντίθετα, η ιδιότητα ότι «*το στοιχείο* -3 *ανήκει στην ομάδα* $(\mathbb{R},+)$» δεν είναι δομική ιδιότητα ομάδων διότι, όπως προκύπτει από το Παράδειγμα 2.8.5, η πολλαπλασιαστική ομάδα $(\mathbb{R}^+,\cdot)$ είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{R},+)$ και $-3\notin\mathbb{R}^+$. ▲

Είναι προφανές ότι, αν υπάρχει μια δομική ιδιότητα την οποία ικανοποιεί μια ομάδα $(G_1,\star)$ και την οποία δεν ικανοποιεί μια ομάδα $(G_2,*)$, τότε οι ομάδες $(G_1,\star)$ και $(G_2,*)$, δεν μπορεί να είναι ισόμορφες.

Παράδειγμα 2.8.12. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{R}^*,\cdot)$ των μη μηδενικών πραγματικών αριθμών, της οποίας το ουδέτερο στοιχείο είναι ο αριθμός 1, και την προσθετική ομάδα $(\mathbb{R},+)$ των πραγματικών αριθμών, της οποίας το ουδέτερο στοιχείο είναι ο αριθμός 0. Αν $x\in\mathbb{R}^*$, τότε $x^2=x\cdot x=1$ αν και μόνο αν $x=1$ ή $x=-1$. Άρα υπάρχει $1\neq x\in\mathbb{R}^*$: $x^2=x\cdot x=1$. Αντίθετα, αν $x\in\mathbb{R}$ και $2x=x+x=0$, τότε προφανώς $x=0$. Έτσι το μόνο στοιχείο του μονοειδούς $(\mathbb{R},+)$ με την ιδιότητα $x+x=0$ είναι το ουδέτερο στοιχείο 0. Επομένως, η εξίσωση $x\cdot x=1$ έχει δύο λύσεις στην ομάδα $(\mathbb{R}^*,\cdot)$ και μία λύση στην ομάδα $(\mathbb{R},+)$. Άρα οι ομάδες $(\mathbb{R}^*,\cdot)$ και $(\mathbb{R},+)$ δεν μπορεί να είναι ισόμορφες.

Αν η ομάδα $(\mathbb{R}^*,\cdot)$ των μη μηδενικών πραγματικών αριθμών είναι ισόμορφη με την ομάδα $(\mathbb{R}^+,\cdot)$ των θετικών πραγματικών αριθμων, όπου και στις δύο περιπτώσεις «$\cdot$» είναι η συνήθης πράξη του πολλαπλασιασμού πραγματικών αριθμών, δηλαδή έχουμε $(\mathbb{R}^*,\cdot)\cong(\mathbb{R}^+,\cdot)$, τότε επειδή $(\mathbb{R},+)\cong(\mathbb{R}^+,\cdot)$, έπεται ότι θα έχουμε $(\mathbb{R}^*,+)\cong(\mathbb{R},+)$. Αυτό όμως είναι άτοπο, όπως προκύπτει από το Παράδειγμα 1.4.32. Άρα $(\mathbb{R}^*,\cdot)\ncong(\mathbb{R}^+,\cdot)$. Συνοψίζοντας, δείξαμε ότι:

$$(\mathbb{R},+)\ \cong\ (\mathbb{R}^+,\cdot)\quad\text{και}\quad(\mathbb{R}^*,\cdot)\ \ncong\ (\mathbb{R},+)\quad\text{και}\quad(\mathbb{R}^*,+)\ \ncong\ (\mathbb{R}^+,\cdot)\quad\surd$$

Παράδειγμα 2.8.13. Έστω X και Y δύο μη κενά σύνολα με το ίδιο πλήθος στοιχείων: $|X|=|Y|$. Τότε οι ομάδες μεταθέσεων $\mathsf{S}(X)$ και $\mathsf{S}(Y)$ επί των συνόλων X και Y είναι ισόμορφες:

$$|X|=|Y|\quad\Longrightarrow\quad\mathsf{S}(X)\ \cong\ \mathsf{S}(Y)$$

Πράγματι, αν $\varphi:X\longrightarrow Y$ είναι μια «1-1» και «επί» απεικόνιση, τότε από την Πρόταση 1.3.24 έπεται ότι η απεικόνιση

$$\Phi:\mathsf{S}(X)\longrightarrow\mathsf{S}(Y),\quad\Phi(f)=\varphi\circ f\circ\varphi^{-1}$$

είναι «1-1» και «επί», και επιπλέον η Φ διατηρεί την σύνθεση απεικονίσεων, δηλαδή $\forall f,g\in\mathsf{S}(X)$:

$$\Phi(f\circ g)=\Phi(f)\circ\Phi(g)$$

Με άλλα λόγια η απεικόνιση Φ είναι ισομορφισμός ομάδων. Επομένως η συμμετρική ομάδα $\mathsf{S}(X)$ υπεράνω ενός συνόλου X δεν εξαρτάται από τη φύση αλλά μόνο από το πλήθος των στοιχείων του X. Έτσι από την πλευρά της θεωρίας ομάδων οι ομάδες $\mathsf{S}(X)$ και $\mathsf{S}(Y)$ θεωρούνται ως ταυτόσημες.

Ιδιαίτερα, βλέπουμε ότι, αν $|X|=n$, τότε:

$$\mathsf{S}(X)\ \cong\ \mathsf{S}(\{1,2,\cdots,n\})\ =\ \mathsf{S}_n\quad\surd$$

Κλείνουμε την παρούσα ενότητα ταξινομώντας, με βάση τη σχέση ισομορφίας ομάδων, όλες τις ομάδες με τάξη ≤ 4.

Παράδειγμα 2.8.14. Έστω $(G,\cdot)$ μια ομάδα, και υποθέτουμε ότι $|G| \leq 4$.

1. Αν $|G| = 1$, τότε $G = \{e\}$, και προφανώς κάθε άλλη ομάδα $G' = \{e'\}$ τάξης 1 είναι ισόμορφη με την G μέσω του ισομορφισμού $f\colon G \longrightarrow G'$, $f(e) = e'$.

   • Άρα υπάρχει ακριβώς μια κλάση ισομορφίας ομάδων με τάξη 1, η κλάση ισομορφίας της τετριμμένης ομάδας.

   Ως αντιπρόσωπος της μοναδικής κλάσης ισομορφίας μπορεί να ληφθεί η τετριμμένη υποομάδα $\{0\}$ της προσθετικής ομάδας $(\mathbb{Z},+)$ ή η τετριμμένη υποομάδα $\{1\}$ της πολλαπλασιαστικής ομάδας $(\mathbb{R}^*,\cdot)$.

2. Αν $|G| = 2$, τότε, από το Παράδειγμα 2.4.26, η G είναι της μορφής $G = \{e,a\}$, όπου $a^2 = e$. Κάθε άλλη ομάδα G' τάξης 2 θα είναι ανάλογης μορφής $G' = \{e',b\}$, όπου $b^2 = e'$, και τότε η απεικόνιση $f\colon G \longrightarrow G'$, όπου $f(e) = e'$ και $f(a) = b$, είναι προφανώς ισομορφισμός ομάδων.

   • Άρα υπάρχει ακριβώς μια κλάση ισομορφίας ομάδων με τάξη 2, η κλάση ισομορφίας της κυκλικής ομάδας τάξης 2.

   Ως αντιπρόσωπος της μοναδικής κλάσης ισομορφίας μπορεί να ληφθεί η προσθετική ομάδα $(\mathbb{Z}_2,+)$ των κλάσεων υπολοίπων mod 2, ή η υποομάδα $\{1,-1\}$ της πολλαπλασιαστικής ομάδας $(\mathbb{R}^*,\cdot)$, ή η συμμετρική ομάδα $(S_2,\circ)$.

3. Αν $|G| = 3$, τότε, από το Παράδειγμα 2.4.26, η G είναι της μορφής $G = \{e,a,a^2\}$, όπου $a^3 = e$. Κάθε άλλη ομάδα G' τάξης 3 θα είναι ανάλογης μορφής $G' = \{e',b,b^2\}$, όπου $b^3 = e'$, και τότε η απεικόνιση $f\colon G \longrightarrow G'$, όπου $f(e) = e'$, $f(a) = b$, και $f(a^2) = b^2$, είναι προφανώς ένας ισομορφισμός ομάδων.

   • Άρα υπάρχει ακριβώς μια κλάση ισομορφίας ομάδων με τάξη 3, η κλάση ισομορφίας της κυκλικής ομάδας τάξης 3.

   Ως αντιπρόσωπος της μοναδικής κλάσης ισομορφίας μπορεί να ληφθεί η προσθετική ομάδα $(\mathbb{Z}_3,+)$ των κλάσεων υπολοίπων mod 2, ή η υποομάδα $\{1,\zeta_3,\zeta_3^2\}$ της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*,\cdot)$ η οποία αποτελείται από τις κυβικές ρίζες της μονάδας.

4. Υποθέτουμε ότι $|G| = 4$. Από το Παράδειγμα 2.4.26, έπεται ότι υπάρχουν δύο διαφορετικές, ως προς τον πίνακα Cayley, ομάδες με τάξη 4: η ομάδα των τεσσάρων στοιχείων $\mathcal{V}_4$ του Klein, και η κυκλική ομάδα C_4 τάξης 4.

   (α′) Για την ομάδα του Klein, έχουμε: $(\mathcal{V}_4,\cdot)$, όπου $\mathcal{V}_4 = \{e,a,b,c\}$, όπου $a^2 = b^2 = c^2 = e$, και $a\cdot b = c = b\cdot a$, $b\cdot c = a = c\cdot b$, και $c\cdot a = b = a\cdot c$. Στην ομάδα $\mathcal{V}_4$, όλα τα στοιχεία $x \in \mathcal{V}_4$ ικανοποιούν τη σχέση $x^2 = e$.

   (β′) Για την κυκλική ομάδα C_4 τάξης 4, έχουμε: $(C_4,*)$, όπου $C_4 = \{\epsilon,x,x^2,x^3\}$, όπου $x^4 = \epsilon$. Στην ομάδα C_4 τα μόνα στοιχεία $x \in C_4$ τα οποία ικανοποιούν τη σχέση $x^2 = \epsilon$ είναι τα ϵ και a^2.

   Από τα παραπάνω, έπεται ότι οι ομάδες $(\mathcal{V}_4,\cdot)$ και $(C_4,*)$ δεν είναι ισόμορφες: $(\mathcal{V}_4,\cdot) \ncong (C_4,*)$.

   Για την τυχούσα ομάδα $G = \{e',a',b',c'\}$ με τάξη 4, υπάρχουν δύο επιλογές: είτε κάθε στοιχείο της x ικανοποιεί τη σχέση $x^2 = e'$, οπότε ο πίνακας Cayley της G θα είναι της μορφής του Πίνακα Α′ παρακάτω, ή θα έχει ακριβώς δύο στοιχεία x, έστω τα e' και a', τα οποία ικανοποιούν τη σχέση $x^2 = e'$, οπότε ο πίνακας Cayley της G θα έχει την μορφή του Πίνακα Β′ παρακάτω:

Πίνακας Α′ :

$\star$	$\mathbf{e'}$	$\mathbf{a'}$	$\mathbf{b'}$	$\mathbf{c'}$
$\mathbf{e'}$	e'	a'	b'	c'
$\mathbf{a'}$	a'	e'	c'	b'
$\mathbf{b'}$	b'	c'	e'	a'
$\mathbf{c'}$	c'	b'	a'	e'

Πίνακας Β′:

$\star$	$\mathbf{e'}$	$\mathbf{a'}$	$\mathbf{b'}$	$\mathbf{c'}$
$\mathbf{e'}$	e'	a'	b'	c'
$\mathbf{a'}$	a'	e'	c'	b'
$\mathbf{b'}$	b'	c'	a'	e'
$\mathbf{c'}$	c'	b'	e'	a'

Στην περίπτωση ομάδας $(G,\star)$ με πίνακα Cayley τον Α′, εύκολα βλέπουμε ότι η απεικόνιση $f\colon G \longrightarrow \mathcal{V}_4$, όπου $f(e) = e'$, $f(a) = a'$, $f(b) = b'$, και $f(c) = c'$, είναι ισομορφισμός ομάδων, και άρα $G \cong \mathcal{V}_4$. Στην περίπτωση ομάδας $(G,\star)$ με πίνακα Cayley τον Β′, εύκολα βλέπουμε ότι η απεικόνιση $f\colon G \longrightarrow C_4$, όπου $f(\epsilon) = e'$, $f(x) = b'$, $f(x^2) = a'$, και $f(x^3) = c'$, είναι ισομορφισμός ομάδων, και άρα $G \cong C_4$.

- Άρα υπάρχουν ακριβώς δύο κλάσεις ισομορφίας ομάδων με τάξη 4, η κλάση ισομορφίας της ομάδας των τεσσάρων στοιχείων του Klein, και η κλάση ισομορφίας της κυκλικής ομάδας τάξης 4.

  Ως αντιπρόσωπος της μιας κλάσης ισομορφίας μπορεί να ληφθεί η προσθετική κυκλική ομάδα $(\mathbb{Z}_4,+)$ των κλάσεων υπολοίπων mod 4, ή η υποομάδα $\{1,i,-1,-i\}$ των τέταρτων ριζών της μονάδας της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*,\cdot)$, και ως αντιπρόσωπος της άλλης κλάσης ισομορφίας μπορεί να ληφθεί η προσθετική ομάδα ευθύ γινόμενο $(\mathbb{Z}_2\times\mathbb{Z}_2,+)$, η πολλαπλασιαστική ομάδα ευθύ γινόμενο $(\{1,-1\}\times\{1,-1\},\cdot)$. $\surd$

Για να είναι εφικτή η ταξινόμηση ομάδων μικρής τάξης $5,6,7,8,\cdots$, απαιτούνται επιπρόσθετες έννοιες και αποτελέσματα, κάποια εκ των οποίων αναπτύσσονται στα επόμενα κεφάλαια.

Στη Θεωρία Ομάδων, αλλά και σε αλγεβρικές δομές παρόμοιου τύπου, ενδιαφερόμαστε για τις δομικές ιδιότητες τις οποίες έχει μια ομάδα, και το κεντρικό πρόβλημα αφορά την ταξινόμηση (κλάσεων) ομάδων με βάση τη σχέση ισομορφίας. Σ' αυτό το πλαίσιο, ισόμορφες ομάδες έχουν τις ίδιες δομικές ιδιότητες και γι' αυτό τις ταυτίζουμε, καθώς η μία ομάδα είναι (ισόμορφο) αντίγραφο της άλλης. Αυτή η προσέγγιση θα ακολουθηθεί στις επόμενες ενότητες.

2.9 Ευθέα Γινόμενα Ομάδων (II)

Σύμφωνα με την Πρόταση 2.7.16, αν μια ομάδα G είναι το εξωτερικό ευθύ γινόμενο πεπερασμένου πλήθους ομάδων, τότε η G είναι το εσωτερικό ευθύ γινόμενο αντίστοιχων υποομάδων της. Στην παρούσα υποενότητα, ολοκληρώνοντας την ανάλυση της βασικής θεωρίας ευθέων γινομένων ομάδων, θα δείξουμε ότι ισχύει και το αντίστροφο, και επιπλέον θα αποδείξουμε διάφορους χαρακτηρισμούς για το πότε μια ομάδα είναι ισόμορφη με το εξωτερικό ή εσωτερικό ευθύ γινόμενο πεπερασμένου πλήθους (υπο)ομάδων.

Θεώρημα 2.9.1. *1. Έστω $(G,\cdot)=(\prod_{k=1}^n G_k,\cdot)$ το εξωτερικό ευθύ γινόμενο πεπερασμένου πλήθους ομάδων $(G_1,\cdot)$, $\cdots$, $(G_n,\cdot)$. Τότε η ομάδα G είναι το εσωτερικό ευθύ γινόμενο υποομάδων της $\widetilde{G}_1,\cdots,\widetilde{G}_n$, και επιπλέον υπάρχουν ισομορφισμοί ομάδων, $\forall k=1,2,\cdots,n$:*

$$\widetilde{G}_k \xrightarrow{\cong} G_k$$

2. Έστω $(G,\cdot)$ μια ομάδα η οποία είναι το εσωτερικό ευθύ γινόμενο πεπερασμένου πλήθους υποομάδων της $H_1,\cdots,H_n$. Τότε η ομάδα G είναι ισόμορφη με το εξωτερικό ευθύ γινόμενο των ομάδων $H_1,\cdots,H_n$:

$$G \xrightarrow{\cong} H_1\times H_2\times\cdots\times H_n$$

Απόδειξη. 1. Από την Πρόταση 2.7.16 έπεται ότι η ομαδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της $\widetilde{G}_1,\cdots,\widetilde{G}_n$, όπου $\widetilde{G}_k=\{e_1\}\times\cdots\times\{e_{k-1}\}\times G_k\times\{e_{k+1}\}\times\cdots\{e_n\}$, $1\le k\le n$. Για κάθε $k=1,2,\cdots,n$, ορίζουμε απεικόνιση

$$f_k:\ G_k\longrightarrow\widetilde{G}_k,\quad f_k(x)=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)$$

Η απεικόνιση f_k είναι ομομορφισμός ομάδων διότι:

$$f_k(x\cdot y)=(e_1,\cdots,e_{k-1},x\cdot y,e_{k+1},\cdots,e_n)=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\cdot(e_1,\cdots,e_{k-1},y,e_{k+1},\cdots,e_n)=f_k(x)\cdot f_k(y)$$

Επίσης η f_k είναι «1-1», διότι: αν $f_k(x)=f_k(y)$, τότε $(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)=(e_1,\cdots,e_{k-1},y,e_{k+1},\cdots,e_n)$ και επομένως $x=y$. Τέλος, η απεικόνιση f_k είναι «επί», διότι κάθε στοιχείο της υποομάδας $\widetilde{G}_k$ είναι της μορφής $(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)=f_k(x)$, όπου $x\in G_k$. Άρα η απεικόνιση f_k, $1\le k\le n$, είναι ένας ισομορφισμός ομάδων.

2. Θα δείξουμε ότι η απεικόνιση

$$f:\ H_1\times H_2\times\cdots\times H_n\longrightarrow G,\quad f(h_1,h_2,\cdots,h_n)=h_1\cdot h_2\cdots h_n$$

είναι ισομορφισμός ομάδων. Έστω $\mathsf{x} = (h_1, h_2, \cdots, h_n)$ και $\mathsf{y} = (h'_1, h'_2, \cdots, h'_n)$ τυχόντα στοιχεία της ομάδας εξωτερικό ευθύ γινόμενο $H_1 \times H_2 \times \cdots \times H_n$. Τότε θα έχουμε

$$f(\mathsf{x}\cdot\mathsf{y}) = f\big((h_1, h_2, \cdots, h_n)\cdot(h'_1, h'_2, \cdots, h'_n)\big) = \big(h_1\cdot h'_1, h_2\cdot h'_2, \cdots, h_n\cdot h'_n\big) = h_1\cdot h'_1\cdot h_2\cdot h'_2\cdots h_n\cdot h'_n$$

Από την άλλη πλευρά, χρησιμοποιώντας το μέρος 1., της Πρότασης 2.7.14, θα έχουμε:

$$h_1\cdot h'_1\cdot h_2\cdot h'_2\cdots h_n\cdot h'_n = (h_1\cdot h_2\cdots h_n)\cdot(h'_1\cdot h'_2\cdots h'_n) = f(\mathsf{x})\cdot f(\mathsf{y})$$

Άρα η απεικόνιση f είναι ομομορφισμός ομάδων. Προφανώς η απεικόνιση f είναι απεικόνιση «επί», διότι αν $h_1\cdot h_2\cdots h_n \in G$, όπου $h_k \in H_k$, $1 \le k \le n$, τότε $f(h_1, h_2, \cdots, h_n) = h_1\cdot h_2\cdots h_n$. Τέλος, έστω ότι $f(h_1, h_2, \cdots, h_n) = f(h'_1, h'_2, \cdots, h'_n)$, όπου $h_i, h'_i \in H_i$, $1 \le i \le n$. Τότε $h_1\cdot h_2\cdots h_n = h'_1\cdot h'_2\cdots h'n$, και άρα από την μοναδικότητα της γραφής στην ομάδα εσωτερικό ευθύ γινόμενο, θα έχουμε ότι $h_i = h'_i$, $1 \le i \le n$. Επομένως $(h_1, h_2, \cdots, h_n) = (h'_1, h'_2, \cdots, h'_n)$, δηλαδή η f είναι «1-1». Συνοψίζοντας, δείξαμε ότι η απεικόνιση f είναι ισομορφισμός ομάδων. ■

Πόρισμα 2.9.2. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και ότι H_1, H_2, $\cdots$, H_n είναι υποομάδες της G. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $H_1, \cdots, H_n$.*
2. *Η απεικόνιση*
$$f : H_1 \times H_2 \times \cdots \times H_n \longrightarrow G, \quad f(h_1, h_2, \cdots, h_n) = h_1\cdot h_2\cdot\cdots\cdot h_n$$
είναι ισομορφισμός ομάδων.

Απόδειξη. 1. $\Longrightarrow$ 2. Προκύπτει από το μέρος 2. του Θεωρήματος 2.9.1.

2. $\Longrightarrow$ 1. Θέτουμε $H = H_1 \times H_2 \times \cdots \times H_n$. Επειδή η απεικόνιση f είναι ισομορφισμός, έπεται ότι

$$G = \mathsf{Im}(f) = \big\{f(h_1, h_2, \cdots, h_n) \in G \mid h_i \in H_i,\ 1 \le i \le n\big\} = \big\{h_1\cdot h_2\cdot\cdots\cdot h_n \in G \mid h_i \in H_i,\ 1 \le i \le n\big\} = H_1\cdot H_2\cdots H_n$$

Θέτοντας $\widetilde{H}_k = \{e_1\} \times \cdots \times \{e_{k-1}\} \times H_k \times \{e_{k+1}\} \times \cdots \{e_n\}$, $1 \le k \le n$, από την Πρόταση 2.7.16, έπεται ότι η ομάδα H είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $\widetilde{H}_k$, και ιδιαίτερα θα έχουμε: $\widetilde{H}_k \trianglelefteq H$, $1 \le k \le n$. Έστω $x \in G$ και $h_k \in H_k$. Επειδή η f είναι ισομορφισμός και επειδή προφανώς $f(\widetilde{H}_k) = H_k$, έπεται ότι υπάρχουν στοιχεία $\mathsf{h} \in H$ και $\mathsf{h}_k \in \widetilde{H}_k$ έτσι ώστε: $f(\mathsf{h}) = x$ και $f(\mathsf{h}_k) = h_k$. Χρησιμοποιώντας ότι $\widetilde{H}_k \trianglelefteq H_k$, θα έχουμε:

$$\mathsf{h}\cdot\mathsf{h}_k\cdot\mathsf{h}^{-1} \in \widetilde{H}_k \quad\Longrightarrow\quad f(\mathsf{h}\cdot\mathsf{h}_k\cdot\mathsf{h}^{-1}) \in f(\widetilde{H}_k) \quad\Longrightarrow\quad f(\mathsf{h})\cdot f(\mathsf{h}_k)\cdot f(\mathsf{h}^{-1}) \in H_k \quad\Longrightarrow\quad x\cdot h_k\cdot x^{-1} \in H_k$$

Επομένως, η H_k είναι κανονική υποομάδα της G: $H_k \trianglelefteq G$, $1 \le k \le n$.

Έστω $x \in G$ και υποθέτουμε ότι $x = h_1\cdot h_2\cdots h_n = h'_1\cdot h'_2\cdots h'_n$, όπου $h_i, h'_i \in H_i$, $1 \le i \le n$. Επειδή η απεικόνιση f είναι απεικόνιση «επί», υπάρχουν στοιχεία $\mathsf{h} \in H$ και $g_i, g'_i \in \widetilde{H}_i$, έτσι ώστε: $f(\mathsf{h}) = x$, $f(g_i) = h_i$, και $f(g'_i) = h'_i$, $1 \le i \le n$. Τότε προφανώς θα έχουμε $f(\mathsf{h}) = f(g_1)\cdot f(g_2)\cdots f(g_n) = f(g'_1)\cdot f(g'_2)\cdots f(g'_n)$, και επειδή η f είναι ομομορφισμός και απεικόνιση «1-1», θα έχουμε:

$$f(\mathsf{h}) = f(g_1\cdot g_2\cdots g_n) = f(g'_1\cdot g'_2\cdots g'_n) \quad\Longrightarrow\quad \mathsf{h} = g_1\cdot g_2\cdots g_n = g'_1\cdot g'_2\cdots g'_n$$

Επειδή η ομάδα H είναι το εσωτερικό ευθύ γινόμενο των υποομάδων $\widetilde{H}_i$, και $g_i, g'_i \in \widetilde{H}_i$, $1 \le i \le n$, από την μοναδικότητα της γραφής, έπεται ότι

$$g_i = g'_i,\ \ 1 \le i \le n \quad\Longrightarrow\quad h_i = f(g_i) = f(g'_i) = h'_i,\ \ 1 \le i \le n$$

Τότε, από την Πρόταση 2.7.15, η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H_i, $1 \le i \le n$. ■

Παράδειγμα 2.9.3. 1. Από το Παράδειγμα 2.7.10, έπεται ότι η ομάδα $\mathcal{V}_4 = \{e, a, b, c\}$ των τεσσάρων στοιχείων του Klein είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της $H_1 = \{e, a\}$ και $H_2 = \{e, b\}$. Επομένως: $\mathcal{V}_4 \cong H_1 \times H_2$. Επειδή καθεμία εκ των υποομάδων H_i είναι κυκλική τάξης 2, από το Παράδειγμα 2.8.14 έπεται ότι υπάρχουν ισομορφισμοί $H_1 \cong \mathbb{Z}_2 \cong H_2$. Επομένως:

$$\mathcal{V}_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

μέσω του ισομορφισμού ομάδων $f: \mathcal{V}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$, $f(e) = ([0]_2, [0]_2)$, $f(a) = ([1]_2, [0]_2)$, $f(b) = ([0]_2, [1]_2)$, και $f(c) = ([1]_2, [1]_2)$.

2. Από το Παράδειγμα 2.7.10 έπεται ότι η ομάδα $(\mathbb{C}^*, \cdot)$ των μη μηδενικών μιγαδικών αριθμών είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της T και $\mathbb{R}^{>0}$. Επομένως

$$\mathbb{C}^* \cong \mathsf{T} \times \mathbb{R}^{>0}$$

μέσω του ισομορφισμού ομάδων $f: \mathbb{C}^* \longrightarrow \mathsf{T} \times \mathbb{R}^{>0}$, $f(z) = \left(\frac{z}{|z|}, |z|\right)$.

3. Θεωρούμε την προσθετική ομάδα $(\mathbb{Z}_6, +)$ των κλάσεων υπολοίπων mod 6, δηλαδή $\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$. Θα δείξουμε ότι

$$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

Θεωρούμε τις κυκλικές υποομάδες $H_1 = \langle [3]_6 \rangle = \{[0]_6, [3]_6\}$ και $H_2 = \langle [2]_6 \rangle = \{[0]_6, [2]_6, [4]_6\}$ της $\mathbb{Z}_6$ οι οποίες παράγονται από τις κλάσεις ισοτιμίας $[3]_6$ και $[2]_6$. Επειδή η $\mathbb{Z}_6$ είναι αβελιανή, έπεται ότι οι υποομάδες H_1 και H_2 είναι κανονικές. Επιπλέον εύκολα υπολογίζουμε ότι $H_1 + H_2 = \mathbb{Z}_6$. Τέλος, επειδή $H_1 \bigcap H_2 = \{[0]_6\}$, έπεται ότι η $\mathbb{Z}_6$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων H_1 και H_2. Επομένως θα έχουμε έναν ισομορφισμό $\mathbb{Z}_6 \cong H_1 \times H_2$. Επειδή οι υποομάδες H_1 και H_2 είναι κυκλικές τάξης 2 και 3 αντίστοιχα, έπεται ότι υπάρχουν ισομορφισμοί $H_1 \cong \mathbb{Z}_2$ και $H_2 \cong \mathbb{Z}_3$. Επομένως $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, μέσω του ισομορφισμού $f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$, $f([k]_6) = ([k]_2, [k]_3)$. $\surd$

Παράδειγμα 2.9.4. Αν $\{(G_k, \cdot)\}_{k=1}^n$ και $\{(H_k, \cdot)\}_{k=1}^n$ είναι δύο οικογένειες ομάδων, και υποθέτουμε ότι $f_k: G_k \longrightarrow H_k$ είναι ομομορφισμοί ομάδων, $1 \leq k \leq n$. Τότε ορίζεται η απεικόνιση

$$\prod_{k=1}^n f_k = f_1 \times f_2 \times \cdots \times f_n : \prod_{k=1}^n G_k \longrightarrow \prod_{k=1}^n H_k, \quad (f_1 \times f_2 \times \cdots \times f_n)(x_1, x_2, \cdots, x_n) = \left(f_1(x_1), f_2(x_2), \cdots f_n(x_n)\right)$$

Θα δείξουμε ότι η απεικόνιση $\prod_{k=1}^n f_k = f_1 \times f_2 \times \cdots \times f_n$ είναι ομομορφισμός ομάδων. Πράγματι, αν $\mathsf{x} = (x_1, x_2, \cdots, x_n)$ και $\mathsf{y} = (y_1, y_2, \cdots, y_n)$ είναι στοιχεία της ομάδας $\prod_{k=1}^n G_k$, τότε $\mathsf{x} \cdot \mathsf{y} = (x_1 \cdot y_1, x_2 \cdot y_2, \cdots, x_n \cdot y_n)$, και θα έχουμε:

$$(\prod_{k=1}^n f_k)(\mathsf{x} \cdot \mathsf{y}) = (\prod_{k=1}^n f_k)(x_1 \cdot y_1, x_2 \cdot y_2, \cdots, x_n \cdot y_n) = (f_1(x_1 \cdot y_1), f_2(x_2 \cdot y_2), \cdots, f_n(x_n \cdot y_n)) =$$

$$= (f_1(x_1) \cdot f_1(y_1), f_2(x_2) \cdot f_2(y_2), \ \cdots, \ f_n(x_n) \cdot f_n(y_n)) = (f_1(x_1), f_2(x_2), \cdots f_n(x_n) \cdot (f_1(y_1), f_2(y_2), \cdots f_n(y_n) =$$

$$= (\prod_{k=1}^n f_k)(\mathsf{x}) \cdot (\prod_{k=1}^n f_k)(\mathsf{y})$$

Επομένως η απεικόνιση $\prod_{k=1}^n f_k: (\prod_{k=1}^n G_k, \cdot) \longrightarrow (\prod_{k=1}^n H_k, \cdot)$ είναι ομομορφισμός ομάδων, ο οποίος καλείται **ομομορφισμός ευθύ γινόμενο** των ομομορφισμών $f_k: (G_k, \star_k) \longrightarrow (H_k, *_k)$, $1 \leq k \leq n$.

Σύμφωνα με την Άσκηση 2.10.45, ο ομομορφισμός $\prod_{k=1}^n f_k$ είναι μονομορφισμός, αντίστοιχα, επιμορφισμός, αντίστοιχα ισομορφισμός, αν και μόνο αν κάθε ομομορφισμός f_k, $1 \leq k \leq n$, είναι μονομορφισμός, αντίστοιχα, επιμορφισμός, αντίστοιχα ισομορφισμός. $\surd$

Παράδειγμα 2.9.5. 1. Έστω $(G, \cdot)$ μια ομάδα, Τότε υπάρχουν ισομορφισμοί: $G \cong \{e\} \times G$ και $G \cong G \times \{e\}$. Πράγματι οι απεικονίσεις $G \longrightarrow \{e\} \times G$, $x \longmapsto (e, x)$ και $G \longrightarrow G \times \{e\}$, $x \longmapsto (x, e)$ είναι προφανώς ισομορφισμοί ομάδων.

2. Έστω $(G_1,\cdot)$ και $(G,\cdot)$ δύο ομάδες. Τότε η απεικόνιση $f\colon G_1\times G_2\longrightarrow G_2\times G_1$, $f(x,y)=(y,x)$ είναι προφανώς ένας ισομορφισμός ομάδων, και άρα:

$$G_1\times G_2\ \cong\ G_2\times G_1$$

3. Γενικότερα, αν $(G_1,\cdot),\cdots,(G_n,\cdot)$ είναι ένα πεπερασμένο πλήθος ομάδων, τότε, σύμφωνα με την Άσκηση 2.10.43, για κάθε μετάθεση $\sigma\in S_n$, υπάρχει ένας ισομορφισμός ομάδων:

$$G_1\times G_2\times\cdots\times G_n\ \cong\ G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)}\quad\surd$$

Θεωρούμε μια πεπερασμένη οικογένεια ομάδων $\{(G_k,\cdot)\}_{k=1}^n$. Ορίζουμε απεικονίσεις

$$\iota_k:\ G_k\ \longrightarrow\ G_1\times G_2\times\cdots\times G_n,\qquad \iota_k(x)=(e_1,e_{k-1},x,e_{k+1},\cdots,e_n)$$

$$\pi_k:\ G_1\times G_2\times\cdots\times G_n\ \longrightarrow\ G_k,\qquad \iota_k(x_1,x_2,\cdots,x_n)=x_k$$

και υπενθυμίζουμε ότι για τυχούσες ομάδες G και H, ορίζεται ο τετριμμένος ομομορφισμός $\epsilon\colon G\longrightarrow H$, $\epsilon(x)=e$. Ιδιαίτερα ορίζονται οι τετριμμένοι ομομορφισμοί $\epsilon_{ij}\colon G_i\longrightarrow G_j$, $\epsilon_{ij}(x)=e_j$, όπου e_j είναι το ουδέτερο στοιχείο της ομάδας G_j.

Αν $(G,\cdot)$ είναι μια ομάδα και $f_1,\cdots,f_n:\ G\longrightarrow G$ είναι απεικονίσεις, όχι απαραίτητα ομομορφισμοί ομάδων, τότε ορίζεται η απεικόνιση

$$f_1\cdot f_2\cdots f_n\ :\ G\ \longrightarrow\ G,\quad (f_1\cdot f_2\cdots f_n)(x)=f_1(x)\cdot f_2(x)\cdots f_n(x)$$

Σημειώνουμε ότι ακόμα και αν οι απεικονίσεις f_k $1\le k\le n$, είναι ομομορφισμοί, τότε γενικά η απεικόνιση $f_1\cdot f_2\cdots f_n$ *δεν* είναι ομομορφισμός ομάδων, βλέπε την Άσκηση 1.5.28.

Λήμμα 2.9.6. *Με τους παραπάνω συμβολισμούς, οι οικογένειες απεικονίσεων*

$$\left\{\iota_k\colon G_k\longrightarrow\prod_{k=1}^n G_k\right\}_{k=1}^n\qquad\text{και}\qquad\left\{\pi_l\colon\prod_{k=1}^n G_k\longrightarrow G_l\right\}_{l=1}^n$$

είναι ομομορφισμοί ομάδων και ικανοποιούνται οι ακόλουθες σχέσεις:

$$\forall 1\le i,j\le n:\qquad \pi_j\circ\iota_i=\begin{cases}\mathrm{Id}_{G_i}, & \text{αν } i=j\\ \epsilon_{ij}, & \text{αν } i\neq j\end{cases}$$

Επιπλέον:

1. *Για κάθε $k=1,2,\cdots,n$, η απεικόνιση $\pi_k\colon\prod_{k=1}^n G_k\longrightarrow G_k$ είναι επιμορφισμός, και η απεικόνιση $\iota_k\colon G_k\longrightarrow\prod_{k=1}^n$ είναι μονομορφισμός με εικόνα την υποομάδα $\widetilde{G}_k=\{e_1\}\times\cdots\{e_{k-1}\}\times G_k\times\{e_{k+1}\}\times\cdots\times\{e_n\}$. Επιπλέον ο μονομορφισμός ι_k επάγει έναν ισομορφισμό ομάδων*

$$\iota_k:\ G_k\ \xrightarrow{\cong}\ \widetilde{G}_k$$

2. *Ικανοποιείται η ακόλουθη σχέση:*

$$\mathrm{Id}_{\prod_{k=1}^n G_k}=(\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)$$

Απόδειξη. Έστω $x,y\in G_k$. Τότε για κάθε $k=1,2,\cdots,n$:

$$\iota_k(x\cdot y)=(e_1,\cdots,e_{k-1},x\cdot y,e_{k+1},\cdots,e_n)=(e_1,\cdots,e_{k-1},x,e_{k+1},\cdots,e_n)\cdot(e_1,\cdots,e_{k-1},y,e_{k+1},\cdots,e_n)=\iota_k(x)\cdot\iota_k(y)$$

Επομένως η απεικόνιση ι_k, $1\le k\le n$, είναι ομομορφισμός ομάδων.

Παρόμοια, θεωρούμε στοιχεία $\mathsf{x} = (x_1, \cdots, x_l, \cdots, x_n)$ και $\mathsf{y} = (y_1, \cdots, y_l, \cdots, y_n)$ της ομάδας εξωτερικό ευθύ γινόμενο $\prod_{k=1}^n G_k$. Τότε:

$$\pi_l(\mathsf{x}\cdot\mathsf{y}) = \pi_l(x_1\cdot y_1, \cdots, x_l\cdot y_l, \cdots, x_n\cdot y_n) = x_l\cdot y_l = \pi_l(x_1, \cdots, x_l, \cdots, x_n)\cdot\pi_l(y_1, \cdots, y_l, \cdots, y_n) = \pi_l(\mathsf{x})\cdot\pi_l(\mathsf{y})$$

Επομένως η απεικόνιση π_l, $1 \le l \le n$, είναι ομομορφισμός ομάδων.

Θεωρούμε δείκτες $1 \le i, j \le n$. Υποθέτουμε πρώτα ότι $i \ne j$, και έστω $x \in G_i$, τότε:

$$(\pi_j \circ \iota_i)(x) = \pi_j(\iota_i(x)) = \pi_j(e_1, \cdots, e_{i-1}, x, e_{i+1}, \cdots, e_n) = e_j \quad \text{άρα} \quad 1 \le i \ne j \le n: \implies \pi_j \circ \iota_i = e_{ij}$$

Υποθέτουμε ότι $i = j$, και έστω $x \in G_i$, τότε:

$$(\pi_i \circ \iota_i)(x) = \pi_i(\iota_i(x)) = \pi_i(e_1, \cdots, e_{i-1}, x, e_{i+1}, \cdots, e_n) = x \quad \text{άρα} \quad 1 \le i = j \le n: \implies \pi_i \circ \iota_i = \mathsf{Id}_{G_i}$$

1. Η απεικόνιση $\pi_k\colon \prod_{k=1}^n \longrightarrow G_k$ είναι επιμορφισμός, διότι για κάθε $x \in G_k$, έχουμε: $\pi_k(e_1, \cdots, e_{k-1}, x, e_{k+1}, \cdots, e_n) = x$. Η απεικόνιση $\iota_k\colon G_k \longrightarrow \prod_{k=1}^n G_k$ είναι μονομορφισμός, διότι, αν $\iota_k(x) = \iota_k(y)$, τότε $\pi_k(\iota_k(x)) = \pi_k(\iota_k(y))$ και επομένως από τις παραπάνω σχέσεις, έπεται ότι $x = y$. Προφανώς $\mathsf{Im}(\iota_k) = \left\{\iota_k(x) \in \prod_{k=1}^n G_k \mid x \in G_k\right\} = \left\{(e_1, \cdots, e_{k-1}, x, e_{k+1}, \cdots, e_n) \in \prod_{k=1}^n G_k \mid x \in G_k\right\} = \widetilde{G}_k$. Επομένως μπορούμε να θεωρήσουμε απεικόνιση

$$\widetilde{\iota}_k\colon G_k \longrightarrow \widetilde{G}_k, \quad \widetilde{\iota}_k(x) = \iota_k(x)$$

η οποία είναι προφανώς ισομορφισμός ομάδων.

2. Για κάθε $\mathsf{x} = (x_1, x_2, \cdots, x_n) \in \prod_{k=1}^n G_k$, θα έχουμε:

$$[(\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)](\mathsf{x}) = (\iota_1\circ\pi_1)(\mathsf{x})\cdot(\iota_2\circ\pi_2)(\mathsf{x})\cdots(\iota_n\circ\pi_n)(\mathsf{x}) = \iota_1(\pi_1(\mathsf{x}))\cdot\iota_2(\pi_2)(\mathsf{x}))\cdots\iota_n(\pi_n)(\mathsf{x})) =$$

$$= \iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n) = (x_1, e_2, \cdots, e_n)\cdot(e_1, x_2, \cdots, e_n)\cdots(e_1, e_2, \cdots x_n) = (x_1, x_2, \cdots, x_n) = \mathsf{x} = \mathsf{Id}_{\prod_{k=1}^n G_k}(\mathsf{x})$$

Επομένως θα έχουμε: $\mathsf{Id}_{\prod_{k=1}^n G_k} = (\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)$. ■

Το ακόλουθο αποτέλεσμα χαρακτηρίζει τις ομάδες οι οποίες είναι (ισόμορφες με) εξωτερικά ευθέα γινόμενα πεπερασμένου πλήθους ομάδων, χωρίς τη χρήση στοιχείων ή υποομάδων, αλλά με βάση ομομορφισμούς ομάδων.

Θεώρημα 2.9.7. *Αν $(G,\cdot)$ και $(G_1,\cdot)$, $\cdots$, $(G_n,\cdot)$ είναι ομάδες, τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα G είναι ισόμορφη με το ευθύ γινόμενο $G_1 \times G_2 \times \cdots \times G_n$ των ομάδων G_i, $1 \le i \le n$.*
2. *Υπάρχουν οικογένειες ομομορφισμών ομάδων $\iota_k\colon G_k \longrightarrow G$ και $\pi_k\colon G \longrightarrow G_k$ έτσι ώστε:*

$$\forall 1 \le i, j \le n: \quad \pi_j \circ \iota_i = \begin{cases} \mathsf{Id}_{G_i}, & \text{αν } i = j \\ \epsilon_{ij}, & \text{αν } i \ne j \end{cases} \qquad \text{και} \qquad \mathsf{Id}_G = (\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)$$

Απόδειξη. 1. $\implies$ 2. Η απόδειξη προκύπτει από το Λήμμα 2.9.6.

2. $\implies$ 1. Ορίζουμε μια απεικόνιση

$$f\colon G \longrightarrow G_1 \times G_2 \times \cdots, \times G_n, \quad f(x) = \big(\pi_1(x), \pi_2(x), \cdots, \pi_n(x)\big)$$

Η απεικόνιση f είναι ομομορφισμός ομάδων, διότι, αν $x, y \in G$, τότε, χρησιμοποιώντας ότι οι απεικονίσεις π_k, $1 \le k \le n$, είναι ομομορφισμοί ομάδων, θα έχουμε:

$$f(x\cdot y) = \big(\pi_1(x\cdot y), \pi_2(x\cdot y), \cdots, \pi_n(x\cdot y)\big) = \big(\pi_1(x)\cdot\pi_1(y), \pi_2(x)\cdot\pi_2(y), \cdots, \pi_n(x)\cdot\pi_n(y)\big) =$$

$$= \big(\pi_1(x), \pi_2(x),, \cdots, \pi_n(x)\big)\cdot\big(\pi_1(y), \pi_2(y),, \cdots, \pi_n(y)\big) = f(x)\cdot f(y)$$

Η απεικόνιση f είναι μονομορφισμός, διότι, αν $f(x) = f(y)$, τότε θα έχουμε:

$$f(x) = f(y) \implies \big(\pi_1(x), \pi_2(x), \cdots, \pi_n(x)\big) = \big(\pi_1(y), \pi_2(y), \cdots, \pi_n(y)\big) \implies \pi_k(x) = \pi_k(y), \ \ 1 \le k \le n \implies$$

$$(\iota_k\circ\pi_k)(x)=(\iota_k\circ\pi_k)(y)),\ 1\le k\le n \implies (\iota_1\circ\pi_1)(x)\cdot(\iota_2\circ\pi_2)(x)\cdots(\iota_n\circ\pi_n)(x)=(\iota_1\circ\pi_1)(y)\cdot(\iota_2\circ\pi_2)(y)\cdots(\iota_n\circ\pi_n)(y)$$

$$\implies [(\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)](x)=[(\iota_1\circ\pi_1)\cdot(\iota_2\circ\pi_2)\cdots(\iota_n\circ\pi_n)](y) \implies \mathsf{Id}_G(x)=\mathsf{Id}_G(y) \implies x=y$$

Τέλος, η απεικόνιση f είναι επιμορφισμός, διότι, αν $\mathsf{x}=(x_1,x_2,\cdots,x_n)\in G_1\times G_2\times\cdots\times G_n$, τότε θεωρούμε το στοιχείο $a=\iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n)\in G$, και θα έχουμε:

$$f(a)=\big(\pi_1(\iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n)),\ \pi_2(\iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n)),\ \cdots,\ \pi_n(\iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n))\big)$$

Θέτουμε $a_k=\pi_k(\iota_1(x_1)\cdot\iota_2(x_2)\cdots\iota_n(x_n))\in G_k$, $1\le k\le n$, και τότε $f(a)=(a_1,a_2,\cdots,a_n)$. Επειδή η απεικόνιση π_k είναι ομομορφισμός ομάδων, λαμβάνοντας υπόψη τις σχέσεις του μέρους 2., θα έχουμε:

$$a_k=\pi_n(\iota_1(x_1))\cdot\pi_k(\iota_2(x_2))\cdots\pi_k(\iota_n(x_n))=(\pi_k\circ\iota_1)(x_1)\cdot(\pi_k\circ\iota_2)(x_2)\cdots(\pi_k\circ\iota_k)(x_k)\cdots(\pi_k\circ\iota_n)(x_n)=$$

$$=\epsilon_{1k}(x_1)\cdot\epsilon_{2k}(x_2)\cdots\mathsf{Id}_{G_k}(x_k)\cdots\epsilon_{nk}(x_n)=e_k\cdot e_k\cdots x_k\cdots e_k=x_k$$

Επομένως θα έχουμε: $f(a)=(a_1,a_2,\cdots,a_n)=(x_1,x_2,\cdots,x_n)=\mathsf{x}$, και η απεικόνιση f είναι επιμορφισμός. Συνοψίζοντας, δείξαμε ότι η απεικόνιση f είναι ισομορφισμός ομάδων. ■

2.10 Ασκήσεις

Άσκηση 2.10.1. *Έστω $(G,\cdot)$ μια ομάδα. Ορίζουμε μια διμελή πράξη «$\star$» επί του G ως εξής:*

$$\cdot^{\mathsf{op}}:\ G\times G\longrightarrow G,\quad a\cdot^{\mathsf{op}}b=b\cdot a$$

Να δειχθεί ότι το ζεύγος $(G,\cdot^{\mathsf{op}})$ είναι ομάδα, η οποία καλείται η **αντίθετη ομάδα** *της ομάδας $(G,\cdot)$ και συμβολίζεται απλώς ως G^{op}. Ποια είναι η αντίθετη ομάδα της αντίθετης ομάδας G^{op} της ομάδας G; Πότε μια ομάδα συμπίπτει, ως ομάδα, με την αντίθετή της;*

Άσκηση 2.10.2. *Έστω $(G,/)$ ένα ζεύγος αποτελούμενο από ένα μη κενό σύνολο G και μια διμελή πράξη $/:G\times G\longrightarrow G$, $(a,b)\longmapsto a/b$, επί του συνόλου G έτσι ώστε:*

1. *Υπάρχει ένα στοιχείο $1\in G$ έτσι ώστε: $a/b=1\iff a=b$.*
2. *Αν $a,b,c\in G$, τότε: $(a/b)/(c/d)=a/b$.*

Να δειχθεί ότι το ζεύγος $(G,\cdot)$ είναι ομάδα, όπου «$\cdot$» είναι η διμελής πράξη

$$\cdot:\ G\times G\longrightarrow G,\quad a\cdot b=a/(1/b)$$

Άσκηση 2.10.3. *Έστω X ένα μη κενό σύνολο και $\mathsf{Rel}(X)$ το σύνολο των σχέσεων επί του X. Τότε το ζεύγος $\mathsf{Rel}(X),\circ)$, όπου «$\circ$» είναι η πράξη μεταξύ σχέσεων επί του X η οποία ορίστηκε στην υποενότητα 1.1.1, είναι ένα μονοειδές (βλέπε Άσκηση 1.5.6). Να προσδιοριστεί η ομάδα $\mathsf{U}(\mathsf{Rel}(X),\circ))$ των αντιστρέψιμων στοιχείων του μονοειδούς $\mathsf{Rel}(X),\circ)$.*

Άσκηση 2.10.4. *Να δειχθεί ότι υπάρχουν παραδείγματα ζευγών $(G,\cdot)$, όπου «$\cdot$» είναι μια προσεταιριστική πράξη επί του συνόλου G έτσι ώστε να ικανοποιούνται οι ακόλουθες συνθήκες 1. και 2. ή οι ακόλουθες συνθήκες 3. και 4.:*

1. *(Ύπαρξη δεξιού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $a\cdot e=a$, $\forall\, a\in G$.*
2. *(Ύπαρξη αριστερού αντίστροφου στοιχείου). Για κάθε στοιχείο $a\in G$, υπάρχει ένα στοιχείο $a'\in G$ έτσι ώστε: $a'\cdot a=e$.*

3. *(Ύπαρξη αριστερού ουδέτερου στοιχείου). Υπάρχει ένα στοιχείο e έτσι ώστε $e \cdot a = a$, $\forall\, a \in G$.*

4. *(Ύπαρξη δεξιού αντίστροφου στοιχείου). Για κάθε στοιχείο $a \in G$, υπάρχει ένα στοιχείο $a' \in G$ έτσι ώστε: $a \cdot a' = e$.*

και το ζεύγος $(G, \cdot)$ **δεν είναι** *ομάδα.*[19]

Άσκηση 2.10.5. *Έστω $(G, \cdot)$ ένα ζεύγος αποτελούμενο από ένα μη κενό σύνολο G και μια προσεταιριστική διμελή πράξη «$\cdot$» επί του G.*

1. *Να δειχθεί ότι αν, για κάθε $a, b \in G$, οι γραμμικές εξισώσεις $a \cdot x = b$ και $y \cdot a = b$ έχουν λύση στο σύνολο G, τότε υπάρχει ουδέτερο στοιχείο για την πράξη «$\cdot$» και το ζεύγος $(G, \cdot)$ είναι ομάδα.*

2. *Να δειχθεί ότι αν, το σύνολο G είναι πεπερασμένο και ισχύουν οι Νόμοι Διαγραφής, δηλαδή $a \cdot c = b \cdot c \Longrightarrow a = b$ και $c \cdot a = c \cdot b \Longrightarrow a = b$, τότε το ζεύγος $(G, \cdot)$ είναι ομάδα.*

Άσκηση 2.10.6. *Έστω $(G, \cdot)$ μια ομάδα, και θεωρούμε το ζεύγος $(\mathscr{P}(G)^*, \cdot)$, όπου $\mathscr{P}(G)^*$ είναι το σύνολο των μη κενών υποσυνόλων της G και «$\cdot$» η πράξη επί του $\mathscr{P}(G)^*$ η οποία ορίζεται ως: $S \cdot T = \{s \cdot t \in G \mid s \in S,\ t \in T\}$.*

1. *Να δειχθεί ότι γενικά η πράξη «$\cdot$» επί του $\mathscr{P}(G)^*$ δεν είναι μεταθετική.*

2. *Να εξεταστεί αν το ζεύγος $(\mathscr{P}(G)^*, \cdot)$ αποτελεί ομάδα.*

3. *Να δειχθεί ότι ένα μη κενό υποσύνολο $H \subseteq G$ είναι υποομάδα της G αν και μόνο $H \cdot H \subseteq H$ και $H^{-1} \subseteq H$ (και τότε $H \cdot H = H$ και $H^{-1} = H$) αν και μόνο αν $H \cdot H^{-1} \subseteq H$ (και τότε $H \cdot H^{-1} = H$).*

Άσκηση 2.10.7. *Θεωρούμε το ανοιχτό διάστημα $(-1, 1) = \{x \in \mathbb{R} \mid -1 < x < 1\}$ της πραγματικής ευθείας $\mathbb{R}$. Να δειχθεί ότι ορίζοντας*

$$\forall\, x, y \in (-1, 1): \quad x \star y = \frac{x + y}{1 + xy}$$

αποκτούμε μια διμελή πράξη επί του $(-1, 1)$ έτσι ώστε το ζεύγος $((-1, 1), \star)$ είναι ομάδα.

Άσκηση 2.10.8. *Να οριστεί κατάλληλη διμελής πράξη «$\star$» επί του ανοιχτού διαστήματος $(-1, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}$ της πραγματικής ευθείας $\mathbb{R}$, έτσι ώστε το ζεύγος $((0, 1), \star)$ είναι ομάδα και το αντίστροφο του στοιχείου x ως προς την πράξη «$\star$» είναι το $1 - x$.*

Άσκηση 2.10.9. *Να δειχθεί ότι κάθε (ανοιχτό ή κλειστό) διάστημα $I \subseteq \mathbb{R}$ της πραγματικής ευθείας, μπορεί να εφοδιαστεί με μια διμελή πράξη «$\star$» έτσι ώστε το ζεύγος $(I, \star)$ είναι ομάδα.*

Άσκηση 2.10.10. *Έστω X ένα μη-κενό σύνολο, και θεωρούμε την ομάδα μεταθέσεων $(\mathsf{S}(X), \circ)$ επι του X. Έστω $Y \subseteq X$ ένα μη-κενό υποσύνολο του X.*

1. *Αν το υποσύνολο Y είναι πεπερασμένο, να δειχθεί ότι το υποσύνολο*

$$H = \{f \in \mathsf{S}(X) \mid f(Y) \subseteq Y\}$$

είναι μια υποομάδα της $\mathsf{S}(X)$.

2. *Να δειχθεί με ένα παράδειγμα ότι, αν το υποσύνολο Y είναι άπειρο, τότε γενικά το υποσύνολο H δεν είναι υποομάδα της $\mathsf{S}(X)$.*

---

[19] Τέτοια παραδείγματα αναλύθηκαν διεξοδικά για πρώτη φορά στις εργασίες των A.H. Clifford: *A system arising from a weakened set of group postulates*, Annals of Mathematics **34** (1933), 865-871 και H. B. Mann: *On certain systems which are almost groups*, Bull. Amer. Math. Soc. **50** (1944), 879–881.

Άσκηση 2.10.11. *Αν $(G,\cdot)$ είναι μια ομάδα.*

1. *Αν η ομάδα G έχει άρτιο πλήθος στοιχείων, να δειχθεί ότι η G περιέχει τουλάχιστον ένα στοιχείο $e \neq a \in G$, έτσι ώστε: $a^2 = e$.*
2. *Αν για κάθε στοιχείο $a \in G$ ισχύει ότι $a^2 = e$, $\forall\, a \in G$, να δειχθεί ότι η ομάδα G είναι αβελιανή.*
3. *Είναι η ομάδα G αβελιανή, αν ισχύει ότι $a^3 = e$, $\forall\, a \in G$;*

Άσκηση 2.10.12. *Να δειχθεί ότι υπάρχουν ακριβώς δύο ομάδες με διαφορετικό πίνακα Cayley και πλήθος στοιχείων ίσο με 4, η ομάδα των τεσσάρων στοιχείων V_4 του Klein και η κυκλική ομάδα C_4 με τέσσερα στοιχεία.*

Πόσες ομάδες τάξης 5 υπάρχουν με διαφορετικό πίνακα Cayley;

Άσκηση 2.10.13. *Να κατασκευαστεί ο πίνακας Cayley της ομάδας $(G,\star)$ του «παιχνιδιού με δύο κέρματα», βλέπε το παράδειγμα 2.2.3, και να δειχθεί ότι το ζεύγος $(G,\star)$ είναι μια ομάδα με οκτώ στοιχεία η οποία δεν είναι αβελιανή.*

Άσκηση 2.10.14. *Να κατασκευαστεί ο πίνακας Cayley της ομάδας Q των τετρανίων του Hamilton, και να σχεδιαστεί το διάγραμμα Hasse των υποομάδων της.*

Άσκηση 2.10.15. *Θεωρούμε το ακόλουθο σύνολο πινάκων*

$$H = \left\{ D(a,b) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathsf{M}_3(\mathbb{Q}) \;\mid\; a,b \in \mathbb{Z} \right\}$$

και

$$K = \left\{ D(a,b,c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathsf{M}_3(\mathbb{Q}) \;\mid\; a,b,c \in \mathbb{Z} \right\}$$

Να δειχθεί ότι: $H, K \leq \mathsf{GL}_3(\mathbb{Z})$. Επίσης να δειχθεί ότι η H είναι αβελιανή, αλλά η K δεν είναι αβελιανή.

Άσκηση 2.10.16. *Έστω $(G,\cdot)$ μια ομάδα. Αν H και K είναι υποομάδες της G, τότε να δειχθεί ότι η ένωση $H \cup K$ των υποσυνόλων H και K είναι μια υποομάδα της G αν και μόνο είτε $H \subseteq K$ είτε $K \subseteq H$.*

Άσκηση 2.10.17. *Έστω $\{H_k\}_{k\geq 0}$ μια οικογένεια υποομάδων μιας ομάδας G, για την οποία ισχύει ότι για κάθε $k,n \geq 0$ είτε $H_k \subseteq H_n$ είτε $H_n \subseteq H_k$. Να δειχθεί ότι η ένωση $\bigcup_{k=0}^{\infty} H_k$ είναι μια υποομάδα της G, η οποία είναι αβελιανή αν κάθε ομάδα H_k είναι αβελιανή.*

Άσκηση 2.10.18.

1. *Να δειχθεί ότι δεν υπάρχει ομάδα η οποία είναι ένωση δύο γνήσιων υποομάδων της.*
2. *Υπάρχει ομάδα η οποία είναι ένωση τριών γνήσιων υποομάδων της;*

Άσκηση 2.10.19. *Θεωρούμε το ακόλουθο σύνολο απεικονίσεων* $: \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}$

$$f_1 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_1(x) = x \quad \text{και} \quad f_2 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_2(x) = \frac{1}{x}$$

$$f_3 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_1(x) = 1-x \quad \text{και} \quad f_4 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_2(x) = \frac{1}{1-x}$$

$$f_5 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_5(x) = \frac{x}{1-x} \quad \text{και} \quad f_6 : \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}, \quad f_6(x) = \frac{1-x}{x}$$

Αν $G = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, να δειχθεί ότι το ζεύγος $(G,\circ)$, όπου «$\circ$» είναι η σύνθεση απεικονίσεων είναι μια μη αβελιανή ομάδα με έξι στοιχεία, και να βρεθεί ένα ελάχιστο σύνολο γεννητόρων της G.

Άσκηση 2.10.20. *Μια ομάδα $(G,\cdot)$ ικανοποιεί τη* ***συνθήκη φθίνουσας αλυσίδας*** *αν για κάθε φθίνουσα ακολουθία*

$$\cdots \leq H_{n+1} \leq H_n \leq \cdots \leq H_2 \leq H_1 \leq G$$

υποομάδων της G, υπάρχει $k \geq 1$ έτσι ώστε: $H_k = H_{k+r}$, $\forall r \geq 1$. Η ομάδα $(G,\cdot)$ ικανοποιεί τη **συνθήκη ελαχίστου**, *αν κάθε μη κενό σύνολο υποομάδων της G έχει ελάχιστο στοιχείο.*

Να δειχθεί ότι η ομάδα G ικανοποιεί τη συνθήκη φθίνουσας αλυσίδας, αν και μόνο αν ικανοποιεί τη συνθήκη ελαχίστου.

Άσκηση 2.10.21. *Έστω$(G,\cdot)$ μια ομάδα, και $S \subseteq G$ ένα μη κενό υποσύνολο της G.*

1. *Να δειχθεί ότι: $\mathsf{Z}(G) = \{x \in G \mid \mathsf{N}_G(x) = G\}$.*
2. *Αν $x \in G$, να δειχθεί ότι: $x\mathsf{N}_G(S)x^{-1} = \mathsf{N}_G(xSx^{-1})$.*

Άσκηση 2.10.22. *Έστω $(G,\cdot)$ μια ομάδα, και $S \subseteq G$ ένα μη-κενό υποσύνολο της G, Να δειχθεί ότι $\mathsf{C}_G(S) \subseteq \mathsf{N}_G(S)$. Αν $S \leq G$ είναι υποομάδα της G, να δειχθεί ότι $S \subseteq \mathsf{N}_G(S)$ και η S είναι κανονική υποομάδα της $\mathsf{N}_G(S)$.*

Άσκηση 2.10.23. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα, για την οποία υπάρχει $n > 1$ έτσι ώστε: $(a\cdot b)^n = a^n \cdot b^n$. Για κάθε $k \geq 1$, θέτουμε*

$$G_k = \{x^k \in G \mid x \in G\} \quad \text{και} \quad G(n) = \{x \in G \mid \exists m = m(x) \in \mathbb{N}:\ x^{n^m} = e\}$$

1. *Να δειχθεί ότι τα υποσύνολα G_n και G_{n-1} είναι κανονικές υποομάδες της G.*
2. *Αν ο n είναι πρώτος, τότε να δειχθεί ότι το υποσύνολο $G(n)$ είναι κανονική υποομάδα της G.*

Άσκηση 2.10.24. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και $S,T \subseteq G$ είναι δύο υποσύνολά της. Να δειχθεί ότι:*

1. $S \subseteq \mathsf{C}_G(\mathsf{C}_G(S))$.
2. $S \subseteq T \implies \mathsf{C}_G(T) \subseteq \mathsf{C}_G(S)$.
3. $\mathsf{C}_{\mathsf{C}_G(S)}(S) = \mathsf{C}_G(S)$.
4. $\mathsf{C}_G(S) = \mathsf{C}_G(\langle S\rangle)$.

Τέλος, να εξεταστεί αν τα παραπάνω εξακολουθούν να ισχύουν, αν ο κεντροποιητής $\mathsf{C}_G(S)$ αντικατασταθεί από τον κανονικοποιητή $\mathsf{N}_G(S)$.

Άσκηση 2.10.25. *Θεωρούμε τους ακόλουθους (αντιστρέψιμους) 2×2 πίνακες πραγματικών αριθμών:*

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \quad \text{και} \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Θεωρώντας τους πίνακες A,B ως στοιχεία της γενικής γραμμικής ομάδας $\mathsf{GL}(2,\mathbb{R})$, έστω $H = \langle A\rangle$ και $K = \langle B\rangle$ οι κυκλικές υποομάδες της $\mathsf{GL}(2,\mathbb{R})$ οι οποίες παράγονται από τους πίνακες A και B. Να δειχθεί ότι το υποσύνολο $H\cdot K$ δεν είναι υποομάδα της $\mathsf{GL}(2,\mathbb{R})$.

Άσκηση 2.10.26. *Έστω $(G,\cdot)$ μια ομάδα και $H,K \subseteq G$ δύο υποομάδες της G. Να δειχθεί ότι το υποσύνολο $H\cdot K$, ισοδύναμα το υποσύνολο $K\cdot H$, είναι υποομάδα της G αν και μόνο αν: $H\cdot K = K\cdot H$.*

Άσκηση 2.10.27. 1. *Να βρεθούν όλα τα ελάχιστα σύνολα γεννητόρων μιας κυκλικής ομάδας τάξης ≤ 10. Τι παρατηρείτε;*

2. *Να βρεθεί ένα σύνολο γεννητόρων της συμμετρικής ομάδας* S_4.

3. *Να περιγραφούν όλα τα ελάχιστα σύνολα γεννητόρων της συμμετρικής ομάδας* S_3, *της ομάδας* Q *των τετρανίων του Hamilton, και τέλος της ομάδας* G *του «παιχνιδιού με δύο κέρματα», όπως αυτή αναλύθηκε στο Παράδειγμα 2.2.3.*

Άσκηση 2.10.28. *Ένα υποσύνολο* S *μιας ομάδας* G *καλείται* **κανονικό υποσύνολο**, *αν:* $gSg^{-1} \subseteq S$, $\forall g \in G$. *Να δειχθεί ότι η υποομάδα* $\langle S \rangle$ *η οποία παράγεται από ένα κανονικό υποσύνολο* $S \subseteq G$ *είναι μια κανονική υποομάδα της* G.

Άσκηση 2.10.29. *Έστω* T *ένα υποσύνολο μιας ομάδας* G. *Να δειχθεί ότι το υποσύνολο*

$$S = \bigcup_{g \in G} gTg^{-1} = \{gxg^{-1} \in G \mid g \in G,\ x \in T\}$$

είναι κανονικό και η υποομάδα $\langle S \rangle$ *είναι η μικρότερη κανονική υποομάδα της* G *η οποία περιέχει το σύνολο* T.

Άσκηση 2.10.30. *Να δειχθεί ότι η* n*-οστή γενικευμένη ομάδα τετρανίων* Q_n, $n \geq 1$, *βλέπε το Παράδειγμα 2.4.39, είναι μια μη αβελιανή ομάδα τάξης* $4n$ *και κάθε αβελιανή υποομάδα της είναι κυκλική.*

Άσκηση 2.10.31. *Να δειχθεί ότι για την διεδρική ομάδα* D_n, $n \geq 3$, *η οποία ορίστηκε στην υποενότητα 2.2, κανοποιούνται οι ακόλουθες σχέσεις:*

$$R^n = T^2 = (R \circ T)^2 = \mathsf{Id}_{\mathbb{R}^2} \quad \text{και} \quad R^k \neq \mathsf{Id}_{\mathbb{R}^2}, \ \text{αν} \ 1 < k < n$$

Αν $H = \langle R \rangle$ *είναι η κυκλική υποομάδα της* D_n, *η οποία παράγεται από τη στροφή* R, *να εξεταστεί αν η* H *είναι κανονική υποομάδα της* D_n.

Άσκηση 2.10.32. *Θεωρούμε τους ακόλουθους αντιστρέψιμους πίνακες πραγματικών αριθμών*

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad \text{και} \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

τους οποίους θεωρούμε ως στοιχεία της ομάδας $\mathsf{GL}(2,\mathbb{R})$. *Έστω* $H = \langle A, B \rangle$ *η υποομάδα της* $\mathsf{GL}(2,\mathbb{R})$ *η οποία παράγεται από τους πίνακες* A *και* B.

1. *Να δειχθεί ότι η* H *είναι μια μη αβελιανή ομάδα τάξης* 8 *η οποία δεν είναι ισόμορφη με την ομάδα* Q *των τετρανίων του Hamilton.*

2. *Να δειχθεί ότι η* H *είναι ισόμορφη με την ομάδα* G *του «παιχνιδιού με δύο κέρματα», όπως αυτή αναλύθηκε στο Παράδειγμα 2.2.3.*

Άσκηση 2.10.33. *Θεωρούμε τους ακόλουθους αντιστρέψιμους πίνακες μιγαδικών αριθμών*

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{και} \qquad D = \begin{pmatrix} \zeta_n & 0 \\ 0 & \zeta_n^{-1} \end{pmatrix}$$

τους οποίους θεωρούμε ως στοιχεία της ομάδας $\mathsf{GL}(2,\mathbb{C})$. *Έστω* $D_n = \langle C, D \rangle$ *η υποομάδα της* $\mathsf{GL}(2,\mathbb{C})$ *η οποία παράγεται από τους πίνακες* C *και* D.

1. *Να δειχθεί ότι:* $C^2 = B^n = (C \cdot B)^2 = I_2$.

2. *Να δειχθεί ότι η ομάδα* D_n *έχει τάξη* $|D_n| = 2n$.

3. *Να δειχθεί ότι η ομάδα D_4 είναι ισόμορφη με την ομάδα G του «παιχνιδιού με δύο κέρματα», όπως αυτή αναλύθηκε στο Παράδειγμα 2.2.3.*

Άσκηση 2.10.34. *Θεωρούμε τους ακόλουθους αντιστρέψιμους 2×2 πίνακες πραγματικών αριθμών:*

$$B=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \qquad \text{και} \qquad S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

Να δειχθεί ότι το ζεύγος $(G,\cdot)$, όπου $G=\{I_2,S,S^2,S^3,B,S\cdot B,S^2\cdot B,S^3\cdot B\}$ και «$\cdot$» είναι η συνήθης πράξη πολλαπλασιασμού πινάκων, είναι μια υποομάδα της $\mathsf{GL}(2,\mathbb{R})$, η οποία είναι ισόμορφη με την ομάδα G του «παιχνιδιού με δύο κέρματα», όπως αυτή αναλύθηκε στο Παράδειγμα 2.2.3.

Άσκηση 2.10.35. *Θεωρούμε τους ακόλουθους αντιστρέψιμους 3×3 πίνακες πραγματικών αριθμών:*

$$A=\begin{pmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & -1\end{pmatrix} \qquad \text{και} \qquad R=\begin{pmatrix}0 & -1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 1\end{pmatrix}$$

Να δειχθεί ότι το ζεύγος $(G,\cdot)$, όπου $G=\{I_3,R,R^2,R^3,A,R\cdot A,R^2\cdot A,R^3\cdot A\}$ και «$\cdot$» είναι η συνήθης πράξη πολλαπλασιασμού πινάκων, είναι μια υποομάδα της $\mathsf{GL}(3,\mathbb{R})$, η οποία είναι ισόμορφη με την ομάδα G του «παιχνιδιού με δύο κέρματα», όπως αυτή αναλύθηκε στο Παράδειγμα 2.2.3.

Άσκηση 2.10.36. *Έστω $(G,\cdot)$ μια ομάδα και x,y,z στοιχεία της G. Να δειχθούν τα ακόλουθα:*

1. $[x,y]\cdot y=x\cdot y\cdot x^{-1}$ *και* $x^{-1}\cdot[x,y]=y\cdot x\cdot y^{-1}$.
2. $[x\cdot y,z]=x\cdot[y,z]\cdot x^{-1}\cdot[x,z]$.
3. $[x,y\cdot z]=[x,y]\cdot y\cdot[x,z]\cdot y^{-1}$.

Άσκηση 2.10.37. *Θεωρούμε την προσθετική ομάδα $(\mathbb{Z},+)$ των ακεραίων. Αν $n,m\in\mathbb{Z}$, να περιγραφούν οι εξής υποομάδες της $\mathbb{Z}$: (α) η υποομάδα $\langle n,m\rangle$ η οποία παράγεται από τα στοιχεία n,m, (β) η υποομάδα $n\mathbb{Z}+m\mathbb{Z}$, (γ) η υποομάδα $\langle n\mathbb{Z}\bigcup m\mathbb{Z}\rangle$, και ($\delta$) η υποομάδα $n\mathbb{Z}\bigcap m\mathbb{Z}$.*

Άσκηση 2.10.38. *Να δειχθεί ότι η προσθετική ομάδα $(\mathbb{Q},+)$ δεν είναι πεπερασμένα παραγόμενη. Είναι οι προσθετικές ομάδες $(\mathbb{R},+)$ και $(\mathbb{C},+)$ πεπερασμένα παραγόμενες;*

Αν $\mathbb{K}\in\{\mathbb{Q},\mathbb{R},\mathbb{C}\}$, είναι οι πολλαπλασιαστικές ομάδες $(\mathbb{K}^*,\cdot)$ πεπερασμένα παραγόμενες;

Άσκηση 2.10.39. *Να δειχθεί ότι το σύνολο $\left\{\frac{1}{p^n}\in\mathbb{Q}\mid p:\ \text{πρώτος},\ \ n\in\mathbb{N}\right\}$ είναι ένα ελάχιστο σύνολο γεννητόρων της προσθετικής ομάδας $(\mathbb{Q},+)$:*

$$\mathbb{Q}=\left\langle\left\{\frac{1}{p^n}\in\mathbb{Q}\mid p:\ \text{πρώτος},\ \ n\in\mathbb{N}\right\}\right\rangle$$

Μια ομάδα $(G,\cdot)$ καλείται **(ευθέως) αναλύσιμη**, αν η G είναι ισόμορφη με το εξωτερικό ευθύ γινόμενο δύο μη τετριμμένων ομάδων. Ισοδύναμα η G είναι αναλύσιμη, αν η G είναι το εσωτερικό ευθύ γινόμενο δύο μη τετριμμένων υποομάδων της. Η ομάδα G καλείται **(ευθέως) μη αναλύσιμη**, αν η G δεν είναι (ευθέως) αναλύσιμη.

Άσκηση 2.10.40. *Να εξεταστεί αν η συμμετρική ομάδα S_3 είναι αναλύσιμη. Είναι η κυκλική ομάδα $(\mathbb{Z}_n,+)$ αναλύσιμη; Είναι η προσθετική ομάδα $(\mathbb{Z},+)$ αναλύσιμη;*

Άσκηση 2.10.41. *1. Να δειχθεί ότι κάθε πεπερασμένα παραγόμενη υποομάδα της προσθετικής ομάδας $(\mathbb{Q},+)$ είναι κυκλική.*

2. Να δειχθεί ότι η προσθετική ομάδα $(\mathbb{Q},+)$ είναι μη αναλύσιμη.

3. Να δειχθεί ότι κάθε πεπερασμένα παραγόμενη υποομάδα της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*,\cdot)$ είναι κυκλική.

4. Να δειχθεί ότι η ομάδα $(\mathbb{C}^*,\cdot)$ είναι αναλύσιμη.

Άσκηση 2.10.42. *Έστω $(G,\cdot)$ μια ομάδα, και θεωρούμε την ομάδα εξωτερικό ευθύ γινόμενο $G\times G$. Να δειχθεί ότι το υποσύνολο*

$$D=\{(x,x)\in G\times G \mid x\in G\}$$

είναι μια υποομάδα της $G\times G$, η οποία είναι κανονική αν και μόνο αν η ομάδα G είναι αβελιανή.

Άσκηση 2.10.43. *Αν $(G_1,\cdot),\cdots,(G_n,\cdot)$ είναι ένα πεπερασμένο πλήθος ομάδων, τότε να δειχθεί ότι για κάθε μετάθεση $\sigma\in\mathsf{S}_n$, υπάρχει ένας ισομορφισμός ομάδων:*

$$G_1\times G_2\times\cdots\times G_n \;\cong\; G_{\sigma(1)}\times G_{\sigma(2)}\times\cdots\times G_{\sigma(n)}$$

Άσκηση 2.10.44. *Αν $(G_1,\cdot),\cdots,(G_n,\cdot)$ είναι ένα πεπερασμένο πλήθος ομάδων, τότε να δειχθεί ότι:*

$$\mathsf{Z}\big(G_1\times G_2\times\cdots\times G_n\big) \;=\; \mathsf{Z}(G_1)\times\mathsf{Z}(G_2)\times\cdots\times\mathsf{Z}(G_n)$$

Άσκηση 2.10.45. *Έστω ότι $f_k\colon G_k\longrightarrow H_k$, $1\le k\le n$, είναι ομομορφισμοί μεταξύ των ομάδων $\{(G_k,\cdot)\}_{k=1}^n$ και $\{(H_k,\cdot)\}_{k=1}^n$. Να δειχθεί οτι ο επαγόμενος ομομορφισμός γινόμενο $\prod_{k=1}^n f_k\colon\prod_{k=1}^n G_k\longrightarrow\prod_{k=1}^n H_k$ είναι μονομορφισμός, αντίστοιχα, επιμορφισμός, αντίστοιχα ισομορφισμός, αν και μόνο αν κάθε ομομορφισμός f_k, $1\le k\le n$, είναι μονομορφισμός, αντίστοιχα, επιμορφισμός, αντίστοιχα ισομορφισμός.*

Άσκηση 2.10.46. *Θεωρούμε το ακόλουθα σύνολα αντιστρέψιμων 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς:*

$$G=\left\{\begin{pmatrix}a & b\\ 0 & d\end{pmatrix}\in\mathsf{M}_2(\mathbb{R})\mid ad\neq 0\right\}\qquad\text{και}\qquad H=\left\{\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}\in\mathsf{M}_2(\mathbb{R})\mid b\in\mathbb{R}\right\}$$

1. *Να δειχθεί ότι το σύνολο G είναι μια υποομάδα της $\mathsf{GL}(2,\mathbb{R})$ και το υποσύνολο H είναι μια υποομάδα της G.*
2. *Να δειχθεί ότι: $\big[\mathsf{GL}(2,\mathbb{R}),\mathsf{GL}(2,\mathbb{R})\big]=\mathsf{SL}(2,\mathbb{R})$.*
3. *Να δειχθεί ότι: $[G,G]=H$.*

Άσκηση 2.10.47. *Αν $(G_1,\cdot),\cdots,(G_n,\cdot)$ είναι ένα πεπερασμένο πλήθος ομάδων, τότε να εξεταστεί αν ισχύει η ακόλουθη ισότητα υποομάδων της ομάδας $G_1\times G_2\times\cdots\times G_n$:*

$$\big[G_1\times G_2\times\cdots\times G_n,\; G_1\times G_2\times\cdots\times G_n\big] \;=\; [G_1,G_1]\times[G_2,G_2]\times\cdots\times[G_n,G_n]$$

Άσκηση 2.10.48. *Έστω $(G,\cdot)$ μια ομάδα. Να δειχθεί ότι η απεικόνιση $f\colon G\longrightarrow G$, $f(x)=x^{-1}$, δεν είναι γενικά ομομορφισμός ομάδων. Πότε η απεικόνιση $f\colon G\longrightarrow G$ είναι ομομορφισμός ομάδων; Να δειχθεί ότι η απεικόνιση f είναι πάντα ομομορφισμός, και μάλιστα ισομορφισμός, ομάδων $f\colon G\longrightarrow G^{\mathsf{op}}$, όπου G^{op} είναι η αντίθετη ομάδα της G, όπως στην Άσκηση 2.10.1:*

$$\text{αν } G \text{ είναι ομάδα, τότε: } \; G\;\cong\; G^{\mathsf{op}}$$

Να βρεθούν τουλάχιστον δύο ισομορφισμοί $\mathsf{GL}(n,\mathbb{R})\xrightarrow{\cong}\mathsf{GL}(n,\mathbb{R})^{\mathsf{op}}$.

Άσκηση 2.10.49. *Έστω $(G_1, \star)$ και $(G_2, *)$ δύο ομάδες, και θεωρούμε το σύνολο*

$$\mathsf{Hom}_{\mathsf{Grp}}(G_1, G_2) = \{f : G_1 \longrightarrow G_2 \mid f : \text{ομομορφισμός ομάδων}\}$$

Αν $f, g \in \mathsf{Hom}_{\mathsf{Grp}}(G_1, G_2)$, ορίζουμε απεικόνιση $f \cdot g : G_1 \longrightarrow G_2$, $(f \cdot g)(x) = f(x) * g(x)$. Να εξεταστεί αν, και υπό ποιες προϋποθέσεις, το ζεύγος $\left(\mathsf{Hom}_{\mathsf{Grp}}(G_1, G_2), \cdot\right)$ είναι ομάδα.

Άσκηση 2.10.50. *Θεωρούμε το σύνολο απεικονίσεων*

$$G = \left\{ f_{a,b} : \mathbb{R} \longrightarrow \mathbb{R}, \;\; f_{a,b}(x) = ax + b \;\mid\; a \in \mathbb{R}^*, b \in \mathbb{R} \right\}$$

1. *Να δειχθεί ότι το ζεύγος $(G, \circ)$, όπου «$\circ$» είναι η σύνθεση απεικονίσεων, αποτελεί μια άπειρη μη αβελιανή ομάδα, υποομάδα της ομάδας μεταθέσεων $(\mathsf{S}(\mathbb{R}), \circ)$.*

2. *Να δειχθεί ότι το υποσύνολο*

$$N = \left\{ f_{1,b} : \mathbb{R} \longrightarrow \mathbb{R}, \;\; f_{1,b}(x) = x + b \;\mid\; b \in \mathbb{R} \right\}$$

   είναι μια κανονική υποομάδα της G η οποία είναι αβελιανή.

3. *Με ποια γνωστή σας ομάδα είναι ισόμορφη η N;*

Άσκηση 2.10.51. *Στο σύνολο $G := \mathbb{R}^* \times \mathbb{R} = \{(a, b) \in \mathbb{R}^2 \mid a \neq 0\}$ ορίζουμε διμελή πράξη*

$$* : G \times G \longrightarrow G, \quad (a, b) * (c, d) = (ac, ad + b)$$

Να δειχθεί ότι το ζεύγος $(G, *)$ είναι ομάδα η οποία είναι ισόμορφη με την ομάδα της Άσκησης 2.10.50. Να δειχθεί επίσης ότι το υποσύνολο $H = \{(1, b) \in G \mid b \in \mathbb{R}\}$ είναι μια κανονική υποοομάδα της G.

Άσκηση 2.10.52. *Έστω $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, και έστω $\mathcal{V}$ ένας διανυσματικός χώρος διάστασης $n < \infty$ υπεράνω του $\mathbb{K}$. Να δειχθεί ότι υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{GL}(\mathcal{V}) \xrightarrow{\cong} \mathsf{GL}(n, \mathbb{K})$$

όπου $\mathsf{GL}(\mathcal{V})$ είναι η ομάδα των ισομορφισμών $\mathbb{K}$-διανυσματικών χώρων από τον $\mathcal{V}$ στον $\mathcal{V}$ με πράξη τη σύνθεση απεικονίσεων, και $\mathsf{GL}(n, \mathbb{K})$ είναι η πολλαπλασιαστική ομάδα των αντιστρέψιμων $n \times n$ πινάκων με στοιχεία από το $\mathbb{K}$.

Κεφάλαιο 3

Το Θεώρημα του Lagrange και οι Εφαρμογές του

Στο παρόν Κεφάλαιο, θα αποδείξουμε το Θεώρημα του Lagrange, το οποίο αποτελεί ένα από τα βασικότερα αποτελέσματα της (στοιχειώδους) θεωρίας ομάδων, και θα δούμε κάποιες από τις άμεσες εφαρμογές του, ιδιαίτερα στη δομή των κυκλικών ομάδων και των ομάδων μικρής τάξης. Το παρόν Κεφάλαιο χωρίζεται σε τρία μέρη. Στο πρώτο μέρος, το οποίο αποτελείται από τις παραγράφους 3.1 και 3.2, αναπτύσσεται η βασική θεωρία τάξης στοιχείου και ομάδας. Στο δεύτερο μέρος, το οποίο αποτελείται από τις παραγράφους 3.3, 3.4, και 3.5, αναλύεται η θεωρία πλευρικών κλάσεων μιας ομάδας ως προς μια υποομάδα, αποδεικνύεται το Θεώρημα του Lagrange, και εξετάζεται αν ισχύει το αντίστροφό του. Τέλος, το τρίτο μέρος του Κεφαλαίου, παράγραφοι 3.6 και 3.8, είναι αφιερωμένο σε κάποιες άμεσες εφαρμογές του Θεωρήματος του Lagrange, για παράδειγμα στη στοιχειώδη Θεωρία Αριθμών. Περισσότερες εφαρμογές αναλύονται σε επόμενα Κεφάλαια.

3.1 Τάξη Στοιχείου και Ομάδας

Στην παρούσα ενότητα θα ορίσουμε και θα μελετήσουμε κάποιες πολύ βασικές έννοιες στη Θεωρία Ομάδων: την έννοια της τάξης μιας ομάδας και την συνοδό έννοια της τάξης στοιχείου μιας ομάδας. Η τελευταία έννοια θα οριστεί μέσω της κυκλικής υποομάδας την οποία παράγει το στοιχείο.

Από τώρα και στο εξής θα χρησιμοποιούμε πολλαπλασιαστικό συμβολισμό για μια ομάδα. Έτσι, όπως στο προηγούμενο Κεφάλαιο, μια ομάδα θα δίνεται ως ζεύγος $(G,\cdot)$, δηλαδή θα συμβολίζουμε με το σύμβολο «$\cdot$» την πράξη της ομάδας, και συνήθως, όταν δεν υπάρχει κίνδυνος σύγχυσης, θα παραλείπουμε το σύμβολο της πράξης. Έτσι, για παράδειγμα, θα γράφουμε ab αντί $a\cdot b$. Επίσης, το ουδέτερο στοιχείο της G θα συμβολίζεται με e, και το αντίστροφο του στοιχείου a θα συμβολίζεται με a^{-1}. Έτσι, για παράδειγμα, θα γράφουμε $a^n = a\cdot a\cdot\cdots\cdot a$ (n-παράγοντες), $\forall\, n\geq 1$.

Όταν σε ορισμένες περιπτώσεις για μια ομάδα G χρησιμοποιούμε τον προσθετικό συμβολισμό «$+$» για την πράξη της (αυτό συμβαίνει κυρίως όταν η ομάδα είναι αβελιανή), τότε θα συμβολίζουμε με 0 το ουδέτερο στοιχείο της, και με $-a$ το αντίστροφο ή αντίθετο στοιχείο του a. Σ' αυτή την περίπτωση θα γράφουμε $na = a+a+\cdots+a$ (n-παράγοντες), $\forall\, n\geq 1$.

3.1.1 Κυκλικές Ομάδες

Υπενθυμίζουμε από προηγούμενες ενότητες τον ορισμό και κάποιες στοιχειώδεις ιδιότητες κυκλικών ομάδων.

Πρόταση 3.1.1. *(Πρόταση 2.4.29) Έστω ότι $(G,\cdot)$ είναι μια ομάδα και $a\in G$ ένα στοιχείο της. Το σύνολο*

$$\langle a\rangle := \{a^n \in G \mid n\in\mathbb{Z}\}$$

είναι μια υποομάδα της G.

Παρατηρούμε ότι η περιγραφή των στοιχείων και η δομή της κυκλικής υποομάδας η οποία παράγεται από ένα στοιχείο μιας ομάδας είναι πολύ απλή. Αυτό μας οδηγεί στην εισαγωγή της κλάσης των κυκλικών ομάδων η οποία μπορεί να θεωρηθεί ως η κλάση ομάδων με την απλούστερη δομή:

Ορισμός 3.1.2. *Έστω $(G,\cdot)$ μια ομάδα και $a \in G$.*

1. *Η υποομάδα $\langle a\rangle$ της G καλείται η **κυκλική υποομάδα της G η οποία παράγεται από το στοιχείο** a, το δε στοιχείο a καλείται **γεννήτορας** της $\langle a\rangle$.*
2. *Η ομάδα G καλείται **κυκλική** αν η G έχει τουλάχιστον έναν **γεννήτορα**, δηλαδή αν υπάρχει στοιχείο $a \in G$ έτσι ώστε: $G = \langle a\rangle$.*

Γενικότερα, μια υποομάδα H της G ονομάζεται **κυκλική υποομάδα** αν υπάρχει $a \in H$ με $\langle a\rangle = H$. Από την άλλη πλευρά τυχόν στοιχείο $a \in G$ μιας ομάδας G ορίζει μια κυκλική ομάδα: την κυκλική υποομάδα $\langle a\rangle$ της G η οποία παράγεται από το a. Σημειώνουμε ότι, όπως θα δούμε στη συνέχεια, μια κυκλική ομάδα μπορεί να έχει περισσότερους από έναν γεννήτορες.

Παράδειγμα 3.1.3. Η προσθετική ομάδα των ακέραιων αριθμών, $(\mathbb{Z},+)$, είναι μια κυκλική ομάδα, διότι το στοιχείο της $1 \in \mathbb{Z}$ είναι γεννήτοράς της, δηλαδή η κυκλική υποομάδα

$$\langle 1\rangle = \{n\cdot 1 \mid n \in \mathbb{Z}\}$$

της $\mathbb{Z}$ η οποία παράγεται από το 1 συμπίπτει με την $\mathbb{Z}$. (Σημειώνουμε ότι, επειδή εδώ χρησιμοποιούμε την προσθετική σημειογραφία, οι ακέραιες δυνάμεις στοιχείων εκφράζονται ως ακέραια πολλαπλάσια στοιχείων).

Επειδή

$$\mathbb{Z} = \langle 1\rangle = \{n\cdot 1 \mid n \in \mathbb{Z}\} = \{-n\cdot 1 \mid n \in \mathbb{Z}\} = \langle -1\rangle$$

έπεται ότι το στοιχείο -1 είναι επίσης γεννήτορας της $\mathbb{Z}$.

Έστω τώρα $k \in \mathbb{Z}$ ένας γεννήτορας της $\mathbb{Z}$. Τότε $1 \in \mathbb{Z} = \langle k\rangle = \{mk \in \mathbb{Z} \mid m \in \mathbb{Z}\}$, και άρα $1 = mk$ για κάποιο $m \in \mathbb{Z}$. Προφανώς τότε θα έχουμε $k = 1$ και $m = 1$ ή $k = -1$ και $m = -1$, και επομένως $k = \pm 1$. Άρα καταλήγουμε ότι οι μόνοι γεννήτορες της κυκλικής ομάδας $(\mathbb{Z},+)$ είναι οι: $1, -1$. $\surd$

Παράδειγμα 3.1.4. Η προσθετική ομάδα $(\mathbb{Z}_n,+)$ των κλάσεων ακέραιων υπολοίπων mod n είναι επίσης μια κυκλική ομάδα. Πράγματι, χρησιμοποιώντας ότι $\forall k \in \mathbb{Z}$, $[k]_n = [r]_n = r[1]_n$, $0 \le r \le n-1$, όπου r είναι το υπόλοιπο της διαίρεσης του k με το n, βλέπουμε ότι η κυκλική υποομάδα η οποία παράγεται από την κλάση $[1]_n \in \mathbb{Z}_n$ συμπίπτει με την $\mathbb{Z}_n$:

$$\langle [1]_n\rangle = \{k[1]_n \in \mathbb{Z}_n \mid k \in \mathbb{Z}\} = \{[k]_n \in \mathbb{Z}_n \mid k \in \mathbb{Z}\} = \mathbb{Z}_n \quad \surd$$

3.1.2 Τάξη Ομάδας και Τάξη Στοιχείου μιας Ομάδας

Υπενθυμίζουμε τον ορισμό της τάξης ομάδας ο οποίος αναφέρθηκε εν συντομία στο Κεφάλαιο 2 (βλέπε τον Ορισμό 2.1.11):

Ορισμός 3.1.5. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα. Η **τάξη** της ομάδας G ορίζεται να είναι το πλήθος των στοιχείων του συνόλου G.*

*Αν η τάξη της G είναι πεπερασμένη, τότε η ομάδα G καλείται ομάδα πεπερασμένης τάξης ή **πεπερασμένη ομάδα**, διαφορετικά η G καλείται ομάδα άπειρης τάξης ή **άπειρη ομάδα**.*

Συμβολισμός 3.1.6. Η τάξη μιας ομάδας $(G,\cdot)$ συμβολίζεται συνήθως με ένα από τα παρακάτω σύμβολα:

$$o(G) \quad \text{ή} \quad |G| \quad \text{ή} \quad [G:1]$$

Σχόλιο 3.1.7. Η προσθετική ομάδα $(\mathbb{Z},+)$ των ακεραίων είναι μια άπειρη ομάδα διότι $\mathsf{o}(\mathbb{Z})=\infty$. Η προσθετική ομάδα $(\mathbb{R},+)$ των πραγματικών αριθμών είναι επίσης άπειρη ομάδα και γράφουμε $\mathsf{o}(\mathbb{R})=\infty$. Όμως τα σύνολα $\mathbb{Z}$ και $\mathbb{R}$, αν και τα δύο είναι άπειρα, δεν έχουν το ίδιο πλήθος στοιχείων, καθώς το $\mathbb{Z}$ είναι αριθμήσιμο σύνολο και το $\mathbb{R}$ είναι υπεραριθμήσιμο σύνολο. Έτσι στο πλαίσιο των σημειώσεων αυτών η έννοια «άπειρη ομάδα» έχει την έννοια «μη πεπερασμένη ομάδα». ▲

Με βάση την έννοια της τάξης μιας ομάδας μπορούμε να ορίσουμε την έννοια της τάξης στοιχείου σε μια ομάδα:

Ορισμός 3.1.8. *Η* **τάξη** $\mathsf{o}(a)$ *του στοιχείου* a *σε μια ομάδα* $(G,\cdot)$ *ορίζεται να είναι η τάξη* $|\langle a\rangle|$ *της κυκλικής υποομάδας* $\langle a\rangle$ *της* G *η οποία παράγεται από το* a*:*

$$\mathsf{o}(a)=|\langle a\rangle|$$

Έτσι η τάξη του στοιχείου a είναι πεπερασμένη, αντίστοιχα άπειρη, αν η κυκλική υποομάδα $\langle a\rangle$ η οποία παράγεται από το a είναι πεπερασμένη, αντίστοιχα άπειρη. Για παράδειγμα, το ταυτοτικό στοιχείο $e\in G$ της G έχει τάξη 1 διότι $|\langle e\rangle|=|\{e\}|=1$. Σημειώνουμε ότι με τον συμβολισμό $\mathsf{o}(a)=\infty$ εννοούμε ότι το στοιχείο a δεν έχει πεπερασμένη τάξη.

Θα περιγράψουμε έναν χρήσιμο τρόπο υπολογισμού της τάξης ενός στοιχείου a σε μια ομάδα $(G,\cdot)$. Θεωρούμε το υποσύνολο των φυσικών αριθμών

$$\mathcal{O}(a)=\left\{m\in\mathbb{N}\mid a^m=e\right\}$$

Το σύνολο $\mathcal{O}(a)$ μπορεί να είναι ή να μην είναι το κενό σύνολο. Αν $\mathcal{O}(a)=\emptyset$, τότε $a^m\neq e$, $\forall m\in\mathbb{N}$. Αν $\mathcal{O}(a)\neq\emptyset$, τότε σύμφωνα με την Αρχή Καλής Διάταξης,[1] το μη κενό σύνολο $\mathcal{O}(a)$ έχει ελάχιστο στοιχείο. Η επόμενη Πρόταση πιστοποιεί ότι αν το στοιχείο a έχει πεπερασμένη τάξη, τότε η τάξη του $\mathsf{o}(a)$ συμπίπτει με το ελάχιστο στοιχείου του συνόλου $\mathcal{O}(a)$.

Πρόταση 3.1.9. *Έστω* $(G,\cdot)$ *μια ομάδα και* $a\in G$ *ένα στοιχείο της.*

1. $\mathsf{o}(a)=\infty \iff \forall m\in\mathbb{N}\colon a^m\neq e$.
2. $\mathsf{o}(a)<\infty \iff \exists m\in\mathbb{N}\colon a^m=e$.
3. *Αν* $\mathsf{o}(a)<\infty$*, τότε:*
$$\mathsf{o}(a)=\min\mathcal{O}(a)=\min\left\{n\in\mathbb{N}\mid a^n=e\right\}$$

Απόδειξη. 1. Έστω ότι $\mathsf{o}(a)=\infty$. Τότε η κυκλική υποομάδα $\langle a\rangle=\left\{a^n\in G\mid n\in\mathbb{Z}\right\}$ η οποία παράγεται από το a έχει άπειρο πλήθος στοιχείων. Έστω ότι υπάρχει θετικός ακέραιος m έτσι ώστε $a^m=e$. Θα δείξουμε ότι $\langle a\rangle=\left\{e,a,a^2,\cdots,a^{m-1}\right\}$. Έστω $a^n\in\langle a\rangle$ ένα τυχόν στοιχείο της $\langle a\rangle$, όπου $n\in\mathbb{Z}$. Από την Ευκλείδεια Διαίρεση του n με το m, θα έχουμε ότι υπάρχει μοναδικό ζεύγος ακεραίων q,r έτσι ώστε:

$$n=mq+r,\quad \text{όπου: } 0\leq r\leq m-1 \tag{†}$$

Τότε θα έχουμε

$$a^n=a^{mq+r}=a^{mq}\cdot a^r=(a^m)^q\cdot a^r=e^q\cdot a^r=e\cdot a^r=a^r$$

Επομένως $a^m\in\left\{e,a,a^2,\cdots,a^{m-1}\right\}$ και άρα $\langle a\rangle=\left\{e,a,a^2,\cdots,a^{m-1}\right\}$. Αυτό είναι άτοπο διότι η κυκλική υποομάδα $\langle a\rangle$ η οποία παράγεται από το a έχει άπειρο πλήθος στοιχείων. Επομένως $a^m\neq e$, $\forall m\in\mathbb{N}$.

Αντίστροφα, υποθέτουμε ότι $a^m\neq e$, $\forall m\in\mathbb{N}$. Θα δείξουμε ότι η κυκλική υποομάδα $\langle a\rangle$ η οποία παράγεται από το a έχει άπειρο πλήθος στοιχείων. Αν δείξουμε ότι το πλήθος των στοιχείων του υποσυνόλου $X=\left\{a^n\in G\mid n\in\mathbb{N}\right\}\subseteq\langle a\rangle$ είναι άπειρο, τότε και το πλήθος των στοιχείων του συνόλου $\langle a\rangle$ θα είναι άπειρο. Πράγματι, αν το πλήθος των στοιχείων του X ήταν πεπερασμένο, θα υπήρχαν φυσικοί αριθμοί i,j με $i\neq j$ και $a^i=a^j$. Υποθέτοντας (χωρίς περιορισμό της γενικότητας) ότι $i>j$, έπεται ότι $i-j\in\mathbb{N}$ και $a^{i-j}=e$. Αυτό όμως είναι άτοπο από την υπόθεση. Άρα το πλήθος των στοιχείων του X είναι άπειρο και έτσι συμπεραίνουμε ότι το πλήθος των στοιχείων της κυκλικής υποοομάδας $\langle a\rangle$ είναι άπειρο. Επομένως θα έχουμε $\mathsf{o}(a)=\infty$.

[1] Υπενθυμίζουμε ότι η **Αρχή Καλής Διάταξης** στο σύνολο $\mathbb{N}$ των φυσικών αριθμών πιστοποιεί ότι: «*Κάθε μη κενό υποσύνολο* S *του* $\mathbb{N}$ *έχει ελάχιστο στοιχείο, δηλαδή υπάρχει* $s\in S$ *έτσι ώστε* $s\leq x$, $\forall x\in S$», βλέπε την υποενότητα 0.3.1.

2. Δεν χρειάζεται να αποδείξουμε τίποτα διότι ο ισχυρισμός του 2. είναι λογικά ισοδύναμος με τον ισχυρισμό του 1.

3. Υποθέτουμε ότι $o(a) < \infty$. Από το μέρος 2. έπεται ότι το σύνολο $\mathcal{O}(a) = \{m \in \mathbb{N} \mid a^m = e\}$ είναι μη κενό. Έστω $n = \min \mathcal{O}(a)$ και θεωρούμε το σύνολο $X = \{e, a, a^2, \cdots, a^{n-1}\}$. Τα στοιχεία a^i, $0 \leq i \leq n-1$, είναι ανά δύο διαφορετικά διότι αν $a^i = a^j$, όπου $0 \leq i \neq j \leq n-1$, τότε, υποθέτοντας χωρίς βλάβη της γενικότητας ότι $j < i$, θα έχουμε $i - j \in \mathbb{N}$ και $a^{i-j} = e$. Τότε $i - j \in \mathcal{O}(a)$ και αυτό είναι άτοπο διότι $i - j < n = \min \mathcal{O}(a)$. Άρα τα στοιχεία a^i, $0 \leq i \leq n-1$, είναι ανά δύο διαφορετικά και τότε το πλήθος των στοιχείων του συνόλου X είναι ίσο με n. Θα δείξουμε ότι $X = \langle a \rangle$. Προφανώς $X \subseteq \langle a \rangle$. Αν $a^k \in \langle a \rangle$, τότε από την Ευκλείδεια Διαίρεση του k με το n θα έχουμε $k = nq + r$, όπου $0 \leq r \leq n-1$. Τότε $a^k = a^{nq+r} = a^{nq} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r \in X$. Άρα $X = \langle a \rangle$ και επομένως $n = |X| = |\langle a \rangle| = o(a)$. ■

Παρατήρηση 3.1.10. Χρησιμοποιώντας την Πρόταση 3.1.9, έπεται ότι αν, $(G, \cdot)$ είναι μια κυκλική ομάδα με γεννήτορα το στοιχείο a, δηλαδή $G = \langle a \rangle$, τότε: $|G| = o(G) = o(a)$. Επιπλέον, η απόδειξη της Πρότασης 3.1.9 δείχνει ότι για την τάξη $o(a)$ ενός στοιχείου a σε μια ομάδα G, τα ακόλουθα είναι ισοδύναμα:

1. $o(a) < \infty$.
2. Υπάρχει θετικός ακέραιος m έτσι ώστε: $a^m = e$.
3. Υπάρχουν ακέραιοι αριθμοί i, j με $i \neq j$ και $a^i = a^j$.
4. Η «επί» απεικόνιση $\mathbb{Z} \longrightarrow \langle a \rangle$, $m \longmapsto a^m$ *δεν* είναι «1-1».

Ισοδύναμα: $o(a) = \infty$ αν και μόνο αν η απεικόνιση $\mathbb{Z} \longrightarrow \langle a \rangle$, $m \longmapsto a^m$ είναι «1-1» και «επί». ▲

Παράδειγμα 3.1.11. Θεωρούμε το σύνολο $G = \{1, -1, i, -i\} \subseteq \mathbb{C}$, το οποίο, όπως γνωρίζουμε, αποτελεί ομάδα όταν εφοδιαστεί με τον συνήθη πολλαπλασιασμό μιγαδικών αριθμών. Επειδή $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, έπεται ότι η τάξη του στοιχείου i είναι 4: $o(i) = 4$. Παρατηρούμε ότι η κυκλική υποομάδα της G η οποία παράγεται από το i συμπίπτει με την G. Έτσι η G είναι κυκλική με γεννήτορα το i: $G = \langle i \rangle$. √

Παράδειγμα 3.1.12. Θεωρούμε τη συμμετρική ομάδα S_3. Υπενθυμίζουμε ότι, χρησιμοποιώντας τον κυκλικό συμβολισμό μεταθέσεων, θα έχουμε:

$$S_3 = \{\iota,\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

Προφανώς $o(\iota) = 1$. Επειδή, όπως μπορούμε να υπολογίσουμε εύκολα

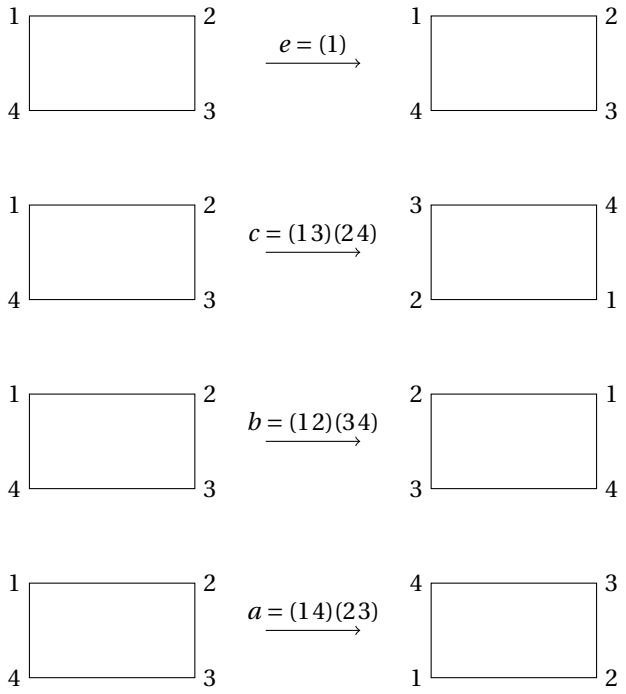
$$(12)^2 = (12)(12) = \iota \quad \text{και} \quad (123)^2 = (123)(123) = (132) \quad \text{και} \quad (123)^3 = (123)^2(123) = (132)(123) = \iota$$

έπεται ότι $o((12)) = 2$ και $o((123)) = 3$. Παρόμοια δείχνουμε ότι $o((13)) = 2 = o((23))$ και $o((132)) = 3$. √

Παράδειγμα 3.1.13. Θεωρούμε την ομάδα των τεσσάρων στοιχείων του Klein $(V_4, \cdot)$, όπου $V_4 = \{e, a, b, c\}$, η οποία, υπενθυμίζουμε, είναι μια αβελιανή μη κυκλική ομάδα με 4 στοιχεία. Γεωμετρικά η G παριστάνει την ομάδα συμμετριών ενός παραλληλογράμμου στο επίπεδο, με κορυφές οι οποίες συμβολίζονται με τους αριθμούς 1,2,3,4, και το οποίο δεν είναι τετράγωνο, βλέπε το Σχήμα 3.1 παρακάτω:

Πράγματι, συμβολίζουμε με: (ϵ_1) την ευθεία η οποία ενώνει τις κορυφές 1 και 4, με (ϵ_2) την ευθεία η οποία ενώνει τις κορυφές 2 και 3, με (ϵ_3) την ευθεία η οποία ενώνει τις κορυφές 1 και 2, και με (ϵ_4) την ευθεία η οποία ενώνει τις κορυφές 3 και 4. Τότε το ουδέτερο στοιχείο e λειτουργεί ως η ταυτοτική απεικόνιση: δεν μετακινεί το παραλληλόγραμμο. Το στοιχείο a παριστάνει ανάκλαση ως προς την ευθεία η οποία ενώνει τα μέσα των πλευρών (ϵ_1) και (ϵ_2), και το στοιχείο b παριστάνει ανάκλαση ως προς την ευθεία η οποία ενώνει τα μέσα των πλευρών (ϵ_3) και (ϵ_4). Τότε το στοιχείο $c = a \cdot b = b \cdot a$ παριστάνει στροφή επιπέδου κατά γωνία π γύρω από το κέντρο του παραλληλογράμμου, δηλαδή την τομή των διαγωνίων του, με φορά αντίθετη της φοράς των δεικτών του ρολογιού. Με βάση την παραπάνω ερμηνεία, τα στοιχεία της ομάδας V_4 περιγράφονται ως μεταθέσεις των κορυφών του παραλληλογράμμου: $e = (1)$, $a = (14) \cdot (23)$, $b = (12) \cdot (34)$, και $c = (13) \cdot (24)$. Όπως μπορούμε να δούμε και γεωμετρικά ισχύει ότι $a \cdot b = c$ και κάθε στοιχείο $e \neq a$ της G έχει τάξη 2. √

Σχήμα 3.1: Η Ομάδα του Klein ως ομάδα συμμετριών παραλληλογράμμου



Παρατηρούμε ότι οι τάξεις των στοιχείων της ομάδας του Klein είναι 1, 2, και οι τάξεις των στοιχείων της συμμετρικής ομάδας S_3 είναι 1, 2, 3, δηλαδή και στις δύο περιπτώσεις οι τάξεις των στοιχείων της ομάδας είναι (γνήσιοι) διαιρέτες του πλήθους των στοιχείων των ομάδων. Όπως θα δούμε αργότερα, αυτό δεν είναι τυχαίο.

Παράδειγμα 3.1.14. 1. Θεωρούμε την προσθετική ομάδα $(\mathbb{Z},+)$. Αν $z\in\mathbb{Z}$ και $o(z)=n<\infty$, τότε $nz=0$. Προφανώς τότε $z=0$ διότι $n\geq 1$. Επομένως το μόνο στοιχείο πεπερασμένης τάξης στην προσθετική ομάδα $\mathbb{Z}$ είναι το ουδέτερο στοιχείο της.

2. Θεωρούμε την πολλαπλασιαστική ομάδα $(GL(2,\mathbb{R}),\cdot)$ των αντιστρέψιμων 2×2 πινάκων υπεράνω του $\mathbb{R}$, και έστω $A=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Ο πίνακας A ανήκει στην ομάδα $GL(2,\mathbb{R})$ διότι $Det(A)=1\neq 0$. Επειδή, όπως προκύπτει εύκολα
$$A^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix},\qquad \forall n\geq 1$$
έπεται ότι $A^n\neq I_2=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $\forall n\geq 1$, και άρα ο πίνακας A ως στοιχείο της ομάδας $GL(2,\mathbb{R})$ έχει άπειρη τάξη: $o(A)=\infty$.

3. Θεωρούμε τον πίνακα $B=\begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}$ ο οποίος είναι στοιχείο της ομάδας $(GL(2,\mathbb{R}),\cdot)$ διότι $Det(B)=-1\neq 0$. Επειδή $B^2=I_2$, έπεται ότι ο πίνακας B έχει τάξη 2: $o(B)=2$.

Από τα τελευταία δύο παραδείγματα βλέπουμε ότι υπάρχουν ομάδες με άπειρο πλήθος στοιχείων, οι οποίες περιέχουν στοιχεία με πεπερασμένη τάξη και στοιχεία με άπειρη τάξη. $\surd$

Η ακόλουθη άμεση συνέπεια των ορισμών δίνει έναν χρήσιμο χαρακτηρισμό των πεπερασμένων κυκλικών ομάδων.

Πόρισμα 3.1.15. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα. Τότε η G είναι κυκλική αν και μόνο αν η G περιέχει ένα στοιχείο a με τάξη την τάξη της ομάδας:* $\mathrm{o}(a)=|G|$.

Απόδειξη. Αν η G είναι κυκλική και a είναι ένας γεννήτορας της, τότε από τον ορισμό και την Πρόταση 3.1.9 προφανώς θα έχουμε: $|G|=|\langle a\rangle|=\mathrm{o}(a)$. Αντίστροφα, έστω $a\in G$ και υποθέτουμε ότι $\mathrm{o}(a)=|G|$. Τότε η κυκλική υποομάδα $\langle a\rangle$ της G η οποία παράγεται από το στοιχείο a έχει $|G|$ το πλήθος στοιχεία και άρα αναγκαστικά θα συμπίπτει με την G. Έτσι $G=\langle a\rangle$ και επομένως η G είναι κυκλική. ■

Παρατήρηση 3.1.16. Παρατηρούμε ότι:

«*Αν μια ομάδα $(G,\cdot)$ είναι πεπερασμένη, τότε κάθε στοιχείο της G έχει πεπερασμένη τάξη*».

Πράγματι, η τάξη του a συμπίπτει με την τάξη της κυκλικής υποομάδας $\langle a\rangle$ που παράγεται από το a. Επειδή $\mathrm{o}(G)<\infty$ και $\langle a\rangle\leq G$, θα έχουμε προφανώς $\mathrm{o}(\langle a\rangle)<\infty$. Επομένως:

$$\mathrm{o}(G)<\infty \quad\Longrightarrow\quad \forall a\in G:\ \ \mathrm{o}(a)<\infty \qquad \blacktriangle$$

Ωστόσο η αντίστροφη συνεπαγωγή στην Παρατήρηση 3.1.16 δεν ισχύει: όπως δείχνει το επόμενο παράδειγμα, υπάρχουν ομάδες άπειρης τάξης κάθε στοιχείο των οποίων έχει πεπερασμένη τάξη.

Παράδειγμα 3.1.17. Πραγματικά, θεωρούμε την ομάδα $(\mathbb{Z}_2,+)=\big(\{[0]_2,[1]_2\},+\big)$ των κλάσεων υπολοίπων modulo 2, και έστω η ομάδα ευθύ γινόμενο

$$\Big(\prod_{n=1}^{\infty}\mathbb{Z}_2,+\Big) \qquad \text{όπου} \qquad \prod_{n=1}^{\infty}\mathbb{Z}_2=\mathbb{Z}_2\times\mathbb{Z}_2\times\cdots=\big\{(x_n)_{n\geq1}\mid x_n\in\mathbb{Z}_2,\ \forall n\geq1\big\}$$

Υπενθυμίζουμε ότι τα στοιχεία του συνόλου $\prod_{n=1}^{\infty}\mathbb{Z}_2$ είναι ακολουθίες $(x_n)_{n\geq1}$ στοιχείων του $\mathbb{Z}_2$, και η πράξη «+» επί του συνόλου $\prod_{n=1}^{\infty}\mathbb{Z}_2$ ορίζεται ως εξής:

$$(x_n)_{n\geq1}+(y_n)_{n\geq1}=(x_n+y_n)_{n\geq1}$$

Το ουδέτερο στοιχείο της ομάδας $\prod_{n=1}^{\infty}\mathbb{Z}_2$ είναι η ακολουθία $(x_n)_{n\geq1}$, όπου $x_n=[0]_2$, $\forall n\geq1$. Προφανώς η ομάδα $\prod_{n=1}^{\infty}\mathbb{Z}_2$ είναι άπειρη. Παρατηρούμε ότι, επειδή $[x]_2+[x]_2=[x+x]_2=[0]_2$, $\forall[x]_2\in\mathbb{Z}_2$, θα έχουμε:

$$\forall(x_n)_{n\geq1}\in\prod_{n=1}^{\infty}\mathbb{Z}_2:\qquad 2(x_n)_{n\geq1}=(x_n)_{n\geq1}+(x_n)_{n\geq1}=(x_n+x_n)_{n\geq1}=([0]_2)_{n\geq1}$$

και άρα κάθε μη ταυτοτικό στοιχείο της ομάδας $\prod_{n=1}^{\infty}\mathbb{Z}_2$ έχει τάξη 2. $\quad\surd$

3.2 Βασικές Ιδιότητες Τάξης Στοιχείου και Ομάδας

Στην παρούσα ενότητα θα αποδείξουμε ορισμένες βασικές ιδιότητες αναφορικά με την τάξη στοιχείου μιας ομάδας οι οποίες θα είναι χρήσιμες στον υπολογισμό της τάξης σε παραδείγματα και εφαρμογές.

Πρόταση 3.2.1. *Έστω $(G,\cdot)$ μια ομάδα και έστω $a\in G$ ένα στοιχείο πεπερασμένης τάξης της G. Τότε:*

$$\forall k\geq1:\qquad a^k=e\quad\Longleftrightarrow\quad \mathrm{o}(a)\mid k$$

Απόδειξη. Θέτουμε $\mathrm{o}(a)=n<\infty$.

«$\Longleftarrow$» Αν $n\mid k$, τότε υπάρχει ακέραιος $\lambda\in\mathbb{Z}$ έτσι ώστε $k=n\lambda$ και τότε $a^k=a^{n\lambda}=(a^n)^\lambda=e^\lambda=e$.

«$\Longrightarrow$» Έστω ότι $a^k=e$, για κάποιον θετικό ακέραιο $k\geq1$. Από την Ευκλείδεια Διαίρεση του k με το n, έπεται ότι υπάρχει μοναδικό ζεύγος ακεραίων q,r έτσι ώστε:

$$k=qn+r,\qquad 0\leq r\leq n-1$$

Παρατηρούμε ότι

$$e = a^k = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^r a^r = ea^r = a^r$$

Το υπόλοιπο r οφείλει να είναι ίσο με 0, διότι διαφορετικά θα ήταν ένας φυσικός αριθμός μικρότερος από την τάξη n του a με $a^r = e$, πράγμα άτοπο, διότι $\mathrm{o}(a) = \min\{m \in \mathbb{N} \mid a^m = e\}$. Ώστε $k = qn$ και επομένως $\mathrm{o}(a) = n \mid k$. ■

Το ακόλουθο Θεώρημα συνοψίζει τα κυριότερα αποτελέσματα γύρω από την τάξη ενός στοιχείου μιας ομάδας.

Θεώρημα 3.2.2. *Έστω $(G,\cdot)$ μια ομάδα και $g \in G$ ένα στοιχείο της G. Τότε για κάθε μη μηδενικό ακέραιο $k \in \mathbb{Z}$ ισχύουν τα εξής:*

1. *Αν το στοιχείο g έχει άπειρη τάξη, τότε το στοιχείο g^k έχει άπειρη τάξη.*
2. *Αν το στοιχείο g έχει πεπερασμένη τάξη, τότε το στοιχείο g^k έχει πεπερασμένη τάξη, και ισχύει ότι:*

$$\mathrm{o}(g^k) = \frac{\mathrm{o}(g)}{(\mathrm{o}(g), k)} = \mathrm{o}(g^{-k})$$

   Ιδαίτερα: $\mathrm{o}(g) = \mathrm{o}(g^{-1})$.

3. *Αν το στοιχείο g έχει πεπερασμένη τάξη, τότε:*

$$k \mid \mathrm{o}(g) \iff \mathrm{o}(g^k) = \frac{\mathrm{o}(g)}{|k|}$$

4. *Αν το στοιχείο g έχει πεπερασμένη τάξη, τότε:*

$$(k, \mathrm{o}(g)) = 1 \iff \mathrm{o}(g^k) = \mathrm{o}(g)$$

Απόδειξη. **1.** Υποθέτουμε ότι η τάξη του στοιχείου g^k, όπου $k \in \mathbb{Z} \setminus \{0\}$ είναι πεπερασμένη, και έστω $\mathrm{o}(g^k) = n < \infty$. Τότε $(g^k)^n = g^{kn} = e$ και επομένως $\mathcal{O}(g) \neq \emptyset$. Αυτό σημαίνει ότι η τάξη του στοιχείου g είναι πεπερασμένη, το οποίο είναι άτοπο. Άρα η τάξη του στοιχείου g^k είναι άπειρη.

2. Θέτουμε $\mathrm{o}(g) = n < \infty$.

Επειδή το στοιχείο g έχει πεπερασμένη τάξη, η κυκλική ομάδα $\langle g \rangle$ είναι πεπερασμένη. Επειδή το στοιχείο g^k ανήκει στην $\langle g \rangle$, από την Παρατήρηση 3.1.16 έπεται ότι το στοιχείο g^k έχει πεπερασμένη τάξη. Έστω $r = \mathrm{o}(g^k) < \infty$. Θα δείξουμε ότι $r = \frac{n}{(n,k)}$. Χρησιμοποιώντας την Πρόταση 3.2.1, θα έχουμε:

$$(g^k)^r = e \implies g^{kr} = e \implies n \mid kr$$

όπου η τελευταία συνεπαγωγή προέκυψε με χρήση της Πρότασης 3.2.1. Άρα υπάρχει $m \in \mathbb{Z}$ έτσι ώστε:

$$kr = nm$$

Επειδή προφανώς $(n,k) \mid n$ και $(n,k) \mid k$, μπορούμε να γράψουμε:

$$n = (n,k)n' \qquad \text{και} \qquad k = (n,k)k', \qquad \text{όπου} \qquad (k',n') = 1$$

Τότε: $n' = \frac{n}{(n,k)}$ και άρα αρκεί να δείξουμε ότι: $r = n'$. Χρησιμοποιώντας στοιχειώδεις ιδιότητες διαιρετότητας ακεραίων, θα έχουμε:

$$kr = nm \implies (n,k)k'r = (n,k)n'm \implies k'r = n'm \implies n' \mid k'r \implies n' \mid r \implies n' \leq r \qquad (1)$$

όπου η προτελευταία συνεπαγωγή προέκυψε διότι $(k',n') = 1$. Από την άλλη πλευρά, παρατηρώντας ότι:

$$kn' = (n,k)k'n' = nk'$$

θα έχουμε:

$$(g^k)^{n'} = g^{kn'} = g^{nk'} = (g^n)^{k'} = e^{k'} = e \implies r \,/\, n' \implies r \le n' \tag{2}$$

Επομένως από τις σχέσεις (1) και (2) έπεται ότι: $\mathrm{o}(g^k) = r = n' = \frac{n}{(k,n)}$. Τέλος, επειδή $(n,k) = (n,-k)$, θα έχουμε και

$$\mathrm{o}(g^{-k}) = \frac{n}{(n,-k)} = \frac{n}{(n,k)} = \mathrm{o}(g^k)$$

Τα μέρη **3.** και **4.** προκύπτουν άμεσα από το μέρος **2.** ■

Πόρισμα 3.2.3. *Έστω $(G,\cdot)$ μια κυκλική ομάδα πεπερασμένης τάξης με γεννήτορα το στοιχείο a: $G = \langle a\rangle$. Τότε:*

$$\forall k \in \mathbb{Z}: \quad G = \langle a^k\rangle \iff (k, \mathrm{o}(a)) = 1$$

Δηλαδή ένα στοιχείο a^k της G είναι γεννήτορας της G αν και μόνο αν $(k, \mathrm{o}(a)) = 1$.

Απόδειξη. Έστω $\mathrm{o}(a) = n$. Παρατηρούμε πρώτα ότι το στοιχείο a^k είναι γεννήτορας της G αν και μόνο αν $\mathrm{o}(a^k) = \mathrm{o}(a)$. Πράγματι, αν το a^k είναι γεννήτορας της G, τότε $\langle a^k\rangle = G$ και επομένως $\mathrm{o}(a^k) = \mathrm{o}(G) = \mathrm{o}(a)$. Αντίστροφα, αν $\mathrm{o}(a^k) = \mathrm{o}(a)$, τότε η υποομάδα $\langle a^k\rangle$ της G η οποία παράγεται από το a^k θα έχει $\mathrm{o}(G) = \mathrm{o}(a)$ το πλήθος στοιχεία και άρα $\langle a^k\rangle = G$, δηλαδή το a^k είναι γεννήτορας της G.

Χρησιμοποιώντας το Θεώρημα 3.2.2, θα έχουμε:

$$G = \langle a^k\rangle \iff \mathrm{o}(a^k) = \mathrm{o}(a) \iff \frac{n}{(k,n)} = n \iff (k,n) = 1$$ ■

Το ακόλουθο Πόρισμα είναι συνέπεια του Πορίσματος 3.2.3.

Πόρισμα 3.2.4. *Έστω $G = \langle a\rangle$ μια κυκλική ομάδα τάξης n. Τότε το σύνολο γεννητόρων της G είναι*

$$\left\{a^k \in G \mid 1 \le k \le n \ \text{ και } \ (k,n) = 1\right\}$$

Το πλήθος των γεννητόρων της G είναι ίσο με

$$\left|\left\{a^k \in G \mid 1 \le k \le n \ \text{ και } \ (k,n) = 1\right\}\right| = \varphi(n)$$

όπου φ είναι η συνάρτηση του Euler.[2]

Παρατήρηση 3.2.5. Υπενθυμίζουμε ότι η **συνάρτηση του Euler** είναι η αριθμητική συνάρτηση

$$\varphi: \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = \left|\{m \in \mathbb{N} \mid 1 \le m \le n \ \text{ και } \ (m,n) = 1\}\right|$$

Δηλαδή η τιμή της στον φυσικό αριθμό n μετρά το πλήθος των φυσικών αριθμών m, όπου $1 \le m \le n$, οι οποίοι είναι σχετικώς πρώτοι τον αριθμό n. Υπενθυμίζουμε κάποιες βασικές ιδιότητες της συνάρτησης του Euler οι οποίες μας επιτρέπουν τον υπολογισμό της τιμής της πάνω σε οποιοδήποτε φυσικό αριθμό:[3]

1. Αν p είναι ένας πρώτος αριθμός και α είναι ένας θετικός ακέραιος, τότε

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

2. Η φ είναι *πολλαπλασιαστική συνάρτηση*: αν n, m είναι δύο φυσικοί αριθμοί, τότε:

$$(n,m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$$

[2] Leonhard Euler (15 Απριλίου 1707 - 18 Σεπτεμβρίου 1873) [http://en.wikipedia.org/wiki/Leonhard_Euler]: Ελβετός μαθηματικός και φυσικος με θεμελιώδη συνεισφορά σε όλους τους κλάδους των Μαθηματικών, αλλά και της Φυσικής. Ο Euler άφησε τεράστιο έργο πίσω του, καθώς ήταν πολυγραφότατος, έργο το οποίο άσκησε μεγάλη επίδραση στα σύγχρονα Μαθηματικά και περιείχε σημαντική συμβολή στη Μαθηματική Ανάλυση, στην Άλγεβρα, στη Θεωρία Αριθμών, στη Θεωρία Γραφημάτων, στη Μηχανική, στη Δυναμική των Ρευστών, στην Οπτική, στην Αστρονομία, αλλά και στη Μουσική. Θεωρείται εκ των επιφανέστερων μαθηματικών όλων των εποχών.

[3] Για περισσότερες λεπτομέρειες παραπέμπουμε στο βιβλίο [28].

3. Αν $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$ είναι η πρωτογενής ανάλυση του φυσικού αριθμού n σε δυνάμεις διακεκριμένων πρώτων αριθμών, τότε:

$$\varphi(n) = \varphi(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{n=1}^{k} (1 - \frac{1}{p_i}) \qquad \blacktriangle$$

Το ακόλουθο παράδειγμα δείχνει ότι για κάθε θετικό ακέραιο n υπάρχει μια αβελιανή, όχι απαραίτητα κυκλική, ομάδα τάξης $\phi(n)$.

Παράδειγμα 3.2.6. Υπενθυμίζουμε ότι το υποσύνολο

$$\mathsf{U}(\mathbb{Z}_n) = \{[k]_n \in \mathbb{Z}_n \mid 1 \le k \le n \ \text{ και } \ (k,n) = 1\} \ \subseteq \ \mathbb{Z}_n$$

εφοδιασμένο με την πράξη πολλαπλασιασμού κλάσεων ισοτιμίας mod n, δηλαδη: $[k]_n \cdot [m]_n = [km]_n$, αποτελεί ομάδα, η οποία καλείται η **ομάδα των αντιστρέψιμων κλάσεων υπολοίπων** mod n. Προφανώς η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ είναι αβελιανή και η τάξη της είναι $o(\mathsf{U}(\mathbb{Z}_n)) = \phi(n)$. Αν η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ είναι κυκλική, τότε, σύμφωνα με την Πρόταση 3.2.4, το πλήθος των γεννητόρων της $\mathsf{U}(\mathbb{Z}_n)$ είναι ίσο με $\phi(\phi(n))$. Τα παρακάτω παραδείγματα δείχνουν ότι η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ δεν είναι πάντα κυκλική.

1. Αν $n = 8$, τότε θα έχουμε $o(\mathsf{U}(\mathbb{Z}_8)) = \phi(8) = 4$, και

$$\mathsf{U}(\mathbb{Z}_8) = \{[1]_8,\ [3]_8,\ [5]_8,\ [7]_8\}$$

Επειδή $[3]_8^2 = [9]_8 = [1]_8$, $[5]_8^2 = [25]_8 = [1]_8$, και $[7]_8^2 = [49]_8 = [1]_8$, κάθε στοιχείο της $\mathsf{U}(\mathbb{Z}_8)$, διαφορετικό του ουδετέρου, έχει τάξη 2 και άρα η ομάδα $\mathsf{U}(\mathbb{Z}_8)$ δεν είναι κυκλική.

Παρόμοια βλέπουμε ότι η ομάδα $\mathsf{U}(\mathbb{Z}_{12})$ δεν είναι κυκλική. Αντίθετα οι ομάδες $\mathsf{U}(\mathbb{Z}_n)$, $2 \le n \le 15$, όπου $n \ne 8, 12, 15$, είναι κυκλικές, βλέπε την Άσκηση 3.9.19.

2. Αν $n = 9$, θα δούμε ότι η ομάδα $\mathsf{U}(\mathbb{Z}_9)$ είναι κυκλική βρίσκοντας έναν γεννήτορά της. Προφανώς θα έχουμε:

$$\mathsf{U}(\mathbb{Z}_9) = \{[k]_9 \in \mathbb{Z}_9 \mid 1 \le k \le 9 \ \text{ και } \ (k,9) = 1\} = \{[1]_9,\ [2]_9,\ [4]_9,\ [5]_9,\ [7]_9,\ [8]_9\}$$

Θεωρούμε την κλάση υπολοίπων $[2]_9$, και τότε:

$$[2]_9^2 = [4]_9, \quad [2]_9^3 = [8]_9, \quad [2]_9^4 = [16]_9 = [7]_9, \quad [2]_9^5 = [14]_9 = [5]_9, \quad [2]_9^6 = [10]_9 = [1]_9$$

Οι παραπάνω σχέσεις δείχνουν ότι το στοιχείο $[2]_9$ είναι γεννήτορας της $\mathsf{U}(\mathbb{Z}_9)$ και άρα η ομάδα $\mathsf{U}(\mathbb{Z}_9)$ είναι κυκλική τάξης 6. Παρατηρούμε ότι θα έχουμε σε πλήθος $\phi(\phi(9)) = \phi(6) = 2$ γεννήτορες της ομάδας $\mathsf{U}(\mathbb{Z}_9)$: ο ένας είναι το στοιχείο $[2]_9$ και ο δεύτερος θα είναι το στοιχείο $[2]_9^k$, όπου $(k,6) = 1$, δηλαδή $k = 5$, και άρα ο δεύτερος γεννήτορας $[2]^5 = [5]_9$ είναι το στοιχείο $[5]_9$. $\surd$

3.2.1 Παραδείγματα Κυκλικών Ομάδων Μικρής Τάξης

Η ομάδα των n-οστών ριζών της μονάδας

Θα μελετήσουμε εν συντομία βασικές ιδιότητες της ομάδας των n-οστών ριζών της μονάδας.

Υπενθυμίζουμε ότι η **ομάδα του κύκλου** είναι η υποομάδα

$$\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\} \ \le \ \mathbb{C}^*$$

της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*, \cdot)$ των μη μηδενικών μιγαδικών αριθμών. Θα δούμε ότι η ομάδα T περιέχει κυκλικές ομάδες τάξης n, για κάθε $n \ge 1$.

Υπενθυμίζουμε ότι, $\forall n \ge 1$, ο μιγαδικός αριθμός $z \in \mathbb{C}$ καλείται μια n-**οστή ρίζα της μονάδας** αν: $z^n = 1$. Τότε:

$$z^n = 1 \implies |z|^n = 1 \implies |z| = 1 \ \text{ και } \ \exists \theta \in [0, 2\pi] : \ z = e^{i\theta}$$

και επομένως:

$$z^n = 1 \implies e^{in\theta} = 1 \implies \exists\, k \in \mathbb{Z}:\ n\theta = k2\pi \implies \theta = \frac{2\pi k}{n}$$

Άρα:

$$z^n = 1 \implies z = e^{\frac{2\pi ik}{n}}, \quad \text{όπου} \quad k \in \mathbb{Z}$$

Παρατηρούμε ότι η τιμή $e^{\frac{2\pi ik}{n}}$ εξαρτάται μόνο από την κλάση ισοδυναμίας του k modulo n:

$$[k]_n = [k']_n \implies n \mid k - k' \implies k - k' = nr, \quad \text{όπου} \quad r \in \mathbb{Z}$$

και άρα θα έχουμε:

$$e^{\frac{2\pi ik}{n}} = e^{\frac{2\pi i(k'+nr)}{n}} = e^{\frac{2\pi ik'+2\pi inr}{n}} = e^{\frac{2\pi ik'}{n}} e^{\frac{2\pi inr}{n}} = e^{\frac{2\pi ik'}{n}} e^{2\pi ir} = e^{\frac{2\pi ik'}{n}}$$

Επομένως θέτοντας:

$$\zeta_n := e^{\frac{2\pi i}{n}}$$

θα έχουμε

$$\zeta_n^{qn+r} = \zeta_n^{qn}\zeta_n^r = (\zeta_n^n)^q\zeta_n^r = 1\zeta_n^r = \zeta_n^r$$

και άρα το σύνολο των διακεκριμένων n-οστών ριζών της μονάδας είναι:

$$\mathsf{U}_n = \left\{\zeta_n^k = e^{\frac{2\pi ik}{n}} \in \mathbb{C} \mid 0 \le k \le n-1\right\} = \left\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}\right\}$$

Επειδή προφανώς το σύνολο U_n είναι κλειστό στον πολλαπλασιασμό μιγαδικών αριθμών, έπεται ότι το σύνολο U_n είναι μια υποομάδα της ομάδας T του κύκλου, και ιδιαίτερα η U_n είναι κυκλική τάξης n, διότι προφανώς:

$$\mathsf{U}_n = \langle\zeta_n\rangle = \left\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}\right\}$$

Υπενθυμίζουμε ότι μια n-οστή ρίζα της μονάδας καλείται **πρωταρχική n-οστή ρίζα της μονάδας** αν είναι γεννήτορας της U_n.

Συνδυάζοντας τις παραπάνω παρατηρήσεις με τα αποτελέσματα αυτής της ενότητας, θα έχουμε το ακόλουθο αποτέλεσμα.

Πρόταση 3.2.7. *Το σύνολο U_n των n-οστών ριζών της μονάδας είναι μια κυκλική υποομάδα τάξης n της ομάδας του κύκλου T:*

$$\mathsf{U}_n = \langle\zeta_n\rangle = \left\{1, \zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}\right\}, \quad \textit{όπου} \quad \zeta_n = e^{\frac{2\pi i}{n}}$$

Υπάρχουν ακριβώς $\varphi(n)$ πρωταρχικές n-οστές ρίζες της ομάδας, οι ακόλουθες:

$$\left\{\zeta_n^k \in \mathsf{U}_n \mid 1 \le k \le n \ \textit{και}\ (n,k) = 1\right\} = \left\{e^{\frac{2\pi ik}{n}} \in \mathsf{U}_n \mid 1 \le k \le n \ \textit{και}\ (n,k) = 1\right\}$$

Κυκλικές Ομάδες Μικρής Τάξης ≤ 4

Έστω $(G, \cdot)$ μια κυκλική ομάδα. Για τους πίνακες Cayley ομάδων με τάξη ≤ 4, παραπέμπουμε σε προηγούμενη ενότητα.

1. Αν $|G| = 1$, τότε $G = \{e\}$ και η G είναι κυκλική $G = \langle e\rangle$.
2. Αν $|G| = 2$, τότε $G = \{e, a\}$ και η G έχει πίνακα Cayley

$\cdot$	**e**	**a**
e	e	a
a	e	e

Άρα $a^2 = e$ και το στοιχείο a είναι γεννήτορας της G. Επομένως η G είναι κυκλική $G = \langle a\rangle$,

3. Αν $|G| = 3$, τότε $G = \{e, a, b\}$ και η G έχει πίνακα Cayley

$\cdot$	**e**	**a**	**b**
e	e	a	b
a	a	b	e
b	b	e	a

Τότε η G είναι κυκλική με γεννήτορα το στοιχείο a: $G = \langle a \rangle$. Πραγματικά, όπως βλέπουμε από τον πίνακα Cayley, θα έχουμε $a^2 = b \neq e$ και άρα $a^3 = ab = e$. Τότε όμως το στοιχείο a είναι γεννήτορας της G και άρα η G είναι κυκλική. Σημειώνουμε ότι $b = a^{-1}$ είναι επίσης γεννήτορας και $G = \langle a \rangle = \langle b \rangle$.

4. Αν $|G| = 4$, τότε $G = \{e, a, b, c\}$ και υπάρχουν δύο διαφορετικοί πίνακες Cayley:

Πίνακας Α΄ :

$\cdot$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Πίνακας Β΄:

$\cdot$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Ο πίνακας Cayley στην περίπτωση Α΄ είναι ο πίνακας Cayley της ομάδας του Klein, μοντέλο της οποίας είδαμε στο Παράδειγμα 3.1.13. Σ΄ αυτήν την ομάδα, κάθε στοιχείο της, εκτός του ουδέτερου e έχει τάξη ίση με 2. Έτσι δεν υπάρχει στοιχείο τάξης 4 και άρα δεν υπάρχει γεννήτορας για την G. Επομένως η ομάδα του Klein με πίνακα Cayley τον Α΄ δεν είναι κυκλική.

Από το Παράδειγμα 2.4.18 έπεται ότι οι υποομάδες της ομάδας του Klein είναι οι εξής:

$$\{e\}, \quad \{e, a\}, \quad \{e, b\}, \quad \{e, c\}, \quad G$$

Επομένως κάθε γνήσια υποομάδα της ομάδας του Klein έχει τάξη ≤ 2 και άρα είναι κυκλική.

Ο πίνακας Cayley στην περίπτωση Β΄ είναι πίνακας κυκλικής ομάδας. Πράγματι, θα έχουμε $b^2 = a$ και άρα $b^4 = aa = a^2 = e$. Επίσης θα έχουμε $b^3 = b^2 b = ab = c$. Έτσι $G = \{e, a, b, c\} = \{b^4 = e, b, b^2 = a, b^3 = c\} = \langle b \rangle$ και άρα το στοιχείο b είναι γεννήτορας της G. Επομένως η G είναι κυκλική.

Συνοψίζουμε κάποια από τα συμπεράσματα της παραπάνω ανάλυσης:

- «**Για κάθε φυσικό αριθμό n υπάρχει μια κυκλική ομάδα με τάξη ίση με n**».

Για παράδειγμα μπορούμε να θεωρήσουμε την προσθετική ομάδα $(\mathbb{Z}_n, +)$ ή την ομάδα U_n των n-οστών ριζών της μονάδας.

- «**Κάθε ομάδα τάξης ≤ 4 είναι κυκλική με εξαίρεση την ομάδα του Klein η οποία είναι μια μη κυκλική ομάδα τάξης 4 με την ιδιότητα ότι κάθε γνήσια υποομάδα της είναι κυκλική**».[4]

[4] Για ομάδες με τάξη ≤ 15 ισχύουν τα εξής (το πλήθος των ομάδων τάξης 16 είναι 14), βλέπε [31], [16]:

1. *Κάθε πεπερασμένη ομάδα με τάξη έναν πρώτο αριθμό είναι κυκλική.*
   Έτσι για παράδειγμα κάθε ομάδα με τάξη 2, 3, 5, 7, 11, 13, κτλ, είναι κυκλική. Εκ των υπολοίπων:
2. *Υπάρχουν ακριβώς 2 ομάδες με τάξη 6, εκ των οποίων η μια είναι κυκλική και η δεύτερη είναι δομικά ίδια με την συμμετρική ομάδα* S_3.
3. *Υπάρχουν ακριβώς 5 ομάδες με τάξη 8 εκ των οποίων μόνο μια είναι κυκλική.*
4. *Υπάρχουν ακριβώς 2 ομάδες με τάξη 9 εκ των οποίων μόνο μια είναι κυκλική.*
5. *Υπάρχουν ακριβώς 2 ομάδες με τάξη 10 εκ των οποίων μόνο μια είναι κυκλική.*
6. *Υπάρχουν ακριβώς 5 ομάδες με τάξη 12 εκ των οποίων μόνο μια είναι κυκλική.*
7. *Υπάρχουν ακριβώς 2 ομάδες με τάξη 14 εκ των οποίων μόνο μια είναι κυκλική.*
8. *Υπάρχουν ακριβώς 1 ομάδα με τάξη 15 η οποία είναι κυκλική.*

Σχόλιο 3.2.8. Φυσιολογικά τώρα τίθεται το ερώτημα:

- «**Για ποιες τιμές του n υπάρχει, με ακρίβεια ισομορφισμού, ακριβώς μια ομάδα τάξης n;**»

Σημειώνουμε ότι, αν υπάρχει ακριβώς μια ομάδα δεδομένης τάξης, τότε αυτή αναγκαστικά είναι κυκλική, και άρα η δομή της είναι γνωστή. Έτσι το παραπάνω αρώτημα διατυπώνεται ισοδύναμα και ως εξής: «**Για ποιες τιμές του n κάθε ομάδα τάξης n είναι κυκλική;**». Την απάντηση στο παραπάνω ερώτημα δίνει το ακόλουθο Θεώρημα του Dickson,[5] η απόδειξη του οποίου ξεφεύγει από τα πλαίσια των σημειώσεων.

Θεώρημα 3.2.9 (Dickson). [6] *Έστω $n \geq 1$ ένας φυσικός αριθμός. Τότε κάθε ομάδα τάξης n είναι κυκλική αν και μόνο αν:*

$$(n, \varphi(n)) = 1$$

όπου φ είναι η συνάρτηση του Euler. Ισοδύναμα: η πρωτογενής ανάλυση του n είναι της μορφής $n = p_1 p_2 \cdots p_k$, όπου $p_i \nmid p_j - 1$, $1 \leq i, j \leq k$.

Επομένως: υπάρχει, με ακρίβεια ισομορφισμού, ακριβώς μια ομάδα τάξης n, αν και μόνο αν $(n, \varphi(n)) = 1$.

Έτσι, για παράδειγμα, τυχούσα ομάδα τάξης 15 ή 561 είναι κυκλική διότι οι πρωτογενείς αναλύσεις των αριθμών 15 και 561 είναι $15 = 3 \cdot 5$ και $561 = 3 \cdot 11 \cdot 17$ και προφανώς ικανοποιούνται οι συνθήκες του Θεωρήματος 3.2.9. Αντίθετα υπάρχουν τουλάχιστον δύο (στην πραγματικότητα ακριβώς δύο) ομάδες τάξης 10, διότι $10 = 2 \cdot 5$ και $2 \mid 5 - 1$. √

3.2.2 Ομάδες στρέψης και ομάδες ελεύθερης στρέψης

Από το Παράδειγμα 3.1.17 βλέπουμε ότι υπάρχουν ομάδες με άπειρη τάξη, κάθε στοιχείο των οποίων έχει πεπερασμένη τάξη. Από την άλλη πλευρά υπάρχουν ομάδες με άπειρη τάξη, κάθε μη ταυτοτικό στοιχείο των οποίων έχει άπειρη τάξη, π.χ. η προσθετική ομάδα $(\mathbb{Z}, +)$. Έτσι οδηγούμαστε στον ακόλουθο ορισμό.

Ορισμός 3.2.10. *Έστω $(G, \cdot)$ μια ομάδα.*

1. *Η ομάδα G καλείται* **ομάδα στρέψης** *ή* **περιοδική ομάδα**, *αν κάθε στοιχείο της G έχει πεπερασμένη τάξη.*
2. *Η ομάδα G καλείται* **ομάδα ελεύθερης στρέψης**, *αν κάθε στοιχείο της G, εκτός του ουδετέρου, έχει άπειρη τάξη.*

Παράδειγμα 3.2.11.

1. Όπως προκύπτει από την Παρατήρηση 3.1.16, κάθε πεπερασμένη ομάδα είναι ομάδα στρέψης. Σύμφωνα με το Παράδειγμα 3.1.17, υπάρχουν ομάδες στρέψης οι οποίες έχουν άπειρη τάξη.
2. Κάθε ομάδα ελεύθερης στρέψης είναι προφανώς ομάδα άπειρης τάξης, και κάθε άπειρη κυκλική ομάδα, π.χ. η $(\mathbb{Z}, +)$, είναι ομάδα ελεύθερης στρέψης.
3. Υπάρχουν ομάδες οι οποίες είναι **μεικτές**, δηλαδή περιέχουν στοιχεία πεπερασμένης τάξης και στοιχεία άπειρης τάξης. Ένα τέτοιο παράδειγμα είναι η ομάδα ευθύ γινόμενο:

   $$\mathbb{Z}_2 \times \mathbb{Z} = \{([x]_2, m) \mid x, m \in \mathbb{Z}\}$$

   με πράξη *κατά συνιστώσα*:

   $$([x]_2, m) + ([y]_2, n) = ([x + y]_2, m + n)$$

   και της οποίας το ουδέτερο στοιχείο είναι το ζεύγος $([0]_2, 0)$.

   Τότε το στοιχείο $([1]_2, 0)$ έχει τάξη 2, και το στοιχείο $([0]_2, 1)$ έχει άπειρη τάξη. √

[5] L.E. Dickson, *Definitions of a group and a field by independent postulates*, Trans. Amer. Math. Soc. **6** (1905), 198–204.

[6] Leonard Eugene Dickson (22 Ιανουαρίου 1874 - 17 Ιανουαρίου 1954) https://en.wikipedia.org/wiki/Leonard_Eugene_Dickson Αμερικανός μαθηματικός με συμβολή στην Άλγεβρα (θεωρία ομάδων και πεπερασμένων σωμάτων), ο οποίος συνέγραψε και ιστορικά βιβλία γύρω από τη Θεωρία Αριθμών.

Παράδειγμα 3.2.12. Υπενθυμίζουμε ότι η ομάδα του κύκλου είναι η υποομάδα

$$\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\}$$

της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*, \cdot)$ των μη μηδενικών μιγαδικών αριθμών.

Έστω p ένας πρώτος αριθμός και έστω

$$\mathbb{Z}(p^\infty) = \{z \in \mathbb{C} \mid z^{p^n} = 1, \text{ για κάποιο } n \in \mathbb{Z}^+\} \subseteq \mathsf{T}$$

Εύκολα βλέπουμε ότι το υποσύνολο $\mathbb{Z}(p^\infty)$ είναι μια υποομάδα της T και κάθε στοιχείο της $\mathbb{Z}(p^\infty)$ έχει πεπερασμένη τάξη, διότι $\forall z \in \mathsf{T}$, υπάρχει φυσικός αριθμός n έτσι ώστε $z^{p^n} = 1$. Έτσι η ομάδα $\mathbb{Z}(p^\infty)$ είναι μια, προφανώς άπειρη, ομάδα στρέψης.

Η ομάδα $\mathbb{Z}(p^\infty)$ καλείται η **p-οστή ομάδα Prüfer**[7] και έχει, μεταξύ άλλων, την ακόλουθη ενδιαφέρουσα ιδιότητα, βλέπε την Άσκηση 3.9.59: «*όλες οι γνήσιες υποομάδες της είναι πεπερασμένες κυκλικές και υπάρχει ακριβώς μια τέτοια υποομάδα τάξης p^n, για κάθε $n \in \mathbb{Z}^+$*». √

Οι παραπάνω παρατηρήσεις και παραδείγματα σχετίζονται με ένα περίφημο πρόβλημα στη Θεωρία Ομάδων:

Παρατήρηση 3.2.13. (Το Πρόβλημα του Burnside).[8] Υπενθυμίζουμε ότι μια ομάδα $(G, \cdot)$ καλείται **πεπερασμένα παραγόμενη**, αν η G έχει ένα πεπερασμένο σύνολο γεννητόρων, ισοδύναμα, αν υπάρχει πεπερασμένο πλήθος στοιχείων $z_1, z_2, \cdots, z_m \in G$, έτσι ώστε κάθε στοιχείο $x \in G$ να γράφεται ως:

$$x = z_1^{n_1} \cdot z_2^{n_2} \cdots z_m^{n_m}, \qquad \text{για κατάλληλα} \quad n_1, n_2, \cdots, n_m \in \mathbb{Z}$$

Το γενικό Πρόβλημα του Burnside διατυπώνεται ως εξής:

«*Είναι κάθε πεπερασμένα παραγόμενη ομάδα στρέψης πεπερασμένη;*»

Το Πρόβλημα του Burnside απαντήθηκε αρνητικά το 1964 από τους E.Golod[9] και I. Shafarevich,[10] οι οποίοι κατασκεύασαν μια πεπερασμένα παραγόμενη άπειρη ομάδα, κάθε στοιχείο της οποίας έχει πεπερασμένη τάξη η οποία είναι δύναμη ενός πρώτου αριθμού p.

Το Πρόβλημα του Burnside έχει θετική απάντηση όταν περιοριστούμε στην κλάση των αβελιανών ομάδων, καθώς ισχύει ότι:

«*Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα στρέψης είναι πεπερασμένη*».

Η ομάδα Prüfer $\mathbb{Z}(p^\infty)$ είναι μια άπειρη αβελιανή ομάδα στρέψης. Επομένως, σύμφωνα με τα παραπάνω δεν μπορεί να είναι πεπερασμένα παραγόμενη. ▲

3.2.3 Τάξη Γινομένου Στοιχείων μιας Ομάδας

Στο παραπάνω πλαίσιο, ανακύπτει το εξής ενδιαφέρον ερώτημα: «*Αν x, y είναι δύο στοιχεία πεπερασμένης τάξης μιας ομάδας, υπάρχει τότε κάποια σχέση μεταξύ των τάξεων των στοιχείων x, y, και xy*»;

Η ακόλουθη σειρά παραδειγμάτων δείχνει ότι, γενικά, δεν είναι δυνατόν να περιμένουμε να υπάρχει κάποια σχέση μεταξύ των τάξεων $o(x)$, $o(y)$, και $o(xy)$:

---

[7] Heinz Prüfer (10 Νοεμβρίου 1896 - 7 Απριλίου 1934) [http://en.wikipedia.org/wiki/Heinz_Prufer]: Γερμανός μαθηματικός με σημαντική συμβολή στη Θεωρία (Αβελιανών) Ομάδων. Επιπρόσθετα είχε συμβολή στη Θεωρία Αλγεβρικών Αριθμών, στη Θεωρία Κόμβων και στις Διαφορικές Εξισώσεις.

[8] William Burnside (2 Ιουλίου 1852 - 21 Αυγούστου 1927) [https://en.wikipedia.org/wiki/William_Burnside]: Βρετανός μαθηματικός, με σημαντική συμβολή στην Άλγεβρα και ιδιαίτερα στη Θεωρία Ομάδων και στη Θεωρία Αναπαραστάσεων.

[9] Evgeny Golod (21 Οκτωβρίου 1935 -) [http://en.wikipedia.org/wiki/Evgeny_Golod]: Ρώσος μαθηματικός (μαθητής του Igor Safarevich) με συμβολή στην Αλγεβρική Θεωρία Αριθμών, στη Θεωρία Αλγεβρών (Lie) και στη Θεωρία Ομάδων.

[10] Igor Shafarevich (3 Ιουνίου 1923 -) [http://en.wikipedia.org/wiki/Igor_Shafarevich]: Διακεκριμένος Ρώσος μαθηματικός με θεμελιώδη συμβολή στην Αλγεβρική Θεωρία Αριθμών και στην Αλγεβρική Γεωμετρία.

Παράδειγμα 3.2.14. Στη συμμετρική ομάδα S_4 θεωρούμε τα στοιχεία:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} = (1\,2\,3) \qquad \text{και} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\,2\,4)$$

Τότε θα έχουμε:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \tau \circ \sigma$$

Εύκολα υπολογίζουμε ότι:

$$\mathsf{o}(\sigma) = 3 = \mathsf{o}(\tau) \qquad \text{και} \qquad \mathsf{o}(\sigma \circ \tau) = 2 = \mathsf{o}(\tau \circ \sigma)$$

Παρατηρούμε ότι: $\mathsf{o}(\sigma \circ \tau) = 2 \neq 9 = \mathsf{o}(\sigma) \cdot \mathsf{o}(\tau)$. $\surd$

Παράδειγμα 3.2.15. Στη συμμετρική ομάδα S_5 θεωρούμε τα στοιχεία:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \qquad \text{και} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}$$

Παρατηρούμε ότι:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix} = \tau \circ \sigma$$

Τότε υπολογίζουμε εύκολα ότι:

$$\mathsf{o}(\sigma) = 3 \qquad \text{και} \qquad \mathsf{o}(\tau) = 5 \qquad \text{και} \qquad \mathsf{o}(\sigma \circ \tau) = 2 = \mathsf{o}(\tau \circ \sigma)$$

Παρατηρούμε ότι: $\mathsf{o}(\sigma \circ \tau) = 2 \neq 15 = \mathsf{o}(\sigma) \cdot \mathsf{o}(\sigma)$. $\surd$

Παράδειγμα 3.2.16. Θεωρούμε την (άπειρη μη αβελιανή) ομάδα

$$\mathsf{GL}(2,\mathbb{R}) = \left\{ A \in \mathsf{M}_2(\mathbb{R}) \mid \mathsf{Det}(A) \neq 0 \right\}$$

και έστω

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{και} \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Τότε προφανώς $A, B, A \cdot B \in \mathsf{GL}(2,\mathbb{R})$. Παρατηρούμε ότι:

$$A^2 = I_2 = B^2$$

Επομένως τα στοιχεία A, B έχουν τάξη 2. Όμως

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \text{και} \qquad BA = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (AB)^{-1}$$

και άρα $\forall\, n \geq 1$:

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad \text{και} \qquad (BA)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$$

Επομένως τα στοιχεία A, B έχουν τάξη 2, αλλά τα γινόμενά τους AB και BA έχουν άπειρη τάξη.

Παρατηρούμε ότι: $AB \neq BA$. $\surd$

Παράδειγμα 3.2.17. Για κάθε $n \geq 3$, υπάρχει μια πεπερασμένη αβελιανή ομάδα G η οποία περιέχει δύο στοιχεία τάξης 2 των οποίων το γινόμενο έχει τάξη n:

Πράγματι θεωρούμε την ομάδα[11]

$$\mathsf{GL}(2,\mathbb{Z}_n) = \{A \in \mathsf{M}_2(\mathbb{Z}_n) \mid A\colon \text{αντιστρέψιμος}\}$$

των αντιστρέψιμων πινάκων με στοιχεία από το σύνολο $\mathbb{Z}_n$. Όπως βλέπουμε εύκολα, οι πίνακες[12]

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{και} \quad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

έχουν τάξη 2 ($A^2 = I_2 = B^2$) και ο πίνακας

$$A \cdot B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

έχει τάξη n διότι

$$(A \cdot B)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

ως πίνακες με στοιχεία από το $\mathbb{Z}_n$, και το n είναι ο μικρότερος φυσικός με αυτή την ιδιότητα. Επομένως τα στοιχεία A, B έχουν τάξη 2, αλλά το γινόμενό τους AB έχει τάξη n.

Παρατηρούμε ότι: $AB \neq BA$, διότι $BA = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ και $-1 \neq 1$ στο $\mathbb{Z}_n$ διότι $n \geq 3$. $\surd$

Σε όλα τα παραπάνω παραδείγματα τα στοιχεία της ομάδας δεν μετατίθενται, και για στοιχεία x, y πεπερασμένης τάξης, δεν μπορουμε να πούμε τίποτα για την τάξη του $x \cdot y$ η οποία μπορεί να είναι άπειρη ή οποιοσδήποτε φυσικός αριθμός. Για παράδειγμα, από ένα αποτέλεσμα του G.A. Miller[13] έπεται ότι: *«αν επιλέξουμε τυχαία θετικούς ακέραιους $m, n, k > 1$, τότε υπάρχει πεπερασμένη ομάδα G η οποία περιέχει στοιχεία x, y έτσι ώστε: $\mathsf{o}(x) = m$, $\mathsf{o}(y) = n$, και $\mathsf{o}(xy) = k$»*.

Από την άλλη πλευρά, υπάρχουν στοιχεία πεπερασμένης τάξης x και y τα οποία μετατίθενται, αλλά η τάξη του στοιχείου $x \cdot y$ είναι διάφορη του γινομένου των τάξεων των στοιχείων:

Παράδειγμα 3.2.18. Θεωρούμε την ομάδα των 10-οστών ριζών της μονάδας:

$$\mathsf{U}_{10} = \left\{ e^{\frac{2kpi}{10}} \in \mathbb{C} \mid 0 \leq k \leq 9 \right\} = \langle \zeta_{10} \rangle$$

η οποία είναι κυκλική, με γεννήτορα μια πρωταρχική δέκατη ρίζα της μονάδας ζ_{10}, και ιδιαίτερα είναι μια αβελιανή ομάδα. Θεωρούμε τα στοιχεία:

$$x = \zeta_{10}^2 \quad \text{και} \quad y = \zeta_{10}^3$$

Τότε θα έχουμε $x \cdot y = \zeta_{10}^5 = y \cdot x$, και

$$\mathsf{o}(x) = \mathsf{o}(\zeta_{10}^2) = \frac{10}{(2,10)} = \frac{10}{2} = 5 \quad \text{και} \quad \mathsf{o}(y) = \mathsf{o}(\zeta_{10}^3) = \frac{10}{(3,10)} = \frac{10}{1} = 10$$

Παρατηρούμε ότι $\mathsf{o}(xy) = \mathsf{o}(\zeta_{10}^5) = \frac{10}{(5,10)} = \frac{10}{5} = 2$, και άρα:

$$\mathsf{o}(xy) = 2 \neq 50 = \mathsf{o}(x)\mathsf{o}(y) \quad \surd$$

[11] Στο σύνολο $\mathsf{M}_2(\mathbb{Z}_n)$ των 2×2 πινάκων με στοιχεία από το $\mathbb{Z}_n$ μπορούμε να ορίσουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «$\cdot$», οι οποίες επάγονται από τις αντίστοιχες πράξεις πρόσθεσης και πολαπλασιασμού στο σύνολο $\mathbb{Z}_n$, και τότε η τριάδα $(\mathsf{M}_2(\mathbb{Z}_n), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα τον μοναδιαίο πίνακα I_n υπεράνω του $\mathbb{Z}_n$, δηλαδή $I_n = (\delta_{ij})$, όπου $\delta_{ij} = \begin{cases} [0]_n, \text{ αν } i \neq j \\ [1]_n, \text{ αν } i = j \end{cases}$, βλέπε το Κεφάλαιο 7 για περισσότερες λεπτομέρειες. Για κάθε μεταθετικό δακτύλιο με μονάδα R ορίζεται η ομάδας $\mathsf{GL}(n,R)$ των αντιστρέψιμων $n \times n$ πινάκων με στοιχεία από τον R με τον ίδιο τρόπο με τον οποίο ορίζεται η ομάδα $\mathsf{GL}(n,R)$, όταν $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Έτσι η ομάδα $\mathsf{GL}(2,\mathbb{Z}_n)$ αποτελείται από όλους τους πίνακες $A \in \mathsf{M}_2(\mathbb{Z}_n)$ για τους οποίους υπάρχει πίνακας $B \in \mathsf{M}_2(\mathbb{Z}_n)$ έτσι ώστε $A \cdot B = I_n = B \cdot A$.

[12] Χάριν απλότητας, γράφουμε $0, 1$, κλπ., αντί $[0]_n, [1]_n$, κλπ.

[13] G.A. Miller: 31 Ιουλίου 1863 - 10 Φεβρουαρίου 1951 [http://en.wikipedia.org/wiki/George_Abram_Miller]: Αμερικανός μαθηματικός με συμβολή κυρίως στη Θεωρία Ομάδων και στην Ιστορία των Μαθηματικών.

Θα δούμε σε λίγο ότι υπό ορισμένες προϋποθέσεις υπάρχει στενή σχέση μεταξύ των τάξεων $\mathsf{o}(x)$, $\mathsf{o}(y)$, και $\mathsf{o}(xy)$.

Παρατηρούμε επίσης ότι στα παραδείγματα αυτής της υποενότητας ισχύει ότι $\mathsf{o}(xy) = \mathsf{o}(yx)$, αν και γενικά $\mathsf{o}(xy) \neq \mathsf{o}(x)\mathsf{o}(y)$. Αυτό δεν είναι τυχαίο: όπως θα διαπιστώσουμε στο παρακάτω αποτέλεσμα, αν a, b είναι στοιχεία πεπερασμένης τάξης μιας ομάδας, τότε, ανεξάρτητα αν τα a, b μετατίθενται, τα στοιχεία ab και ba έχουν την ίδια τάξη:

Πρόταση 3.2.19. *Έστω $(G,\cdot)$ μια ομάδα, και a, b, x τυχόντα στοιχεία της G. Τότε:*

$$\mathsf{o}(x^{-1}ax) = \mathsf{o}(a) = \mathsf{o}(xax^{-1}) \qquad \text{και} \qquad \mathsf{o}(ab) = \mathsf{o}(ba)$$

Απόδειξη. 1. Για κάθε $x, a \in G$ έχουμε:

$$(x^{-1}ax)^n = (x^{-1}ax)\cdot(x^{-1}ax)\cdots(x^{-1}ax) = x^{-1}a^n x$$

και άρα, για κάθε $n \in \mathbb{N}$, θα έχουμε:

$$(x^{-1}ax)^n = e \iff x^{-1}a^n x = e \iff a^n = xex^{-1} \iff a^n = e \qquad (*)$$

Η παραπάνω σχέση $(*)$ δείχνει ότι

$$\{n \in \mathbb{N} \mid a^n = e\} = \{n \in \mathbb{N} \mid (x^{-1}ax)^n = e\}$$

και επομένως:

$$\mathsf{o}(a) = \min\{m \in \mathbb{N} \mid a^m = e\} = \min\{m \in \mathbb{N} \mid (x^{-1}ax)^m = e\} = \mathsf{o}(x^{-1}ax)$$

Η απόδειξη της ισότητας $\mathsf{o}(a) = \mathsf{o}(xax^{-1})$ είναι παρόμοια (μπορούμε να χρησιμοποιήσουμε επίσης την αποδειχθείσα σχέση $\mathsf{o}(x^{-1}ax) = \mathsf{o}(a)$ σε συνδυασμό με τη σχέση $xax^{-1} = (x^{-1})^{-1}ax^{-1}$).

2. Έστω $a, b \in G$. Επειδή

$$a^{-1}\cdot ab\cdot a = eba = ba$$

από το 1. έχουμε το ζητούμενο: $\mathsf{o}(ab) = \mathsf{o}(a^{-1}aba) = \mathsf{o}(ba)$. ■

Πρόταση 3.2.20. *Έστω ότι $(G,\cdot)$ είναι μια ομάδα και a, b είναι δύο στοιχεία της με $ab = ba$. Αν οι τάξεις $\mathsf{o}(a), \mathsf{o}(b)$ είναι πεπερασμένες και $(\mathsf{o}(a), \mathsf{o}(b)) = 1$, τότε η τάξη του στοιχείου ab είναι πεπερασμένη και είναι ίση με $\mathsf{o}(a)\cdot\mathsf{o}(b)$:*

$$\max\{\mathsf{o}(a), \mathsf{o}(b)\} < \infty \quad \text{και} \quad (\mathsf{o}(a), \mathsf{o}(b)) = 1 \quad \& \quad ab = ba \quad \Longrightarrow \quad \mathsf{o}(ab) = \mathsf{o}(a)\cdot\mathsf{o}(b)$$

Απόδειξη. Έστω ότι $\mathsf{o}(a) = n$, $\mathsf{o}(b) = m$ και $\mathsf{o}(ab) = k$. Άρα $a^n = e$, $b^m = e$ και επειδή $ab = ba$ έπεται ότι

$$(ab)^{nm} = ab\cdot ab\cdots ab = a^{nm}b^{nm} = (a^n)^m(b^m)^n = e^m e^n = e \implies \mathsf{o}(ab) = k \mid nm = \mathsf{o}(a)\mathsf{o}(b) \qquad (1)$$

Επειδή $\mathsf{o}(ab) = k$ και $ab = ba$, χρησιμοποιώντας το Θεώρημα 3.2.2, θα έχουμε

$$(ab)^k = e \implies a^k b^k = e \implies a^k = b^{-k} \implies \mathsf{o}(a^k) = \mathsf{o}(b^{-k}) = \mathsf{o}(b^k)$$

Τότε από την τελευταία σχέση έχουμε:

$$\begin{cases} \mathsf{o}(a^k) = \frac{\mathsf{o}(a)}{\mathsf{o}(a),k} = \frac{n}{(n,k)} \\ \mathsf{o}(b^k) = \frac{\mathsf{o}(b)}{\mathsf{o}(b),k} = \frac{m}{(m,k)} \end{cases} \implies \frac{n}{(n,k)} = \frac{m}{(m,k)} \implies n\cdot(m,k) = m\cdot(n,k)$$

$$\implies \begin{cases} n \mid m\cdot(n,k) \\ m \mid n\cdot(m,k) \end{cases} \overset{(n,m)=1}{\Longrightarrow} \begin{cases} n \mid (n,k) \\ m \mid (m,k) \end{cases}$$

$$\implies \begin{cases} n = (n,k) \\ m = (m,k) \end{cases} \implies \begin{cases} n \mid k \\ m \mid k \end{cases}$$

και άρα, επειδή $(n,m)=1$, έπεται ότι

$$\mathrm{o}(a)\mathrm{o}(b)=nm \mid k=\mathrm{o}(ab) \tag{2}$$

Από τις σχέσεις (1) και (2) συμπεραίνουμε ότι $\mathrm{o}(a)\mathrm{o}(b)=\mathrm{o}(ab)$. ■

Παρατήρηση 3.2.21. Γενικότερα, όπως θα δείξουμε αργότερα, ισχύει η ακόλουθη γενίκευση της Πρότασης 3.2.20. Έστω $(G,\cdot)$ μια ομάδα και $a,b\in G$ στοιχεία πεπερασμένης τάξης της G. Υποθέτουμε ότι:

1. $a\cdot b=b\cdot a$,
2. Για κάθε πρώτο διαιρέτη p του $\mathrm{o}(a)\cdot\mathrm{o}(b)$, η μεγαλύτερη δύναμη του p η οποία διαιρεί τον $\mathrm{o}(a)$ δεν είναι ίση με την μεγαλύτερη δύναμη του p η οποία διαιρεί τον $\mathrm{o}(b)$.

Τότε η τάξη του στοιχείου ab είναι ίση με το ελάχιστο κοινό πολλαπλάσιο των τάξεων στοιχείων a και b:

$$\mathrm{o}(a\cdot b)=[\mathrm{o}(a),\mathrm{o}(b)] \quad ▲$$

3.2.4 Τάξη στοιχείων σε Ευθέα Γινόμενα Ομάδων

Έστω $(G_1,\cdot)$, $(G_2,\cdot)$, $\cdots$, $(G_n,\cdot)$ μια πεπερασμένη οικογένεια ομάδων, όπου, χάριν ευκολίας και χωρίς να υπάρχει κίνδυνος σύγχυσης, διατηρούμε το ίδιο σύμβολο για την πράξη καθεμιάς από τις ομάδες.

Υπενθυμίζουμε ότι η ομάδα *ευθύ γινόμενο* $(\prod_{k=1}^n G_k,\cdot)$ ορίζεται να είναι το καρτεσιανό γινόμενο των συνόλων $\prod_{k=1}^n G_k=G_1\times G_2\times\cdots\times G_n$ εφοδιασμένο με την ακόλουθη πράξη

$$(x_1,x_2,\cdots,x_n)\cdot(x_1,x_2,\cdots,x_n)=(x_1\cdot y_1,x_2\cdot y_2,\cdots,x_n\cdot y_n)$$

Το ουδέτερο στοιχείο της ομάδας $\prod_{k=1}^n G_k$ είναι το στοιχείο $\mathrm{e}=(e_1,e_2,\cdots,e_n)$, όπου e_k είναι το ουδέτερο στοιχείο της ομάδας G_k, $1\le k\le n$.

Πρόταση 3.2.22. *Για ένα στοιχείο $\mathrm{x}=(x_1,x_2,\cdots,x_n)$ της ομάδας ευθέος γινομένου $\prod_{k=1}^n G_k$, τα ακόλουθα είναι ισοδύναμα:*

1. *Το στοιχείο $\mathrm{x}\in\prod_{k=1}^n G_k$ έχει πεπερασμένη τάξη.*
2. *Για κάθε $k=1,2,\cdots,n$, το στοιχείο $x_k\in G_k$ έχει πεπερασμένη τάξη.*

Αν το στοιχείο x έχει πεπερασμένη τάξη, τότε[14]*:*

$$\mathrm{o}(\mathrm{x})=\mathrm{o}(x_1,x_2,\cdots,x_n)=\big[\mathrm{o}(x_1),\mathrm{o}(x_2),\cdots,\mathrm{o}(x_n)\big]$$

Ιδιαίτερα αν $(\mathrm{o}(x_i),\mathrm{o}(x_j))=1$, για κάθε $1\le i\ne j\le n$, τότε: $\mathrm{o}(\mathrm{x})=\mathrm{o}(x_1)\cdot\mathrm{o}(x_2)\cdots\mathrm{o}(x_n)$.

Απόδειξη. Για κάθε θετικό ακέραιο r, θα έχουμε:

$$\mathrm{x}^r=(x_1,x_2,\cdots,x_n)^r=(x_1^r,x_2^r,\cdots,x_n^r)$$

και επομένως, $\mathrm{x}^r=\mathrm{e}$ αν και μόνο αν $(x_1^r,x_2^r,\cdots,x_n^r)=(e_1,e_2,\cdots,e_n)$ αν και μόνο αν $x_k^r=e_k$, $\forall k=1,2,\cdots,n$. Ισοδύναμα, το στοιχείο x έχει πεπερασμένη τάξη στην $\prod_{k=1}^n G_k$ αν και μόνο αν, για κάθε $k=1,2,\cdots,n$, το στοιχείο $x_k\in G_k$ έχει πεπερασμένη τάξη.

Υποθέτουμε ότι $\mathrm{o}(\mathrm{x})=m$ και $\mathrm{o}(x_k)=m_k$, $1\le k\le n$. Θα δείξουμε ότι:

$$m=\big[m_1,m_2,\cdots,m_n\big] \tag{†}$$

[14] Αν $m_1,m_2,\cdots,m_n$ είναι ακέραιοι αριθμοί, τότε $[m_1,m_2,\cdots,m_n]$ ή ΕΚΠ$(m_1,m_2,\cdots,m_n)$ συμβολίζει το Ελάχιστο Κοινό Πολλαπλάσιο των αριθμών $m_1,m_2,\cdots,m_n$.

Έστω $l = [m_1, m_2, \cdots, m_n]$. Τότε υπάρχουν θετικοί ακέραιοι $l_1, l_2, \cdots, l_n$ έτσι ώστε: $l = l_k m_k$, $1 \le k \le n$. Χρησιμοποιώντας οτι $\mathsf{o}(x_k) = m_k$, $1 \le k \le n$, θα έχουμε

$$\mathsf{x}^l = (x_1, x_2, \cdots, x_n)^l = (x_1^l, x_2^l, \cdots, x_n^l) = (x_1^{l_1 m_1}, x_2^{l_2 m_2}, \cdots, x_n^{l_n m_n}) = ((x_1^{m_1})^{l_1}, (x_2^{m_2})^{l_2}, \cdots, (x_n^{m_n})^{l_n}) =$$

$$= (e_1^{l_1}, e_2^{l_2}, \cdots, e_n^{l_n}) = (e_1, e_2, \cdots, e_n) = \mathsf{e}$$

Επομένως από την Πρόταση 3.2.1 έπεται ότι $\mathsf{o}(\mathsf{x}) = m \mid l$. Από την άλλη πλευρά, επειδή $\mathsf{o}(\mathsf{x}) = m$, θα έχουμε

$$(e_1, e_2, \cdots, e_n) = \mathsf{e} = \mathsf{x}^m = (x_1, x_2, \cdots, x_n)^m = (x_1^m, x_2^m, \cdots, x_n^m) \quad \Longrightarrow \quad x_k^m = e_k, \quad 1 \le k \le n$$

Επομένως από την Πρόταση 3.2.1 έπεται ότι $\mathsf{o}(x_k) = m_k \mid m$, $1 \le k \le n$. Τότε όμως και το ελάχιστο κοινό πολλαπλάσιο $l = [m_1, m_2, \cdots, m_n]$ των $m_1, m_2, \cdots, m_n$ διαιρεί το m και επομένως $l \mid m$. Έτσι δείξαμε ότι $l \mid m$ και $m \mid l$, και άρα $l = m$. ■

Πόρισμα 3.2.23. *Έστω η ομάδα ευθύ γινόμενο $G = \prod_{k=1}^n G_k$ των ομάδων $(G_k, \cdot)$, $1 \le k \le n$.*

1. *Η ομάδα G είναι ομάδα στρέψης αν και μόνο αν η ομάδα G_k είναι ομάδα στρέψης, για κάθε $k = 1, 2, \cdots, n$.*
2. *Η ομάδα G είναι ομάδα ελεύθερης στρέψης αν και μόνο αν η ομάδα G_k είναι ομάδα ελεύθερης στρέψης, για κάθε $k = 1, 2, \cdots, n$.*

Απόδειξη. 1. Έστω ότι η G είναι ομάδα στρέψης, δηλαδή όλα τα στοιχεία της έχουν πεπερασμένη τάξη. Έστω $x_k \in G_k$ ένα τυχόν στοιχείο της G_k, και θεωρούμε το στοιχείο $\mathsf{x} = (e_1, \cdots, e_{k-1}, x_k, e_{k+1}, \cdots, e_n)$. Επειδή το x έχει πεπερασμένη τάξη, από την Πρόταση 3.2.22 έπεται ότι η τάξη του x_k είναι πεπερασμένη. Επομένως, για κάθε $k = 1, 2, \cdots$, η τάξη κάθε στοιχείου της G_k είναι πεπερασμένη και άρα η G_k είναι ομάδα στρέψης. Αντίστροφα, αν αυτό ισχύει, έστω $\mathsf{x} = (x_1, x_2, \cdots, x_n)$ ένα τυχόν στοιχείο της ομάδας ευθέος γινομένου $G = \prod_{k=1}^n G_k$. Επειδή οι ομάδες G_k είναι ομάδες στρέψης, έπεται ότι $\mathsf{o}(x_k) = m_k < \infty$. Θέτοντας $m = m_1 m_2 \cdots m_k$, βλέπουμε άμεσα ότι $\mathsf{x}^m = \mathsf{e}$, και άρα το x έχει πεπερασμένη τάξη. Επομένως η ομάδα G είναι ομάδα στρέψης.

2. Η απόδειξη είναι ανάλογη με την απόδειξη του 1. και αφήνεται ως άσκηση. ■

Παράδειγμα 3.2.24. (α) Θεωρούμε την ομάδα ευθύ γινόμενο $\mathbb{Z}_4 \times \mathbb{Z}_{25} \times \mathsf{S}_3$, και έστω το στοιχείο της $\mathsf{x} = ([2]_4, [17]_{25}, (132))$. Επειδή

$$\mathsf{o}([2]_4 = 2, \qquad \mathsf{o}([17]_{25}) = \frac{25}{(17, 25)} = \frac{25}{1} = 25, \quad \text{και} \quad \mathsf{o}((132)) = 3$$

έπεται ότι $\mathsf{o}(\mathsf{x}) = [2, 25, 3] = 150$.

(β) Θεωρούμε την ομάδα ευθύ γινόμενο $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_m}$, των προσθετικών ομάδων $(\mathbb{Z}_{n_k}, +)$, όπου οι θετικοί ακέραιοι n_k, $1 \le k \le m$, είναι σχετικώς πρώτοι μεταξύ τους, δηλαδή: $(n_i, n_j) = 1$, αν $i \ne j$.

Ισχυρισμός: Η ομάδα G είναι κυκλική.

Απόδειξη του Ισχυρισμού: Πράγματι, θεωρούμε το στοιχείο $\mathsf{x} = \left([1]_{n_1}, [1]_{n_2}, \cdots, [1]_{n_m}\right) \in G$. Επειδή κάθε $\mathbb{Z}_{n_k}$ είναι κυκλική με γεννήτορα το στοιχείο $[1]_{n_k}$, έπεται ότι $\mathsf{o}([1]_{n_k}) = n_k$. Επειδή οι αριθμοί n_k είναι ανά δύο πρώτοι μεταξύ τους, $1 \le k \le m$, ως γνωστόν θα έχουμε $[n_1, n_2, \cdots, n_m] = n_1 \cdot n_2 \cdots n_k$, και τότε από την Πρόταση 3.2.22 έπεται ότι η τάξη του στοιχείου x είναι $\mathsf{o}(\mathsf{x}) = n_1 \cdot n_2 \cdots \cdot n_k$. Επειδή η τάξη της G είναι προφανώς $n_1 \cdot n_2 \cdots n_k$, έπεται ότι η G έχει ένα στοιχείο, το x, με τάξη ίση με την τάξη της G. Από το Πόρισμα 3.1.15 έπεται τότε ότι η G είναι κυκλική με γεννήτορα το στοιχείο x. $\surd$

3.3 Υποομάδες και Σχέσεις Ισοδυναμίας, Πλευρικές Κλάσεις

Έστω $(G,\cdot)$ μια ομάδα. Ως συνήθως συμβολίζουμε με e ή e_G το ουδέτερο στοιχείο της ομάδας G και με a^{-1} το αντίστροφο του στοιχείου $a \in G$.

Για κάθε υποσύνολο $H \subseteq G$ του G, ορίζουμε τις ακόλουθες σχέσεις $\mathscr{R}_H$ και $\mathscr{R}^H$ επί του συνόλου G:

$$\forall x,y \in G\colon \quad x\mathscr{R}_H y \quad \Longleftrightarrow \quad x^{-1}\cdot y \in H$$

$$\forall x,y \in G\colon \quad x\mathscr{R}^H y \quad \Longleftrightarrow \quad x\cdot y^{-1} \in H$$

Το επόμενο αποτέλεσμα χαρακτηρίζει πότε οι σχέσεις $\mathscr{R}_H$ και $\mathscr{R}^H$ είναι σχέσεις ισοδυναμίας επί του συνόλου G.

Πρόταση 3.3.1. *Έστω $(G,\cdot)$ μια ομάδα και $H \subseteq G$ ένα υποσύνολο της G. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Το υποσύνολο H είναι υποομάδα της G.*
2. *Η σχέση $\mathscr{R}_H$ είναι σχέση ισοδυναμίας επί του συνόλου G.*
3. *Η σχέση $\mathscr{R}^H$ είναι σχέση ισοδυναμίας επί του συνόλου G.*

Απόδειξη. **1.** «$\Longrightarrow$» **2.** Θα έχουμε:

- $\forall x \in G$, ισχύει ότι $x\mathscr{R}_H x$, διότι $x^{-1}\cdot x = e \in H$ επειδή το υποσύνολο H είναι υποομάδα.
- $\forall x,y \in G$, έστω $x\mathscr{R}_H y$ και άρα $x^{-1}\cdot y \in H$. Επειδή το υποσύνολο H είναι υποομάδα, έπεται ότι

$$(x^{-1}\cdot y)^{-1} \in H \quad \Longrightarrow \quad y^{-1}\cdot (x^{-1})^{-1} = y^{-1}\cdot x \in H$$

και άρα $y\mathscr{R}_H x$.

- $\forall x,y,z \in G$, έστω $x\mathscr{R}_H y$ και $y\mathscr{R}_H z$. Τότε $x^{-1}\cdot y \in H$ και $y^{-1}\cdot z \in H$. Επειδή το υποσύνολο H είναι υποομάδα θα έχουμε:

$$(x^{-1}\cdot y)\cdot (y^{-1}\cdot z) = x^{-1}\cdot y\cdot y^{-1}\cdot z = x^{-1}\cdot e\cdot z = x^{-1}\cdot z \in H$$

και άρα $x\mathscr{R}_H z$.

Επομένως η σχέση $\mathscr{R}_H$ είναι σχέση ισοδυναμίας επί του συνόλου G.

2. «$\Longrightarrow$» **1.** Θα έχουμε:

- Επειδή $\forall x \in G$: $x\mathscr{R}_H x$ και $e \in G$, θα έχουμε $e\mathscr{R}_H e$ δηλαδή $e^{-1}\cdot e = e \in H$. Έτσι $e \in H$ και ιδιαίτερα $H \neq \emptyset$.
- Έστω $x,y \in H$. Τότε:

$$H \ni x = e\cdot x = e^{-1}\cdot x \implies e\mathscr{R}_H x \qquad \text{και} \qquad H \ni y = e\cdot y = e^{-1}\cdot y \implies e\mathscr{R}_H y$$

Επειδή η σχέση $\mathscr{R}_H$ είναι σχέση ισοδυναμίας, θα έχουμε: $x\mathscr{R}_H e$ και $e\mathscr{R}_H y$, δηλαδή $x^{-1}\cdot e = x^{-1} \in H$ και $y^{-1}\cdot e = y^{-1} \in H$. Ιδιαίτερα: $x^{-1} \in H$, $\forall x \in H$.

Τέλος από τις παραπάνω σχέσεις θα έχουμε $x^{-1}\mathscr{R}_H e$ και $e\mathscr{R}_H y^{-1}$. Λόγω της μεταβατικής ιδιότητας θα έχουμε: $x^{-1}\mathscr{R}_H y^{-1}$, το οποίο σημαίνει ότι $(x^{-1})^{-1}\cdot y^{-1} = x\cdot y^{-1} \in H$. Επομένως το υποσύνολο H είναι υποομάδα της G.

Η απόδειξη της ισοδυναμίας **1.** «$\Longleftrightarrow$» **3.** είναι παρόμοια και αφήνεται ως άσκηση. ■

Από τώρα και στο εξής υποθέτουμε ότι: *το υποσύνολο H είναι μια υποομάδα της ομάδας $(G,\cdot)$:*

$$H \leq G$$

Γνωρίζουμε τότε ότι οι σχέσεις $\mathscr{R}_H$ και $\mathscr{R}^H$ είναι σχέσεις ισοδυναμίας επί του συνόλου G. Για κάθε $x \in G$, συμβολίζουμε με:

$$[x]_H = \{y \in G \mid y \mathscr{R}_H x\} \qquad \text{και} \qquad [x]^H = \{y \in G \mid y \mathscr{R}^H x\}$$

την κλάση ισοδυναμίας του $x \in G$ ως προς τις σχέσεις ισοδυναμίας $\mathscr{R}_H$ και $\mathscr{R}^H$ αντίστοιχα.

Λήμμα 3.3.2. $\forall x \in G$:

$$[x]_H = x \cdot H := \{x \cdot h \in G \mid h \in H\}$$
$$_H[x] = H \cdot x := \{h \cdot x \in G \mid h \in H\}$$

Απόδειξη. Για την πρώτη ισότητα θα έχουμε (η δεύτερη αποδεικνύεται παρόμοια):

$$[x]_H = \{y \in G \mid y \mathscr{R}_H x\} = \{y \in G \mid x \mathscr{R}_H\} = \{y \in G \mid x^{-1} \cdot y \in H\} =$$
$$= \{y \in G \mid x^{-1} \cdot y = h \in H\} = \{y \in G \mid y = x \cdot h, \ \ h \in H\} = \{x \cdot h \in G \mid h \in H\} = x \cdot H$$ ■

Ορισμός 3.3.3. *Η κλάση ισοδυναμίας $[x]_H = x \cdot H$ του στοιχείου $x \in G$ ως προς την σχέση ισοδυναμίας $\mathscr{R}_H$ καλείται* **αριστερό σύμπλοκο** *ή* **αριστερή πλευρική κλάση** *του x ως προς την υποομάδα H.*

Η κλάση ισοδυναμίας $[x]^H = H \cdot x$ του $x \in G$ ως προς τη σχέση ισοδυναμίας $\mathscr{R}^H$ καλείται **δεξιό σύμπλοκο** *ή* **δεξιά πλευρική κλάση** *του x ως προς την υποομάδα H.*

Σχόλιο 3.3.4. Έστω $H \leq G$ μια υποομάδα της ομάδας G. Επειδή τα αριστερά σύμπλοκα της H στην G είναι οι κλάσεις ισοδυναμίας της σχέσης $\mathscr{R}_H$ επί του συνόλου G, έπεται ότι το σύνολο πηλίκο

$$G/\mathscr{R}_H = \{x \cdot H \subseteq G \mid x \in G\}$$

των διακεκριμένων αριστερών συμπλόκων της H στην G αποτελεί μια διαμέριση του συνόλου G και ιδιαίτερα:

1. $\forall x \in G$: $xH \neq \emptyset$.
2. $\forall x, y \in G$: είτε $xH = yH$ ή $xH \cap yH = \emptyset$.
3. Η ομάδα G είναι η ένωση των διακεκριμένων αριστερών συμπλόκων της H στην G.

Η ακόλουθη βοηθητική πρόταση πιστοποιεί ιδιαίτερα ότι το πλήθος των διακεκριμένων αριστερών συμπλόκων της H στην G συμπίπτει με το πλήθος των διακεκριμένων δεξιών συμπλόκων της H στην G.

Λήμμα 3.3.5. *Με τους παραπάνω συμβολισμούς:*

1. *$\forall x \in G$: τα σύμπλοκα $x \cdot H$ και $H \cdot x$ έχουν το ίδιο πλήθος στοιχείων.*

2. *Τα σύνολα πηλίκα $G/\mathscr{R}_H$ και $G/\mathscr{R}^H$, του συνόλου G ως προς τις σχέσεις ισοδυναμίας $\mathscr{R}_H$ και $\mathscr{R}^H$ αντίστοιχα έχουν το ίδιο πληθος στοιχείων, δηλαδή: $|G/\mathscr{R}_H| = |G/\mathscr{R}^H|$.*

Απόδειξη. **1.** Για κάθε $x \in G$, ορίζουμε απεικόνιση

$$\phi : x \cdot H \longrightarrow H \cdot x, \quad \phi(x \cdot h) = h \cdot x$$

Έστω $\phi(x \cdot h_1) = \phi(x \cdot h_2)$, δηλαδή $h_1 \cdot x = h_2 \cdot x$. Τότε $(h_1 \cdot x) \cdot x^{-1} = (h_2 \cdot x) \cdot x^{-1}$ από όπου άμεσα βλέπουμε ότι $h_1 = h_2$ και άρα $x \cdot h_1 = x \cdot h_2$. Επομένως η ϕ είναι «1-1». Αν $h \cdot x \in H \cdot x$, τότε $\phi(x \cdot h) = h \cdot x$ και άρα η ϕ είναι «επί». Συνοψίζοντας, η απεικόνιση ϕ είναι «1-1» και «επί» και επομένως $|x \cdot H| = |H \cdot x|$.

2. Ορίζοντας

$$\psi : G/\mathscr{R}_H \longrightarrow G/\mathscr{R}^H, \quad \psi(x\cdot H) = H\cdot x^{-1}$$

θα δείξουμε ότι η ϕ είναι μια «1-1» και «επί» απεικόνιση.

- Κατ' αρχήν η ψ είναι καλά ορισμένη: έστω $x\cdot H = y\cdot H$ και άρα $x\mathscr{R}_H y$. Τότε $x^{-1}\cdot y \in H$. Έστω $x^{-1}\cdot y = h \in H$. Τότε $x^{-1} = h\cdot y^{-1} \in H\cdot y^{-1} = [y^{-1}]^H$. Όπως γνωρίζουμε τότε, τα στοιχεία x^{-1} και y^{-1} ορίζουν την ίδια κλάση ισοδυναμίας ως προς τη σχέση ισοδυναμίας $\mathscr{R}^H$ και επομένως θα έχουμε $[x^{-1}]^H = [y^{-1}]^H$. Αυτό όμως σημαίνει ότι $H\cdot x^{-1} = H\cdot y^{-1}$ και άρα $\psi(x\cdot H) = \psi(y\cdot H)$, δηλαδή η ψ είναι καλά ορισμένη.
- Έστω $\psi(x\cdot H) = \psi(y\cdot H)$, δηλαδή $H\cdot x^{-1} = H\cdot y^{-1}$ ή ισοδύναμα $[x^{-1}]^H = [y^{-1}]^H$. Τότε όμως $x^{-1}\mathscr{R}^H y^{-1}$ και άρα $x^{-1}\cdot (y^{-1})^{-1} \in H$. Δηλαδή $x^{-1}\cdot y \in H$ και επομένως $x^{-1}\cdot y = h \in H$. Τότε $y = x\cdot h \in x\cdot H = [x]_H$ και άρα $[y]_H = [x]_H \implies y\cdot H = x\cdot H$. Επομένως η ψ είναι «1-1».
- Έστω $[z]^H = H\cdot z \in G/\mathscr{R}^H$. Τότε προφανώς $\psi([z^{-1}]_H) = \psi(z^{-1}\cdot H) = H\cdot (z^{-1})^{-1} = H\cdot z$ και άρα η ψ είναι «επί».

Συνοψίζουμε: η απεικόνιση ϕ είναι «1-1» και «επί» και επομένως $|G/\mathscr{R}_H| = |G/\mathscr{R}^H|$. ■

Από τώρα και στο εξής: σταθεροποιούμε όπως και πριν μια υποομάδα $H \leq G$ της ομάδας G και εργαζόμαστε με τη σχέση ισοδυναμίας $\mathscr{R}_H$:

$$\forall x, y \in G: \quad x\mathscr{R}_H y \iff x^{-1}\cdot y \in H$$

Σημειώνουμε ότι, αν $x \in G$, τότε $H = xH$ αν και μόνο αν $eH = xH$ αν και μόνο αν $[e]_H = [x]_H$ αν και μόνο αν $e\mathscr{R}_H x$ αν και μόνο αν $e^{-1}\cdot x \in H$ αν και μόνο αν $x \in H$.

Το σύνολο πηλίκο $G/\mathscr{R}_H$ θα το συμβολίζουμε με

$$G/\mathscr{R}_H = \{x\cdot H \subseteq G \mid x \in G\} := G/H$$

Ανάλογα συμπεράσματα ισχύουν για την σχέση ισοδυναμίας $\mathscr{R}^H$.

Λήμμα 3.3.6. *Έστω $x, y \in G$. Τότε τα αριστερά σύμπλοκα $[x]_H$ και $[y]_H$ έχουν το ίδιο πλήθος στοιχείων. Αναλυτικότερα η απεικόνιση*

$$\phi : [x]_H = x\cdot H \longrightarrow y\cdot H = [y]_H, \qquad \phi(x\cdot h) = y\cdot h$$

είναι «1-1» και «επί».

Απόδειξη. Έστω ότι $\phi(x\cdot h_1) = \phi(x\cdot h_2)$, δηλαδή $y\cdot h_1 = y\cdot h_2$. Τότε προφανώς, από τον Νόμο Διαγραφής για ομάδες, θα έχουμε $h_1 = h_2$ και άρα $x\cdot h_1) = x\cdot h_2$. Επομένως η ψ είναι «1-1».

Αν $y\cdot h \in y\cdot H$, τότε $\psi(x\cdot h) = y\cdot h$ και άρα η ψ είναι «επί». ■

Πόρισμα 3.3.7. *Έστω $(G,\cdot)$ μια ομάδα και $H \leq G$ μια υποομάδα της G. Τότε:*

$$\forall x \in G: \qquad o(H) = |H| = |x\cdot H| = |H\cdot x|$$

Απόδειξη. Θέτοντας $y = e$ στο Λήμμα 3.3.6, θα έχουμε ότι τα σύμπλοκα $e\cdot H$ και $x\cdot H$ έχουν το ίδιο πλήθος στοιχείων. Όμως προφανώς

$$e\cdot H = \{e\cdot h \in G \mid h \in H\} = \{h \in G \mid h \in H\} = H$$

και επομένως πάλι με χρήση του Λήμματος 3.3.6 θα έχουμε, $\forall x \in G$:

$$o(H) = |H| = |x\cdot H| = |H\cdot x|$$ ■

Από το Λήμμα 3.3.6 και το Πόρισμα 3.3.7 έπεται ότι τυχόν αριστερό (δεξιό) σύμπλοκο έχει το ίδιο πλήθος στοιχείων με τυχόν δεξιό (αριστερό) σύμπλοκο. Όμως, όπως δείχνει το επόμενο παράδειγμα, δεν είναι αλήθεια ότι τυχόν αριστερό σύμπλοκο συμπίπτει με ένα δεξιό σύμπλοκο:

Παράδειγμα 3.3.8. Θεωρούμε τη συμμετρική ομάδα:

$$\mathsf{S}_3 = \{(1),\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

Τότε $H = \{(1), (12)\}$ είναι μια υποομάδα της S_3 και τα διεκεκριμένα αριστερά σύμπλοκα της H στην S_3 είναι:

$$\{(1),(12)\},\quad \{(13),(123)\},\quad \{(23),(132)\}$$

Παρατηρούμε ότι το δεξιό σύμπλοκο $H(13) = \{(13),(132)\}$ δεν συμπίπτει με κανένα αριστερό σύμπλοκο. Γενικότερα βλέπουμε ότι τα δεξιά σύμπλοκα της H της S_3 είναι

$$\{(1),(12)\},\quad \{(13),(132)\},\quad \{(23),(123)\}$$

άρα είναι, όπως περιμένουμε, τρία, και κανένα δεξιό σύμπλοκο (εκτός του H) δεν συμπίπτει με κανένα αριστερό σύμπλοκο. $\surd$

Αν η ομάδα G είναι αβελιανή, τότε προφανώς, για κάθε υποομάδα H της G, οι σχέσεις ισοδυναμίας $\mathscr{R}_H$ και $\mathscr{R}^H$ ταυτίζονται, $\forall x, y \in G$:

$$x\mathscr{R}_H y \iff x^{-1}\cdot y \in H \iff y\cdot x^{-1} \in H \iff y\mathscr{R}^H x \iff x\mathscr{R}^H y$$

και επομένως κάθε αριστερό σύμπλοκο της H στην G συμπίπτει με το αντίστοιχο δεξιό σύμπλοκο: $\forall x \in G$: $x\cdot H = H\cdot x$.

Παράδειγμα 3.3.9. Έστω $H = n\mathbb{Z}$ η κυκλική υποομάδα της προσθετικής ομάδας $(\mathbb{Z},+)$ η οποία παράγεται από τον θετικό ακέραιο $n>1$. Τότε για τυχόντες ακεραίους x, y: $x\mathscr{R}_{n\mathbb{Z}} y$ αν και μόνο αν $-x+y \in n\mathbb{Z}$ αν και μόνο αν $x-y = nk$, για κάποιον ακέραιο k, αν και μόνο αν $n \mid x-y$. Έτσι η σχέση ισοδυναμίας $\mathscr{R}_{n\mathbb{Z}}$ επί του $\mathbb{Z}$ την οποία ορίζει η υποομάδα $n\mathbb{Z}$ συμπίπτει με την σχέση ισοτιμίας $\bmod n$. Ως συνέπεια έχουμε ότι τα διακεκριμένα (αριστερά) σύμπλοκα της $n\mathbb{Z}$ στην $\mathbb{Z}$ συμπίπτουν με τις διακεκριμένες κλάσεις ισοτιμίας $\bmod n$, και επομένως είναι τα εξής:

$$[0]_n = 0+n\mathbb{Z},\ \ [1]_n = 1+n\mathbb{Z},\ \ \cdots,\ \ [n-1]_n = (n-1)+n\mathbb{Z},\quad \text{όπου}\quad [r]_n = r+n\mathbb{Z} = \{r+nk \in \mathbb{Z} \mid k \in \mathbb{Z}\},\ 0 \le r \le n-1\ \surd$$

Υπάρχουν όμως και μη αβελιανές ομάδες G οι οποίες διαθέτουν υποομάδες H έτσι ώστε οι σχέσεις ισοδυναμίας $\mathscr{R}_H$ και $\mathscr{R}^H$ ταυτίζονται, και κάθε αριστερό σύμπλοκο της H στην G συμπίπτει με το αντίστοιχο δεξιό σύμπλοκο:

Παράδειγμα 3.3.10. Θεωρούμε τη μη αβελιανή ομάδα $(\mathsf{GL}(n,\mathbb{R}),\cdot)$ των αντιστρέψιμων $n\times n$ πινάκων υπεράνω του $\mathbb{R}$, και έστω η υποομάδα της $\mathsf{SL}(n,\mathbb{R}) = \{A \in \mathsf{GL}(n,\mathbb{R}) \mid |A| = 1\}$ η οποία αποτελείται από όλους τους $n\times n$ πίνακες με ορίζουσα ίση με 1. Εύκολα βλέπουμε ότι για κάθε αντιστρέψιμο πίνακα A, θα έχουμε:

$$A\cdot\mathsf{SL}(n,\mathbb{R}) = [A]_{\mathsf{SL}(n,\mathbb{R})} = \{X \in \mathsf{GL}(n,\mathbb{R}) \mid X\mathscr{R}_{\mathsf{SL}(n,\mathbb{R})} A\} = \{X \in \mathsf{GL}(n,\mathbb{R}) \mid X^{-1}\cdot A \in \mathsf{SL}(n,\mathbb{R})\} =$$

$$= \{X \in \mathsf{GL}(n,\mathbb{R}) \mid |X^{-1}\cdot A| = 1\} = \{X \in \mathsf{GL}(n,\mathbb{R}) \mid |X|^{-1}\cdot|A| = 1\} = \{X \in \mathsf{GL}(n,\mathbb{R}) \mid |X| = |A|\}$$

Για την περιγραφή του συνόλου πηλίκο $\mathsf{GL}(n,\mathbb{R})/\mathsf{SL}(n,\mathbb{R}) = \mathsf{GL}(n,\mathbb{R})/\mathscr{R}_{\mathsf{SL}(n,\mathbb{R})}$, ορίζουμε απεικόνιση

$$\varphi:\ \mathsf{GL}(n,\mathbb{R})/\mathsf{SL}(n,\mathbb{R}) \longrightarrow \mathbb{R}^*,\quad \varphi(A\cdot\mathsf{SL}(n,\mathbb{R})) = |A|$$

Η απεικόνιση φ είναι καλά ορισμένη διότι, αν $A\cdot\mathsf{SL}(n,\mathbb{R}) = B\cdot\mathsf{SL}(n,\mathbb{R})$, τότε $B^{-1}\cdot A \in \mathsf{SL}(n,\mathbb{R})$, δηλαδή $|B^{-1}\cdot A| = 1$ από όπου προκύπτει άμεσα ότι $|A| = |B|$, και επομένως $\varphi(A\cdot\mathsf{SL}(n,\mathbb{R})) = \varphi(B\cdot\mathsf{SL}(n,\mathbb{R}))$. Η απεικόνιση φ είναι «1-1» διότι, αν ισχύει $\varphi(A\cdot\mathsf{SL}(n,\mathbb{R})) = \varphi(B\cdot\mathsf{SL}(n,\mathbb{R}))$, τότε $|A| = |B|$ και επομένως $B \in A\cdot\mathsf{SL}(n,\mathbb{R})$. Αυτό όμως σημαίνει ότι $A\cdot\mathsf{SL}(n,\mathbb{R}) = B\cdot\mathsf{SL}(n,\mathbb{R})$. Επίσης η απεικόνιση φ είναι «επί» διότι, αν $0 \neq r \in \mathbb{R}$, τότε $\varphi(A\cdot\mathsf{SL}(n,\mathbb{R})) = r$, όπου A είναι ο $n\times n$ πίνακας

$$A = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

Επομένως το σύνολο πηλίκο $\mathsf{GL}(n,\mathbb{R})/\mathsf{SL}(n,\mathbb{R})$ είναι σε «1-1» και «επί» αντιστοιχία με το σύνολο $\mathbb{R}^*$ των μη μηδενικών πραγματικών αριθμών. Δεν είναι τυχαίο ότι το σύνολο $\mathbb{R}^*$ εφοδιασμένο με την πράξη του πολλαπλασιασμού αποτελεί μια (αβελιανή) ομάδα. Όπως θα δούμε αργότερα και στο σύνολο πηλίκο $\mathsf{GL}(n,\mathbb{R})/\mathsf{SL}(n,\mathbb{R})$ μπορεί να οριστεί δομή ομάδας, και τότε η «1-1» και «επί» απεικόνιση φ είναι ισομορφισμός, κάτι που θα μας επιτρέψει να «ταυτίσουμε» τις δύο αυτές ομάδες.

Τέλος παρατηρούμε ότι για κάθε $A,B \in \mathsf{GL}(n,\mathbb{R})$:

$$A\mathscr{R}_{\mathsf{SL}(n,\mathbb{R})}B \iff A^{-1}\cdot B \in \mathsf{SL}(n,\mathbb{R}) \iff |A^{-1}\cdot B| = 1 \iff |A| = |B|$$

$$A\mathscr{R}^{\mathsf{SL}(n,\mathbb{R})}B \iff A\cdot B^{-1} \in \mathsf{SL}(n,\mathbb{R}) \iff |A\cdot B^{-1}| = 1 \iff |A| = |B|$$

Επομένως οι δύο σχέσεις ισοδυναμίας τις οποίες ορίζει η υποομάδα $\mathsf{SL}(n,\mathbb{R})$ επί της ομάδας $\mathsf{GL}(n,\mathbb{R})$ ταυτίζονται, δηλαδή έχουμε: $\mathscr{R}_{\mathsf{SL}(n,\mathbb{R})} = \mathscr{R}^{\mathsf{SL}(n,\mathbb{R})}$, και ιδιαίτερα τα αριστερά και δεξιά σύμπλοκα της $\mathsf{SL}(n,\mathbb{R})$ στην $\mathsf{GL}(n,\mathbb{R})$ ταυτίζονται. $\surd$

Παράδειγμα 3.3.11. Θεωρούμε τη συμμετρική ομάδα S_4 και την υποομάδα της $H = \{\sigma \in \mathsf{S}_4 \mid \sigma(4) = 4\}$.

Θα προσδιορίσουμε, με χρήση του Σχολίου 3.3.4, τα αριστερά σύμπλοκα της H στην S_4. Προφανώς

$$H = \{\iota,\ (12),\ (13),\ (23),\ (123),\ (132)\} \leq \mathsf{S}_4$$

Από το Πόρισμα 3.3.7, κάθε αριστερό σύμπλοκο της H στην S_4 έχει $o(H) = 6$ στοιχεία, και προφανώς όλα τα στοιχεία της H προσδιορίζουν το ίδιο αριστερό σύμπλοκο: την υποομάδα H.

1. $H = \iota H = (12)H = (13)H = (23)H = (123)H = (132)H$. Έτσι:
$$\iota H = \{\iota,\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

2. Θεωρούμε ένα στοιχείο της S_4 το οποίο δεν ανήκει στην H, για παράδειγμα το στοιχείο (34). Τότε το αριστερό σύμπλοκο $(34)H$ δεν συμπίπτει με το αριστερό σύμπλοκο H, και θα έχουμε:
$$(34)H = \{(34)\iota,\ (34)(12),\ (34)(13),\ (34)(23),\ (34)(123),\ (34)(132)\} =$$
$$= \{(34),\ (12)(34),\ (143),\ (243),\ (1243),\ (1432)\}$$

3. Θεωρούμε ένα στοιχείο της S_4 το οποίο δεν ανήκει στα αριστερά σύμπλοκα H και $(34)H$, για παράδειγμα το στοιχείο (24). Τότε το αριστερό σύμπλοκο $(24)H$ δεν συμπίπτει με κανένα από τα αριστερά σύμπλοκα H και $(34)H$, και θα έχουμε:
$$(24)H = \{(24)\iota,\ (24)(12),\ (24)(13),\ (24)(23),\ (24)(123),\ (24)(132)\} =$$
$$= \{(24),\ (142),\ (13)(24),\ (234),\ (1423),\ (1342)\}$$

4. Θεωρούμε ένα στοιχείο της S_4 το οποίο δεν ανήκει στα αριστερά σύμπλοκα H, $(34)H$, και $(24)H$, για παράδειγμα το στοιχείο (14). Τότε το αριστερό σύμπλοκο $(14)H$ δεν συμπίπτει με κανένα από τα αριστερά σύμπλοκα H, $(34)H$, και $(24)H$, και θα έχουμε:
$$(14)H = \{(14)\iota,\ (14)(12),\ (14)(13),\ (14)(23),\ (14)(123),\ (14)(132)\} =$$
$$= \{(14),\ (124),\ (134),\ (14)(23),\ (1234),\ (1324)\}$$

Έτσι έχουμε προσδιορίσει τα εξής 4 διακεκριμένα αριστερά σύμπλοκα της H στην S_4: H, $(34)H$, $(24)H$, και $(14)H$. Χρησιμοποιώντας το Σχόλιο 3.3.4, έπεται ότι τα παραπάνω αριστερά σύμπλοκα είναι όλα τα διακεκριμένα αριστερά σύμπλοκα της H στην S_4, και ιδιαίτερα $\mathsf{S}_4 = H \cup (34)H \cup (24)H \cup (14)H$.

Παρατηρούμε ότι υπάρχουν 4 διακεκριμένα αριστερά σύμπλοκα της υποομάδας H (η οποία έχει τάξη 6) καθένα εκ των οποίων περιέχει 6 στοιχεία, στην ομάδα S_4 (η οποία έχει $24 = 4\cdot 6$ στοιχεία). Όπως θα δούμε στην επόμενη υποενότητα, αυτό δεν είναι τυχαίο. $\surd$

3.4 Το Θεώρημα του Lagrange

Έστω, όπως και πριν, $(G,\cdot)$ μια ομάδα και $H \leq G$ μια υποομάδα της G. Συμβολίζουμε με

$$G/H = G/\mathscr{R}_H = \{[x]_H \subseteq G \mid x \in G\} = \{x \cdot H \subseteq G \mid x \in G\}$$

το σύνολο πηλίκο της G ως προς τη σχέση ισοδυναμίας $\mathscr{R}_H$. Το σύνολο G/H καλείται το **σύνολο πηλίκο των αριστερών συμπλόκων ή αριστερών πλευρικών κλάσεων** της H στην G. Όπως γνωρίζουμε, το σύνολο υποσυνόλων G/H αποτελεί μια διαμέριση του G και άρα θα έχουμε:

$$G = \bigcup_{x \in G} [x]_H = \bigcup_{x \in G} x \cdot H$$

Ορισμός 3.4.1. *Έστω $(G,\cdot)$ μια ομάδα και $H \leq G$ μια υποομάδα της G. Το πλήθος των στοιχείων του συνόλου πηλίκου G/H καλείται ο* **δείκτης** *της H στην G και συμβολίζεται με:*

$$[G : H]$$

Παράδειγμα 3.4.2.

1. Θεωρούμε την υποομάδα $H = \{\sigma \in \mathsf{S}_4 \mid \sigma(4) = 4\}$ της S_4. Τότε από το Παράδειγμα 3.3.11 έπεται ότι $[\mathsf{S}_4 : H] = 4$.

2. Θεωρούμε την υποομάδα $\mathsf{SL}(n,\mathbb{R})$ της $\mathsf{GL}(n,\mathbb{R})$. Τότε από το Παράδειγμα 3.3.10 έπεται ότι $[\mathsf{GL}(n,\mathbb{R}) : \mathsf{SL}(n,\mathbb{R})] = |\mathbb{R}^*|$. $\surd$

Παρατήρηση 3.4.3. Ορίσαμε τον δείκτη της υποομάδας H στην ομάδα G ως το πλήθος των διακεκριμένων αριστερών πλευρικών κλάσεων της H στην G, δηλαδή το πλήθος των στοιχείων του συνόλου πηλίκου $G/\mathscr{R}_H$. Επειδή, σύμφωνα με το Λήμμα 3.3.5, έχουμε $|G/\mathscr{R}_H| = |G/\mathscr{R}^H|$, έπεται ότι ο δείκτης $[G : H]$ της H στην G είναι επίσης ίσος και με το πλήθος των διακεκριμένων δεξιών συμπλόκων της H στην G:

$$|G/\mathscr{R}_H| = [G : H] = |G/\mathscr{R}^H|$$

Ιδιαίτερα αν η ομάδα G είναι πεπερασμένη, τότε και η υποομάδα H θα είναι πεπερασμένη και το σύνολο των διακεκριμένων κλάσεων ισοδυναμίας των στοιχείων της ως προς τη σχέση ισοδυναμίας $\mathscr{R}_H$ ή την σχέση ισοδυναμίας $\mathscr{R}^H$, θα είναι πεπερασμένο. Δηλαδή το σύνολο πηλίκο G/H των αριστερών (δεξιών) συμπλόκων της H στην G θα είναι πεπερασμένο. ▲

Παράδειγμα 3.4.4. Θεωρούμε τη συμμετρική ομάδα:

$$\mathsf{S}_3 = \{(1),\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

Τότε, όπως στο Παράδειγμα 3.3.8, το υποσύνολο $H = \{(1), (12)\}$ είναι μια υποομάδα της S_3 και τα διεκεκριμένα αριστερά σύμπλοκα της H στην S_3 είναι:

$$\{(1),(12)\},\quad \{(13),(123)\},\quad \{(23),(132)\}$$

Επομένως ο δείκτης της H στην S_3 είναι $[\mathsf{S}_3 : H] = 3$. $\surd$

Παράδειγμα 3.4.5. Έστω $(G,\cdot)$ μια ομάδα.

1. Αν $H = \{e\}$ είναι η τετριμμένη υποομάδα της G, τότε προφανώς $[G : H] = |G|$.

2. Έστω $H = n\mathbb{Z}$ η κυκλική υποομάδα της προσθετικής ομάδας $(\mathbb{Z},+)$ η οποία παράγεται από τον θετικό ακέραιο $n > 1$. Από το Παράδειγμα 3.3.9 έπεται ότι τα διακεκριμένα (αριστερά) σύμπλοκα της $n\mathbb{Z}$ στην $\mathbb{Z}$ είναι τα n το πλήθος υποσύνολα $\{r + n\mathbb{Z} \subseteq \mathbb{Z} \mid 0 \leq r \leq n-1\}$. Άρα $[\mathbb{Z} : n\mathbb{Z}] = n$. $\surd$

Έστω τώρα $(G,\cdot)$ μια *πεπερασμένη* ομάδα και H μια υποομάδα της G. Τότε προφανώς ο δείκτης της H στην G είναι πεπερασμένος, δηλαδή θα έχουμε $|G|<\infty$, $|H|<\infty$, και $[G:H]<\infty$. Θέτουμε:

1. $\mathrm{o}(G)=n$
2. $\mathrm{o}(H)=m$
3. $[G:H]=k$, και έστω $G/H=\{[x_1]_H,\ [x_2]_H,\ \cdots,\ [x_k]_H\}=\{x_1\cdot H,\ x_2\cdot H,\ \cdots,\ x_k\cdot H\}$.

Επειδή τα υποσύνολα $[x_1]_H,[x_2]_H,\cdots,[x_k]_H$ αποτελούν μια διαμέριση του G, έπεται ότι θα έχουμε:

$$G=[x_1]_H\bigcup[x_2]_H\bigcup\cdots\bigcup[x_k]_H\qquad\text{και}\qquad[x_i]_H\bigcap[x_j]_H=\emptyset,\quad 1\le i\ne j\le k$$

Το ακόλουθο Θεώρημα, το οποίο οφείλεται στον Lagrange και είναι θεμελιώδες στη Θεωρία Ομάδων, δείχνει ότι με τους παραπάνω συμβολισμούς: $n=m\cdot k$, δηλαδή η τάξη της H διαιρεί την τάξη της G:

Θεώρημα 3.4.6. *(**Lagrange (1771)**[15] Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της G. Τότε:*

$$\mathrm{o}(G)=\mathrm{o}(H)\cdot[G:H]$$

Επομένως η τάξη μιας υποομάδας H μιας πεπερασμένης ομάδας G διαιρεί την τάξη της ομάδας:

$$\mathrm{o}(H)\,|\,\mathrm{o}(G)$$

Απόδειξη. Διατηρώντας τους παραπάνω συμβολισμούς, επειδή

$$G=[x_1]_H\bigcup[x_2]_H\bigcup\cdots\bigcup[x_k]_H$$

είναι μια διαμέριση του συνόλου G, σύμφωνα με το Σχόλιο 3.3.4, θα έχουμε:[16]

$$|G|=\sum_{i=1}^{k}|[x_i]_H|=\sum_{i=1}^{k}|x_i\cdot H|$$

Από το Πόρισμα 3.3.7, έχουμε: $|x_i\cdot H|=\mathrm{o}(H)$, $\forall i=1,2,\cdots,k$. Έτσι η παραπάνω σχέση δίνει:

$$\mathrm{o}(G)=|G|=\sum_{i=1}^{k}|x_i\cdot H|=k\cdot|H|=k\cdot\mathrm{o}(H)=[G:H]\cdot\mathrm{o}(H)$$ ■

Το επόμενο σημαντικό αποτέλεσμα αποτελεί μια απλή εφαρμογή του Θεωρήματος Lagrange.

Πρόταση 3.4.7. *Έστω $(G,\cdot)$ μια πεπερασμενη ομάδα. Τότε $\forall x\in G$:*

1. $x^{\mathrm{o}(G)}=e$.

2. $\mathrm{o}(x)\,|\,\mathrm{o}(G)$.

Απόδειξη. **1.** Η τάξη $\mathrm{o}(x)$ του x, είναι εξ ορισμού η τάξη της κυκλικής υποομάδας που παράγεται από το x. Απο το Θεώρημα του Lagrange έπεται ότι $\mathrm{o}(x)\,|\,\mathrm{o}(G)$, και άρα:

$$\mathrm{o}(G)=k_x\cdot\mathrm{o}(x),\qquad\text{όπου}\quad k_x\ge 1$$

Έτσι θα έχουμε:

$$x^{\mathrm{o}(G)}=x^{k_x\cdot\mathrm{o}(x)}=(x^{\mathrm{o}(x)})^{k_x}=e^{k_x}=e$$

2. Επειδή $\mathrm{o}(x)=\mathrm{o}(\langle x\rangle)$, το ζητούμενο προκύπτει απο το Θεώρημα του Lagrange 3.4.6. ■

[15] Joseph-Luis Lagrange (25 Ιανουαρίου 1736 - 10 Απριλίου 1813) [http://en.wikipedia.org/wiki/Joseph-Louis_Lagrange]: Διαπρεπής Ιταλός μαθηματικός, ο οποίος έζησε το μεγαλύτερο μέρος της ζωής του στη Γαλλία, με σημαντική συμβολή, μεταξύ άλλων, στον Λογισμό Μεταβολών, στη Θεωρία Διαφορικών Εξισώσεων, στη Μηχανική, στην Ανάλυση, στη Θεωρία Ομάδων, και στη Θεωρία Αριθμών.

[16] Αν για ένα σύνολο X ισχύει ότι $X=\cup_{i=1}^{n}X_i$, για κάποια υποσύνολα $X_1,\cdots,X_n$ του X για τα οποία $X_i\cap X_j=\emptyset$, αν $1\le i\ne j\le n$, τότε: $|X|=\sum_{i=1}^{n}|X_i|$.

Παράδειγμα 3.4.8. Θα προσδιορίσουμε τις υποομάδες μιας ομάδας G με τάξη 4. Όπως γνωρίζουμε, υπάρχουν δύο ομάδες τάξης 4: η ομάδα του Klein και η κυκλική τάξης 4 με αντίστοιχους πίνακες Cayley:

Πίνακας Cayley της Ομάδας του Klein:

·	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Πίνακας Cayley Κυκλικής Ομάδας τάξης 4:

·	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Για την ομάδα του Klein: $G = \{e, a, b, c\}$ προφανώς θα έχουμε τις (ανά δύο διαφορετικές) υποομάδες

$$\langle e\rangle = \{e\}, \quad \langle a\rangle = \{e, a\}, \quad \langle b\rangle = \{e, b\}, \quad \langle c\rangle = \{e, c\}, \quad G \tag{$*$}$$

Αν H είναι μια υποομάδα της G, τότε από το Θεώρημα του Lagrange 3.4.6 θα έχουμε $o(H) = 1$ ή 2 ή 4. Αν $o(H) = 1$, τότε προφανώς $H = \{e\}$. Αν $o(H) = 2$, τότε $H = \{e, x\}$, όπου $x \in G \setminus \{e\}$, και προφανώς η τάξη του x είναι 2. Επειδή τα στοιχεία τάξης 2 της G είναι τα a, b, c, έπεται ότι η H είναι μια εκ των $\{e, a\}$, $\{e, b\}$, $\{e, c\}$. Τέλος, αν $o(H) = 4$, τότε $H = G$. Έτσι οι υποομάδες στη σχέση $(*)$ είναι όλες οι υποομάδες της G.

Για την κυκλική ομάδα $G = \{e, a, b, c\}$ θα έχουμε $b^2 = a$ και άρα $b^4 = e$. Επίσης θα έχουμε $b^3 = ab = c$. Έτσι $G = \{e, a, b, c\} = \{b^4 = e, b, b^2 = a, b^3 = c\} = \langle b\rangle$. Από το Πόρισμα 3.2.4 το στοιχείο b^3 είναι επίσης γεννήτορας της G και έτσι έχουμε τις υποομάδες

$$\langle e\rangle = \{e\}, \quad \langle b^2\rangle = \{e, b^2\}, \quad \langle b^3\rangle = \langle b\rangle = G \tag{$**$}$$

Αν H είναι μια υποομάδα της G, τότε, όπως και πριν, από το Θεώρημα του Lagrange 3.4.6 θα έχουμε $o(H) = 1$ ή 2 ή 4. Αν $o(H) = 1$, τότε προφανώς $H = \{e\}$. Αν $o(H) = 2$, τότε $H = \{e, x\}$, όπου $x \in G \setminus \{e\}$, και προφανώς η τάξη του x είναι 2. Επειδή το μόνο στοιχείο τάξης 2 της G είναι τα b^2, έπεται ότι η H είναι η $\{e, b^2\}$. Τέλος, αν $o(H) = 4$, τότε $H = G$. Έτσι οι υποομάδες στη σχέση $(**)$ είναι όλες οι υποομάδες της G. √

Παράδειγμα 3.4.9. Θα περιγράψουμε τις υποομάδες μιας κυκλικής ομάδας $G = \langle a\rangle$ τάξης 6. Από το Πόρισμα 3.2.4, οι γεννήτορες της G είναι τα στοιχεία a^k, όπου $(k, 6) = 1$, δηλαδή $k = 1$, ή 5, και άρα $\langle a^5\rangle = G = \langle a\rangle$. Από το Θεώρημα 3.2.2, έπεται ότι $o(a^2) = 3$ και $o(a^3) = 2$ και έτσι έχουμε τις υποομάδες:

$$\langle e\rangle = \{e\}, \quad \langle a^2\rangle = \langle a^4\rangle = \{e, a^2, a^4\}, \quad \langle a^3\rangle = \{e, a^3\}, \quad \langle a^5\rangle = \langle a\rangle = G = \{e, a, a^2, a^3, a^4, a^5\} \tag{$\dagger$}$$

Αν H είναι μια υποομάδα της G, τότε, όπως και πριν, από το Θεώρημα του Lagrange 3.4.6 θα έχουμε $o(H) = 1$ ή 2 ή 3 ή 6. Αν $o(H) = 1$, τότε προφανώς $H = \{e\}$. Αν $o(H) = 2$, τότε $H = \{e, x\}$, όπου $x \in G \setminus \{e\}$, και προφανώς η τάξη του x είναι 2. Επειδή το μόνο στοιχείο τάξης 2 της G είναι τα a^3, έπεται ότι η H είναι η $\{e, a^3\}$. Αν $o(H) = 3$, τότε $H = \{e, x, y\}$, όπου $x, y \in G \setminus \{e\}$, και προφανώς $y = x^2$ και η τάξη των x και y είναι 3. Επειδή, τα μόνα στοιχεία τάξης 3 είναι τα a^2 και a^4, και επειδή $\langle a^2\rangle = \langle a^4\rangle$, έπεται ότι η H είναι η $\langle a^2\rangle$. Τέλος, αν $o(H) = 6$, τότε $H = G$. Έτσι οι υποομάδες στη σχέση $(\dagger)$ είναι όλες οι υποομάδες της G. √

Η ακόλουθη άμεση συνέπεια του Θεωρήματος του Lagrange δείχνει ότι πεπερασμένες ομάδες με τάξη έναν πρώτο αριθμό έχουν ενδιαφέρουσες ιδιότητες.

Πόρισμα 3.4.10. *Έστω G μια πεπερασμένη ομάδα με τάξη έναν πρώτο αριθμό. Τότε η G είναι κυκλική και διαθέτει ακριβώς δύο υποομάδες, τις εξής: $\{e\}$ και G.*

Απόδειξη. Επειδή $|G| = p$, όπου p είναι πρώτος, θα έχουμε $G \neq \{e\}$. Αν $H \leq G$ είναι μια μη τετριμμένη υποομάδα της G, για παράδειγμα μπορούμε να επιλέξουμε $H = G$, τότε υπάρχει στοιχείο $e \neq a \in H$ το οποίο παράγει μια υποομάδα $K = \langle a \rangle \leq G$. Όπως και παραπάνω, απο τό Θεώρημα του Lagrange 3.4.6 έπεται ότι $o(a) = |K| \,|\, |G| = p$, και άρα $o(a) = p$ διότι $o(x) \neq 1$ καθώς $x \neq e$. Τότε από το Πόρισμα 3.1.15 έχουμε ότι η G είναι κυκλική τάξης p με γεννήτορα το στοιχείο a. Ιδιαίτερα έπεται ότι $H = G = \langle a \rangle$, και η μόνη μη-τετριμμένη υποομάδα της G είναι η ίδια η ομάδα G. ■

Η τετριμμένη ομάδα τάξης 1 έχει προφανώς το απλούστερο διάγραμμα Hasse: αυτό αποτελείται από μια κορυφή και δεν υπάρχει καμία ακμή. Το ακόλουθο αποτέλεσμα χαρακτηρίζει τις κυκλικές ομάδες με τάξη έναν πρώτο αριθμό ως τις μη τετριμμένες ομάδες με το απλούστερο διάγραμμα Hasse, δηλαδή τις ομάδες G οι οποίες διαθέτουν μόνο δύο υποομάδες: την τετριμμένη υποομάδα $\{e\}$ και την ομάδα G. Το διάγραμμα Hasse αυτών των ομάδων αποτελείται από δύο κορυφές και μια ακμή η οποία τις συνδέει.

Πρόταση 3.4.11. *Για μια ομάδα $(G, \cdot)$, τα ακόλουθα είναι ισοδύναμα:*

1. *Η G διαθέτει ακριβώς δύο υποομάδες.*
2. *Η G είναι πεπερασμένη (κυκλική) με τάξη έναν πρώτο αριθμό.*

Απόδειξη. **2.** $\Longrightarrow$ **1.** Προκύπτει από το Πόρισμα 3.4.10.

1. $\Longrightarrow$ **2.** Έστω ότι η G διαθέτει ακριβώς δύο υποομάδες. Επειδή κάθε ομάδα G έχει τουλάχιστον δύο υποομάδες, την τετριμμένη $\{e\}$ και την G, από την υπόθεση αυτές είναι οι μόνες υποομάδες της G. Προφανώς $G \neq \{e\}$, διότι διαφορετικά η G θα είχε μόνο μια υποομάδα, την $G = \{e\}$. Επομένως υπάρχει $e \neq a \in G$. Αν $H = \langle a \rangle$ είναι η κυκλική υποομάδα της G η οποία παράγεται από το a, τότε προφανώς $H \neq \{e\}$, διότι $a \neq e$, και άρα $H = \langle a \rangle = G$. Δηλαδή η G είναι κυκλική με γεννήτορα ατο a.

- Έστω ότι η μη τετριμμένη ομάδα G είναι πεπερασμένη: $|G| = o(a) = n < \infty$. Αν ο αριθμός n είναι σύνθετος, τότε $n = r \cdot s$, όπου $1 < r, s < n$. Θεωρούμε το στοιχείο a^r του οποίου η τάξη, σύμφωνα με το Θεώρημα 3.2.2, είναι:

$$o(a^r) = \frac{o(a)}{(o(a), r)} = \frac{n}{(r, n)} = \frac{n}{r} = s > 1$$

και επομένως η κυκλική υποομάδα $K = \langle a^r \rangle$ της G η οποία παράγεται από το a^r έχει τάξη s. Αυτό είναι άτοπο διότι $n \neq s \neq 1$ και άρα $G \neq K \neq \{e\}$. Άρα η τάξη n της G είναι πρώτος αριθμός.

- Έστω ότι η G είναι άπειρη κυκλική με γεννήτορα το στοιχείο a. Τότε προφανώς η τάξη $o(a)$ του a είναι άπειρη. Για κάθε $k \geq 2$, έστω $K = \langle a^k \rangle$ η κυκλική υποομάδα της G η οποία παράγεται από το στοιχείο a^k. Αν $K = \{e\}$, τότε $a^k = e$ και άρα η τάξη του a είναι πεπερασμένη, το οποίο είναι άτοπο. Αν $K = G = \langle a \rangle$, τότε $a \in \langle a^k \rangle$ και άρα υπάρχει ακέραιος r έτσι ώστε $a = (a^k)^r = a^{rk}$. Τότε $a^{rk-1} = e$. Προφανώς $rk - 1 \neq 0$ διότι $k \geq 2$. Αν $rk - 1 > 0$, τότε η σχέση $a^{rk-1} = e$ συναπάγει ότι το a έχει πεπερασμένη τάξη, το οποίο είναι άτοπο. Αν $rk - 1 < 0$, τότε η σχέση $a^{rk-1} = e$ συνεπάγει ότι $(a^{rk-1})^{-1} = a^{1-rk} = e$, όπου $1 - rk > 0$, και όπως πριν καταλήγουμε στην αντίφαση ότι το a έχει πεπερασμένη τάξη. Άρα η G δεν μπορεί να είναι άπειρης τάξης.

Συνοψίζουμε: η G είναι πεπερασμένη κυκλική με τάξη έναν πρώτο αριθμό. ■

Σχόλιο 3.4.12. Επειδή κάθε υποομάδα μιας αβελιανής ομάδας είναι κανονική, και επειδή κάθε κυκλική ομάδα είναι αβελιανή, από την Πρόταση 3.4.11 έπεται ότι κάθε κυκλική ομάδα με τάξη έναν πρώτο αριθμό είναι απλή, δηλαδή δεν έχει γνήσιες μη τετριμμένες κανονικές υποομάδες (διότι δεν περιέχει γνήσιες μη τετριμμένες υποομάδες).

Αντίστροφα, έστω G μια μη τετριμμένη αβελιανή απλή ομάδα. Επειδή η G είναι αβελιανή, κάθε υποομάδα της είναι κανονική, και επομένως η G διαθέτει ακρβώς δύο υποομάδες: την $\{e\}$ και την G. Από την Πρόταση 3.4.11, έπεται τότε ότι η G είναι πεπερασμένη κυκλική με τάξη έναν πρώτο αριθμό.

Συνοψίζοντας, αν G είναι μια μη τετριμμένη ομάδα, τότε:

Η ομάδα G είναι απλή αβελιανή $\iff$ *η G είναι πεπερασμένη κυκλική με τάξη έναν πρώτο αριθμό*

Για την κλάση μη-τετριμμένων ομάδων οι οποίες έχουν το απλούστερο διάγραμμα Hasse μετά τις κυκλικές ομάδες με τάξη έναν πρώτο αριθμό, παραπέμπουμε στην Άσκηση 3.9.55. Συνδυάζοντας την Πρόταση 3.4.11 και το Παράδειγμα 3.4.8, προκύπτει η δομή των υποομάδων μιας ομάδας με τάξη ≤ 5. Στην επόμενη υποενότητα θα μελετήσουμε την δομή των υποομάδων των ομάδων μεταθέσεων S_3 και S_4, και στο επόμενο Κεφάλαιο 4 θα αναλυθεί η δομή των υποομάδων τυχούσας κυκλικής ομάδας.

Κλείνουμε την παρούσα υποενότητα με ένα πολύ χρήσιμο αποτέλεσμα το οποίο πιστοποιεί ότι υποομάδες δείκτη 2 είναι κανονικές. Υπενθυμίζουμε οτι η υποομάδα H μιας ομάδας G είναι κανονική αν $\forall x \in G$: $xHx^{-1} = H$.

Πρόταση 3.4.13. *Έστω $H \leq G$ μια υποομάδα της ομάδας $(G,\cdot)$. Αν ο δείκτης της H στην G είναι $[G:H] = 2$, τότε η H είναι κανονική υποομάδα της G.*

Απόδειξη. Έστω H μια υποομάδα της G με δείκτη $[G:H] = 2$. Τότε, για κάθε $x \in G \setminus H$, τα αριστερά σύμπλοκα H, xH είναι διαφορετικά (διότι $H = xH$ αν-ν $x \in H$). Άρα το σύνολο υποσυνόλων $\{H, xH\}$ του G είναι μια διαμέριση του συνόλου G, και επομένως θα έχουμε $G = H \cup xH$ και $H \cap xH = \emptyset$. Προφανώς τότε θα έχουμε $xH = G \setminus H$. Παρόμοια θα έχουμε $Hx = G \setminus H$. Άρα θα έχουμε $xH = G \setminus H = Hx$, $\forall x \in G \setminus H$, και προφανώς $xH = Hx$, $\forall x \in H$ διότι $H \leq G$. Ισοδύναμα θα έχουμε $xH = Hx$, $\forall x \in G$. Αυτό προφανώς σημαίνει ότι $\forall x \in G$: $xHx^{-1} = H$. Επομένως η H είναι κανονική. ■

3.5 Το αντίστροφο του Θεωρήματος του Lagrange και η Εναλλάσσουσα Ομάδα A_4

Στην παρούσα ενότητα θα εξετάσουμε αν ισχύει το αντίστροφο του Θεωρήματος του Lagrange: «*Αν d είναι ένας θετικός διαιρέτης της τάξης μιας πεπερασμένης ομάδας G, υπάρχει υποομάδα H της G με τάξη ίση με του διαιρέτη;*».

3.5.1 Οι υποομάδες της S_3

Υπενθυμίζουμε ότι, χρησιμοποιώντας κυκλικό συμβολισμό μεταθέσεων, η συμμετρική ομάδα S_3 είναι η εξής:

$$S_3 = \{\iota = (1),\ (12),\ (13),\ (23),\ (123),\ (132)\}$$

Πίνακας Cayley της S_3

$\circ$	**(1)**	**(12)**	**(13)**	**(23)**	**(123)**	**(132)**
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Ισχυρισμός: Τα ακόλουθα υποσύνολα είναι όλες οι υποομάδες της S_3:

1. Υποομάδες Τάξης 1: $H_0 = \{(1)\}$.
2. Υποομάδες Τάξης 2: $H_1 = \{(1), (12)\} = \langle(12)\rangle$, $H_2 = \{(1), (13)\} = \langle(13)\rangle$, $H_3 = \{(1), (23)\} = \langle(23)\rangle$.
3. Υποομάδες Τάξης 3: $H_4 = \{(1), (123), (132)\} = \langle(123)\rangle$.
4. Υποομάδες Τάξης 6: $H_5 = S_3$.

Πράγματι προφανώς τα παραπάνω υποσύνολα είναι υποομάδες της S_3 (για παράδειγμα εκτός της τετριμμένης υποομάδας $H_0 = \{(1)\}$ και της ομάδας $H_5 = S_3$, οι οι υπόλοιπες υποομάδες H_i, $1 \le 4$, είναι κυκλικές). Αντίστροφα, αν H είναι μια υποομάδα της S_3, τότε από το Θεώρημα του Lagrange 3.4.6 έπεται ότι η τάξη της είναι διαιρέτης της τάξης της S_3 και άρα $o(H) = 1$, ή 2, ή 3, ή 6. Αν $o(H) = 1$, τότε προφανώς $H = H_0 = \{(1)\}$ και αν $o(H) = 6$, τότε προφανώς $H = H_5 = S_3$. Αν $o(H) = 2$, τότε θα έχουμε ότι $H = \{(1), x\}$ όπου $x \in S_3$ και προφανώς $o(x) = 2$. Επειδή τα μόνα στοιχεία τάξης 2 της S_3 είναι τα (12), (13), και (23), έπεται ότι η H είναι μια εκ των H_1, H_2, H_3. Αν $o(H) = 3$, τότε $H = \{(1), x, y\}$ όπου $x, y \in S_3$, και από το Θεώρημα του Lagrange τα στοιχεία x, y έχουν τάξη 3. Επειδή τα μόνα στοιχεία τάξης 3 της S_3 είναι τα (123), και (132), και επειδή $(123)^2 = (132)$ και $(132)^2 = (123)$, έπεται ότι η H σύμπίπτει με την H_4. Έτσι δείξαμε ότι οι υποομάδες της S_3 είναι οι υποομάδες H_i, $0 \le i \le 5$ και μόνο αυτές.

Επομένως βλέπουμε ότι για την S_3 ισχύει το αντίστροφο του Θεωρήματος του Lagrange, δηλαδή για κάθε διαιρέτη $d \in \{1,2,3,6\}$ της τάξης $o(S_3) = 6$ της S_3 υπάρχει (τουλάχιστον μια) υποομάδα της S_3 με τάξη τον διαιρέτη.

3.5.2 Οι υποομάδες της εναλλάσσουσας υποομάδας A_4

Το αντίστροφο του Θεωρήματος του Lagrange γενικά δεν ισχύει: υπάρχουν πεπερασμένες ομάδες G και διαιρέτες k της τάξης της ομάδας έτσι ώστε η G να μην έχει υποομάδες τάξης k. Η μικρότερη ομάδα για την οποία το αντίστροφο του Θεωρήματος του Lagrange δεν ισχύει, είναι η *εναλλάσσουσα ομάδα* A_4 με τάξη 12, την οποία θα μελετήσουμε αναλυτικότερα σε μεταγενέστερο Κεφάλαιο. Όπως θα δείξουμε, η A_4 έχει υποομάδες τάξης $1,2,3,4,12$ αλλά δεν έχει καμία υποομάδα τάξης 6.

Για τους σκοπούς της παρούσας ενότητας, θεωρούμε το ακόλουθο υποσύνολο της συμμετρικής ομάδας S_4:

$$A_4 = \{(1),\ (123),\ (124),\ (134),\ (234),\ (132),\ (142),\ (143),\ (243),\ (12)(34),\ (13)(24),\ (14)(23)\}$$

Ισχυρισμός: Το σύνολο A_4 είναι μια υποομάδα της συμμετρικής ομάδας S_4.

Απόδειξη του Ισχυρισμού. Σύμφωνα με την Πρόταση 2.4.8, αρκεί να δείξουμε ότι το υποσύνολο A_4 είναι κλειστό στην πράξη «$\circ$» της S_4. Αυτό προκύπτει εύκολα από τον πίνακα πολλαπλασιασμού (πίνακας Cayley) της A_4, τον οποίο παραθέτουμε στη συνέχεια για μεταγενέστερη χρήση:

Πίνακας Cayley της A_4

$\circ$	**(1)**	**(123)**	**(124)**	**(134)**	**(234)**	**(132)**	**(142)**	**(143)**	**(243)**	**(12)(34)**	**(13)(24)**	**(14)(23)**
(1)	(1)	(123)	(124)	(134)	(234)	(132)	(142)	(143)	(243)	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(132)	(13)(24)	(234)	(12)(34)	(1)	(143)	(14)(23)	(124)	(134)	(243)	(142)
(124)	(124)	(14)(23)	(142)	(13)(24)	(123)	(134)	(1)	(243)	(12)(34)	(143)	(132)	(234)
(134)	(134)	(124)	(12)(34)	(143)	(13)(24)	(14)(23)	(234)	(1)	(132)	(123)	(142)	(243)
(234)	(234)	(13)(24)	(134)	(14)(23)	(243)	(142)	(12)(34)	(123)	(1)	(132)	(143)	(124)
(132)	(132)	(1)	(243)	(12)(34)	(134)	(123)	(14)(23)	(142)	(13)(24)	(234)	(124)	(143)
(142)	(142)	(234)	(1)	(132)	(14)(23)	(13)(24)	(124)	(12)(34)	(143)	(243)	(134)	(123)
(143)	(143)	(12)(34)	(123)	(1)	(142)	(243)	(13)(24)	(134)	(14)(23)	(124)	(234)	(132)
(243)	(243)	(143)	(14)(23)	(124)	(1)	(12)(34)	(132)	(13)(24)	(234)	(142)	(123)	(134)
(12)(34)	(12)(34)	(243)	(234)	(142)	(124)	(143)	(134)	(132)	(123)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(142)	(143)	(243)	(132)	(234)	(123)	(124)	(134)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(134)	(132)	(123)	(143)	(124)	(243)	(234)	(142)	(13)(24)	(12)(34)	(1)

Επομένως το υποσύνολο A_4 είναι μια υποομάδα της S_4 με τάξη $|A_4| = 12$, η οποία καλείται η *εναλλάσσουσα ομάδα* βαθμού 4.

Σημειώνουμε ότι, όπως μπορεί να υπολογιστεί εύκολα, βλέπε και τον παραπάνω πίνακα Cayley, στην ομάδα A_4:

1. Η ταυτοτική μετάθεση $(1) = \iota$ έχει τάξη 1.
2. Τα στοιχεία (123), (124), (134), (234), (132), (142), (143), (243), έχουν τάξη 3.
3. Τα στοιχεία (12)(34), (13)(24), (14)(23) έχουν τάξη 2.

4. Η εναλλάσσουσα υποομάδα A_4 δεν έχει στοιχεία τάξης 4, 6 ή 12.

Πρόταση 3.5.1. *Η εναλλάσσουσα ομάδα* A_4 *τάξης* 12*:*

1. *έχει υποομάδες τάξης* 1, 2, 3, 4, *και* 12.

2. *δεν έχει υποομάδα τάξης* 6.

Απόδειξη. **1.** Προφανώς η A_4 έχει υποομάδες τάξης 1, και 12. Εύκολα βλέπουμε ότι το στοιχείο $(12)(34)$ έχει τάξη 2 και άρα παράγει μια κυκλική ομάδα τάξης 2, και το στοιχείο (123) έχει τάξη 3 και άρα παράγει μια υποομάδα τάξης 3. Τέλος, το υποσύνολο

$$\{(1),\ (12)(34),\ (13)(24),\ (14)(23)\} \subseteq \mathsf{A}_4$$

είναι κλειστό στην πράξη της ομάδας A_4 και άρα, σύμφωνα με την Πρόταση 2.4.8, αποτελεί μια υποομάδα τάξης 4 της A_4.

2. Υποθέτουμε ότι H είναι μια υποομάδα της A_4 με $\mathsf{o}(H) = 6$. Από το Θεώρημα του Lagrange τότε προφανώς ο δείκτης της H στην A_4 θα είναι

$$[\mathsf{A}_4 : H] = \frac{|\mathsf{A}_4|}{|H|} = \frac{12}{6} = 2$$

και επομένως η H έχει 2 διακεκριμένα αριστερά σύμπλοκα στην A_4.

Θα δείξουμε ότι κάθε στοιχείο της A_4 το οποίο είναι της μορφής g^2, όπου $g \in \mathsf{A}_4$, ανήκει στην H:

$$\mathscr{M} = \{g^2 \in A_4 \mid g \in \mathsf{A}_4\} \subseteq H \qquad (*)$$

Πράγματι: έστω $g \in \mathsf{A}_4$. Αν $g \in H$, τότε $g^2 \in H$ διότι η H είναι υποομάδα της A_4. Αν $g \notin H$, τότε τα σύμπλοκα $(1)H = H$ και gH, δεν συμπίπτουν, διότι διαφορετικά αν $H = gH$, τότε $g \in H$, που είναι άτοπο. Άρα, επειδή τα σύμπλοκα $(1)H = H$ και gH είναι διαφορετικά και επειδή η H έχει 2 διακεκριμένα αριστερά σύμπλοκα στην A_4, έπεται ότι τα σύμπλοκα H και gH αποτελούν μια διαμέριση της A_4, και άρα:

$$\mathsf{A}_4 = H \cup gH, \qquad H \cap gH = \emptyset$$

Το σύμπλοκο g^2H θα συμπίπτει με ένα εκ των H και gH. Αν $g^2H = gH$, τότε $(g^2)^{-1} \circ g = g^{-2} \circ g = g^{-1} \in H$. Επειδή η H είναι υποομάδα, θα έχουμε $g \in H$ το οποίο είναι άτοπο. Συμπεραίνουμε ότι: $g^2H = H$ κάτι το οποίο σημαίνει ότι $g^2 \in H$. Άρα η έγκλειση $(*)$ ισχύει.

Όμως το πλήθος των στοιχείων του συνόλου $\mathscr{M}$ των τετραγώνων στοιχείων της A_4 είναι, όπως βλέπουμε από τον πίνακα πολλαπλασιασμού της A_4:

$$\mathscr{M} = \{(1),\ (123),\ (124),\ (134),\ (234),\ (132),\ (14,2),\ (143),\ (243)\}$$

δηλαδή όλοι οι 3-κύκλοι και η ταυτοτική μετάθεση. Άρα $|\mathscr{M}| = 9$ και επομένως δεν μπορεί να ισχύει η σχέση $(*)$, διότι $|H| = 6$. Στο άτοπο καταλήξαμε υποθέτοντας ότι η A_4 έχει μια υποομάδα τάξης 6. Άρα η εναλλάσσουσα ομάδα A_4 δεν έχει υποομάδα τάξης 6. ■

Πόρισμα 3.5.2. *Οι υποομάδες της εναλλάσσουσας ομάδας* A_4 *είναι οι εξής:*

1. *Υποομάδες Τάξης* 1*:*

$$H_1 = \{(1)\}$$

2. *Υποομάδες Τάξης* 2*:*

$$H_2 = \langle (12)(34) \rangle = \{(1), (12)(34)\}, \quad H_3 = \langle (13)(24) \rangle = \{(1), (13)(24)\}, \quad H_4 = \langle (14)(23) \rangle = \{(1), (14)(23)\}$$

3. *Υποομάδες Τάξης* 3*:*

$$H_5 = \langle (123) \rangle = \langle (132) \rangle = \{(1), (123), (132)\}, \qquad H_6 = \langle (124) \rangle = \langle (142) \rangle = \{(1), (124), (142)\}$$

$$H_7 = \langle (134) \rangle = \langle (143) \rangle = \{(1), (134), (143)\}, \qquad H_8 = \langle (234) \rangle = \langle (243) \rangle = \{(1), (234), (243)\},$$

4. *Υποομάδες Τάξης* 4*:*

$$H_9 = \{(1), (12)(34), (13)(24), (14)(23)\}$$

5. *Υποομάδες Τάξης* 12*:*

$$H_{10} = \mathsf{A}_4$$

Απόδειξη. Προφανώς τα υποσύνολα H_i, $1 \leq i \leq 10$, είναι υποομάδες της A_4, βλέπε και την Πρόταση 3.5.1.

Έστω H μια υποομάδα της A_4. Τότε από το Θεώρημα του Lagrange 3.4.6 έπεται ότι η τάξη της είναι διαιρέτης της τάξης της A_4 και άρα $\mathsf{o}(H) = 1$, ή 2, ή 3, ή 6 ή 12. Η Πρόταση 3.5.1 εξασφαλίζει ότι η A_4 δεν έχει υποομάδες τάξης 6 και προφανώς αν $\mathsf{o}(H) = 1$, τότε $H = H_1 = \{(1)\}$ και αν $\mathsf{o}(H) = 12$, τότε $H = H_{10} = \mathsf{A}_4$. Αν $\mathsf{o}(H) = 2$, τότε θα έχουμε ότι $H = \{(1), x\}$ όπου $x \in \mathsf{A}_4$ και προφανώς $\mathsf{o}(x) = 2$. Επειδή τα μόνα στοιχεία τάξης 2 της A_4 είναι τα $(12)(34)$, $(13)(24)$, και $(23)(14)$, έπεται ότι η H είναι μια εκ των H_2, H_3, H_4. Αν $\mathsf{o}(H) = 3$, τότε $H = \{(1), x, y\}$ όπου $x, y \in \mathsf{A}_4$, και προφανώς τα στοιχεία x, y έχουν τάξη 3. Τότε $x^2 = y$, $y^2 = x$, και $H = \langle x \rangle = \langle x^2 \rangle$. Επειδή τα μόνα στοιχεία τάξης 3 της A_4 είναι οι 3-κύκλοι

$$(123), \quad (124), \quad (134), \quad (234), \quad (132), \quad (142), \quad (143), \quad (243)$$

και

$$(132) = (123)^2, \quad (142) = (124)^2, \quad (143) = (134)^2, \quad (243) = (234)^2$$

έπεται ότι η H σύμπίπτει με μια εκ των H_5, H_6, H_7, H_8. Τέλος, αν $\mathsf{o}(H) = 4$, τότε, επειδή η A_4 δεν έχει στοιχεία τάξης 4, έπεται ότι θα έχουμε $H = \{(1), x, y, z\}$ όπου $x, y, z \in \mathsf{A}_4$ και προφανώς $\mathsf{o}(x) = \mathsf{o}(y) = \mathsf{o}(z) = 2$, δηλαδή η H είναι αντίγραφο της ομάδας του Klein. Επειδή τα μόνα στοιχεία τάξης 2 της A_4 είναι τα $(12)(34)$, $(13)(24)$, και $(23)(14)$, έπεται ότι η H είναι η H_9. Έτσι δείξαμε ότι οι υποομάδες της A_4 είναι οι υποομάδες H_i, $1 \leq i \leq 10$ και μόνο αυτές. ■

Παρατήρηση 3.5.3. 1. Το αμέσως επόμενο, ως προς την τάξη, παράδειγμα ομάδας στην οποία δεν ισχύει το αντίστροφο του Θεωρήματος Lagrange αποτελεί η ομάδα $\mathsf{SL}(2, \mathbb{Z}_3)$ των 2×2 πινάκων με ορίζουσα 1 υπεράνω του συνόλου $\mathbb{Z}_3$ των κλάσεων υπολοίπων ακεραίων mod 3 (το οποίο θεωρείται ότι είναι εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού κλάσεων υπολοίπων mod 3). Η $\mathsf{SL}(2, \mathbb{Z}_3)$ είναι μια μη αβελιανή ομάδα τάξης 24 και άρα οι διαιρέτες της τάξης της είναι: 1, 2, 3, 4, 6, 8, 12, 24. Μπορεί κανείς να αποδείξει ότι η $\mathsf{SL}(2, \mathbb{Z}_3)$ έχει υποομάδες τάξης 1, 2, 3, 4, 6, 8, 24 αλλά δεν έχει υποομάδες τάξης 12.

2. Όπως θα δούμε αργότερα, κάθε κυκλική ομάδα (πεπερασμένης τάξης) ικανοποιεί το αντίστροφο του Θεωρήματος Lagrange. Γενικότερα μπορεί να δειχθεί ότι: (α) κάθε πεπερασμένη αβελιανή ομάδα, (β) κάθε ομάδα με τάξη η οποία είναι δύναμη ενός πρώτου αριθμού, και (γ) κάθε διεδρική ομάδα, ικανοποιεί το αντίστροφο του Θεωρήματος του Lagrange. ▲

3.6 Εφαρμογές του Θεωρήματος Lagrange στην τομή και στο γινόμενο υποομάδων

Στην παρούσα ενότητα θα δούμε κάποιες άμεσες εφαρμογές του Θεωρήματος Lagrange 3.4.6. Ιδιαίτερα θα δούμε εφαρμογές του στον υπολογισμό της τάξης της τομής ή γινομένου δύο υποομάδων μιας ομάδας.

Πρόταση 3.6.1. *Έστω H και K δύο υποομάδες μιας πεπερασμένης ομάδας $(G, \cdot)$, και υποθέτουμε ότι:*

$$K \subseteq H \subseteq G$$

Τότε:

$$[G : K] = [G : H] \cdot [H : K]$$

Απόδειξη. Προφανώς η K είναι υποομάδα της H και άρα από το Θεώρημα του Lagrange 3.4.6 για τις υποομάδες H και K, θα έχουμε:

$$\mathsf{o}(G) = \mathsf{o}(H)\cdot[G:H] \quad \text{και} \quad \mathsf{o}(G) = \mathsf{o}(K)\cdot[G:K] \quad \text{και} \quad \mathsf{o}(H) = \mathsf{o}(K)\cdot[H:K]$$

Επομένως

$$\mathsf{o}(G) = \mathsf{o}(K)\cdot[H:K]\cdot[G:H] \quad \text{και} \quad \mathsf{o}(G) = \mathsf{o}(K)\cdot[G:K] \quad \Longrightarrow \quad [G:K] = [G:H]\cdot[H:K] \qquad \blacksquare$$

Η Πρόταση 3.6.1 μπορεί να γενικευτεί κατάλληλα σε άπειρες ομάδες, βλέπε την Άσκηση 3.9.49.

Πρόταση 3.6.2. *Έστω H και K δύο υποομάδες μιας πεπερασμένης ομάδας $(G,\cdot)$, και έστω $\mathsf{o}(H) = m$ και $\mathsf{o}(K) = n$. Αν $(m,n) = 1$, τότε:*

$$H \bigcap K = \{e\}$$

Απόδειξη. Γνωρίζουμε ότι η τομή υποομάδων μιας ομάδας είναι υποομάδα. Έτσι η τομή $H \cap K$ είναι υποομάδα των πεπεπερασμένων ομάδων H και K, και τότε απο το Θεώρημα του Lagrange 3.4.6 θα έχουμε:

$$\mathsf{o}(H\cap K) \mid \mathsf{o}(H) = m \qquad \text{και} \qquad \mathsf{o}(H\cap K) \mid \mathsf{o}(K) = n$$

Τότε όμως $\mathsf{o}(H\cap K) \mid (m,n)$, και επειδή $(m,n) = 1$, θα έχουμε $\mathsf{o}(H\cap K) = 1$ ή ισοδύναμα: $H\cap K = \{e\}$. $\blacksquare$

Υπενθυμίζουμε ότι, αν $H, K \subseteq G$ είναι υποσύνολα μιας ομάδας G, τότε:

$$HK = \big\{hk \in G \mid h \in H,\ k \in K\big\}$$

Σημειώνουμε ότι αν τα υποσύνολα $H, K \subseteq G$ είναι υποομάδες της G, τότε γενικά το υποσύνολο HK δεν είναι υποομάδα της G.

Πρόταση 3.6.3. *Έστω H, K δύο πεπερασμένες υποομάδες της ομάδας G. Τότε το πλήθος $\big|HK\big|$ των στοιχείων του συνόλου HK είναι:*

$$|HK| = \frac{\mathsf{o}(H)\,\mathsf{o}(K)}{\mathsf{o}(H\cap K)}$$

Απόδειξη. Θεωρούμε την απεικόνιση

$$f:\ H\times K \longrightarrow HK, \quad f(h,k) = hk$$

η οποία προφανώς είναι απεικόνιση «επί». Υπενθυμίζουμε ότι,[17] βλέπε την Πρόταση 1.2.24 στην υποενότητα 1.2.4, η f ορίζει μια σχέση ισοδυναμίας $\mathscr{R}_f$ επί του συνόλου $H\times K$, ως εξής:

$$\forall (h_1,k_1),(h_2,k_2) \in H\times K: \quad (x_1,y_1)\,\mathscr{R}_f\,(x_2,y_2) \quad \Longleftrightarrow \quad f(h_1,k_1) = f(h_2,k_2), \quad \text{δηλαδή} \quad h_1k_1 = h_2k_2$$

Επιπλέον υπάρχει μια «1-1» και «επί» απεικόνιση μεταξύ του συνόλου πηλίκο $(H\times K)/\mathscr{R}_f$ και της εικόνας $\mathsf{Im}(f) = HK$ της απεικόνισης f, και επομένως:

$$\big|(H\times K)/\mathscr{R}_f\big| \ = \ \big|HK\big| \qquad (*)$$

Όπως γνωρίζουμε, τα στοιχεία του συνόλου πηλίκο $(H\times K)/\mathscr{R}_f$ είναι οι διακεκριμένες κλάσεις ισοδυναμίας $[(h,k)]_{\mathscr{R}_f}$ των στοιχείων του συνόλου $H\times K$ και επιπλέον

$$[(h,k)]_{\mathscr{R}_f} = f^{-1}\big\{f(h,k)\big\} = f^{-1}\big\{hk\big\}$$

[17] Αν $f: X \longrightarrow Y$ είναι μια απεικόνιση μεταξύ συνόλων, τότε, ορίζοντας $\forall x_1,x_2 \in X$: $x_1\,\mathscr{R}_f\,x_2$ αν και μόνο αν $f(x_1) = f(x_2)$, αποκτούμε μια σχέση ισοδυναμίας επί του συνόλου X, και επιπλέον, αν $x \in X$, τότε $[x]_{\mathscr{R}_f} = f^{-1}(\{f(x)\})$. Επιπρόσθετα η απεικόνιση $\widetilde{f}: X/\mathscr{R}_f \longrightarrow \mathsf{Im}(f)$, $\widetilde{f}([x]_{\mathscr{R}_f}) = f(x)$ είναι «1-1» και «επί».

Θα δείξουμε ότι, $\forall (h,k) \in H \times K$:

$$f^{-1}\{hk\} = \{(hr, r^{-1}k) \in G \times G \mid r \in H \cap K\} \tag{†}$$

Πραγματικά: αν $(hr, r^{-1}k) \in G \times G$, όπου $h \in H$, $k \in K$, και $r \in H \cap K$, τότε προφανώς $(hr, r^{-1}k) \in H \times K$, και $f(hr, r^{-1}k) = hrr^{-1}k = hek = hk$. Επομένως $(hr, r^{-1}k) \in f^{-1}\{hk\} = [(h,k)]_{\mathscr{R}_f}$. Αντίστροφα, αν $(x,y) \in f^{-1}\{hk\} = [(h,k)]_{\mathscr{R}_f}$, τότε $x \in H$, $y \in K$, και $f(x,y) = hk$. Επομένως $hk = xy$ και τότε $x^{-1}hk = y$. Επειδή $x, h \in H$ και η H είναι υπομάδα της G, θα έχουμε $x^{-1}h \in H$, και επειδή $y, k \in K$ και η K είναι υποομάδα της G, θα έχουμε $yk^{-1} \in K$. Άρα:

$$x^{-1}h = yk^{-1} \ \in \ H \cap K$$

Ισοδύναμα, επειδή το υποσύνολο $H \cap K$ είναι υποομάδα, θα έχουμε:

$$(x^{-1}h)^{-1} = (yk^{-1})^{-1} \ \in \ H \cap K \quad \Longrightarrow \quad h^{-1}x = ky^{-1} := r \ \in \ H \cap K$$

Τότε θα έχουμε:

$$(x,y) = (ex, ye) = \big((hh^{-1})x, y(k^{-1}k)\big) = \big(h(h^{-1}x), (yk^{-1})k\big) = (hr, r^{-1}k)$$

Άρα αποδείξαμε την σχέση (†) με βάση την οποία ορίζουμε μια απεικόνιση, $\forall h \in H, \forall k \in K$:

$$\phi : \ H \cap K \longrightarrow f^{-1}\{hk\}, \quad \phi(r) = (hr, r^{-1}k)$$

Η παραπάνω ανάλυση δείχνει ότι η απεικόνιση ϕ είναι καλά ορισμένη και είναι απεικόνιση «επί». Επιπλέον η ϕ είναι «1-1» διότι, αν $\phi(r) = \phi(s)$ τότε $(hr, r^{-1}k) = (hs, s^{-1}k)$ και άρα: $hr = hs$ και $r^{-1}k = s^{-1}k$. Τότε προφανώς θα έχουμε $r = s$ και έτσι η ϕ είναι «1-1» και «επί».

Αυτό σημαίνει ότι για την τυχούσα κλάση ισοδυναμίας $[(h,k)]_{\mathscr{R}_f}$ θα έχουμε:

$$\mathrm{o}(H \cap K) = \big|H \cap K\big| = \big|[(h,k)]_{\mathscr{R}_f}\big|$$

Επειδή το σύνολο όλων των κλάσεων ισοδυναμίας αποτελεί μια διαμέριση του $H \times K$, επειδή από το Πόρισμα 3.3.7 κάθε κλάση ισοδυναμίας έχει τόσα στοιχεία όσα και η υποομάδα $H \cap K$, και επειδή από τη σχέση (*) το πλήθος των διακεκριμένων κλάσεων ισοδυναμίας είναι ίσο με το πλήθος $\big|HK\big|$, θα έχουμε:

$$\big|H \times K\big| = \big|H \cap K\big| \cdot \big|HK\big|$$

Επομένως:

$$|HK| = \frac{\big|H \times K\big|}{\big|H \cap K\big|} = \frac{\big|H\big|\big|K\big|}{\mathrm{o}(H \cap K)} = \frac{\mathrm{o}(H)\,\mathrm{o}(K)}{\mathrm{o}(H \cap K)}$$ ■

Θα δούμε τώρα κάποιες εφαρμογές της παραπάνω Πρότασης.

Πόρισμα 3.6.4. *Έστω H και K δύο υποομάδες μιας πεπερασμένης ομάδας G. Τότε:*

$$\mathrm{o}(H) \ > \ \sqrt{\mathrm{o}(G)} \quad \textit{και} \quad \mathrm{o}(K) \ > \ \sqrt{\mathrm{o}(G)} \quad \Longrightarrow \quad H \cap K \neq \{e\}$$

Απόδειξη. Από την Πρόταση 3.6.3, έχουμε:

$$\mathrm{o}(G) \geq |HK| = \frac{\mathrm{o}(H)\,\mathrm{o}(K)}{\mathrm{o}(H \cap K)} > \frac{\sqrt{\mathrm{o}(G)}\,\sqrt{\mathrm{o}(G)}}{\mathrm{o}(H \cap K)} = \frac{\mathrm{o}(G)}{\mathrm{o}(H \cap K)} \quad \Longrightarrow \quad \mathrm{o}(H \cap K) > 1$$ ■

Πόρισμα 3.6.5. *Έστω G μια ομάδα τάξης $\mathrm{o}(G) = pq$, όπου p, q είναι πρώτοι αριθμοί με $p > q$. Τότε η G έχει το πολύ μια υποομάδα τάξης p.*

Απόδειξη. Έστω H και K δύο υποομάδες της G τάξης p. Τότε ικανοποιούνται τετριμμένα οι υποθέσεις του Πορίσματος 3.6.4 και άρα $H \cap K \neq \{e\}$, δηλαδή $o(H \cap K) > 1$. Όμως, επειδή η $H \cap K$ είναι υποομάδα της H και της K, και επειδή η τάξη της H και η τάξη της K είναι ο πρώτος αριθμός p, από το Θεώρημα του Lagrange έπεται ότι $o(H \cap K) \mid p$ και άρα $o(H \cap K) = p$ διότι, όπως είδαμε, $o(H \cap K) > 1$. Τότε όμως $H \cap K = H$ και $H \cap K = K$, δηλαδή $H \subseteq K$ και $K \subseteq H$. Επομένως $H = K$. ■

Παρατήρηση 3.6.6. Ως ειδική περίπτωση (Θεώρημα Cauchy[18]) ενός σημαντικού Θεωρήματος το οποίο οφείλεται στον Sylow, [19] έπεται ότι κάθε ομάδα G τάξης $o(G) = pq$, όπου p, q είναι πρώτοι αριθμοί με $p > q$, έχει τουλάχιστον μια υποομάδα τάξης p. Έτσι, σύμφωνα με το παραπάνω πόρισμα, έπεται ότι η G έχει ακριβώς μια υποομάδα τάξης p. ▲

3.7 Οι ομάδες τάξης pq, όπου p, q είναι πρώτοι αριθμοί

Στην παρούσα ενότητα θα ταξινομήσουμε, με ακρίβεια ισομορφισμού, όλες τις ομάδες τάξης τάξης $2p$, όπου p είναι ένας πρώτος αριθμός. Με άλλα λόγια, θα περιγράψουμε όλες τις κλάσεις ισομορφίας ομάδων τάξης $2p$.

3.7.1 Ομάδες τάξης $2p$, p: πρώτος

Υπενθυμίζουμε ότι, αν $n \geq 3$, η n-οστή διεδρική ομάδα D_n είναι η ομάδα των συμμετριών του κανονικού n-γώνου. Έτσι για παράδειγμα:

1. Αν $n = 1$, η D_n είναι η κυκλική τάξης 2.
2. Άν $n = 2$, η D_2 είναι η ομάδα V_4 των τεσσάρων στοιχείων του Klein.
3. Άν $n = 3$, η D_3 είναι η ομάδα συμμετριών του ισόπλευρου τριγώνου και συμπίπτει με τη συμμετρική ομάδα S_3.
4. Άν $n = 3$, η D_4 είναι η ομάδα συμμετριών του τετραγώνου.

Η ομάδα D_n περιγράφεται, βλέπε την υποενότητα 2.2, ως εξής:

$$D_n = \{e,\ a,\ a^2,\ \cdots,\ a^{n-1},\ b,\ ab,\ a^2b,\ \cdots,\ a^{n-1}b \mid \text{όπου } a^n = e,\quad b^2 = e,\quad \text{και} \quad bab = a^{-1}\}$$

Σημειώνουμε ότι οι σχέσεις $a^n = e$, $b^2 = e$, $bab = a^{-1}$ καθορίζουν πλήρως την ομάδα D_n. Δηλαδή κάθε ομάδα, η οποία παράγεται από δύο στοιχεία a, b τα οποία ικανοποιούν τις παραπάνω σχέσεις, είναι ισόμορφη με την D_n. Θεωρώντας την διεδρική ομάδα D_n ως την ομάδα των συμμετριών του κανονικού n-γώνου, τα στοιχεία a, b έχουν την ακόλουθη ερμηνεία: το στοιχείο a παριστάνει στροφή επιπέδου κατά γωνία $\frac{2\pi}{n}$ και το στοιχείο b παριστάνει ανάκλαση επιπέδου ως προς τον άξονα yy'.

Θεώρημα 3.7.1. *Έστω ότι G είναι μια ομάδα τάξης $o(G) = 2p$, όπου p: πρώτος. Τότε:*

1. *Είτε η G είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{2p}$.* *(όταν η G είναι αβελιανή)*
2. *είτε η G είναι ισόμορφη με την διεδρική ομάδα D_p.* *(όταν η G δεν είναι αβελιανή)*

και οι ομάδες $\mathbb{Z}_{2p}$ και D_p δεν είναι ισόμορφες.

[18] Augustin-Louis Cauchy (21 Αυγούστου 1789 - 23 Μαίου 1857) [http://en.wikipedia.org/wiki/Augustin-Louis_Cauchy]: Διαπρεπής Γάλλος μαθηματικός με σημαντική συμβολή στη Μαθηματική Ανάλυση, στη Θεωρία Μιγαδικών Συναρτήσεων, και στη Θεωρία Ομάδων.

[19] Peter Ludwig Mejdell Sylow (12 Δεκεμβρίου 1832 - 7 Σεπτεμβρίου 1918) [http://en.wikipedia.org/wiki/Peter_Ludwig_Mejdell_Sylow]: Νορβηγός μαθηματικός με σημαντική συμβολή στη Θεωρία Ομάδων.

Για την απόδειξη θα χρειαστούμε κάποιες βοηθητικές προτάσεις οι οποίες είναι ενδιαφέρουσες από μόνες τους.

Λήμμα 3.7.2. *Έστω G μια πεπερασμένη αβελιανή ομάδα. Αν η G περιέχει δύο στοιχεία a, b τάξης 2, όπου $a \neq b$, τότε το σύνολο $V = \{e, a, b, ab\}$ είναι μια υποομάδα της G, ισόμορφη με την ομάδα του Klein, και επομένως $4 \mid o(G)$.*

Απόδειξη. Επειδή η G είναι αβελιανή έπεται ότι $ab = ba$ και η τάξη του ab είναι ίση με 2, διότι $(ab)^2 = abab = aabb = a^2b^2 = ee = e$, και $ab \neq e$ διότι αν $ab = e$, τότε $a = b^{-1} = b$, το οποίο είναι άτοπο. Το σύνολο V είναι πεπερασμένο και κλειστό στην πράξη πολλαπλασιασμού της G. Επομένως το υποσύνολο V είναι μια υποομάδα της G. Τέλος, από το Θεώρημα του Lagrange έπεται ότι $o(V) = 4 \mid o(G)$. ■

Λήμμα 3.7.3. *Έστω G μια ομάδα άρτιας τάξης. Τότε η G περιέχει ένα στοιχείο τάξης 2.*

Απόδειξη. Θεωρούμε το σύνολο

$$X = \{x \in G \mid x \neq x^{-1}\} = \{x \in G \mid x^2 \neq e_G\}$$

Ισχυρισμός: Το πλήθος των στοιχείων του X είναι άρτιο.

Πράγματι, αν $X = \emptyset$, τότε το πλήθος των στοιχείων του είναι ίσο με μηδέν.[20] Αν $X \neq \emptyset$, τότε, όταν $x \in X$ συμπεραίνουμε ότι και $x^{-1} \in X$, αφού $x \neq x^{-1}$ δίνει $x^{-1} \neq (x^{-1})^{-1} = x$. Ώστε και τα δύο x και x^{-1} ανήκουν στο X. Σχηματίζουμε το συμπλήρωμα τού X στο G, δηλαδή το σύνολο

$$G \setminus X = \{x \in G \mid x = x^{-1}\} = \{x \in G \mid x^2 = e\}$$

Το ουδέτερο στοιχείο e_G ανήκει στο $G \setminus X$, επειδή $e = e^{-1}$. Επομένως $G \setminus X \neq \emptyset$. Ώστε το πλήθος των στοιχείων τού $G \setminus X$ είναι ≥ 1. Επειδή τώρα και το X και το G έχουν άρτιο πλήθος στοιχείων, συμπεραίνουμε ότι και το πλήθος των στοιχείων τού $G \setminus X$ είναι άρτιο και ως εκ τούτου ≥ 2 (αφού, όπως είδαμε, είναι ≥ 1).

Επομένως, υπάρχει κάποιο στοιχείο $a \in G \setminus X$ με $a \neq e$ και, αφού $a \in G \setminus X$, έπεται $a^2 = e$. ■

Η παρακάτω πρόταση μάς εξασφαλίζει την ύπαρξη ενός μοναδικού στοιχείου τάξης 2 σε μια ομάδα άρτιας τάξης, υπό την προϋπόθεση ότι η τάξη της ομάδας δεν διαιρείται από το 4.

Λήμμα 3.7.4. *Έστω G μια πεπερασμένη αβελιανή ομάδα άρτιας τάξης. Αν $4 \nmid o(G)$, τότε η G περιέχει ακριβώς ένα στοιχείο τάξης 2.*

Απόδειξη. Απο το Λήμμα 3.7.3, η G περιέχει τουλάχιστον ένα στοιχείο a τάξης 2. Αν η G περιέχει δύο διαφορετικά στοιχεία a, b τάξης 2, τότε, σύμφωνα με το Λήμμα 3.7.2, θα έπρεπε $4 \mid o(G)$, κάτι το οποίο είναι άτοπο. Άρα η G περιέχει ακριβώς ένα στοιχείο τάξης 2. ■

Λήμμα 3.7.5. *Έστω G μια ομάδα. Αν κάθε μη ταυτοτικό στοιχείο της G έχει τάξη 2, τότε η G είναι αβελιανή.*

Απόδειξη. Επειδή $o(x) = 2$, $\forall x \in G \setminus \{e\}$, έπεται ότι $x^2 = e$ και άρα

$$\forall x \in G: \quad x^{-1} = x$$

Έστω τώρα ότι $x, y \in G$. Τότε

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

και άρα η G είναι αβελιανή. ■

Μπορούμε τώρα να αποδείξουμε το Θεώρημα 3.7.1:

Απόδειξη. (*του Θεωρήματος 3.7.1*) Θα διακρίνουμε περιπτώσεις:

[20] Σ' αυτή την περίπτωση θα έχουμε ότι $\forall x \in G: \ x = x^{-1}$, και επομένως $\forall x \in G: \ x^2 = x \cdot x = e$.

1. Αν η G περιέχει ένα στοιχείο τάξης $2p$, τότε προφανώς η G είναι κυκλική και άρα ισόμορφη[21] με την κυκλική ομάδα $\mathbb{Z}_{2p}$.

2. Υποθέτουμε ότι η G δεν έχει κανένα στοιχείο τάξης $2p$.

   (α') Αν $p=2$, τότε $o(G)=4$, και επειδή η G δεν είναι κυκλική η G θα είναι ισόμορφη με την ομάδα του Klein V_4 η οποία συμπίπτει με την D_2.

   (β') Έστω $p>2$. Τότε p είναι περιττός και επομένως $4\nmid 2p=o(G)$.

   i. Αν όλα τα στοιχεία της G (εκτός του ταυτοτικού) έχουν τάξη 2, τότε από το Λήμμα 3.7.5 η G είναι αβελιανή και τότε από το Λήμμα 3.7.2 έπεται ότι η G έχει ως υποομάδα μια ομάδα ισόμορφη με την ομάδα του Klein η οποία έχει τάξη 4, κάτι το οποίο είναι άτοπο διότι $4\nmid 2p=o(G)$.

   ii. Επομένως δεν έχουν όλα τα στοιχεία της G τάξη 2. Έτσι, αν a είναι ένα στοιχείο της G, θα είναι: $o(a)=1,2,p$, ή $2p$. Οι περιπτώσεις $o(a)=1,2,2p$, έχουν αποκλειστεί και άρα, η G περιέχει ένα στοιχείο a τάξης p.

   Θεωρούμε την κυκλική υποομάδα $H=\langle a\rangle$ της G η οποία παράγεται από το a. Προφανώς $[G:H]=2$, και άρα η H έχει ακριβώς δύο διακεκριμένα αριστερά σύμπλοκα στην G: H και bH, και τότε:

$$G=H\cup bH,\qquad \text{όπου}\qquad b\in G\setminus H\qquad \text{και}\qquad H\cap bH=\emptyset$$

   Ισχυρισμός: $b^2=e$.

   Πραγματικά: $b^2\in H\cup bH$. Αν $b^2\in bH$, τότε $b^2=bh$, $h\in H$ και τότε $b=h\in H$, που είναι άτοπο. Άρα $b^2\in H$ και άρα $b^2=a^k$ για κάποιο $k\in\mathbb{Z}$. Αν $k\neq 0$, τότε η κυκλική υποομάδα $\langle b\rangle$ η οποία παράγεται από το b θα περιέχει την H αφού το στοιχείο $b^2=a^k$ θα την παράγει, και το $b\notin H$, και άρα η $\langle b\rangle$ θα περιέχει τουλάχιστον $p+1$ στοιχεία. Επειδή $o(H)=2p$, έπεται ότι $\langle b\rangle=G$ και άρα η G είναι κυκλική, το οποίο είναι άτοπο.

   Άρα δείξαμε ότι κάθε στοιχείο $b\in G\setminus H$ έχει τάξη $o(b)=2$.

   Θεωρούμε το στοιχείο $bab\in G$. Τότε θα έχουμε:

$$b^2=e\implies b^{-1}=b\implies bab=b^{-1}ab\implies o(bab)=o(b^{-1}ab)=o(a)=p$$

   Τότε όμως

$$b^{-1}ab=bab=a^k\qquad \text{για κάποιο}\qquad k\in\mathbb{Z}^+ \tag{†}$$

   και επομένως:

$$a=bbabb=ba^kb=(bab)^k=(a^k)^k=a^{k^2}\implies a^{k^2-1}=e$$

   Επειδή $o(a)=p$ είναι ένας πρώτος αριθμός, έπεται ότι

$$p\mid k^2-1\implies p\mid (k+1)(k-1)\implies p\mid k+1\quad \text{ή}\quad p\mid k-1$$

   Α'. Αν $p\mid k-1$, τότε θα έχουμε $k-1=pr$, για κάποιο $r\geq 1$, και άρα $k=pr+1$. Τότε από την σχέση (†) θα έχουμε:

$$bab=a^k=a^{pr+1}=(a^p)^r a^1=e^r a=a$$

   Τότε όμως θα έχουμε $bab=a$ και άρα $babb=ab\implies ba=ab$. Επειδή $o(a)=p$ και $o(b)=2$ και $(2,p)=1$, θα έχουμε ότι το στοιχείο ab έχει τάξη $o(ab)=2p$, κάτι το οποίο είναι άτοπο.

   Β'. Επομένως $p\mid k+1$, και τότε θα έχουμε $k+1=ps$, για κάποιο $s\geq 1$, και άρα $k=ps-1$. Τότε από την σχέση (†) θα έχουμε:

$$bab=a^k=a^{ps-1}=(a^p)^s a^{-1}=e^r a^{-1}=a^{-1}$$

[21] Εδώ χρησιμοποιούμε ότι δύο κυκλικές ομάδες με την ίδια τάξη είναι ισόμορφες, βλέπε το Θεώρημα 4.1.21 του επόμενου Κεφαλαίου.

Συνοψίζοντας την δεύτερη περίπτωση, θα έχουμε ότι η G περιέχει δύο στοιχεία a, b έτσι ώστε:

$$a, b \in G: \quad a^p = e = b^2 \qquad \text{και} \qquad bab = b^{-1}ab = a^{-1}$$

Τότε όμως, σύμφωνα με τη συζήτηση που προηγήθηκε του Θεωρήματος 3.7.1, η G είναι ισόμορφη με την διεδρική ομάδα D_p.

Προφανώς οι ομάδες $\mathbb{Z}_{2p}$ και D_p δεν είναι ισόμορφες διότι, για παράδειγμα, η $\mathbb{Z}_{2p}$ είναι αβελιανή και η D_p δεν είναι αβελιανή. ■

Το Θεώρημα 3.7.1 μας εξασφαλίζει ότι υπάρχουν μόνο δύο, δομικά διαφορετικές ομάδας τάξης $6, 10, 14, 22, \cdots$: η κυκλική ομάδα τάξης $6, 10, 14, 22, \cdots$, και η ομάδα συμμετριών του κανονικού τριγώνου, πενταγώνου, επταγώνου, εντεκαγώνου, $\cdots$.

3.7.2 Ομάδες τάξης pq

Γενικότερα ενδιεφερόμαστε για ομάδες G τάξης pq όπου p, q είναι πρώτοι αριθμοί. Αυτή η περίπτωση είναι περισσότερο σύνθετη και χρειαζόμαστε περισσότερες γνώσεις για να την αναλύσουμε. Όταν όμως η ομάδα G είναι αβελιανή, τότε έχουμε το ακόλουθο αποτέλεσμα το οποίο περιγράφει πλήρως την G όταν $p \neq q$:

Θεώρημα 3.7.6. *Έστω G μια ομάδα με τάξη pq, όπου p, q είναι διακεκριμένοι πρώτοι αριθμοί: $p \neq q$. Αν η G είναι αβελιανή, τότε η G είναι κυκλική.*

Απόδειξη. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $p > q$. Αν υπάρχει στοιχείο τάξης pq στην G, τότε προφανώς η G είναι κυκλική.

Υποθέτουμε ότι η G δεν έχει κανένα στοιχείο τάξης pq, και θα οδηγηθούμε σε άτοπο.

Έστω $e \neq a \in G$. Τότε $\mathsf{o}(a) \mid pq$ και άρα $\mathsf{o}(a) = p$ ή q ή pq. Επειδή έχουμε υποθέσει ότι η G δεν έχει στοιχείο τάξης pq, θα έχουμε:

$$\forall a \in G \setminus \{e\}: \quad \mathsf{o}(a) = p \quad \text{ή} \quad q$$

1. Έστω ότι η G έχει ένα στοιχείο a τάξης p. Τότε θα έχουμε την υποομάδα $H = \langle a \rangle$ της G τάξης p. Από το Πόρισμα 3.6.5 έπεται ότι η H είναι η μοναδική υποομάδα τάξης p της G.

   Επομένως, για κάθε $b \in G \setminus H$, θα έχουμε ότι η υποομάδα $K = \langle b \rangle$ έχει τάξη q. Πραγματικά, αν $\mathsf{o}(K) = p$, τότε θα πρέπει $H = K$ και άρα $b \in H$, το οποίο είναι άτοπο. Άρα, επειδή η G δεν έχει στοιχείο τάξης pq, έπεται ότι $\mathsf{o}(K) = q$.

   Για ένα τέτοιο στοιχείο $b \in G \setminus H$ τάξης q, θεωρούμε το στοιχείο ab. Τότε: $\mathsf{o}(ab) \neq 1$, διότι διαφορετικά: $ab = e$ και άρα $b = a^{-1} \in H$, το οποίο είναι άτοπο. Αν $\mathsf{o}(ab) = p$, τότε, όπως και πριν, $\langle a \rangle = \langle ab \rangle$ και άρα $ab = a^k$ το οποίο δίνει $b = a^{k-1} \in H$ το οποίο είναι άτοπο. Άρα $\mathsf{o}(ab) = q$, και επομένως $(ab)^q = e$. Επειδή η G είναι αβελιανή, και επειδή $\mathsf{o}(b) = q$, θα έχουμε:

   $$(ab)^q = a^q b^q = e \implies a^q = e$$

   το οποίο είναι άτοπο διότι $\mathsf{o}(a) = p > q$. Άρα σ' αυτή την περίπτωση καταλήξαμε σε άτοπο.

2. Έστω ότι η G δεν έχει κανένα στοιχείο τάξης p. Τότε όλα τα στοιχεία της G εκτός του ταυτοτικού έχουν τάξη q.

   Έστω $e \neq a \in G$ και έστω $H = \langle a \rangle$. Τότε $\mathsf{o}(a) = q$. Διαλέγουμε ένα στοιχείο $b \in G \setminus H$ και θέτουμε $K = \langle b \rangle$. Τότε $\mathsf{o}(H) = q = \mathsf{o}(K)$.

   Επειδή η G είναι αβελιανή έπεται άμεσα ότι το υποσύνολο $HK = KH$ είναι μια υποομάδα της G, και επομένως, επειδή προφανώς $\mathsf{o}(HK) > 1$, θα έχουμε:

   $$\mathsf{o}(HK) \in \{p, q, pq\}$$

Αν $o(HK) = p$, τότε η HK είναι κυκλική και άρα η G έχει ένα στοιχείο τάξης p το οποίο είναι άτοπο. Άρα $o(HK) = q$ ή pq. Όμως από την Πρόταση 3.6.3, θα έχουμε:

$$o(HK) = \frac{o(H)\,o(K)}{o(H \cap K)} = \frac{q^2}{o(H \cap K)} = q \quad \text{ή} \quad pq$$

Επομένως:

$$o(H \cap K)p = q \quad \text{ή} \quad o(H \cap K) = q$$

Όμως η περίπτωση $o(H \cap K)p = q$ οδηγεί στο άτοπο $p \leq q$. Άρα μένει η περίπτωση $o(H \cap K) = q$. Όμως, επειδή $K \supseteq H \cap K \subseteq H$ και $o(K) = o(H \cap K) = q = o(H)$ έπεται ότι $H \cap K = H$ και $H \cap K = K$. Τότε όμως $H = K$, κατι το οποίο είναι άτοπο διότι $K = \langle b \rangle$, όπου $b \neq H = \langle a \rangle$.

Άρα η μόνη δυνατή περίπτωση είναι η G να διαθέτει ένα στοιχείο τάξης $pq = |G|$ και τότε προφανώς η G είναι κυκλική. ■

Με χρήση περισσότερο προχωρημένων εργαλείων αποδεικνύονται τα ακόλουθα γενικότερα αποτελέσματα τα οποία περιγράφουν πλήρως τις ομάδες τάξης pq, όπου p, q είναι διακεκριμένοι πρώτοι αριθμοί:

Θεώρημα 3.7.7. *Έστω G μια ομάδα τάξης pq, όπου p, q είναι πρώτοι αριθμοί, έτσι ώστε: $p < q$.*

1. *Η G είναι κυκλική αν:*
   - *(α΄) είτε η G είναι αβελιανή,*
   - *(β΄) ή $p \nmid q - 1$.*
2. *Αν η G είναι μη αβελιανή, και $p \mid q - 1$, τότε η G παράγεται από ένα στοιχείο a τάξης p και ένα στοιχείο b τάξης q, έτσι ώστε: $a^{-1}ba = b^r$, όπου $q \mid r^p - 1$:*

$$G = \langle a, b \;\mid\; a^p = e = b^q \quad \text{και} \quad a^{-1}ba = b^r \quad \text{όπου} \quad q \mid r^p - 1 \rangle \quad \blacksquare$$

Τι συμβαίνει αν $p = q$;

Θεώρημα 3.7.8. *Έστω G μια ομάδα τάξης p^2, όπου p είναι ένας πρώτος αριθμός. Τότε:*

1. *Η G είναι αβελιανή.*
2. *Η G είναι ισόμορφη με μια από τις ακόλουθες μη ισόμορφες ομάδες:*

$$\mathbb{Z}_{p^2} \qquad \text{ή} \qquad \mathbb{Z}_p \times \mathbb{Z}_p \quad \blacksquare$$

Για περισσότερες λεπτρομέρειες παραπέμπουμε στα βιβλία [26], [31], και [16].

3.8 Εφαρμογές του Θεωρήματος Lagrange στη Θεωρία Αριθμών

Στην παρούσα ενότητα θα δούμε μια άλλη κατηγορία εφαρμογών του Θεωρήματος του Lagrange στη Θεωρία Αριθμών. Ιδιαίτερα θα αποδείξουμε, με χρήση θεωρίας ομάδων, τα θεωρήματα των Euler, Fermat, και Wilson από την στοιχειώδη Θεωρία Αριθμών.

Πρώτα υπενθυμίζουμε ότι η **συνάρτηση ϕ του Euler** ορίζεται ως εξής:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = \left|\{k \in \mathbb{N} \mid 1 \leq k \leq n \;\text{ και }\; (n,k) = 1\}\right|$$

Υπενθυμίζουμε επίσης ότι, αν $a, b \in \mathbb{Z}$, και $n \geq 1$, τότε

$$a \equiv b \bmod n \iff n \mid a - b \iff [a]_n = [b]_n$$

όπου η τελευταία ισότητα νοείται στην προσθετική ομάδα $\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$.

Πρόταση 3.8.1 (Θεώρημα Euler). *Έστω $n \geq 1$ και $a \in \mathbb{Z}$ με $(a,n) = 1$. Τότε:*

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Απόδειξη. Η ζητούμενη σχέση γράφεται ισοδύναμα στο σύνολο $\mathbb{Z}_n$:

$$[a^{\varphi(n)}]_n = ([a]_n)^{\varphi(n)} = [1]_n$$

Επειδή $(a,n) = 1$, έπεται οτι $[a]_n \in \mathsf{U}(\mathbb{Z}_n)$. Επειδή, βλέπε Παράδειγμα 3.2.6, η πολλαπλασιαστική ομάδα $\mathsf{U}(\mathbb{Z}_n)$ έχει τάξη $\varphi(n)$, από την Πρόταση 3.4.7 έπεται το ζητούμενο: $([a]_n)^{\varphi(n)} = [1]_n$. ■

Πόρισμα 3.8.2 (Μικρό Θεώρημα Fermat). [22] *Έστω p ένας πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$. Τότε:*

$$a^{p-1} \equiv 1 \bmod (p)$$

Απόδειξη. Επειδή p είναι πρώτος, έπεται ότι $\varphi(p) = p-1$ και $(a,p) = 1$. Τότε το αποτέλεσμα προκύπτει από το Θεώρημα του Euler 3.8.1. ■

Πρόταση 3.8.3 (Θεώρημα Wilson). [23] *Για έναν θετικό ακέραιο $p \geq 2$, τα ακόλουθα είναι ισοδύναμα:*

1. *Ο αριθμός p είναι πρώτος.*
2. $(p-1)! \equiv -1 \bmod p$.

Απόδειξη. (α) Αν $p = 2$, τότε ο αριθμός p είναι πρώτος και πράγματι ισχύει $2 \mid (2-1)! + 1 = 2$.

(β) Υποθέτουμε ότι $p \geq 3$.

1. $\Longrightarrow$ **2.** Υποθέτουμε ότι ο αριθμός p είναι πρώτος, και άρα ο p είναι περιττός διότι $p \geq 3$. Θεωρούμε την ομάδα $\mathsf{U}(\mathbb{Z}_p)$ των αντιστρέψιμων κλάσεων υπολοίπων mod p με πράξη τον πολλαπλασιασμό. Τότε $[1]_p \neq [-1]_p$, διότι διαφορετικά $p \mid 2$ και άρα $p = 2$, το οποίο είναι άτοπο διότι $p \geq 3$. Θα έχουμε

$$\mathsf{U}(\mathbb{Z}_p) = \{[1]_p, [2]_p, \cdots, [p-1]_p\}$$

και $|\mathsf{U}(\mathbb{Z}_p)| = \phi(p) = p-1$. Έστω $[x]_p$ ένα στοιχείο της $\mathsf{U}(\mathbb{Z}_p)$ έτσι ώστε $[x]_p^2 = [1]_p$. Τότε:

$$[x]_p^2 = [1]_p \implies [x^2]_p = [1]_p \implies p \mid x^2 - 1 \implies p \mid (x-1)(x+1) \implies$$

$$\implies p \mid x-1 \text{ ή } p \mid x+1 \implies [x]_p = [1]_p \text{ ή } [x]_p = [-1]_p = [p-1]_p$$

Επομένως το μόνο στοιχείο τάξης 2 στην $\mathsf{U}(\mathbb{Z}_p)$ είναι το $[-1]_p$. Ισοδύναμα το μόνο στοιχείο $[x]_p$ στην $\mathsf{U}(\mathbb{Z}_p)$, εκτός του ταυτοτικού $[1]_p$, το οποίο συμπίπτει με το αντίστροφό του $[x]_p^{-1}$, δηλαδή έχουμε $[x]_p = [x]_p^{-1}$, είναι το $[-1]_p = [p-1]_p$. Τότε όμως στο γινόμενο όλων των στοιχείων της ομάδας $\mathsf{U}(\mathbb{Z}_p)$

$$[1]_p \cdot [2]_p \cdots [p-1]_p = [1 \cdot 2 \cdots (p-1)]_p = [(p-1)!]_p$$

τα στοιχεία $[2]_p, \cdots, [p-2]_p$ εμφανίζονται ως ζεύγη $\{[x]_p, [x]_p^{-1}\}$ και $[x]_p \neq [x]_p^{-1}$, και επομένως δεν συνεισφέρουν στο παραπάνω γινόμενο παρά μόνο το ουδέτερο στοιχείο. Άρα:

$$[(p-1)!]_p = [1]_p \cdot [2]_p \cdots [p-1]_p = [1]_p \cdot [p-1]_p = [p-1]_p = [-1]_p$$

Άρα $[(p-1)!]_p = [-1]_p$ και επομένως $(p-1)! \equiv -1 \bmod p$.

[22] Pierre de Fermat (17 Αυγούστου 1601 - 12 Ιανουαρίου 1665) [http://en.wikipedia.org/wiki/Pierre_de_Fermat]: Γάλλος δικηγόρος και ερασιτέχνης μαθηματικός με σημαντική συμβολή κυρίως στη Θεωρία Αριθμών, αλλά και στον Διαφορικό/Ολοκληρωτικό Λογισμό.

[23] John Wilson (6 Αυγούστου 1741 - 18 Οκτωβρίου 1793) [http://en.wikipedia.org/wiki/John_Wilson_(mathematician)]: Βρεττανός μαθηματικός, γνωστός κυρίως για το ομώνυμο Θεώρημα, αν και η πρώτη απόδειξή του οποίου οφείλεται στον Lagrange.

2. $\Longrightarrow$ **1.** Αν ο p δεν είναι πρώτος, τότε $p = a \cdot b$, όπου $1 < a, b < p$. Επειδή $a \leq p-1$, θα έχουμε $a \mid (p-1)!$, και επειδή $a \mid p$, και $p \mid (p-1)!+1$, θα έχουμε και $a \mid (p-1)!+1$. Τότε όμως $a \mid ((p-1)!+1-(p-1)!)$, δηλαδή $a \mid 1$ και $a = 1$. Αυτό είναι άτοπο διότι $a > 1$. Άρα ο p είναι πρώτος. ■

Θα δούμε επιπρόσθετες εφαρμογές της Θεωρίας Ομάδων στη Θεωρία Αριθμών σε ασκήσεις, καθώς και σε μεταγενέστερα Κεφάλαια, ιδιαίτερα στο επόμενο Κεφάλαιο, στο οποίο αναλύεται η δομή των κυκλικών ομάδων, π.χ. παραπέμπουμε στην απόδειξη του Θεωρήματος του Gauss 4.1.2.

3.9 Ασκήσεις

Άσκηση 3.9.1. *Να βρεθεί η τάξη του στοιχείου a της ομάδας $(G, \star)$, όπου*

1. $a = [4]_9$, $(G, \star) = (\mathsf{U}(\mathbb{Z}_9), \cdot)$,

2. $a = [x]_{12}$, $(G, \star) = (\mathsf{U}(\mathbb{Z}_{12}), \cdot)$,

3. $a = \omega_{36}^{17}$, $(G, \star) = (\mathsf{U}_{36} = \langle \zeta_{36} \rangle, \cdot)$,

4. $a = -i$, $(G, \star) = (\mathbb{C}^\star, \cdot)$,

5. $a = -1 + i\sqrt{3}$, $(G, \star) = (\mathbb{C}^\star, \cdot)$,

6. $a = (-1 + i\sqrt{3})/2$, $(G, \star) = (\mathbb{C}^\star, \cdot)$,

7. $\cos(2\pi/7) + i\sin(2\pi/7)$, $(G, \star) = (\mathbb{C}^\star, \cdot)$.

8. $a = [2]_3$, $(G, \star) = (\mathbb{Z}_3, +)$,

9. $a = [6]_{10}$, $(G, \star) = (\mathbb{Z}_{10}, +)$,

10. $a = [6]_{15}$, $(G, \star) = (\mathbb{Z}_{15}), +)$,

11. $a = [10]_{12}$, $(G, \star) = (\mathbb{Z}_{12}), +)$,

12. $a = [77]_{210}$, $(G, \star) = (\mathbb{Z}_{210}), +)$,

13. $a = [40]_{210}$, $(G, \star) = (\mathbb{Z}_{210}), +)$,

14. $a = [70]_{210}$, $(G, \star) = (\mathbb{Z}_{210}), +)$.

Άσκηση 3.9.2. **1.** *Να βρεθεί το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle [25]_{30} \rangle$ της ομάδας $(\mathbb{Z}_{30}, +)$.*

2. *Να βρεθεί το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle [30]_{42} \rangle$ της ομάδας $(\mathbb{Z}_{42}, +)$.*

3. *Να βρεθεί το πλήθος των στοιχείων των κυκλικών υποομάδων $\langle i \rangle$ και $\langle 3i \rangle$ της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$ των μη μηδενικών μιγαδικών αριθμών.*

4. *Να βρεθεί το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle 1 + i \rangle$ της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$ των μη μηδενικών μιγαδικών αριθμών.*

Άσκηση 3.9.3. **1.** *Να βρεθεί το πλήθος των γεννητόρων μιας κυκλικής ομάδας με τάξη:* 5, 8, 12, 60.

2. *Να βρεθούν οι πρωταρχικές n-οστές ρίζες της μονάδας για $n = 4$, $n = 17$, $n = 24$, και $n = 31$.*

3. *Να βρεθούν όλοι οι γεννήτορες των ομάδων $(\mathbb{Z}_{10}, +)$, $(\mathbb{Z}_{12}, +)$ και $(\mathbb{Z}_{15}, +)$.*

Άσκηση 3.9.4. *Έστω $(G, \cdot)$ μια ομάδα και $a, b \in G$ δύο στοιχεία της έτσι ώστε $G = \langle \{a, b\} \rangle$, δηλαδή η ομάδα G παράγεται από τα στοιχεία a, b.*

1. *Αν ισχύει ότι: $a^2 = b^2 = (a \cdot b)^2 = e$, να βρεθεί η τάξη της ομάδας G.*
   Με ποια γνωστή ομάδα είναι τότε ισόμορφη η G;
2. *Αν ισχύει ότι: $a^3 = b^2 = (a \cdot b)^3 = e$, να βρεθεί η τάξη της ομάδας G.*
3. *Αν ισχύει ότι: $a \cdot b^2 = b^3 \cdot a$ και $b \cdot a^3 = a^2 \cdot b$, να βρεθεί η τάξη της ομάδας G.*

Άσκηση 3.9.5. *Έστω* $(\mathsf{U}(\mathbb{Z}_n),\cdot)$ *η πολλαπλασιαστική ομάδα των αντιστρέψιμων κλάσεων υπολοίπων* mod n. *Να εξετασεί αν η* $(\mathsf{U}(\mathbb{Z}_n)$ *είναι κυκλική, όταν:* $n = 8, 12, 14, 17$.

Άσκηση 3.9.6. *Έστω* G *μια πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας* $(\mathbb{C}^*,\cdot)$, *αντίστοιχα της πολλαπλασιαστικής ομάδας του κύκλου* $\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\}$. *Να δειχθεί ότι η* G *είναι κυκλική.*

Άσκηση 3.9.7. **1.** *Έστω* p *και* q *πρώτοι αριθμοί, και έστω* G *μια κυκλική ομάδα τάξης* pq. *Να βρεθεί το πλήθος των γεννητόρων της* G, *καθώς και το διάγραμμα Hasse των υποομάδων της.*

2. *Έστω* p *ένας πρώτος αριθμός, και* G *μια κυκλική ομάδα τάξης* p^r, *όπου* $r \geq 1$. *Να βρεθεί το πλήθος των γεννητόρων της* G, *καθώς και το διάγραμμα Hasse των υποομάδων της.*

Άσκηση 3.9.8. *Θεωρούμε την ομάδα* Q *των τετρανίων του Hamilton, δηλαδή την υποομάδα της* $\mathsf{GL}(2,\mathbb{C})$ *η οποία αποτελείται από τους ακόλουθους πίνακες:*

$$Q = \{\pm I_2,\ \pm I,\ \pm J,\ \pm K\}$$

όπου:

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Να σχεδιαστεί το διάγραμμα Hasse των υποομάδων της Q.

Άσκηση 3.9.9. *Να σχεδιασθεί το διάγραμμα Hasse των υποομάδων της εναλλάσσουσας ομάδας* A_4.

Άσκηση 3.9.10. *Έστω* $(G,\cdot)$ *μια ομάδα και υποθέτουμε ότι κάθε στοιχείο της έχει τάξη* ≤ 2. *Να δειχθεί ότι η* G *είναι αβελιανή. Να δειχθεί επίσης ότι υπάρχουν μη αβελιανές ομάδες κάθε στοιχείο των οποίων έχει τάξη* $\leq n$, *όπου* $n = 3, 4$.

Άσκηση 3.9.11. *Να δειχθεί ότι κάθε πεπερασμένη ομάδα άρτιας τάξης περιέχει τουλάχιστον ένα στοιχείο τάξης* 2.

Άσκηση 3.9.12. *Έστω* $G = \{g_1 = e, g_2, \cdots, g_n\}$ *μια πεπερασμένη αβελιανή ομάδα.*

1. *Να δειχθεί ότι:* $(g_1 g_2 \cdots g_n)^2 = e$.

2. *Να δειχθεί με δύο τρόπους ότι,* $\forall g \in G$: $g^n = e$.

3. *Ποια επιπροσθετη πληροφορία αποκτούμε αν η τάξη της* G *είναι περιττός αριθμός;*

Άσκηση 3.9.13. *Έστω* $(G,\cdot)$ *μια πεπερασμένη αβελιανή ομάδα,* $G = \{g_1, g_2, \cdots, g_n\}$.

1. *Να δειχθεί ότι αν η* G *περιέχει ακριβώς ένα στοιχείο* x *τάξης* 2, *τότε:* $x = g_1 g_2 \cdots g_n$.

2. *Να δειχθεί ότι αν η* G *περιέχει περισσότερα από ένα στοιχεία τάξης* 2, *τότε:* $g_1 g_2 \cdots g_n = e$.

Άσκηση 3.9.14. *Να δειχθεί ότι κάθε ομάδα τάξης* p^n, *όπου* p *είναι ένας πρώτος αριθμός, περιέχει ένα στοιχείο, και άρα μια (κυκλική) υποομάδα, τάξης* p.

Άσκηση 3.9.15. *Έστω* $(G,\cdot)$ *μια πεπερασμένη ομάδα. Αν κάθε μη ταυτοτικό στοιχείο της* G *έχει τάξη* 2, *να δειχθεί ότι η τάξη της* G *είναι δύναμη του* 2.[24]

[24] Παράδειγμα τέτοιας ομάδας, αποτελεί η ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (n-παράγοντες).

Άσκηση 3.9.16. *Να δειχθεί ότι κάθε πεπερασμένη ομάδα G με τάξη $o(G) \leq 5$ είναι αβελιανή.*

Άσκηση 3.9.17. *Δείξτε ότι υπάρχουν ακριβώς δύο μη ισόμορφες ομάδες τάξης 4 ή 6.*

Άσκηση 3.9.18. *Να σχεδιαστεί το διάγραμμα Hasse των υποομάδων μιας ομάδας G με τάξη $|G| \leq 7$.*

Άσκηση 3.9.19. *Να εξεταστεί ποιες από τις ομάδες $U(\mathbb{Z}_n)$, όπου $1 \leq n \leq 15$ είναι κυκλικές. Σε περίπτωση κατά την οποία η ομάδα $U(\mathbb{Z}_n)$ είναι κυκλική να βρεθούν όλοι οι γεννήτορές της.*

Άσκηση 3.9.20. *Έστω $(G_i, \cdot)$, $1 \leq i \leq 3$, τρεις κυκλικές ομάδες τάξης 2. Να βρεθούν όλες οι υποομάδες της ομάδας ευθύ γινόμενο $G = G_1 \times G_2 \times G_3$.*

Άσκηση 3.9.21.

1. *Να δειχθεί ότι η ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών εφοδιασμένη με τη συνήθη πράξη της πρόσθεσης ρητών αριθμών δεν είναι κυκλική ομάδα.*
2. *Να δειχθεί ότι η ομάδα των πραγματικών αριθμών $(\mathbb{R}, +)$ εφοδιασμένη με τη συνήθη πράξη της πρόσθεσης πραγματικών αριθμών δεν είναι κυκλική ομάδα.*

Άσκηση 3.9.22. *Έστω $n \geq 2$ ένας σταθερός φυσικός αριθμός και $(G, \cdot)$ η ομάδα ευθύ γινόμενο $\prod_{k\in\mathbb{N}} G_k = G_1 \times G_2 \times \cdots$, όπου G_k είναι η προσθετική ομάδα $(\mathbb{Z}_n, +)$, $\forall k \in \mathbb{N}$. Να δειχθεί ότι η ομάδα ευθύ γινόμενο G είναι άπειρη, αλλά κάθε στοιχείο της έχει πεπερασμένη τάξη $\leq n$. Γενικότερα να δειχθεί ότι η ομάδα ευθύ γινόμενο $\prod_{k\in\mathbb{N}} G_k$, όπου $G_k = G$, $\forall k \in \mathbb{N}$, είναι μια ομάδα πεπερασμένης τάξης, είναι μια άπειρη ομάδα κάθε στοιχείο της οποίας έχει πεπερασμένη τάξη $\leq o(G)$.*

Άσκηση 3.9.23. *Να δειχθεί ότι μια ομάδα η οποία έχει πεπερασμένο πλήθος υποομάδων είναι πεπερασμένη ομάδα.*

Άσκηση 3.9.24. *Να δειχθούν τα ακόλουθα:*

1. *Κάθε πεπερασμένη ομάδα είναι ομάδα στρέψης.*
2. *Κάθε άπειρη κυκλική ομάδα είναι ομάδα ελεύθερης στρέψης.*
3. *Να δοθεί παράδειγμα μεικτής ομάδας.*
4. *Υπάρχουν ομάδες στρέψης με άπειρη τάξη.*
5. *Κάθε ομάδα η οποία ικανοποιεί την συνθήκη φθίνουσας αλυσίδας*[25] *είναι ομάδα στρέψης.*

Άσκηση 3.9.25. *Να βρεθεί η τάξη των ακόλουθων στοιχείων:*

$$x = \left((1\,2\,3),\ [5]_{12},\ [14]_{20},\ \frac{-1+i\sqrt{3}}{2}\right) \in S_3 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{C}^*$$

$$y = \left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ (1\,2\cdots p)\right) \in GL(2,\mathbb{R}) \times S_p$$

όπου p είναι ένας πρώτος αριθμός $\neq 2$.

[25] Υπενθυμίζουμε ότι μια ομάδα G ικανοποιεί τη *συνθήκη φθίνουσας αλυσίδας* αν, για κάθε φθίνουσα ακολουθία

$$\cdots \leq H_{n+1} \leq H_n \leq \cdots \leq H_2 \leq H_1$$

υποομάδων της G, υπάρχει $k \geq 1$ έτσι ώστε: $H_k = H_{k+r}$, $\forall r \geq 1$.

Άσκηση 3.9.26. *Έστω $(G,\cdot)$ μια αβελιανή ομάδα. Δείξτε ότι για κάθε φυσικό αριθμό $n \in \mathbb{N}$ το υποσύνολο*

$$G_n = \{x \in G \mid o(x) \mid n\}$$

είναι μια υποομάδα της G. Ισχύει το συμπέρασμα αν η ομάδα G δεν είναι απαραίτητα αβελιανή;

Άσκηση 3.9.27. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και H μια υποομάδα της G.*

1. *Να δειχθεί ότι για κάθε $x \in G$, υπάρχει θετικός ακέραιος k έτσι ώστε: $x^k \in H$.*
2. *Αν $x \in G$ και m_x είναι ο μικρότερος θετικός ακέραιος k έτσι ώστε $x^k \in H$, να δειχθεί ότι $m_x \mid o(x)$.*

Άσκηση 3.9.28. *Έστω $G = \langle a \rangle$ μια άπειρη κυκλική ομάδα. Τότε:*

1. $$\langle a^n \rangle \cdot \langle a^m \rangle = \langle a^{(m,n)} \rangle$$
2. $$\langle a^n \rangle \bigcap \langle a^m \rangle = \langle a^{[n,m]} \rangle$$

Να εξεταστεί αν ισχύουν οι παραπάνω σχέσεις, όταν η κυκλική ομάδα G είναι πεπερασμένη.

Άσκηση 3.9.29. *Για κάθε φυσικό αριθμό n, έστω η ομάδα U_n των n-οστών ριζών της μονάδας, θεωρούμενη ως υποομάδα της ομάδας T του κύκλου. Αν $n \neq m$, να περιγράψετε τις υποομάδες $\mathsf{U}_n \cap \mathsf{U}_m$ και $\mathsf{U}_n \cdot \mathsf{U}_m$.*

Άσκηση 3.9.30. *Αν $n, m,$ είναι φυσικοί αριθμοί, να περιγραφούν οι υποομάδες $n\mathbb{Z} \cap m\mathbb{Z}$ και $n\mathbb{Z} + m\mathbb{Z}$ της προσθετικής ομάδας $(\mathbb{Z},+)$.*

Άσκηση 3.9.31. *Έστω $(G,\cdot)$ μια ομάδα η οποία διαθέτει ακριβώς ένα στοιχείο a με τάξη 2. Να δειχθεί ότι το a ανήκει στο κέντρο $\mathsf{Z}(G)$ της G.*

Άσκηση 3.9.32. *Βρείτε όλα τα σύμπλοκα (πλευρικές κλάσεις) της υποομάδας $H \leq G$ της ομάδας G στις ακόλουθες περιπτώσεις: (α) $H = 6\mathbb{Z} \leq \mathbb{Z} = G$, (β) $H = 8\mathbb{Z} \leq 4\mathbb{Z} = G$, (γ) $H = \langle [14]_{36} \rangle \leq \mathbb{Z}_{36} = G$.*

Άσκηση 3.9.33. *Να βρεθούν όλα τα αριστερά σύμπλοκα της υποομάδας H στην ομάδα G στις ακόλουθες περιπτώσεις, όπου T είναι η ομάδα του κύκλου $\{z \in \mathbb{Z} \mid |z| = 1\}$, και $\mathbb{R}^{>0}$ η πολλαπλασιαστική ομάδα των θετικών πραγματικών αριθμών:*

1. *$H = \mathbb{R}$ και $G = (\mathbb{C},+)$.*
2. *$H = \mathbb{Z}$ και $G = (\mathbb{R},+)$.*
3. *$H = \mathsf{T}$ και $G = (\mathbb{C}^*,\cdot)$.*
4. *$H = \mathbb{R}^{>0}$ και $G = (\mathbb{C}^*,\cdot)$.*
5. *$H = \mathsf{U}_n$ και $G = (\mathbb{C}^*,\cdot)$.*
6. *$H = \mathsf{U}_n$ και $G = (\mathsf{T},\cdot)$.*

Άσκηση 3.9.34.

1. *Να βρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα) της υποομάδας $\langle 5 \rangle = 5\mathbb{Z}$ στην ομάδα $(\mathbb{Z},+)$.*
2. *Να βρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα) της υποομάδας $\langle 9 \rangle = 9\mathbb{Z}$ στην ομάδα $(\mathbb{Z},+)$ και της $\langle 9 \rangle = 9\mathbb{Z}$ στην (υπο)ομάδα $\langle 3 \rangle = 3\mathbb{Z}$ της $(\mathbb{Z},+)$.*
3. *Να βρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα) της υποομάδας $\langle [6]_{12} \rangle$ στην ομάδα $(\mathbb{Z}_{12},+)$ και της $\langle [6]_{12} \rangle$ στην (υπο)ομάδα $\langle [2]_{12} \rangle$ της $(\mathbb{Z}_{12},+)$.*

Άσκηση 3.9.35. *Θεωρούμε τις ακόλουθες (κυκλικές) υποομάδες της* S_3*:*

$$H = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle \quad \text{και} \quad K = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$$

Να βρεθούν οι δεξιές και αριστερές πλευρικές κλάσεις των υποομάδων H, K *στην* S_3.

Άσκηση 3.9.36. *Θεωρούμε τη διεδρική ομάδα* $(\mathsf{D}_4, \cdot)$ *των συμμετριών του τετραγώνου, και έστω* τ *μια συμμετρία του τετραγώνου η οποία προκύπτει από ανάκλαση ως προς άξονα συμμετρίας που κείται επί του επιπέδου του τετραγώνου. Να βρεθούν τα αριστερά και δεξιά σύμπλοκα της υποομάδας* $\langle \tau \rangle$ *στην* D_4.

Άσκηση 3.9.37. *Έστω* G *μια ομάδα και* X *ένα μη κενό υποσύνολο της* G. *Να εξεταστεί αν το* X *μπορεί να είναι ταυτόχρονα δεξιό σύμπλοκο δύο διακεκριμένων υποομάδων της* G.

Άσκηση 3.9.38. *Έστω η συμμετρική ομάδα* S_4 *και*

$$H = \{\sigma \in \mathsf{S}_4 \mid \sigma(3) = 3\} \quad \text{και} \quad K = \{\sigma \in \mathsf{S}_4 \mid \sigma(4) = 4\}$$

Να δειχθεί ότι τα υποσύνολα H *και* K *είναι υποομάδες της* S_4 *και ακολούθως να υπολογιστούν τα αριστερά σύμπλοκα των* K *και* $H \cap K$ *στην* S_4, *καθώς και οι δείκτες* $[\mathsf{S}_4 : K]$, $[\mathsf{S}_4 : H \cap K]$ *και* $[K : H \cap K]$.

Άσκηση 3.9.39. *Να βρεθεί ο δείκτης* $[\mathsf{S}_n : H]$, *όπου*

$$H = \{\sigma \in \mathsf{S}_n \mid \sigma(n) = n\}$$

Άσκηση 3.9.40. *Έστω ότι* $(G, \cdot)$ *είναι μια ομάδα και ότι* $H \leq G$ *είναι μια υποομάδα της.*

1. *Να δοθεί παράδειγμα ομάδας* $(G, \cdot)$ *και υποομάδας* H *της* G, *έτσι ώστε* $a \in G$ *και* $aH \neq Ha$.
2. *Να δειχθεί ότι, αν μια ομάδα* $(G, \cdot)$ *είναι αβελιανή, τότε για κάθε* $a \in G$ *ισχύει:* $aH = Ha$. *Να εξεταστεί αν ισχύει το αντίστροφο.*

Άσκηση 3.9.41. 1. *Βρείτε του δείκτη* $[G : H]$ *της υποομάδας* $H \leq G$ *στις ακόλουθες περιπτώσεις:*

   (α) $H = n\mathbb{Z}$ *και* $G = \mathbb{Z}$.

   (β) $H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$ *και* $G = \mathbb{R} \times \mathbb{R}$.

2. *Βρείτε μια υποομάδα* H *της πολλαπλασιαστικής ομάδας* $(\mathbb{R}^*, \cdot)$ *έτσι ώστε:* $[\mathbb{R}^* : H] = 2$.

Άσκηση 3.9.42. *Έστω* H *μια γνήσια υποομάδα της προσθετικής ομάδας* $(\mathbb{Q}, +)$. *Να εξεταστεί αν* $[\mathbb{Q} : H] < \infty$.

Έστω $P(x_1, x_2, \cdots, x_n)$ ένα πολυώνυμο n-μεταβλητών με πραγματικούς συντελεστές, και έστω το ακόλουθο σύνολο μεταθέσεων

$$\mathsf{S}(P) = \{\sigma \in \mathsf{S}_n \mid P(x_{\sigma(1)}, x_{\sigma(2)}, \cdots, x_{\sigma(n)}) = P(x_1, x_2, \cdots, x_n)\}$$

Άσκηση 3.9.43. *Με τους παραπάνω συμβολισμούς, να δειχθεί ότι για κάθε πολυώνυμο* n*-μεταβλητών* $P(x_1, x_2, \cdots, x_n)$, *το υποσύνολο* $\mathsf{S}(P)$ *είναι μια υποομάδα της συμμετρικής ομάδας* S_n.

Άσκηση 3.9.44. 1. *Αν* $P(x_1, x_2, x_3) = x_1^2 + x_1x_2x_3 + x_3^2$, *να βρεθεί η υποομάδα* $\mathsf{S}(P)$, *ο δείκτης της* $\mathsf{S}(P)$ *στην* S_3, *και να περιγραφούν τα αριστερά σύμπλοκα της* $\mathsf{S}(P)$ *στην* S_3.

2. *Αν* $P(x_1,x_2,x_3,x_4) = x_1x_2 + x_3x_4$, *να βρεθεί η υποομάδα* $\mathsf{S}(P)$, *ο δείκτης της* $\mathsf{S}(P)$ *στην* S_4, *και να περιγραφούν τα αριστερά σύμπλοκα της* $\mathsf{S}(P)$ *στην* S_4.

Άσκηση 3.9.45. *Έστω* $\mathsf{GL}(2,\mathbb{R})$ *η ομάδα των αντιστρέψιμων* 2×2 *πινάκων με στοιχεία πραγματικούς αριθμούς, και θεωρούμε τα ακόλουθα υποσύνολά της:*[26]

$$G = \left\{X_{a,b} \in \mathsf{M}_2(\mathbb{R}) \mid a,b \in \mathbb{R} \;\&\; a \neq 0\right\} \qquad \text{και} \qquad H = \left\{X_{1,b} \in \mathsf{M}_2(\mathbb{R}) \mid b \in \mathbb{R}\right\}$$

όπου

$$X_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

1. *Δείξτε ότι:* $H \leq G \leq \mathsf{GL}(2,\mathbb{R})$.

2. *Δείξτε ότι:* $\forall A \in G$: $A \cdot H = H \cdot A$.

3. *Περιγράψτε το σύνολο πηλίκο* G/H.

Άσκηση 3.9.46. *Έστω* $(G,\cdot)$ *μια ομάδα και* H, K *δύο πεπερασμένες υποομάδες της* G, *έτσι ώστε* $(\mathsf{o}(H),\mathsf{o}(K)) = 1$. *Να δειχθεί ότι, αν η ομάδα* G *είναι αβελιανή, ή γενικότερα αν* $HK = KH$, *τότε το υποσύνολο* HK *είναι μια υποομάδα της* G *με τάξη* $\mathsf{o}(HK) = \mathsf{o}(H)\cdot\mathsf{o}(K)$.

Άσκηση 3.9.47. *Να δειχθεί ότι μια ομάδα τάξης* 30 *μπορεί να περιέχει το πολύ* 7 *υποομάδες τάξης* 5.

Άσκηση 3.9.48. *Έστω* $(G,\cdot)$ *μια ομάδα τάξης* $2p$, *όπου* p *είναι ένας περιττός πρώτος. Να δειχθεί ότι η* G *περιέχει μια υποομάδα* H *με δείκτη* $[G:H] = 2$.

Άσκηση 3.9.49. *Έστω* H *και* K *δύο υποομάδες μιας ομάδας* $(G,\cdot)$, *και υποθέτουμε ότι* $K \subseteq H \subseteq G$. *Να δείξετε ότι ο δείκτης* $[G:K]$ *της* K *στην* G *είναι πεπερασμένος αν και μόνο αν οι δείκτες* $[G:H]$ *της* H *στην* G *και* $[H:K]$ *της* K *στην* H *είναι πεπερασμένοι, και τότε ισχύει ότι:*

$$[G:K] = [G:H]\cdot[H:K]$$

Άσκηση 3.9.50. *Έστω ότι* $(G,\cdot)$ *είναι μια ομάδα και* H *και* K *είναι δύο υποοομάδες της* G.

1. *Να δειχθεί ότι, αν* $[G:K] < \infty$, *τότε* $[H:H\bigcap K] < \infty$ *και* $[H:H\bigcap K] \leq [G:K]$.
2. *Να δειχθεί ότι, αν* $[G:K] < \infty$, *τότε* $[H:H\bigcap K] = [G:K]$ *αν και μόνο αν* $G = HK$.
3. *Να δειχθεί ότι, αν* $[G:K] < \infty$ *και* $[G:H] < \infty$, *τότε* $[G:H\bigcap K] \leq [G:H]\cdot[G:K]$ *και η ισότητα ισχύει αν και μόνο αν* $G = HK$.

Άσκηση 3.9.51. *Έστω ότι* $(G,\cdot)$ *είναι μια ομάδα και* H *και* K *είναι δύο υποοομάδες της* G. *Υποθέτουμε ότι* $[G:K] < \infty$ *και* $[G:H] < \infty$. *Αν* $\big([G:K],[G:H]\big) = 1$, *να δειχθεί ότι* $G = HK$.

Άσκηση 3.9.52. *Έστω ότι* $(G,\cdot)$ *είναι μια ομάδα και* H *και* K *είναι δύο κανονικές υποοομάδες της* G. *Υποθέτουμε ότι* $[G:K] < \infty$, $[G:H] < \infty$ *και* $H\bigcap K = \{e\}$. *Να δειχθεί η ομάδα* G *είναι το (εσωτερικό) ευθύ γινόμενο των υποομάδων* H *και* K *αν και μόνο αν* $|G| = [G:H]\cdot[G:K]$.

[26] Η ομάδα G καλείται η *ομοπαραλληλική ομάδα* των 2×2 αντιστρέψιμων πινάκων υπεράνω του $\mathbb{R}$.

Άσκηση 3.9.53. *Έστω $G = G_1 \times G_2$ η ομάδα ευθύ γινόμενο των πεπερασμένων ομάδων G_1 καί G_2. Να δείχθεί ότι η ομάδα G είναι κυκλική αν και μόνο αν οι ομάδες G_1 και G_2 είναι κυκλικές και $(|G_1|, |G_2|) = 1$.*

Να εξετάσετε αν το παραπάνω συμπέρασμα ισχύει για την ομάδα ευθυ γινόμενο $G = \prod_{k=1}^{n} G_k$ πεπερασμένων ομάδων G_k, $1 \leq k \leq n$, όπου $n \geq 3$.

Άσκηση 3.9.54. *Σύμφωνα με την παραπάνω Άσκηση 3.9.53, αν G_1 και G_2 είναι πεπερασμένες κυκλικές ομάδες, τότε η ομάδα ευθύ γινόμενο $G_1 \times G_2$ είναι κυκλική αν και μόνο αν $(|G_1|, |G_2|) = 1$. Να δειχθεί γενικότερα ότι: η ομάδα ευθύ γινόμενο $G_1 \times G_2$, όπου οι G_1, G_2 είναι τυχούσες ομάδες, είναι κυκλική αν και μόνο αν:*

1. *είτε οι ομάδες G_1 και G_2 είναι πεπερασμένες και $(|G_1|, |G_2|) = 1$,*
2. *είτε μία εκ των ομάδων G_1, G_2 είναι η τετριμμένη ομάδα.*

Ιδιαίτερα το ευθύ γινόμενο δύο άπειρων κυκλικών ομάδων δεν είναι ποτέ κυκλική ομάδα.

Άσκηση 3.9.55. *Μια ομάδα $(G, \cdot)$ καλείται* **μονοσειραϊκή** *(uniserial) αν ικανοποιεί την παρακάτω ιδιότητα:*[27]

$$\text{αν} \quad H \leq G \quad \& \quad K \leq G \quad \text{είναι τυχούσες υποομάδες της } G, \text{ τότε:} \quad \text{είτε} \quad H \subseteq K \quad \text{είτε} \quad K \subseteq H$$

Να δειχθεί ότι οι μονοσειραϊκές ομάδες είναι ακριβώς οι πεπερασμένες κυκλικές ομάδες με τάξη δύναμη ενός πρώτου αριθμού.

Άσκηση 3.9.56. **1.** *Να δειχθεί ότι υπάρχει στοιχείο $[a]_{41} \in \mathsf{U}(\mathbb{Z}_{41})$ έτσι ώστε: $[a]_{41}^2 = [-1]_{41}$.*

2. *Αν p είναι ένας πρώτος αριθμός της μορφής $4n+3$, να δειχθεί ότι δεν υπάρχει στοιχείο $[a]_p \in \mathsf{U}(\mathbb{Z}_p)$ έτσι ώστε $[a]_p^2 = [-1]_p$.*

Άσκηση 3.9.57. *Να εξεταστεί αν οι προσθετικές ομάδες $(\mathbb{R}, +)$ και $(\mathbb{C}, +)$ περιέχουν γνήσια υποομάδα με πεπερασμένο δείκτη.*

Άσκηση 3.9.58. *Έστω η ομάδα ευθύ γινόμενο $G = \prod_{k=1}^{n} G_k$ των ομάδων $(G_k, \cdot)$, $1 \leq k \leq n$. Να δειχθεί ότι η ομάδα G είναι ομάδα ελεύθερης στρέψης αν και μόνο αν η ομάδα G_k είναι ομάδα ελεύθερης στρέψης, για κάθε $k = 1, 2, \cdots, n$.*

Άσκηση 3.9.59. *Έστω p ένας πρώτος αριθμός.*

1. *Να δείξετε ότι, $\forall n \geq 0$, η ομάδα U_{p^n} των p^n-οστών ριζών της μονάδας, είναι υποομάδα της p-οστής ομάδας Prüfer $\mathbb{Z}(p^\infty)$,*[28] *και ισχύει:*

$$\mathsf{U}_{p^0} \subseteq \mathsf{U}_{p^1} \subseteq \mathsf{U}_{p^2} \subseteq \cdots \subseteq \mathsf{U}_{p^n} \subseteq \mathsf{U}_{p^{n+1}} \subseteq \cdots$$

2. *Να δειχθεί ότι:*

$$\mathbb{Z}(p^\infty) = \bigcup_{n \geq 0} \mathsf{U}_{p^n}$$

3. *Να δειχθεί ότι κάθε πεπερασμένη υποομάδα της p-οστής ομάδας Prüfer $\mathbb{Z}(p^\infty)$ είναι κυκλική.*

4. *Είναι η ομάδα $\mathbb{Z}(p^\infty)$ κυκλική;*

Άσκηση 3.9.60. *Έστω p ένας πρώτος αριθμός και έστω*

$$\mathbb{Q}_p = \left\{ \frac{m}{p^n} \in \mathbb{Q} \mid m, n \in \mathbb{Z} \right\}$$

1. *Να δειχθεί ότι το υποσύνολο $\mathbb{Q}_p$ είναι υποομάδα της προσθετικής ομάδας $(\mathbb{Q}, +)$.*

2. *Να δειχθεί ότι η ομάδα $\mathbb{Q}_p$ περιέχει την ομάδα των ακεραίων $\mathbb{Z}$ ως υποομάδα και το σύνολο πηλίκο $\mathbb{Q}_p/\mathbb{Z}$ είναι σε «1-1» και «επί» αντιστοιχία με την p-οστή ομάδα Prüfer $\mathbb{Z}(p^\infty)$.*

---

[27] Ένα μερικώς διατεταγμένο σύνολο $(X, \preccurlyeq)$ καλείται *ολικώς διατεταγμένο* ή *αλυσίδα*, αν: $\forall x, y \in X$: είτε $x \preccurlyeq y$ είτε $y \preccurlyeq x$. Έτσι μια ομάδα $(G, \cdot)$ είναι μονοσειραϊκή αν και μόνο αν το μερικώς διατεταγμενο σύνολο $(\mathsf{Sub}(G), \leq)$ των υποομάδων της G, όπου «≤» είναι η σχέση υποομάδας, είναι ολικώς διατεταγμένο.

[28] Υπενθυμίζουμε ότι: $\mathbb{Z}(p^\infty) = \{ z \in \mathbb{C} \mid z^{p^n} = 1, \text{ για κάποιο } n \in \mathbb{Z}^+ \} \subseteq \mathsf{T}$, όπου T είναι η ομάδα του κύκλου.

Κεφάλαιο 4

Η Δομή των Κυκλικών Ομάδων

Στο παρόν Κεφάλαιο θα μελετήσουμε την κλάση των κυκλικών ομάδων, η οποία είναι η απλούστερη μη τετριμμένη κλάση ομάδων. Ιδιαίτερα θα ταξινομήσουμε τις κυκλικές ομάδες σε κλάσεις ισομορφίας, θα περιγράψουμε τις υποομάδες τους, καθώς και τα επαγόμενα διαγράμματα Hasse, και τέλος θα αποδείξουμε διάφορους χαρακτηρισμούς κυκλικών ομάδων οι οποίοι είναι χρήσιμοι σε άλλες περιοχές των Μαθηματικών. Στο Κεφάλαιο 6 θα περιγράψουμε όλους τους ομομορφισμούς μεταξύ κυκλικών ομάδων.

4.1 Ταξινόμηση Κυκλικών Ομάδων και των Υποομάδων τους

Στην παρούσα ενότητα θα ταξινομήσουμε τις κυκλικές ομάδες, τις υποομάδες τους, και τους γεννήτορές τους. Οι ταξινομήσεις αυτές θα βασιστούν στην αριθμητική των θετικών ακεραίων αριθμών.

Απο τώρα και στο εξής σταθεροποιούμε μια κυκλική ομάδα

$$G = \langle a \rangle$$

με γεννήτορα το στοιχείο $a \in G$.

Το ακόλουθο αποτέλεσμα δείχνει ότι οι κυκλικές ομάδες συμπεριφέρονται καλά ως προς τις υποομάδες.

Θεώρημα 4.1.1. *Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική ομάδα.*

Απόδειξη. Έστω όπως παραπάνω ότι $G = \langle a \rangle$ είναι μια κυκλική ομάδα, και έστω $H \leq G$ μια υποομάδα της G.

- Αν $H = \{e\}$, τότε προφανώς $H = \langle e \rangle$ και η H είναι κυκλική.
- Έστω $H \neq \{e\}$, και επομένως υπάρχει $g \in H \setminus \{e\}$. Θα έχουμε $g = a^k$ για κάποιο $k \in \mathbb{Z}$. Τότε $k \neq 0$ διότι διαφορετικά $g = a^0 = e$, το οποίο είναι άτοπο. Αν $k < 0$, τότε, επειδή η H είναι υποομάδα θα έχουμε ότι $g^{-1} = (a^k)^{-1} = a^{-k} \in H$ και $-k > 0$. Επομένως η υποομάδα H περιέχει *θετικές* δυνάμεις a^k, $k > 0$, του γεννήτορα a της G. Αυτό σημαίνει ότι το σύνολο φυσικών αριθμών

$$\{k \in \mathbb{N} \mid a^k \in H\}$$

είναι μη κενό και επομένως από την Αρχή Καλής Διάταξης έχει ελάχιστο στοιχείο. Έστω $n = \min\{k \in \mathbb{N} \mid a^k \in H\}$ το ελάχιστο στοιχείο του παραπάνω συνόλου, δηλαδή n είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $a^n \in H$. Θα δείξουμε ότι:

$$H = \langle a^n \rangle$$

Επειδή $a^n \in H$ και η H είναι υποομάδα, έπεται ότι $\langle a^n \rangle \subseteq H$. Έστω $h \in H$. Τότε $h = a^m$, για κάποιο $m \in \mathbb{Z}$. Από την Ευκλείδεια Διαίρεση θα έχουμε τότε:

$$m = nq + r, \qquad 0 \leq r < n$$

και επομένως:

$$a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r \quad \Longrightarrow \quad a^r = (a^n)^{-q}a^m$$

Επειδή εκ κατασκευής $a^n \in H$, θα έχουμε $(a^n)^{-q} \in H$. Επιπλέον, επειδή $a^m \in H$, θα έχουμε $a^r = (a^n)^{-q}a^m \in H$ διότι η H είναι υποομάδα. Επειδή n είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $g^n \in H$, και επειδή $a^r \in H$, όπου $0 \le r < n$, έπεται ότι αναγκαστικά: $r = 0$. Επομένως

$$h = a^m = a^{nq} = (a^n)^q \ \in \ \langle a^n \rangle$$

Συμπεραίνουμε ότι $H \subseteq \langle a^n \rangle$. Άρα $H = \langle a^n \rangle$ και επομένως η H είναι κυκλική. ■

4.1.1 Υποομάδες και Γεννήτορες Άπειρων Κυκλικών Ομάδων

Στην παρούσα υποενότητα υποθέτουμε ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι άπειρης τάξης, ή ισοδύναμα ο γεννήτορας a έχει άπειρη τάξη: $o(a) = \infty$. Τότε:

$$G = \langle a \rangle = \{\cdots, a^{-n}, \ \cdots \ a^{-2}, a^{-1}, a, a^2, \cdots, a^n, \cdots\}$$

Θεώρημα 4.1.2. *Έστω G μια άπειρη κυκλική ομάδα.*

1. *Η G έχει μόνο δύο γεννήτορες: αν a είναι ένας γεννήτορας, τότε ο μοναδικός διαφορετικός γεννήτορας της G είναι ο a^{-1}.*
2. *Αν $G = \langle a \rangle$, τότε οι υποομάδες της G είναι οι ακόλουθες και μόνο αυτές:*

$$H \le G \iff H = \langle a^n \rangle, \ \ n \ge 0$$

$$\cdots, \ \ \langle a^n \rangle, \ \ \langle a^{n-1} \rangle, \ \ \cdots, \ \ \langle a^2 \rangle, \ \ \langle a \rangle = G, \ \ \langle a^0 \rangle = \{e\}$$

3. *Αν $H_n = \langle a^n \rangle$ και $H_m = \langle a^m \rangle$ είναι δύο υποομάδες της $G = \langle a \rangle$, τότε:*

$$H_n \subseteq H_m \iff m \mid n \quad \text{και} \quad H_n = H_m \iff m = n$$

Απόδειξη. 1. Έστω a ένας γεννήτορας της G, δηλαδή $G = \langle a \rangle$. Αν b είναι ένας άλλος γεννήτορας της G, δηλαδή $G = \langle b \rangle$, τότε θα έχουμε $b = a^k$ για κάποιο $n \in \mathbb{Z}$, και τότε:

$$\langle a \rangle = \langle a^n \rangle$$

Άρα $a \in \langle a^n \rangle$ και επομένως $a = (a^n)^k = a^{nk}$ για κάποιο $k \in \mathbb{Z}$. Τότε όμως θα έχουμε:

$$a = a^{nk} \ \Longrightarrow \ aa^{-nk} = e \ \Longrightarrow \ a^{1-nk} = e \ \Longrightarrow \ 1 - nk = 0$$

διότι το ατοιχείο a έχει άπειρη τάξη. Έτσι $1 = nk$. Επειδή όμως $n, k \in \mathbb{Z}$, θα έχουμε ότι είτε $n = k = 1$, ή $n = k = -1$. Στην πρώτη περίπτωση $b = a^n = a$ και στην δεύτερη περίπτωση $b = a^n = a^{-1}$.

2. Έστω $H \le G$ μια υποομάδα της G. Από το Θεώρημα 4.1.1 έπεται ότι η H είναι κυκλική και επομένως $H = \langle a^n \rangle$. Μπορούμε να υποθέσουμε ότι $n \ge 0$, διότι, αν $n \le 0$, τότε από το μέρος 1. έπεται ότι $H = \langle (a^n)^{-1} \rangle = \langle a^{-n} \rangle$ και $-n \ge 0$. Επομένως δείξαμε ότι η H είναι υποομάδα της G αν και μόνο αν η H είναι της μορφής $H = \langle a^n \rangle$, $n \ge 0$, και έτσι μένει να δείξουμε ότι:

$$\forall n, m \ge 0, \quad n \ne m \ \Longrightarrow \ \langle a^n \rangle \ne \langle a^m \rangle$$

Υποθέτουμε ότι η παραπάνω συνεπαγωγή δεν είναι αληθής και θα καταλήξουμε σε άτοπο. Θα έχουμε:

$$\langle a^n \rangle = \langle a^m \rangle \ \Longrightarrow \ a^n \in \langle a^m \rangle \ \ \text{και} \ \ a^m \in \langle a^n \rangle \ \Longrightarrow \ \exists \ k, l \in \mathbb{Z}: \ a^n = a^{mk} \ \ \text{και} \ \ a^m = a^{nl} \ \Longrightarrow$$

$$\Longrightarrow \ a^{n-mk} = e = a^{m-nl}$$

Επειδή ο γεννήτορας a της G έχει άπειρη τάξη, έπεται ότι:

$$n-mk=0=m-nl \implies n=mk \text{ και } m=nl \implies n\mid m \text{ και } m\mid n \implies n=m$$

Άρα οι διακεκριμένες υποομάδες της G είναι οι εξής: $H_n=\langle a^n\rangle,\ \forall n\geq 0$.

3. Έστω $H_n=\langle a^n\rangle\subseteq H_m=\langle a^m\rangle$. Τότε, όπως είδαμε και στο μέρος 2., θα έχουμε: $a^n\in\langle a^m\rangle$ και τότε $m\mid n$. Αντίστροφα, αν $m\mid n$, τότε $n=mk$ για κάποιο $k\in\mathbb{Z}$ και τότε $a^n=a^{mk}=(a^m)^k\in\langle a^m\rangle$. Αυτό όμως σημαίνει ότι $H_n=\langle a^n\rangle\subseteq H_m=\langle a^m\rangle$. Τέλος αν $n,m\geq 1$, τότε $H_n=H_m$ αν και μόνο αν $n\mid m$ και $m\mid n$ αν και μόνο αν $n=m$. ■

Ως άμεση συνέπεια έχουμε την ακόλουθη ταξινόμηση των υποομάδων και των γεννητόρων μιας άπειρης κυκλικής ομάδας.

Πόρισμα 4.1.3. *Έστω $G=\langle a\rangle$ μια άπειρη κυκλική ομάδα. Τότε οι απεικόνισεις*

$$\Phi:\mathbb{N}_0\longrightarrow\{\textit{Υποομάδες της } G\},\quad \Phi(n)=\langle a^n\rangle$$

$$\Psi:\{1,-1\}\longrightarrow\{\textit{Γεννήτορες της } G\},\quad \Psi(k)=\langle a^n\rangle$$

είναι «1-1» και «επί». Επιπλέον: $m\mid n \iff \Phi(n)\subseteq\Phi(m)$.

Υπενθυμίζουμε ότι η τομή $H\cap K$ υποομάδων H,K μιας ομάδας $(G,\cdot)$ είναι υποομάδα, και το γινόμενο HK των H, K είναι υποομάδα, όταν η G είναι αβελιανή ή γενικότερα αν ισχύει: $HK=KH$. Στην περίπτωση κατά την οποία η G είναι (άπειρη) κυκλική, άρα αβελιανή, και οι ομάδες $H\cap K$ και HK θα είναι κυκλικές, σύμφωνα με το Θεώρημα 4.1.1.

Η επόμενη Πρόταση δίνει ακριβείς πληροφορίες γι' αυτές τις κυκλικές υποομάδες.

Πρόταση 4.1.4. *Έστω $G=\langle a\rangle$ μια άπειρη κυκλική ομάδα.*

1.
$$\langle a^n\rangle\cdot\langle a^m\rangle=\langle a^{(m,n)}\rangle$$

2.
$$\langle a^n\rangle\bigcap\langle a^m\rangle=\langle a^{[n,m]}\rangle$$

Απόδειξη. 1. Έστω $d=(m,n)$. Τότε

$$d\mid n \implies n=dk \qquad \text{και} \qquad d\mid m \implies n=dl, \qquad \text{όπου} \qquad k,l\in\mathbb{Z}$$

και επομένως:

$$a^n=a^{dk}=(a^d)^k\in\langle a^d\rangle \qquad \text{και} \qquad a^m=a^{dl}=(a^d)^l\in\langle a^d\rangle$$

Άρα

$$a^n\in\langle a^d\rangle\ni a^m \implies \langle a^n\rangle\subseteq\langle a^d\rangle\supseteq\langle a^m\rangle$$

Επειδή η $\langle a^d\rangle$ είναι υποομάδα, προφανώς θα έχουμε ότι

$$\langle a^n\rangle\cdot\langle a^m\rangle\subseteq\langle a^d\rangle \tag{$*$}$$

Από την άλλη πλευρά, επειδή $d=(m,n)$, έπεται ότι υπάρχουν ακέραιοι $r,s\in\mathbb{Z}$, έτσι ώστε $d=nr+ms$. Τότε:

$$a^d=a^{nr+ms}=a^{nr}a^{ms}=(a^n)^r(a^m)^s\in\langle a^n\rangle\cdot\langle a^m\rangle$$

Αυτό όμως σημαίνει ότι

$$\langle a^d\rangle\subseteq\langle a^n\rangle\cdot\langle a^m\rangle \tag{$**$}$$

Από τις σχέσεις $(*)$ και $(**)$, θα έχουμε: $\langle a^n\rangle\cdot\langle a^m\rangle=\langle a^d\rangle$.

2. Έστω $\delta = [m,n]$. Τότε:

$$\delta = mk = nl \implies a^\delta = a^{nl} = (a^n)^l \in \langle a^n\rangle \qquad \text{και} \qquad a^\delta = a^{mk} = (a^m)^k \in \langle a^m\rangle$$

Επομένως $a^\delta \in \langle a^n\rangle \cap \langle a^m\rangle$ το οποίο προφανώς σημαίνει ότι:

$$\langle a^\delta\rangle \subseteq \langle a^n\rangle \cap \langle a^m\rangle \tag{†}$$

Αντίστροφα, έστω $x \in \langle a^n\rangle \cap \langle a^m\rangle$. Τότε $x = (a^n)^p$ και $x = (a^m)^q$, όπου $p,q \in \mathbb{Z}$. Επομένως, χρησιμοποιώντας ότι το στοιχείο a έχει άπειρη τάξη, θα έχουμε:

$$x = (a^n)^p = (a^m)^q \implies a^{np} = a^{mq} \implies a^{np-mq} = e \implies np = mq$$

Θέτοντας $t := np = mq$, θα έχουμε ότι: $x \in \langle a^t\rangle$. Επιπλέον $m \mid t$ και $n \mid t$. Τότε όμως $\delta \mid t$, και επομένως από το Θεώρημα 5.2 θα έχουμε:

$$x \in \langle a^t\rangle \subseteq \langle a^\delta\rangle$$

το οποίο σημαίνει ότι:

$$\langle a^n\rangle \cap \langle a^m\rangle \subseteq \langle a^\delta\rangle \tag{††}$$

Από τις σχέσεις (†) και (††), θα έχουμε: $\langle a^n\rangle \cap \langle a^m\rangle = \langle a^\delta\rangle$. ■

Παρατήρηση 4.1.5. Αν η κυκλική ομάδα G έχει δοθεί με προσθετικό συμβολισμό, τότε το Θεώρημα 4.1.2, το Πόρισμα 4.1.3, και η Πρόταση 4.1.4 παίρνουν την ακόλουθη μορφή. Έστω $(G,+)$ μια άπειρη προσθετική κυκλική ομάδα.

1. Η G έχει μόνο δύο γεννήτορες: αν a είναι ένας γεννήτορας, τότε ο μοναδικός διαφορετικός γεννήτορας της G είναι ο $-a$.
2. Αν $G = \langle a\rangle$, τότε οι υποομάδες της G είναι οι ακόλουθες και μόνο αυτές:

$$H \leq G \iff H = \langle na\rangle, \quad n \geq 0$$

$$\cdots, \quad \langle na\rangle, \quad \langle (n-1)a\rangle, \quad \cdots, \quad \langle 2a\rangle, \quad \langle a\rangle = G, \quad \langle 0a\rangle = \{0\}$$

3. Αν $H_n = \langle na\rangle$ και $H_m = \langle ma\rangle$ είναι δύο υποομάδες της $G = \langle a\rangle$, τότε:

$$H_n \subseteq H_m \iff m \mid n \quad \& \quad H_n = H_m \iff m = n$$

4. $$\langle na\rangle + \langle ma\rangle = \langle (n,m)a\rangle$$

5. $$\langle na\rangle \bigcap \langle ma\rangle = \langle [n,m]a\rangle \quad ▲$$

Συνοψίζουμε τα παραπάνω αποτελέσματα εφαρμοσμένα στην άπειρη κυκλική (προσθετική) ομάδα $(\mathbb{Z},+)$.

Παράδειγμα 4.1.6. Θεωρούμε την άπειρη κυκλική ομάδα $(\mathbb{Z},+)$. Όπως θα δούμε αργότερα στο Θεώρημα 4.1.21, κάθε άλλη άπειρη κυκλική ομάδα είναι ισόμορφη, δηλαδή δομικά ίδια, με την ομάδα $(\mathbb{Z},+)$.

1. Οι μόνοι γεννήτορες της $(\mathbb{Z},+)$ είναι το 1 και το -1.
2. Οι διακεκριμένες υποομάδες της $(\mathbb{Z},+)$ είναι οι εξής

$$n\mathbb{Z} = \{nz \in \mathbb{Z} \mid z \in \mathbb{Z}\}, \qquad \forall n \geq 0$$

3. $$n\mathbb{Z} \leq m\mathbb{Z} \iff m \mid n$$

4. $$n\mathbb{Z} \bigcap m\mathbb{Z} = [n,m]\mathbb{Z} \qquad \text{και} \qquad n\mathbb{Z} + m\mathbb{Z} = (n,m)\mathbb{Z} \quad \surd$$

4.1.2 Υποομάδες και Γεννήτορες Πεπερασμένων Κυκλικών Ομάδων

Σκοπός μας είναι να αποδείξουμε ένα Θεώρημα για πεπερασμένες κυκλικές ομάδες το οποίο να είναι ανάλογο με το Θεώρημα 4.1.2 για άπειρες κυκλικές ομάδες. Για την διατύπωση και απόδειξη αυτού του ανάλογου αποτελέσματος, Θα χρειαστούμε μια σειρά από βοηθητικές προτάσεις.

Στην παρούσα υποενότητα υποθέτουμε ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι πεπερασμένης τάξης: $\mathrm{o}(G) = n$, ή ισοδύναμα ο γεννήτορας a έχει πεπερασμένη τάξη $\mathrm{o}(a) = n$. Τότε:

$$G = \langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$$

Λήμμα 4.1.7. *Έστω $H = \langle a^m \rangle$ μια υποομάδα της $G = \langle a \rangle$, όπου $\mathrm{o}(a) = n$. Τότε:*

$$H = \langle a^d \rangle, \quad \text{όπου} \quad d = (n, m) \quad \text{και} \quad \mathrm{o}(H) = \mathrm{o}(a^m) = \frac{n}{d}$$

Απόδειξη. Επειδή $d = (n, m)$, θα έχουμε $m = dk$ και τότε:

$$a^m = a^{dk} = (a^d)^k \in \langle a^d \rangle \quad \Longrightarrow \quad \langle a^m \rangle \subseteq \langle a^d \rangle$$

Επίσης, επειδή $d = (n, m)$, θα έχουμε $d = nx + my$ για κάποια $x, y \in \mathbb{Z}$. Τότε, επειδή $\mathrm{o}(a) = n$:

$$a^d = a^{nx+my} = a^{nx} a^{my} = (a^n)^x (a^m)^y = e^x (a^m)^y = (a^m)^y \in \langle a^m \rangle \implies a^d \in \langle a^m \rangle \implies \langle a^d \rangle \subseteq \langle a^m \rangle$$

Από τις παραπάνω σχέσεις βλέπουμε ότι $\langle a^m \rangle = \langle a^d \rangle$. Τέλος, χρησιμοποιώντας το Θεώρημα 3.2.2, θα έχουμε:

$$\mathrm{o}(H) = \mathrm{o}(\langle a^m \rangle) = \mathrm{o}(a^m) = \frac{\mathrm{o}(a)}{(\mathrm{o}(a), m)} = \frac{n}{(n, m)} = \frac{n}{d}$$ ■

Λήμμα 4.1.8. *Έστω $G = \langle a \rangle$, όπου $\mathrm{o}(a) = n$, και $r, s \geq 1$. Τότε:*

$$\langle a^r \rangle = \langle a^s \rangle \quad \Longleftrightarrow \quad (n, r) = (n, s)$$

Απόδειξη. «$\Longrightarrow$» Θα έχουμε:

$$\langle a^r \rangle = \langle a^s \rangle \implies \mathrm{o}(a^r) = \mathrm{o}(a^s) \iff \frac{\mathrm{o}(a)}{(\mathrm{o}(a), r)} = \frac{\mathrm{o}(a)}{(\mathrm{o}(a), s)} \iff \frac{n}{(n, r)} = \frac{n}{(n, s)} \iff (n, r) = (n, s)$$

«$\Longleftarrow$» Θα έχουμε όπως και παραπάνω: $(n, r) = (n, s) \implies \mathrm{o}(a^r) = \mathrm{o}(a^s)$. Όμως, χρησιμοποιώντας το Λήμμα 4.1.7, και την υπόθεση $(n, r) = (n, s)$, θα έχουμε:

$$\langle a^r \rangle = \langle a^{(n,r)} \rangle \quad \text{και} \quad \langle a^s \rangle = \langle a^{(n,s)} \rangle \implies \langle a^r \rangle = \langle a^s \rangle$$ ■

Λήμμα 4.1.9. *Έστω $G = \langle a \rangle$, όπου $\mathrm{o}(a) = n$. Το στοιχείο a^m είναι γεννήτορας της G αν και μόνο αν $(m, n) = 1$:*

$$\langle a \rangle = \langle a^m \rangle \iff (n, m) = 1$$

Απόδειξη. Χρησιμοποιώντας το Λήμμα 4.1.8, θα έχουμε:

$$a^m \text{ είναι γεννήτορας της } G \iff \langle a^m \rangle = \langle a \rangle \iff (n, m) = (n, 1) \iff (n, m) = 1$$ ■

Μπορούμε τώρα να αποδείξουμε το ακόλουθο αποτέλεσμα το οποίο είναι ανάλογο του Θεωρήματος 4.1.2.

Θεώρημα 4.1.10. *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης $\mathrm{o}(G) = \mathrm{o}(a) = n$. Τότε:*

1.
$$\text{Σύνολο γεννητόρων της } G = \{a^m \in G \mid (n, m) = 1\}$$
$$\text{Πλήθος γεννητόρων της } G = \varphi(n) = \left|\{m \in \mathbb{N} \mid 1 \leq m \leq n \text{ και } (n, m) = 1\}\right|$$

2. *Τα ακόλουθα είναι ισοδύναμα:*

   (α΄) $m \mid n$.

   (β΄) *Υπάρχει υποομάδα* $H \leq G$ *έτσι ώστε:* $\mathrm{o}(H) = m$.

   Αν $m \mid n$, *τότε υπάρχει μοναδική υποομάδα της* G *με τάξη* m *η οποία είναι η εξής:*

$$H_m = \langle a^{\frac{n}{m}} \rangle$$

3. *Έστω* m, k *δύο διαιρέτες της τάξης* n *της* G, *και έστω* H_m *και* H_k *οι μοναδικές υποομάδες της* G *με τάξεις* m *και* k *αντίστοιχα. Τότε:*

$$H_m \subseteq H_k \iff m \mid k$$

Απόδειξη. 1. Προκύπτει άμεσα από το Λήμμα 4.1.9.

2. Αν υπάρχει υποομάδα H της G με τάξη $\mathrm{o}(H) = m$, τότε από το Θεώρημα του Lagrange έπεται ότι $m \mid \mathrm{o}(G)$ και άρα $m \mid n$.

   Αντίστροφα, αν $m \mid n$, τότε θεωρούμε την υποομάδα $H = \langle a^{\frac{n}{m}} \rangle$ της G. Τότε, επειδή

$$\mathrm{o}(a^{\frac{n}{m}}) = \frac{n}{(n, \frac{n}{m})} = \frac{n}{\frac{n}{m}} = m$$

   έπεται ότι $\mathrm{o}(H) = m$.

   Έστω ότι $m \mid n$ και έστω H_1 και H_2 υποομάδες της G έτσι ώστε: $\mathrm{o}(H_1) = m = \mathrm{o}(H_2)$. Από το Θεώρημα 4.1.1 θα έχουμε

$$H_1 = \langle a^{k_1} \rangle \quad \text{και} \quad H_2 = \langle a^{k_2} \rangle \quad \text{όπου} \quad 1 \leq k_1, k_2 \leq n$$

   Επομένως

$$\frac{n}{(n, k_1)} = \mathrm{o}(a^{k_1}) = \mathrm{o}(H_1) = m = \mathrm{o}(H_2) = \mathrm{o}(a^{k_2}) = \frac{n}{(n, k_2)} \quad \Longrightarrow \quad (n, k_1) = (n, k_2)$$

   Τότε από το Λήμμα 4.1.8 έπεται ότι θα έχουμε $H_1 = \langle a^{k_1} \rangle = \langle a^{k_2} \rangle = H_2$. Άρα, για κάθε διαιρέτη $m \mid n$, υπάρχει μοναδική υποομάδα της G με τάξη m. Από το Λήμμα 4.1.7, η μοναδική υποομάδα είναι η $H_m = \langle a^{\frac{n}{m}} \rangle$.

3. Έστω m, k δύο διαιρέτες της τάξης n της G, και έστω H_m και H_k οι μοναδικές υποομάδες της G με τάξεις m και k αντίστοιχα. Τότε από το μέρος 2. θα έχουμε:

$$H_m \subseteq H_k \iff \langle a^{\frac{n}{m}} \rangle \leq \langle a^{\frac{n}{k}} \rangle \iff \mathrm{o}(a^{\frac{n}{m}}) \mid \mathrm{o}(a^{\frac{n}{k}}) \iff m \mid k$$

■

Το ακόλουθο αποτέλεσμα είναι άμεση συνέπεια του Θεωρήματος 4.1.10.

Πόρισμα 4.1.11. *Έστω* $G = \langle a \rangle$ *μια κυκλική ομάδα τάξης* $\mathrm{o}(G) = \mathrm{o}(a) = n$. *Οι απεικονίσεις*

$$\Phi : \mathscr{D}(n) = \{d \geq 1 \mid d \mid n\} \longrightarrow \{\text{Υποομάδες της } G\}, \quad \Phi(d) = \langle a^{\frac{n}{d}} \rangle$$

$$\Psi : \{k \in \mathbb{N} \mid 1 \leq k \leq n \text{ και } (n, k) = 1\} \longrightarrow \{\text{Γεννήτορες της } G\}, \quad \Psi(k) = \langle a^k \rangle$$

είναι «1-1» και «επί». Επιπλέον: $\mathrm{o}(\Phi(d)) = d$, *και* $d_1 \mid d_2 \iff \Phi(d_1) \subseteq \Phi(d_2)$.

Πόρισμα 4.1.12 (Διαδικασία εύρεσης Υποομάδων Πεπερασμένης Κυκλικής Ομάδας)**.** *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης $\mathrm{o}(G) = \mathrm{o}(a) = n$.*

Υπενθυμίζουμε ότι η αριθμητική συνάρτηση τ ορίζεται ως εξής:

$$\tau : \mathbb{N} \longrightarrow \mathbb{N}, \quad \tau(n) = \sum_{d|n} 1 = \text{ πλήθος διαιρετών του } n$$

- *Υπολογίζουμε τους θετικούς διαιρέτες του n, έστω ότι αυτοί είναι οι εξής: $d_1, d_2, \cdots, d_{\tau(n)}$.*
- *Για κάθε θετικό διαιρέτη $d_i \mid n$ του n, θεωρούμε την κυκλική υποομάδα $H_i := \langle a^{\frac{n}{d_i}} \rangle$ η οποία παράγεται από το στοιχείο $a^{\frac{n}{d_i}}$. Τότε η H_i είναι η μοναδική υποομάδα τάξης d_i της G.*
- *Οι υποομάδες $H_1, H_2, \cdots, H_{\tau(n)}$ είναι όλες οι διακεκριμένες υποομάδες της G:*

Διαιρέτης του n	**Υποομάδα της** G	**Τάξη Υποομάδας**
d_1	$H_1 = \langle a^{\frac{n}{d_1}} \rangle$	d_1
d_2	$H_2 = \langle a^{\frac{n}{d_2}} \rangle$	d_2
$\vdots$	$\vdots$	$\vdots$
$d_{\tau(n)}$	$H_{\tau(n)} = \langle a^{\frac{n}{d_{\tau(n)}}} \rangle$	$d_{\tau(n)}$

- *Ισχύει:*

$$\forall i, j = 1, 2, \cdots, \tau(n): \quad H_i \leq H_j \iff d_i \mid d_j$$

Παράδειγμα 4.1.13. Η κυκλική ομάδα $(\mathbb{Z}_{18}, +) = \langle [1] \rangle = \{[0], [1], [2], \cdots, [17]\}$, όπου $[k] = [k]_{18}$, $0 \leq k \leq 17$.

- Οι διαιρέτες του 18 είναι: $1, 2, 3, 6, 9, 18$ και άρα $\tau(18) = 6$. Επομένως, θα έχουμε ακριβώς 6 υποομάδες $H_1, H_2, H_3, H_4, H_5, H_6$ στην $\mathbb{Z}_{18}$, ακριβώς μια για κάθε διαιρέτη του 18, με τάξη αντίστοιχα: $1, 2, 3, 6, 9, 18$. Αυτές οι υποομάδες περιγράφονται στον ακόλουθο πίνακα:

Διαιρέτης του 18	**Υποομάδα της** G	**Τάξη Υποομάδας**
1	$H_1 = \langle \frac{18}{1}[1] \rangle = \langle 18[1] \rangle = \langle [18] \rangle = \langle [0] \rangle = \{[0]\}$	1
2	$H_2 = \langle \frac{18}{2}[1] \rangle = \langle 9[1] \rangle = \langle [9] \rangle$	2
3	$H_3 = \langle \frac{18}{3}[1] \rangle = \langle 6[1] \rangle = \langle [6] \rangle$	3
6	$H_4 = \langle \frac{18}{6} \rangle = \langle 3[1] \rangle = \langle [3] \rangle$	6
9	$H_5 = \langle \frac{18}{9}[1] \rangle = \langle 2[1] \rangle = \langle [2] \rangle$	9
18	$H_6 = \langle \frac{18}{18}[1] \rangle = \langle [1] \rangle = \mathbb{Z}_{18}$	18

Για παράδειγμα:

$$H_6 = \langle [3] \rangle = \{[3], [6], [9], [12], [15], [0]\}$$

- Οι αριθμοί k με $1 \leq k \leq 18$ και $(18, k) = 1$ είναι

$$\varphi(18) = \varphi(2 \cdot 3^2) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 18 \cdot \frac{1}{2} \cdot \frac{2}{3} = 6$$

Πραγματικά:

$$\{k \in \mathbb{N} \mid 1 \leq k \leq 18 \quad \text{και} \quad (18, k) = 1\} = \{1, 5, 7, 11, 13, 17\}$$

Επομένως οι γεννήτορες της $\mathbb{Z}_{18}$ είναι οι ακόλουθοι:

$$1[1] = [1], \quad 5[1] = [5], \quad 7[1] = [7], \quad 11[1] = [11], \quad 13[1] = [13], \quad 17[1] = [17]$$

- Επειδή μεταξύ των διαιρετών $d = 1, 2, 3, 6, 9, 18$ του 18 έχουμε τις ακόλουθες, εκτός από τις προφανείς $d \mid 18$, σχέσεις διαιρετότητας:

$$2 \mid 6, \quad 3 \mid 6, \quad 3 \mid 9$$

μεταξύ των υποομάδων $H_1, H_2, H_3, H_6, H_9, H_{18}$ θα έχουμε τις ακόλουθες εγκλείσεις (εκτός από τις προφανείς $H_d \leq \mathbb{Z}_{18} = H_{18}$ και $H_1 = \{[0]\} \leq H_d$):

$$H_2 \leq H_6, \qquad H_3 \leq H_6, \qquad H_3 \leq H_9$$

δηλαδή:

$$\langle [9] \rangle \leq \langle [3] \rangle, \qquad \langle [6] \rangle \leq \langle [3] \rangle, \qquad \langle [6] \rangle \leq \langle [2] \rangle \quad \surd$$

Η εκτεθείσα θεωρία μάς επιτρέπει να σχεδιάσουμε το διάγραμμα Hasse κάθε κυκλικής ομάδας. Υπενθυμίζουμε από την υποενότητα 2.4.3, ότι το διάγραμμα Hasse μιας ομάδας G είναι το διάγραμμα Hasse του μερικώς διατεταγμένου συνόλου

$$(\mathsf{Sub}(G), \leq), \quad \text{όπου} \quad \mathsf{Sub}(G) = \{H \leq G\} \text{ είναι το σύνολο των υποομάδων της } G$$

εφοδιασμένο με την σχέση: $H_1 \leq H_2$ αν και μόνο αν η H_1 είναι υποομάδα της H_2 ή ισοδύναμα $H_1 \subseteq H_2$ (δηλαδή στην περίπτωσή μας η σχέση $\leq$ περιορισμένη στο σύνολο $\mathsf{Sub}(G)$ συμπίπτει με την σχέση $\subseteq$ του περιέχεσθαι).

Στη συνέχεια θα δούμε ένα χαρακτηριστικό παράδειγμα διαγράμματος Hasse μιας κυκλικής ομάδας.

Παράδειγμα 4.1.14 (Το διάγραμμα Hasse των υποομάδων της $(\mathbb{Z}_{60}, +)$)**.**

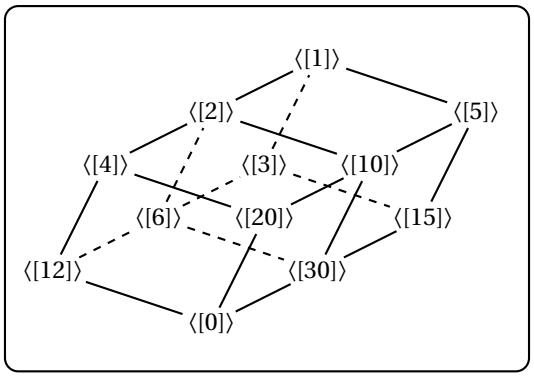
Το σύνολο των διαιρετών του 60 είναι $\{60, 30, 20, 15, 12, 10, 6, 5, 4, 3, 2, 1\}$. Έτσι υπάρχουν $\tau(60) = 12$ διαιρέτες $d_1, d_2, \cdots, d_{12}$ του 60 και επομένως υπάρχουν 12 υποομάδες $H_1, H_2, \cdots, H_{12}$ της $\mathbb{Z}_{60}$.

Ο παρακάτω πίνακας δίνει για κάθε διαιρέτη d_i του 60 την αντίστοιχη κυκλική υποομάδα H_i της $\mathbb{Z}_{60}$ με τον γεννήτορα της, και την τάξη της. Χάριν ευκολίας γράφουμε $[k] = [k]_{60}$, $\forall\, k \in \mathbb{Z}$.

Διαιρέτης του 60	**Υποομάδα της** G	**Τάξη Υποομάδας**
1	$H_1 = \langle \frac{60}{1}[1] \rangle = \langle 60[1] \rangle = \langle [60] \rangle = \langle [0] \rangle = \{[0]\}$	1
2	$H_2 = \langle \frac{60}{2}[1] \rangle = \langle 30[1] \rangle = \langle [30] \rangle$	2
3	$H_3 = \langle \frac{60}{3}[1] \rangle = \langle 20[1] \rangle = \langle [20] \rangle$	3
4	$H_4 = \langle \frac{60}{4} \rangle = \langle 15[1] \rangle = \langle [15] \rangle$	4
5	$H_5 = \langle \frac{60}{5}[1] \rangle = \langle 12[1] \rangle = \langle [12] \rangle$	5
6	$H_6 = \langle \frac{60}{6}[1] \rangle = \langle 10[1] \rangle = \langle [10] \rangle$	6
10	$H_7 = \langle \frac{60}{10}[1] \rangle = \langle 6[1] \rangle = \langle [6] \rangle$	10
12	$H_8 = \langle \frac{60}{12}[1] \rangle = \langle 5[1] \rangle = \langle [5] \rangle$	12
15	$H_9 = \langle \frac{60}{15}[1] \rangle = \langle 4[1] \rangle = \langle [4] \rangle$	15
20	$H_{10} = \langle \frac{60}{20}[1] \rangle = \langle 3[1] \rangle = \langle [3] \rangle$	20
30	$H_{11} = \langle \frac{60}{30}[1] \rangle = \langle 2[1] \rangle = \langle [2] \rangle$	30
60	$H_{12} = \langle \frac{60}{60}[1] \rangle = \langle [1] \rangle = \mathbb{Z}_{18}$	60

Λαμβάνοντας υπόψη τον παραπάνω πίνακα και τον ορισμό του διαγράμματος Hasse όπως στην υποενότητα 2.4.3, θα έχουμε:

Το διάγραμμα Hasse των υποομάδων τής $(\mathbb{Z}_{60}, +)$



Η υποομάδα $\langle[2]\rangle \leq \mathbb{Z}_{60}$ η οποία είναι τάξης 30 περιέχει όλες τις υποομάδες H τής $\mathbb{Z}_{60}$ με τάξη διαιρέτη του 30, δηλαδή περιέχει ακριβώς τις: $\langle[2]\rangle$, $\langle[4]\rangle$, $\langle[10]\rangle$, $\langle[20]\rangle$, $\langle[6]\rangle$, $\langle[12]\rangle$, $\langle[30]\rangle$ και $\langle[0]\rangle$.

Η υποομάδα $\langle[5]\rangle \leq \mathbb{Z}_{60}$ η οποία είναι τάξης 12 περιέχει όλες τις υποομάδες H τής $\mathbb{Z}_{60}$ με τάξη διαιρέτη του 12, δηλαδή περιέχει ακριβώς τις: $\langle[5]\rangle$, $\langle[10]\rangle$, $\langle[15]\rangle$, $\langle[20]\rangle$, $\langle[30]\rangle$ και $\langle[0]\rangle$.

Η υποομάδα $\langle[3]\rangle \leq \mathbb{Z}_{60}$ η οποία είναι τάξης 20 περιέχει όλες τις υποομάδες H τής $\mathbb{Z}_{60}$ με τάξη διαιρέτη του 20, δηλαδή περιέχει ακριβώς τις: $\langle[3]\rangle$, $\langle[6]\rangle$, $\langle[15]\rangle$, $\langle[30]\rangle$, $\langle[12]\rangle$ και $\langle[0]\rangle$.

Ανάλογες παρατηρήσεις ισχύουν και για τις υπόλοιπες υποομάδες. $\surd$

Το Θεώρημα του Gauss

Υπενθυμίζουμε ότι, σύμφωνα με το Πόρισμα 3.2.3, αν $\mathsf{C} = \langle x\rangle$ είναι μια πεπερασμένη κυκλική ομάδα με γεννήτορα x και τάξη n, τότε το στοιχείο x^k είναι επίσης γεννήτορας τής C αν και μόνο αν οι k και n είναι σχετικά πρώτοι αριθμοί: $(k,n) = 1$. Έτσι έχουμε

$$|\mathsf{Gen}(\mathsf{C})| = \phi(n)$$

όπου $\mathsf{Gen}(\mathsf{C})$ συμβολίζει το σύνολο των γεννητόρων τής C και ϕ είναι η συνάρτηση του Euler.

Το Θεώρημα που ακολουθεί είναι ένα πολύ χρήσιμο αποτέλεσμα της στοιχειώδους Θεωρίας Αριθμών, το οποίο αποδεικνύουμε με μεθόδους της Θεωρίας Ομάδων.

Θεώρημα 4.1.15 (Θεώρημα του Gauss). [1] *Αν n είναι ένας θετικός ακέραιος, τότε*

$$n = \sum_{d|n} \phi(d).$$

Απόδειξη. Αν G είναι μια τυχούσα πεπερασμένη ομάδα, τότε εύκολα βλέπουμε ότι η G είναι μια ξένη ένωση

$$G = \bigcup_{\mathsf{C}\in\mathsf{Cyc}(G)} \mathsf{Gen}(\mathsf{C}) \qquad (\dagger)$$

όπου το C διατρέχει το σύνολο $\mathsf{Cyc}(G)$ όλων των κυκλικών υποομάδων της G. Πράγματι, κάθε στοιχείο x της G παράγει μια κυκλική υποομάδα της G, και άρα $\bigcup_{\mathsf{C}\in\mathsf{Cyc}(G)} \mathsf{Gen}(\mathsf{C}) = G$. Έστω C και D δύο κυκλικές υποομάδες της G και έστω $z \in \mathsf{Gen}(\mathsf{C}) \bigcap \mathsf{Gen}(\mathsf{D})$. Τότε $\mathsf{C} = \langle z\rangle = \mathsf{D}$, και επομένως αν $\mathsf{C} \neq \mathsf{D}$, τότε $\mathsf{Gen}(\mathsf{C}) \bigcap \mathsf{Gen}(\mathsf{D}) = \emptyset$. Άρα η σχέση $(\dagger)$ περιγράφει μια ξένη ένωση μη κενών υποσυνόλων της G, και επομένως:

$$|G| = \Big|\bigcup_{\mathsf{C}\in\mathsf{Cyc}(G)} \mathsf{Gen}(\mathsf{C})\Big| = \sum_{\mathsf{C}\in\mathsf{Cyc}(G)} |\mathsf{Gen}(\mathsf{C})| = \sum_{\mathsf{C}\in\mathsf{Cyc}(G)} \phi(d), \quad \text{όπου} \quad d = |\mathsf{C}|$$

Αν η ομάδα G είναι τάξης n, τότε θα έχουμε $n = |G| = \sum_{\mathsf{C}\in\mathsf{Cyc}(G)} \phi(d)$, όπου $d = |\mathsf{C}|$. Αν η ομάδα G είναι κυκλική τάξης n, τότε γνωρίζουμε ότι κάθε υποομάδα της G είναι κυκλική και το πλήθος των υποομάδων της είναι όσοι και οι διαιρέτες της τάξης n της G. Ιδιαίτερα, επειδή για κάθε διαιρέτη d της τάξης $n = |G|$ της G υπάρχει μοναδική υπομάδα της G με τάξη τον διαιρέτη, έπεται ότι στο παραπάνω άθροισμα $n = \sum_{\mathsf{C}\in\mathsf{Cyc}(G)} \phi(d)$ μπορούμε να γράψουμε:

$$n = \sum_{\mathsf{C}\in\mathsf{Cyc}(G)} \phi(d) = \sum_{d|n} \phi(d) \qquad \blacksquare$$

[1] Carl Friedrich Gauss (30 Απριλίου 1777 - 23 Φεβρουαρίου 1855) [http://en.wikipedia.org/wiki/Carl_Friedrich_Gauss]: Γερμανός μαθηματικός, γνωστός και ως ο *Πρίγκιπας των Μαθηματικών*. Θεωρείται από τους επιφανέστερους και επιδραστικότερους μαθηματικούς όλων των εποχών. Το έργο του αποτελεί θεμελιώδη συμβολή σε πολλές περιοχές των Μαθηματικών αλλά και άλλων επιστημών. Αναφέρουμε ενδεικτικά: Θεωρία Αριθμών, Άλγεβρα, Διαφορική Γεωμετρία, Μαθηματική Ανάλυση, Στατιστική, Θεωρία Πινάκων, Γεωφυσική-Γεωδεσία, Οπτική κλπ.

4.1.3 Ευθέα Γινόμενα Κυκλικών Ομάδων

Υπενθυμίζουμε ότι, αν G και H είναι δύο ομάδες, τότε το **ευθύ γινόμενο** $G \times H$ των G και H είναι το σύνολο

$$G \times H = \{(g,h) \in G \times H \mid g \in G \text{ και } h \in H\}$$

το οποίο αποτελεί ομάδα όταν εφοδιαστεί με την πράξη:

$$(g_1,h_1)(g_2,h_2) = (g_1g_2, h_1h_2)$$

Σημειώνουμε ότι γράφοντας g_1g_2 υπονοούμε την πράξη της G και γράφοντας h_1h_2 υπονοούμε την πραξη της H. Το ουδέτερο στοιχείο της ομάδας $G \times H$ είναι το ζεύγος (e_G, e_H), όπου e_G είναι το ουδέτερο στοιχείο της G και e_H είναι το ουδέτερο στοιχείο της H. Τέλος, το αντίστροφο του στοιχείου $(g,h) \in G \times H$ είναι το στοιχείο (g^{-1}, h^{-1}), όπου g^{-1} είναι το αντίστροφο του στοιχείου g στην G και h^{-1} είναι το αντίστροφο του στοιχείου h στην H. Συνήθως θα συμβολίζουμε με το ίδιο σύμβολο e το ουδέτερο στοιχείο των δύο ομάδων G και H.

Το παρακάτω χρήσιμο αποτέλεσμα χαρακτηρίζει ιδιαίτερα πότε το ευθύ γινόμενο κυκλικών ομάδων είναι κυκλική ομάδα: το ευθύ γινόμενο δύο κυκλικών ομάδων είναι κυκλική ομάδα αν και μόνο αν είτε η μία εκ των δύο είναι η τετριμμένη ομάδα ή και οι δύο ομάδες είναι πεπερασμένες με τάξεις σχετικά πρώτους αριθμούς.

Θεώρημα 4.1.16. *Έστω G και H δύο κυκλικές ομάδες.*

1. *Αν μια εκ των G και H είναι η τετριμμένη ομάδα, τότε η ομάδα ευθύ γινόμενο $G \times H$ είναι κυκλική.*
2. *Υποθέτουμε ότι οι κυκλικές ομάδες G και H είναι μη τετριμμένες.*
   (α΄) Αν μια από τις G και H είναι άπειρη κυκλική, τότε η ομάδα ευθύ γινόμενο $G \times H$ δεν είναι ποτέ κυκλική.
   (β΄) Αν G και H είναι πεπερασμένες κυκλικές, τότε η ομάδα ευθύ γινόμενο $G \times H$ είναι κυκλική αν και μόνο αν:
   $$\big(o(G), o(H)\big) = 1$$

Απόδειξη. Υποθέτουμε ότι οι ομάδες G και H είναι κυκλικές με γεννήτορες τα στοιχεία a και b αντίστοιχα:

$$G = \langle a \rangle = \{a^k \in G \mid k \in \mathbb{Z}\} \qquad \text{και} \qquad H = \langle b \rangle = \{b^l \in H \mid l \in \mathbb{Z}\}$$

1. Υποθέτουμε ότι η κυκλική ομάδα H είναι τετριμμένη, δηλαδή $b = e_H$: $H = \langle e_H \rangle = \{e_H\}$. Τότε το στοιχείο (a, e_H) είναι γεννήτορας της ομάδας $G \times H$. Πράγματι, αν $(x,y) \in G \times H$, τότε $y = e_H$ και, επειδή $x \in G$, θα έχουμε $x = a^k$ για κάποιον ακέραιο k. Τότε $(a,e_H)^k = (a^k, e_H^k) = (a^k, e_H) = (x,y)$. Επομένως, πράγματι $G \times H = \langle (a, e_H) \rangle$ και άρα η ομάδα $G \times H$ είναι κυκλική. Παρόμοια, αν η ομάδα G είναι τετριμμένη, τότε η ομάδα $G \times H$ είναι κυκλική με γεννήτορα το στοιχείο (e_G, b).

2. Υποθέτουμε ότι καμία εκ των κυκλικών ομάδων G και H δεν είναι τετριμμένη.

   (α΄) Έστω ότι η ομάδα $G \times H$ είναι κυκλική και έστω $(x,y) \in G \times H$ ένας γεννήτοράς της: $G \times H = \langle (x,y) \rangle$. Τότε, επειδή $x \in G = \langle a \rangle$ και $y \in H = \langle b \rangle$, θα έχουμε:

   $$x = a^k \quad \text{και} \quad y = b^l, \qquad \text{όπου} \qquad k, l \in \mathbb{Z}$$

   Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι η κυκλική ομάδα H είναι άπειρη, και τότε $o(b) = \infty$. Θεωρούμε το στοιχείο $(a, e_H) \in G = \langle (x,y) \rangle$. Τότε υπάρχει ακέραιος i έτσι ώστε:

   $$(a, e_H) = (x,y)^i = (x^i, y^i) = ((a^k)^i, b^l)^i) = (a^{ki}, b^{li}) \quad \Longrightarrow \quad a = a^{ki} \text{ και } e_H = b^{li}$$

   Επειδή το στοιχείο b έχει άπειρη τάξη, έπεται ότι $li = 0$, και επομένως, είτε $l = 0$ είτε $i = 0$. Αν $i = 0$, τότε $a = a^{ki} = a^0 = e_G$, το οποίο είναι άτοπο, διότι η κυκλική ομάδα G δεν είναι η

τετριμμένη. Άρα $l = 0$ και τότε $y = b^l = b^0 = e_H$. Έτσι ο γεννήτορας (x, y) της $G \times H$ είναι της μορφής $(x, e_H) = (a^k, e_H)$. Θεωρούμε το στοιχείο $(e_G, b) \in G \times H = \langle (x, e_H) \rangle$. Τότε, υπάρχει ακέραιος j έτσι ώστε:

$$(e_G, b) = (x, e_H)^j = (x^j, e_H^j) = ((a^k)^j, e_H) = (a^{kj}, e_H) \quad \Longrightarrow \quad e_G = a^{kj} \quad \text{και} \quad b = e_H$$

Επομένως $H = \langle b \rangle = \langle e_H \rangle = \{e_H\}$, το οποίο είναι άτοπο, διότι η H δεν είναι τετριμμένη. Έτσι, σε κάθε περίπτωση καταλήγουμε σε άτοπο, και επομένως η ομάδα $G \times H$ δεν είναι κυκλική. Παρόμοια εργαζόμαστε, αν η κυκλική ομάδα G είναι άπειρη.

(β') [2] Υποθέτουμε ότι οι κυκλικές ομάδες G και H είναι πεπερασμένες, και έστω:

$$\mathrm{o}(G) = \mathrm{o}(a) = n \qquad \text{και} \qquad \mathrm{o}(H) = \mathrm{o}(b) = m$$

«$\Longleftarrow$» Υποθέτουμε πρώτα ότι $(n, m) = 1$. Θα δείξουμε ότι το στοιχείο (a, b) είναι γεννήτορας της $G \times H$. Επειδή η $G \times H$ έχει τάξη $|G \times H| = |G| \cdot |H| = mn < \infty$, έπεται ότι το στοιχείο (a, b) θα έχει πεπερασμένη τάξη, έστω $\mathrm{o}((a, b)) = r$. Τότε από το Θεώρημα του Lagrange θα έχουμε $r \mid nm$, και επειδή $(a, b)^r = (e, e)$, θα έχουμε $(a^r, b^r) = (e, e)$. Τότε $a^r = e$ και $b^r = e$. Τότε όμως θα έχουμε και $\mathrm{o}(a) \mid r$ και $\mathrm{o}(b) \mid r$, δηλαδή: $n \mid r$ και $m \mid r$. Τότε όμως $[n, m] \mid r$ και επειδή $(n, m) = 1$, έπεται ότι $[n, m] = nm$ και άρα θα έχουμε $nm \mid r$. Έτσι $\mathrm{o}((a, b)) = r = nm = \mathrm{o}(G \times H)$ και επομένως η κυκλική υποομάδα της $G \times H$ η οποία παράγεται από το στοιχείο (a, b) συμπίπτει με την $G \times H$, δηλαδή: $G \times H = \langle (a, b) \rangle$ και άρα η $G \times H$ είναι κυκλική.

«$\Longrightarrow$» Αντίστροφα, υποθέτουμε ότι η $G \times H$ είναι κυκλική και έστω $G \times H = \langle (x, y) \rangle$. Τότε $\mathrm{o}((x, y)) = nm$. Υποθέτουμε ότι $(n, m) = d \neq 1$. Τότε $d \mid n$ και $d \mid m$ και άρα: $\frac{n}{d}, \frac{m}{d} \in \mathbb{N}$. Επειδή $x \in G$ και $\mathrm{o}(G) = n$, θα έχουμε $x^n = e_G$, και επειδή $x \in G$ και $\mathrm{o}(H) = m$, θα έχουμε $y^m = e_H$. Επομένως θα έχουμε:

$$(x, y)^{\frac{mn}{d}} = (x^{\frac{mn}{d}}, y^{\frac{mn}{d}}) = \left((x^n)^{\frac{m}{d}}, (y^m)^{\frac{n}{d}}\right) = \left(e^{\frac{m}{d}}, e^{\frac{n}{d}}\right) = (e_G, e_H) = e_{G \times H}$$

και άρα $mn \mid \frac{mn}{d}$, δηλαδή $mn \leq \frac{mn}{d}$ και επειδή $d \neq 1$ καταλήγουμε στο άτοπο $mn < \frac{mn}{d}$. Επομένως θα έχουμε $d = (m, n) = 1$. ■

Παράδειγμα 4.1.17. Σύμφωνα με το Θεώρημα 4.1.16, η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_2$ (η οποία είναι ισόμορφη με την ομάδα του Klein) δεν είναι κυκλική ομάδα, η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_3$ είναι κυκλική ομάδα με γεννήτορα το στοιχείο $([1]_2, [1]_3)$, και οι ομάδες $\mathbb{Z} \times \mathbb{Z}$ και $\mathbb{Z} \times \mathbb{Z}_2$ δεν είναι κυκλικές ομάδες. √

Παράδειγμα 4.1.18. Θεωρούμε την ομάδα ευθύ γινόμενο $\mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{31}$. Επειδή $(5, 13) = 1$, έπεται ότι η ομάδα $\mathbb{Z}_5 \times \mathbb{Z}_{13}$ είναι κυκλική με τάξη $5 \cdot 13 = 65$. Επειδή $(65, 31) = 1$, έπεται ότι η ομάδα $(\mathbb{Z}_5 \times \mathbb{Z}_{13}) \times \mathbb{Z}_{31}$ είναι κυκλική τάξης $65 \cdot 31 = 2015$. √

---

[2] Διαφορετική Απόδειξη με χρήση της Πρότασης 3.2.22 και της, γνωστής από τη Θεωρία Αριθμών, σχέσης $(n, m)[n, m] = nm$ (βλέπε την Πρόταση 0.3.7(:

«$\Longleftarrow$» Υποθέτουμε πρώτα ότι $(n, m) = 1$. Τότε από την Πρόταση 3.2.22, έπεται ότι

$$\mathrm{o}((a, b)) = [\mathrm{o}(a), \mathrm{o}(b)] = [n, m] = nm, \quad \text{διότι} \quad (n, m) = 1$$

επομένως η κυκλική υποομάδα της $G \times H$ η οποία παράγεται από το στοιχείο (a, b) συμπίπτει με την $G \times H$, δηλαδή: $G \times H = \langle (a, b) \rangle$ και άρα η $G \times H$ είναι κυκλική.

«$\Longrightarrow$» Αντίστροφα υποθέτουμε ότι η $G \times H$ είναι κυκλική και έστω $G \times H = \langle (x, y) \rangle$. Τότε $x \in G = \langle a \rangle$, και άρα $x = a^k$, για κάποιο $k \in \mathbb{Z}$, και $y \in H = \langle b \rangle$, και άρα $y = b^l$, για κάποιο $l \in \mathbb{Z}$. Χρησιμοποιώντας ότι $\mathrm{o}(x) = \mathrm{o}(a^k) = \frac{\mathrm{o}(a)}{(\mathrm{o}(a), k)} = \frac{n}{(n, k)}$ και $\mathrm{o}(y) = \mathrm{o}(b^l) = \frac{\mathrm{o}(b)}{(\mathrm{o}(b), l)} = \frac{m}{(m, k)}$, θα έχουμε

$$nm = |G \times H| = \mathrm{o}((x, y)) = [\mathrm{o}(x), \mathrm{o}(y)] = \frac{\mathrm{o}(x)\mathrm{o}(y)}{(\mathrm{o}(x), \mathrm{o}(y))} = \frac{\frac{n}{(n,k)}\frac{m}{(m,k)}}{\left(\frac{n}{(n,k)}, \frac{m}{(m,k)}\right)} = \frac{nm}{(n,k)(m,k)\left(\frac{n}{(n,k)}, \frac{m}{(m,k)}\right)} \quad \Longrightarrow \quad (n,k)(m,k)\left(\frac{n}{(n,k)}, \frac{m}{(m,k)}\right) = 1$$

Τότε θα έχουμε $(n, k) = (m, k) = \left(\frac{n}{(n,k)}, \frac{m}{(m,k)}\right) = 1$ από όπου έπεται ότι $(n, m) = 1$.

Παράδειγμα 4.1.19. Αν p και q είναι πρώτοι αριθμοί, όπου $p \neq q$, και $r, s \geq 1$, τότε επειδή $(p^r, q^s) = 1$, από το Θεώρημα 4.1.16, έπεται ότι η ομάδα ευθύ γινόμενο $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ είναι κυκλική με τάξη $p^r q^s$, και μάλιστα θα έχουμε:

$$\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s} = \left\langle ([1]_{p^r}, [1]_{q^s}) \right\rangle$$

Επειδή οι διαιρέτες του $p^r q^s$ είναι σε πλήθος $\tau(p^r q^s) = (1+r)(1+s)$, δηλαδή οι αριθμοί

$$1, p, p^2, \cdots, p^r, q, q^2, \cdots, q^s, pq, pq^2, \cdots, pq^s, \ \cdots, \ p^r q, p^r q^2, \cdots, p^r q^s$$

έπεται ότι η κυκλική ομάδα $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ έχει $(1+r)(1+s)$ υποομάδες, δηλαδή μια και μόνο μια υποομάδα τάξης $p^i q^j$, οπου $0 \leq i \leq r$ και $0 \leq j \leq s$.

Από την άλλη πλευρά, επειδή

$$\varphi(p^r q^s) = p^r q^s (1 - \frac{1}{p})(1 - \frac{1}{q}) = p^{r-1}(p-1) q^{s-1}(q-1)$$

έπεται ότι η κυκλική ομάδα $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ θα έχει $p^{r-1}(p-1)q^{s-1}(q-1)$ το πλήθος γεννήτορες. $\surd$

4.1.4 Ταξινόμηση Κυκλικών Ομάδων

Στην παρούσα υποενότητα θα δούμε την ταξινόμηση των κυκλικών ομάδων σε κλάσεις ισομορφίας, μέσω οικείων μοντέλων.

Υπενθυμίζουμε ότι:

1. Η ομάδα $(\mathbb{Z}, +)$ είναι μια άπειρη κυκλική ομάδα.
2. $\forall n \geq 2$, η ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική τάξης n.

Ιδιαίτερα θα δούμε ότι κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την $(\mathbb{Z}, +)$, και κάθε πεπερασμένη κυκλική ομάδα τάξης n είναι ισόμορφη με την $(\mathbb{Z}_n, +)$.

Από την υποενότητα 2.8, υπενθυμίζουμε ότι

Ορισμός 4.1.20. *Μια απεικόνιση $f: G \longrightarrow G'$ μεταξύ δύο ομάδων G και G' καλείται* **ισομορφισμός** *αν:*

1. *Η f είναι «1-1» και «επί».*
2. $\forall x, y \in G$: $f(xy) = f(x) f(y)$.

Η δεύτερη συνθήκη του παραπάνω ορισμού δείχνει ότι ένας ισομορφισμός $f: G \longrightarrow G'$ στέλνει γινόμενα xy στοιχείων x, y της G σε γινόμενα $f(x)f(y)$ των εικόνων $f(x), f(y)$ των στοιχείων x, y μέσω της f στην G'. Υπενθυμίζουμε επίσης ότι με **Grp** συμβολίζουμε τη συλλογή όλων των ομάδων, επί της οποίας η σχέση ισομορφίας «$\cong$»

$$\forall G_1, G_2 \in \mathbf{Grp}: \quad G_1 \cong G_2 \quad \Longleftrightarrow \quad \text{υπάρχει ισομορφισμός} \quad f: G_1 \longrightarrow G_2$$

είναι μια σχέση ισοδυναμίας.

Θεώρημα 4.1.21. *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα.*

1. *Αν η G είναι άπειρη, τότε η G είναι ισόμορφη με την προσθετική ομάδα των ακεραίων:*
$$G \ \cong \ (\mathbb{Z}, +)$$
2. *Αν η G είναι πεπερασμένη τάξης n, τότε η G είναι ισόμορφη με την προσθετική ομάδα των κλάσεων υπολοίπων ακεραίων* mod n*:*
$$G \ \cong \ (\mathbb{Z}_n, +)$$

3. Δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνο αν έχουν την ίδια τάξη:

$$G_1 \cong G_2 \iff \mathrm{o}(G_1) = \mathrm{o}(G_2)$$

Απόδειξη. 1. Θεωρούμε την απεικόνιση

$$f : \mathbb{Z} \longrightarrow G, \quad f(n) = a^n$$

Επειδή $G = \{a^n \mid n \in \mathbb{Z}\}$, προφανώς η απεικόνιση f είναι «επί». Αν $f(n) = f(m)$, τότε $a^n = a^m$, από όπου έπεται ότι $a^{n-m} = e$. Επειδή η ομάδα $G = \langle a \rangle$ είναι άπειρη, θα έχουμε $\mathrm{o}(a) = \infty$, και επομένως $n - m = 0$, δηλαδή $n = m$ και η f είναι «1-1». Τέλος, επειδή

$$f(n+m) = a^{n+m} = a^n a^m = f(n) f(m)$$

έπεται ότι η απεικόνιση f είναι ισομορφισμός, και επομένως οι ομάδες G και $(\mathbb{Z}, +)$ είναι ισόμορφες.

2. Δείχνουμε πρώτα ότι ορίζοντας

$$f : \mathbb{Z}_n \longrightarrow G, \quad f([k]_n) = a^k$$

αποκτούμε μια καλά ορισμένη απεικόνιση. Πραγματικά, αν $[k]_n = [m]_n$, τότε $n \mid k - m$ και επομένως $k - m = rn$ για κάποιον ακέραιο r. Τότε $k = m + rn$, και θα έχουμε:

$$a^k = a^{m+rn} = a^m a^{rn} = a^m (a^n)^r = a^m e = a^m \quad \Longrightarrow \quad f([k]_n) = f([m]_n)$$

Έτσι η f είναι καλά ορισμένη. Αν $f([k]_n) = f([m]_n)$, τότε $a^k = a^m$ και άρα $a^{k-m} = e$. Τότε $n = |G| = \mathrm{o}(a) \mid k - m$, και επομένως $[k]_n = [m]_n$. Δηλαδή η f είναι «1-1». Επειδή $G = \{a^n \mid n \in \mathbb{Z}\}$, προφανώς η απεικόνιση f είναι «επί». Τέλος, θα έχουμε:

$$f([k]_n + [m]_n) = f([k+m]_n) = a^{k+m} = a^k a^m = f([k]_n) f([m]_n)$$

Επομένως η f είναι ισομορφισμός ομάδων, και άρα οι ομάδες G και $(\mathbb{Z}_n, +)$ είναι ισόμορφες.

3. Αν οι κυκλικές ομάδες G_1 και G_2 είναι ισόμορφες, τότε οι έχουν το ίδιο πλήθος στοιχείων διότι υπάρχει μια «1-1» και «επί» απεικόνιση μεταξύ αυτών. Άρα οι G_1 και G_2 έχουν την ίδια τάξη.

Αντίστροφα, υποθέτουμε ότι οι G_1 και G_2 έχουν την ίδια τάξη.

(α) Έστω ότι $\mathrm{o}(G_1) = \infty = \mathrm{o}(G_2)$. Τότε οι G_1 και G_2 είναι κάθεμιά τους ισόμορφη με την προσθετική ομάδα $(\mathbb{Z}, +)$, όπως προκύπτει από το μέρος 1.. Επομένως θα είναι και μεταξύ τους ισόμορφες, διότι η σχέση ισομορφίας στην συλλογή όλων των ομάδων είναι μια σχέση ισοδυναμίας. Άρα $G_1 \cong \mathbb{Z} \cong G_2$.

(β) Έστω ότι $\mathrm{o}(G_1) = n = \mathrm{o}(G_2)$. Τότε οι G_1 και G_2 είναι κάθεμιά τους ισόμορφη με την προσθετική ομάδα $(\mathbb{Z}_n, +)$, όπως προκύπτει από το μέρος 2. Επομένως θα είναι και μεταξύ τους ισόμορφες, διότι η σχέση ισομορφίας στην συλλογή όλων των ομάδων είναι μια σχέση ισοδυναμίας. Άρα $G_1 \cong \mathbb{Z}_n \cong G_2$. ■

Σύμφωνα με το Θεώρημα 4.1.21, όλες οι κυκλικές ομάδες άπειρης τάξης είναι ισόμορφες μεταξύ τους και ισόμορφες με το βασικό μοντέλο άπειρης κυκλικής ομάδας: την $(\mathbb{Z}, +)$. Επίσης όλες οι κυκλικές ομάδες πεπερασμένης τάξης n είναι ισόμορφες μεταξύ τους και ισόμορφες με το βασικό μοντέλο κυκλικής ομάδας τάξης n: την $(\mathbb{Z}_n, +)$. Συνοψίζοντας: με ακρίβεια ισομορφισμού, οι μόνες κυκλικές ομάδες είναι οι εξής (όπου $(\mathbb{Z}_1, +)$ είναι η τετριμμένη κυκλική ομάδα με ένα στοιχείο):

$$(\mathbb{Z}, +), \ (\mathbb{Z}_1, +), \ (\mathbb{Z}_2, +), \ (\mathbb{Z}_3, +), \ \cdots, \ (\mathbb{Z}_n, +), \ \cdots$$

Κάθε άλλη κυκλική ομάδα, ανάλογα με την τάξη της είναι ισόμορφη με μια από τις παραπάνω.

Οι παραπάνω παρατηρήσεις μάς επιτρέπουν να περιγράψουμε το σύνολο πηλίκο $\mathbf{CyGrp}/\cong$ της κλάσης όλων των κυκλικών ομάδων **CyGrp** ως προς την σχέση ισομορφίας «$\cong$»:

Θεώρημα 4.1.22. *Η απεικόνιση* $\mathrm{o}\colon \mathbf{Grp} \longrightarrow \mathbb{N}\cup\{\infty\},\ G \longmapsto \mathrm{o}(G) = |G|$ *η οποία στέλνει μια ομάδα στην τάξη της, επάγει μια απεικόνιση «επί»:*

$$\mathrm{o}\colon \mathbf{Grp}/\cong \ \longrightarrow\ \mathbb{N}\cup\{\infty\},\quad \mathrm{o}([G]_\cong) = \mathrm{o}(G)$$

η οποία με τη σειρά της επάγει μια «1-1» και «επί» απεικόνιση

$$\mathrm{o}\colon \mathbf{CyGrp}/\cong \ \longrightarrow\ \mathbb{N}\cup\{\infty\},\quad \mathrm{o}([G]_\cong) = \mathrm{o}(G)$$

Επιπλέον το σύνολο πηλίκο

$$\mathbf{CyGrp}/\cong \ = \ \Big\{[\mathbb{Z}]_\cong,\ [\mathbb{Z}_1]_\cong,\ [\mathbb{Z}_2]_\cong,\ \cdots,\ [\mathbb{Z}_n]_\cong,\ \cdots\Big\}$$

περιγράφει το σύνολο όλων των κλάσεων ισομορφίας των κυκλικών ομάδων.

Απόδειξη. Η απεικόνιση «o» επί του συνόλου πηλίκου $\mathbf{Grp}/\cong$ είναι καλά ορισμένη διότι ισόμορφες ομάδες έχουν την ίδια τάξη. Η απεικόνιση αυτή είναι «επί» διότι για κάθε $n \in \mathbb{N}\cup\{\infty\}$, υπάρχει ομάδα G έτσι ώστε $\mathrm{o}([G]_\cong) = n$, για παράδειγμα $G = (\mathbb{Z}_n, +)$ αν $n \in \mathbb{N}$ και $G = (\mathbb{Z}, +)$ αν $n = \infty$.

Προφανώς η απεικόνιση «o» είναι καλά ορισμένη απεικόνιση επί του συνόλου πηλίκου $\mathbf{CyGrp}/\cong$, η οποία είναι προφανώς απεικόνιση «επί». Αν $[G_1]_\cong, [G_2]_\cong$ είναι στοιχεία του συνόλου πηλίκου $\mathbf{CyGrp}/\cong$, δηλαδή είναι κλάσεις ισομορφίας δύο κυκλικών ομάδων G_1 και G_2, και ισχύει $\mathrm{o}([G_1]_\cong) = \mathrm{o}([G_2]_\cong)$, τότε $\mathrm{o}(G_1) = \mathrm{o}(G_2)$. Απο το Θεώρημα 4.1.21, έπεται ότι οι ομάδες G_1 και G_2 είναι ισόμορφες: $G_1 \cong G_2$. Τότε προφανώς $[G_1]_\cong = [G_2]_\cong$, και επομένως η απεικόνιση «o» είναι και «1-1».

Τέλος, η περιγραφή του συνόλου πηλίκο $\mathbf{CyGrp}/\cong$ προκύπτει από το Θεώρημα 4.1.21. ■

Στο επόμενο παράδειγμα θα χρησιμοποιήσουμε τα αποτελέσματα τα οποία έχουμε αποδείξει μέχρι τώρα για να ταξινομήσουμε, ως προς τη σχέση ισομορφίας, όλες τις ομάδες $(G,\cdot)$ με τάξη $\mathrm{o}(G) \le 7$.

Παράδειγμα 4.1.23. (Ταξινόμηση ομάδων τάξης ≤ 7). Έστω $(G,\cdot)$ μια ομάδα με τάξη $\mathrm{o}(G) \le 7$.

1. Αν $\mathrm{o}(G) = 1$, τότε η G είναι η τετριμμένη ομάδα $\{e\} \cong \mathbb{Z}_1$.

2. Αν η τάξη της G είναι πρώτος αριθμός, δηλαδή στην περίπτωσή μας $\mathrm{o}(G) = 2,3,5$ ή 7, τότε σύμφωνα με την Πρόταση 3.4.10 η ομάδα G είναι κυκλική, και επομένως, σύμφωνα με το Θεώρημα 4.1.21, θα είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, και $\mathbb{Z}_7$ αντίστοιχα.

3. Αν $\mathrm{o}(G) = 4$, τότε από το Παράδειγμα 2.8.14 γνωρίζουμε ότι υπάρχουν ακριβώς δύο μη ισόμορφες ομάδας με τάξη 4, η ομάδα του Klein και η κυκλική ομάδα τάξης 4. Επομένως έχουμε τις εξής δύο μη ισόμορφες ομάδες τάξης 4: $\mathbb{Z}_4$, και $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Υποθέτουμε ότι: $\mathrm{o}(G) = 6$.

   (α') Αν η ομάδα G περιέχει ένα στοιχείο τάξης 6, τότε το στοιχείο αυτό είναι προφανώς γεννήτορας της G και επομένως η G είναι κυκλική τάξης 6. Σε αυτή την περίπτωση, από το Θεώρημα 4.1.21, η G είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_6$.

   (β') Υποθέτουμε ότι κανένα στοιχείο της G δεν έχει τάξη 6. Τότε, από το Θεώρημα του Lagrange, η τάξη κάθε στοιχείου της G, διαφορετικού του ουδετέρου, θα είναι 2 ή 3.

   Αν όλα τα στοιχεία $a \in G$, όπου $a \neq e$, έχουν τάξη ίση με 2, τότε η G θα περιέχει τουλάχιστον τα εξής στοιχεία $e, a, b, ab = ba$, και επομένως θα υπάρχει ένα στοιχείο $c \in G \setminus \{e, a, b, ab\}$ το οποίο επίσης θα έχει τάξη 2. Τότε όμως η ομάδα G θα περιέχει και τα στοιχεία ac και bc. Επειδή τα στοιχεία e, a, b, ab, c είναι διαφορετικά, και επειδή η G έχει 6 στοιχεία, θα πρέπει τα στοιχεία e, a, b, ab, c, ac, bc να μην είναι όλα διαφορετικά. Προφανώς $ac \neq e$, διότι διαφορετικά θα είχαμε $c = a^{-1} = a$, και $ac \neq ab$, διότι διαφορετικά θα είχαμε $b = c$, και $ac \neq a$, διότι διαφορετικά θα είχαμε $c = e$. Άρα μένει η περίπτωση $ac = b$, και τότε θα είχαμε $bac = bb = e$, και άρα $c = c^{-1} = ba = ab$, το οποίο είναι άτοπο διότι $c \neq ab$. Άρα τα 6 στοιχεία e, a, b, c, ab, ac είναι διαφορετικά και άρα $G = \{e, a, b, c, ab, ac\}$. Για το στοιχείο bc, θα έχουμε ότι $bc \neq e$, διότι διαφορετικά θα είχαμε

$c = b^{-1} = b$, και $bc \neq b$, διότι διαφορετικά θα είχαμε $c = e$, και $bc \neq c$, διότι διαφορετικά θα είχαμε $b = e$, και $bc \neq ba$, διότι διαφορετικά θα είχαμε $c = a$. Άρα μένει η περίπτωση $bc = a$, και τότε θα είχαμε $c = ec = bbc = ba = ab$, το οποίο είναι άτοπο, διότι $c \neq ab$. Άρα μένει η περίπτωση $ac = bc$ η οποία μας οδηγεί στην αντίφαση $a = b$. Συνοψίζοντας, δείξαμε ότι δεν μπορεί κάθε στοιχείο της G, εκτός του ουδετέρου, να έχει τάξη 2.

Επομένως υπάρχουν στοιχεία $a, b \in G$, όπου $a \neq b$ και $o(a) = 2$ και $o(b) = 3$. Θα δείξουμε ότι η G είναι ισόμορφη με την συμμετρική ομάδα S_3. Παρατηρούμε ότι θα πρέπει $ab \neq ba$. Πράγματι, αν $ab = ba$, τότε από την Πρόταση 3.2.20 θα είχαμε ότι $o(ab) = 6$, το οποίο είναι άτοπο διότι η G δεν έχει στοιχεία τάξης 6. Επομένως $ab \neq ba$ και τότε εύκολα βλέπουμε ότι τα έξι στοιχεία e, a, b, b^2, ab, ba είναι διαφορετικά και επομένως $G = \{e, a, b, b^2, ab, ba\}$. Θεωρούμε την απεικόνιση

$$f : G \longrightarrow S_3, \quad f(e) = \iota, \quad f(a) = (12), \quad f(b) = (123), \quad f(b^2) = (132), \quad f(ab) = (23), \quad f(ba) = (13)$$

η οποία είναι προφανώς «1-1» και «επί». Εύκολα βλέπουμε ότι $f(xy) = f(x)f(y)$, $\forall x, y \in G$. Επομένως η απεικόνιση f είναι ισομορφισμός, και άρα $G \cong S_3$. $\surd$

Παράδειγμα 4.1.24. (Ταξινόμηση ομάδων τάξης ≤ 15 και $\neq 8, 9, 12$). Έστω $(G, \cdot)$ μια ομάδα με τάξη $o(G) \leq 15$ και υποθέτουμε ότι $o(G) \neq 8, 9, 12$.

1. Αν $|G| \leq 7$, τότε η δομή της G είναι γνωστή από το Παράδειγμα 4.1.23.

2. Αν $|G| = 10$, τότε από το Θεώρημα 3.7.1 έπεται ότι η G είναι ισόμορφη είτε με την κυκλική ομάδα $\mathbb{Z}_{10}$ (αν η G είναι αβελιανή) είτε με τη διεδρική ομάδα D_5 των συμμετριών του κανονικού πενταγώνου (αν η G δεν είναι αβελιανή).

   Σημειώνουμε ότι, επειδή $(2, 5) = 1$, από το Θεώρημα 4.1.16 η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_5$ είναι κυκλική και τότε από το Θεώρημα 4.1.21 θα έχουμε έναν ισομορφισμό ομάδων $\mathbb{Z}_2 \times \mathbb{Z}_5 \cong \mathbb{Z}_{10}$.

   Έτσι με ακρίβεια ισομορφίας οι μόνες ανά δύο μη ισόμορφες ομάδες τάξης 10 είναι οι εξής:

   $$\mathbb{Z}_{10} \quad \text{και} \quad D_5$$

3. Αν $|G| = 14$, τότε από το Θεώρημα 3.7.1 έπεται ότι η G είναι ισόμορφη είτε με την κυκλική ομάδα $\mathbb{Z}_{14}$ (αν η G είναι αβελιανή) είτε με τη διεδρική ομάδα D_7 των συμμετριών του κανονικού επταγώνου (αν η G δεν είναι αβελιανή).

   Σημειώνουμε ότι επειδή $(2, 7) = 1$, από το Θεώρημα 4.1.16 η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_7$ είναι κυκλική και τότε από το Θεώρημα 4.1.21 θα έχουμε έναν ισομορφισμό ομάδων $\mathbb{Z}_2 \times \mathbb{Z}_7 \cong \mathbb{Z}_{14}$.

   Έτσι με ακρίβεια ισομορφίας οι μόνες ανά δύο μή ισόμορφες ομάδες τάξης 14 είναι οι εξής:

   $$\mathbb{Z}_{14} \quad \text{και} \quad D_7$$

4. Αν $|G| = 11$ τότε επειδή οι αριθμός 11 είναι πρώτος, η ομάδα G θα είναι κυκλική και άρα ισόμορφη με την $\mathbb{Z}_{11}$. Έτσι, με ακρίβεια ισομορφίας, υπάρχει μόνο μια ομάδα τάξης 11, η

   $$\mathbb{Z}_{11}$$

5. Αν $|G| = 13$, τότε, επειδή οι αριθμός 13 είναι πρώτος, η ομάδα G θα είναι κυκλική και άρα ισόμορφη με την $\mathbb{Z}_{13}$. Έτσι, με ακρίβεια ισομορφίας, υπάρχει μόνο μια ομάδα τάξης 13, η

   $$\mathbb{Z}_{13}$$

6. Αν $|G| = 15$, τότε, από το Θεώρημα 3.7.7, έπεται ότι αναγκαστικά η G είναι αβελιανή. Από το Θεώρημα 3.7.6, έπεται ότι η G είναι κυκλική και επομένως από το Θεώρημα 4.1.21 θα είναι ισόμορφη με την $\mathbb{Z}_{15}$ η οποία, σύμφωνα με το Θεώρημα 4.1.16, επειδή $(3, 5) = 1$, είναι ισόμορφη με το ευθύ γινόμενο $\mathbb{Z}_3 \times \mathbb{Z}_5$.

   Έτσι με ακρίβεια ισομορφίας η μόνη ομάδα τάξης 15 είναι η:

   $$\mathbb{Z}_{15}$$

Σημειώνουμε ότι για τις ομάδες με τάξη 8, 9, και 14, αποδεικνύεται με περισσότερο προχωρημένες μεθόδους ότι ισχύουν τα ακόλουθα, βλέπε τα βιβλία [16], [26], [31]:

(α) Αν $|G| = 8$, τότε οι μόνες ανά δύο μη ισόμορφες ομάδες με τάξη 8 είναι, με ακρίβεια ισομορφίας, οι εξής:

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathsf{D}_4, \quad Q$$

όπου D_4 είναι η διεδρική ομάδα των συμμετριών του τετραγώνου και η Q είναι η ομάδα των τετρανίων του Hamilton.

(β) Αν $|G| = 9$, τότε με ακρίβεια ισομορφίας η μόνες ανά δύο μη ισόμορφες ομάδες τάξης 9 είναι οι εξής:

$$\mathbb{Z}_9 \quad \text{και} \quad \mathbb{Z}_3 \times \mathbb{Z}_3$$

(γ) Αν $|G| = 12$, τότε οι μόνες ανά δύο μη ισόμορφες ομάδες με τάξη 12 είναι, με ακρίβεια ισομορφίας, οι εξής:

$$\mathbb{Z}_{12}, \quad \mathbb{Z}_6 \times \mathbb{Z}_2, \quad \mathsf{A}_4, \quad \mathsf{D}_6, \quad \mathsf{Dic}_{12}$$

όπου D_6 είναι η διεδρική ομάδα των συμμετριών του κανονικού εξαγώνου, η A_4 είναι η εναλλάσσουσα ομάδα βαθμού 4, και Dic_{12} είναι μια ομάδα[3] η οποία παράγεται από τρία στοιχεία x, y και z για τα οποία ισχύει ότι: $x^3 = y^2 = z^2 = xyz$.

4.2 Χαρακτηρισμοί Πεπερασμένων Κυκλικών Ομάδων

Σύμφωνα με την πρόταση 3.4.7, αν $(G, \cdot)$ είναι μια πεπερασμένη ομάδα, τότε η τάξη της $\mathsf{o}(G)$ έχει την ιδιότητα: $x^{\mathsf{o}(G)} = e, \quad \forall x \in G$.

Η ακόλουθη πρόταση δείχνει ότι μια πεπερασμένη *κυκλική* ομάδα ικανοποιεί κάτι ισχυρότερο:

Πρόταση 4.2.1. *Έστω $(G, \cdot)$ μια πεπερασμένη κυκλική ομάδα. Τότε ο φυσικός αριθμός $\mathsf{o}(G)$ είναι ο μικρότερος φυσικός αριθμός n έτσι ώστε: $x^n = e, \quad \forall x \in G$.*

Απόδειξη. Έστω g ένας γεννήτορας της G: $G = \langle g \rangle$. Τότε $\mathsf{o}(G) = \mathsf{o}(g) := n$ και, όπως γνωρίζουμε, n είναι ο μικρότερος φυσικός m έτσι ώστε $g^m = e$. Έστω $x \in G$. Επειδή

$$G = \langle g \rangle = \{e = g^0, g, g^2, \cdots, g^{n-1}\}$$

θα έχουμε $x = g^k$ για κάποιο $k \leq n-1$. Τότε $x^{\mathsf{o}(g)} = (g^k)^{\mathsf{o}(g)} = e$. Προφανώς ο φυσικός n είναι ο μικρότερος ο μικρότερος φυσικός m έτσι ώστε $x^m = e$, $\forall x \in G$, διότι, αν υπήρχε φυσικός $m < n$ έτσι ώστε $x^m = e$, $\forall x \in G$, τότε θα ίσχυε $g^m = e$, κάτι που είναι άτοπο διότι $\mathsf{o}(g) = n$. ■

Οι κύριοι σκοποί της παρούσας ενότητας είναι οι εξής:

1. Πρώτος σκοπός είναι να αποδείξουμε ότι η ιδιότητα η οποία περιγράφεται στην πρόταση 4.2.1 χαρακτηρίζει τις κυκλικές ομάδες στην κλάση των πεπερασμένων αβελιανών ομάδων.

2. Από την άλλη πλευρά, όπως δείξαμε στο Θεώρημα 4.1.10, μια κυκλική ομάδα G τάξης n έχει το πολύ μια υποομάδα τάξης k, $\forall k \geq 1$: πράγματι, αν $k \nmid n$, τότε δεν έχει καμία υποομάδα τάξης k, και αν $k \mid n$, τότε έχει ακριβώς μια υποομάδα τάξης k.

   Δεύτερος σκοπός της παρούσας ενότητας είναι να αποδείξουμε ότι η παραπάνω ιδιότητα χαρακτηρίζει τις κυκλικές ομάδες στην κλάση των πεπερασμένων ομάδων.

Για την απόδειξη θα χρειαστούμε κάποιες βοηθητικές προτάσεις οι οποίες παρουσιάζουν ενδιαφέρον από μόνες τους. Στην απόδειξή τους θα χρησιμοποιήσουμε στοιχειώδη αποτελέσματα της Θεωρίας Αριθμών.

[3] Η ομάδα Dic_{12} καλείται η **δικυκλική ομάδα** τάξης 12 ή **δυαδική διεδρική ομάδα** τάξης 12.

4.2.1 Τάξη στοιχείων τα οποία μετατίθενται σε μια ομάδα

Θα αποδείξουμε κάποια αποτελέσματα τα οποία αφορούν τάξη γινομένου στοιχείων τα οποία μετατίθενται σε μια ομάδα.

Λήμμα 4.2.2. *Έστω ότι $(G,\cdot)$ είναι μια αβελιανή ομάδα και $x,y\in G$ στοιχεία της G έτσι ώστε:*

$$\mathrm{o}(x)<\infty \qquad \text{και} \qquad \mathrm{o}(x)<\infty \qquad \text{και} \qquad \big(\mathrm{o}(x),\mathrm{o}(y)\big)=1$$

Τότε:

$$\langle x\rangle\cap\langle y\rangle=\{e\} \qquad \text{και} \qquad \mathrm{o}(xy)=\mathrm{o}(x)\cdot\mathrm{o}(y)\big)$$

Απόδειξη. Θέτουμε $\mathrm{o}(x)=m<\infty$ και $\mathrm{o}(x)=n<\infty$. Έστω $z\in\langle x\rangle\cap\langle y\rangle$ και επομένως $z\in\langle x\rangle$ και $z\in\langle y\rangle$. Άρα $z=x^k=y^l$, για κάποιους ακέραιους k,l. Τότε

$$z^m=x^{km}=(x^m)^k=e \qquad \text{και} \qquad z^n=y^{ln}=(y^n)^l=e$$

Επομένως:

$$\mathrm{o}(z)\mid m \qquad \text{και} \qquad \mathrm{o}(z)\mid n \qquad \Longrightarrow \qquad \mathrm{o}(z)\mid(n,m) \qquad \overset{(m,n)=1}{\Longrightarrow} \qquad \mathrm{o}(z)=1$$

Άρα $z=e$ και επομένως: $\langle x\rangle\cap\langle y\rangle=\{e\}$.

Επειδή η ομάδα G είναι αβελιανή, ο ισχυρισμός ότι $\mathrm{o}(xy)=mn$ προκύπτει από την Πρόταση 3.2.20. Χάριν πληρότητας θα δώσουμε μια σύντομη απόδειξη. Έστω $\mathrm{o}(x\cdot y)=r$. Τότε, λαμβάνοντας υπόψη ότι η G είναι αβελιανή, θα έχουμε:

$$x^r\cdot y^r=(x\cdot y)^r=e \quad\Longrightarrow\quad x^r=(y^r)^{-1}=y^{-r}\in\langle x\rangle\cap\langle y\rangle=\{e\}$$

και επομένως:

$$x^r=e \quad\text{και}\quad y^{-r}=e \quad\Longrightarrow\quad x^r=e \quad\text{και}\quad y^r=e \quad\Longrightarrow\quad \mathrm{o}(x)=\frac{m}{r} \quad\text{και}\quad \mathrm{o}(y)=\frac{n}{r}$$

Τότε $[m,n]\mid r$ και, επειδή, όπως γνωρίζουμε από τη στοιχειώδη Θεωρία Αριθμών, ισχύει ότι $[m,n](m,n)=mn$, η υπόθεση $(m,n)=1$, συνεπάγεται ότι: $mn\mid r$. Από τη άλλη πλευρά:

$$(xy)^{mn}=x^{mn}\cdot y^{mn}=(x^m)^n\cdot(y^n)^m=e\cdot e=e \quad\Longrightarrow\quad r\mid mn$$

Συμπεραίνουμε ότι $mn=r$, δηλαδή:

$$\mathrm{o}(xy)=\mathrm{o}(x)\mathrm{o}(y)$$

■

Λήμμα 4.2.3. *Έστω ότι $(G,\cdot)$ είναι μια πεπερασμένη αβελιανή ομάδα. Τότε η G περιέχει ένα στοιχείο g του οποίου η τάξη είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων όλων των στοιχείων της G:*

$$\exists g\in G: \quad \mathrm{o}(g)=[\mathrm{o}(g_1),\mathrm{o}(g_2),\cdots,\mathrm{o}(g_n)]$$

Απόδειξη. • Δείχνουμε πρώτα ότι:

$$\text{αν } x,y\in G \text{ και } \mathrm{o}(x)=m,\ \mathrm{o}(y)=n, \text{ τότε υπάρχει ένα στοιχείο } z\in G \text{ έτσι ώστε: } \mathrm{o}(z)=[m,n]$$

Για τους θετικούς ακεραίους m,n από την υποενότητα 0.3.2, έπεται ότι μπορούμε να γράψουμε:

$$m=p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k} \qquad \text{και} \qquad n=p_1^{f_1}p_2^{f_2}\cdots p_k^{f_k}$$

όπου οι $p_1,p_2,\cdots,p_k$ είναι διακεκριμένοι πρώτοι αριθμοί, και $e_i,f_i\geq 0$, $1\leq i\leq k$. Χωρίς βλάβη της γενικότητας, (εν ανάγκη αναδιατάσσοντας τους πρώτους αριθμούς $p_1,p_2,\cdots,p_k$), μπορούμε να υποθέσουμε ότι:

$$e_1\leq f_1,\ \cdots,\ e_j\leq f_j \qquad \text{και} \qquad e_{j+1}\geq f_{j+1},\ \cdots,\ e_k\geq f_k, \qquad \text{για κάποιο} \quad 1\leq j\leq k$$

Θέτοντας

$$r = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j} \qquad \text{και} \qquad s = p_{j+1}^{f_{j+1}} p_{j+2}^{f_{j+2}} \cdots p_k^{f_k}$$

βλέπουμε εύκολα ότι:

$$[m,n] = \frac{n}{s}\frac{m}{r} = p_1^{f_1} p_2^{f_2} \cdots p_j^{f_j} p_1^{e_{j+1}} p_2^{e_{j+2}} \cdots p_k^{e_k} \qquad \text{και} \qquad (\frac{m}{r}, \frac{n}{s}) = 1$$

Επιπλέον:

$$\mathrm{o}(x^r) = \frac{m}{r} \qquad \text{και} \qquad \mathrm{o}(y^s) = \frac{n}{s}$$

και επομένως από το Λήμμα 4.2.2 θα έχουμε ότι:

$$\text{το στοιχείο} \quad z = x^r \cdot z^s \quad \text{έχει τάξη} \quad \mathrm{o}(z) = [m,n] = \frac{n}{s}\frac{m}{r}$$

- Χρησιμοποιώντας την ακόλουθη γνωστή ταυτότητα ελαχίστου κοινού πολλαπλασίου:

$$\forall\, m,n,t \in \mathbb{N}: \qquad [[m,n],t] = [m,n,t]$$

και επαναλαμβάνοντας την παραπάνω διαδικασία, θα έχουμε ότι:

$$\text{αν } x,y,z \in G \text{ και } \mathrm{o}(x) = m,\ \mathrm{o}(y) = n,\ \mathrm{o}(z) = t, \text{ τότε υπάρχει ένα στοιχείο } w \in G \text{ έτσι ώστε:}$$

$$\mathrm{o}(w) = [m,n,t]$$

- Συνεχίζοντας την παραπάνω διαδικασία, και λαμβάνοντας υπόψη ότι η αβελιανή ομάδα είναι πεπερασμένη, μπορούμε επαγωγικά να κατασκευάσουμε ένα στοιχείο g με την επιθυμητή ιδιότητα, δηλαδή η τάξη του g να είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της G. ■

Γενικότερα η τάξη του γινομένου δυο στοιχείων πεπερασμένης τάξης τα οποία μετατίθενται σε μια ομάδα δεν είναι πάντα ίση με το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων. Το ακόλουθο αποτέλεσμα δείχνει τι συμβαίνει στην γενική περίπτωση.

Πρόταση 4.2.4. *Έστω x,y στοιχεία πεπερασμένης τάξης σε μια ομάδα G. Υποθέτουμε ότι:*

1. $xy = yx$.
2. *Για κάθε πρώτο αριθμό $p \mid \mathrm{o}(x)\mathrm{o}(y)$, η μέγιστη δύναμη του p η οποία διαιρεί την τάξη $\mathrm{o}(x)$ δεν είναι ίση με την μέγιστη δύναμη του p η οποία διαιρεί την τάξη $\mathrm{o}(x)$.*

Τότε:

$$\mathrm{o}(xy) = [\mathrm{o}(x), \mathrm{o}(y)]$$

Απόδειξη. Θέτουμε $\mathrm{o}(x) = n$, $\mathrm{o}(y) = m$, και $l = [n,m]$. Τότε $l = nk_1$ και $l = mk_2$, και επομένως, χρησιμοποιώντας ότι $xy = yx$, θα έχουμε:

$$(xy)^l = x^l y^l = x^{nk_1} y^{mk_2} = (x^n)^{k_1} (y^m)^{k_2} = e$$

Θα δείξουμε ότι ο αριθμός l είναι ο μικρότερος φυσικός k έτσι ώστε $(xy)^k = e$. Έστω $(xy)^k = e$, όπου $1 \le k \le l$. Τότε $(xy)^k = x^k y^k = e$ και επομένως $x^k = y^{-k}$. Συνεπώς $\mathrm{o}(x^k) = \mathrm{o}(y^{-k})$, και επειδή $\mathrm{o}(y^{-k}) = \mathrm{o}((y^k)^{-1}) = \mathrm{o}(y^k$, θα έχουμε

$$\frac{n}{(n,k)} = \mathrm{o}(x^k) = \mathrm{o}(y^k) = \frac{m}{(m,k)}$$

Έστω p ένας πρώτος διαιρέτης του nm ή ισοδύναμα του l, και έστω

1. a η μεγαλύτερη δύναμη του p η οποία διαιρεί τον n,
2. b η μεγαλύτερη δύναμη του p η οποία διαιρεί τον m,

3. c η μεγαλύτερη δύναμη του p η οποία διαιρεί τον k,

Τότε από την υπόθεση έχουμε: $a \neq b$.

Επειδή $k \leq l$, θα έχουμε προφανώς $c \leq a$ και $c \leq b$. Υποθέτουμε πρώτα ότι $b < a$. Αν $c < a$, τότε, χρησιμοποιώντας για παράδειγμα αναλύσεις σε πρώτους παράγοντες, εύκολα βλέπουμε ότι η μεγαλύτερη δύναμη του p η οποία διαιρεί την τάξη $\mathsf{o}(x^k) = \frac{n}{(n,k)}$ του x^k είναι $a-c$, και η μεγαλύτερη δύναμη του p η οποία διαιρεί την τάξη $\mathsf{o}(y^k) = \frac{m}{(m,k)}$ του y^k είναι $\max\{0, b-c\}$. Άρα θα πρέπει $a-c = \max\{0, b-c\}$ και αυτό είναι αδύνατο, διότι $b < a$ και $c < a$. Επομένως $c = a$. Παρόμοια δείχνουμε ότι αν $a < b$, τότε $c = b$. Αυτό σημαίνει ότι, για κάθε πρώτο διαιρέτη p του l, έχουμε ότι η μεγαλύτερη δύναμη του p η οποία διαιρεί τον k είναι ίση με την μεγαλύτερη δύναμη του p η οποία διαιρεί τον l. Επειδή $k \leq l$, συμπεραίνουμε ότι $k = l$, και επομένως l είναι η μικρότερος φυσικός αριθμός k με την ιδιότητα $(xy)^k = e$, δηλαδή $\mathsf{o}(xy) = l$. ■

4.2.2 Χαρακτηρισμοί Κυκλικών Ομάδων

Έστω ότι G είναι μια ομάδα. Υποθέτουμε ότι υπάρχει $m \in \mathbb{N}$ έτσι ώστε $x^m = e$, $\forall x \in G$. Για παράδειγμα, αυτή η υπόθεση ισχύει αν η G είναι πεπερασμένη (τότε μπορούμε να διαλέξουμε $m = |G|$) ή αν η G είναι το ευθύ γινόμενο $\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots$ της πεπερασμένης κυκλικής ομάδας $\mathbb{Z}_n$ με τον εαυτό της άπειρες φορές (τότε μπορούμε να διαλέξουμε $m = n$). Ο μικρότερος φυσικός $k \in \mathbb{N}$ έτσι ώστε $x^k = e$, $\forall x \in G$, καλείται ο **εκθέτης** της G και συμβολίζεται με $\exp(G)$:

$$\exp(G) = \min\left\{k \in \mathbb{N} \mid x^k = e,\ \forall x \in G\right\}$$

Προφανώς, αν G είναι μια αβελιανή ομάδα, τότε $\exp(G) \mid |G|$ και ιδιαίτερα $\exp(G) = |G|$.

Λήμμα 4.2.5. *Έστω $G = \{g_1, g_2, \cdots, g_n\}$ μια πεπερασμένη αβελιανή ομάδα. Τότε:*

$$\exp(G) = [\mathsf{o}(g_1), \mathsf{o}(G_2, \cdots, \mathsf{o}(g_n)]$$

και υπάρχει στοιχείο g στην G με τάξη τον εκθέτη της G:

$$\exists g \in G: \quad \mathsf{o}(g) = \exp(G)$$

Απόδειξη. Έστω $m = [\mathsf{o}(g_1), \mathsf{o}(G_2, \cdots, \mathsf{o}(g_n)]$. Τότε προφανώς $x^m = e$, $\forall x \in G$, και επομένως $\exp(G) \leq m$. Από την άλλη πλευρά, εξ ορισμού θα έχουμε, $\mathsf{o}(x) \mid \exp(G)$, $\forall x \in G$, και άρα $m \mid \exp(G)$, και ιδιαίτερα $m \leq \exp(G)$. Επομένως $\exp(G) = m = [\mathsf{o}(g_1), \mathsf{o}(G_2, \cdots, \mathsf{o}(g_n)]$. Ο τελευταίος ισχυρισμός προκύπτει από το Λήμμα 4.2.3. ■

Πρόβλημα: *Πότε ισχύει ότι $\exp(G) = |G|$, αν η G είναι μια πεπερασμένη αβελιανή ομάδα;*

Την απάντηση δίνει το ακόλουθο Θεώρημα.

Θεώρημα 4.2.6. *Έστω $(G, \cdot)$ μια πεπερασμένη αβελιανή ομάδα. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η G είναι κυκλική.*
2. *$\exp(G) = |G|$, δηλαδή, η τάξη $|G|$ της G είναι ο μικρότερος φυσικός αριθμός n έτσι ώστε: $x^n = e$, $\forall x \in G$.*

Απόδειξη. 1. $\Longrightarrow$ 2. Αποδείχθηκε στην Πρόταση 4.2.1.

2. $\Longrightarrow$ 1. Από το Λήμμα 4.2.5 έπεται ότι υπάρχει ένα στοιχείο $g \in G$ έτσι ώστε:

$$\mathsf{o}(g) = [\mathsf{o}(g_1), \mathsf{o}(g_2), \cdots, \mathsf{o}(g_n]$$

Επειδή $\mathsf{o}(x) \mid \mathsf{o}(g)$, $\forall x \in G$, προφανώς θα έχουμε: $x^{\mathsf{o}(g)} = e$. Αν υπάρχει $m \in \mathbb{N}$ έτσι ώστε: $x^m = e$, $\forall x \in G$, τότε θα έχουμε $g^m = e$ και άρα $\mathsf{o}(g) \leq m$. Έτσι $\mathsf{o}(g)$ είναι ο μικρότερος θετικός ακέραιος m με την ιδιότητα $x^m = e$, $\forall x \in G$. Τότε όμως από την υπόθεση θα έχουμε ότι

$$\mathsf{o}(g) = \mathsf{o}(G) = |G|$$

Όμως $\langle g\rangle \subseteq G$ και $\mathsf{o}(g) = \langle g\rangle = |G| = \mathsf{o}(G)$ και επομένως:

$$G = \langle g\rangle$$

και άρα η G είναι κυκλική. ■

Ως άμεση συνέπεια του Θεωρήματος 4.2.6 έχουμε το ακόλουθο χρήσιμο αποτέλεσμα:

Θεώρημα 4.2.7. *Έστω $(G,\cdot)$ μια πεπερασμένη αβελιανή ομάδα. Υποθέτουμε ότι για κάθε $d \geq 1$ το πλήθος του σύνολου των λύσεων στην G της εξίσωσης*

$$x^d = e$$

είναι το πολύ d. Τότε η G είναι κυκλική.

Απόδειξη. Για κάθε $d \geq 1$, έστω

$$G_d \;=\; \{x \in G \mid x^d = e\}$$

Τότε από την υπόθεση: $|G_d| \leq d$. Έστω $\mathsf{o}(G) = n$. Γνωρίζουμε ότι $x^n = e$, $\forall x \in G$. Έστω $m \in \mathbb{N}$ έτσι ώστε: $x^m = e$, $\forall x \in G$. Τότε $G = G_m$. Υποθέτουμε ότι $m < n$. Τότε από την υπόθεση θα έχουμε ότι

$$n = |G| = |G_d| \leq m < n$$

το οποίο είναι άτοπο. Άρα $m \geq n$ και επομένως $n = \mathsf{o}(G)$ είναι ο μικρότερος θετικός ακέραιος m έτσι ώστε: $x^m = e$, $\forall x \in G$. Από το Θεώρημα 4.2.6 έπεται ότι η G είναι κυκλική. ■

Το ακόλουθο σημαντικό αποτέλεσμα δίνει έναν ακόμη χαρακτηρισμό κυκλικών ομάδων:

Θεώρημα 4.2.8. *Έστω G μια πεπερασμένη ομάδα τάξης n. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η G είναι κυκλική.*
2. *Για κάθε διαιρέτη d του n υπάρχει το πολύ μία κυκλική υποομάδα της G τάξης d.*

Απόδειξη. «$\Longrightarrow$» Αν η ομάδα G είναι κυκλική, τότε το αποτέλεσμα προκύπτει από το Θεώρημα 4.1.10.

«$\Longleftarrow$» Για το αντίστροφο, ας γράψουμε την G (όπως στην απόδειξη του Θεωρήματος 4.1.15) ως ένωση ξένων ανά δύο συνόλων

$$G = \bigcup_{\mathsf{C} \in \mathsf{Cyc}(G)} \mathsf{Gen}(\mathsf{C}) \qquad (\dagger)$$

όπου η C διατρέχει το σύνολο $\mathsf{Cyc}(G)$ όλων των κυκλικών υποομάδων της G, και $\mathsf{Gen}(\mathsf{C})$ συμβολίζει το σύνολο των γεννητόρων της C. Επομένως

$$n \;=\; |G| \;=\; \sum_{\mathsf{C} \in \mathsf{Cyc}(G)} |\mathsf{Gen}(\mathsf{C})|$$

όπου η άθροιση εκτελείται υπεράνω όλων των κυκλικών υποομάδων C της G. Επειδή η G διαθέτει το πολύ μία κυκλική υποομάδα τάξης d, το Θεώρημα 4.1.15 δίνει

$$n \;=\; \sum_{\mathsf{C} \in \mathsf{Cyc}(G)} |\mathsf{Gen}(\mathsf{C})| \;\leq\; \sum_{d \mid n} \phi(d) = n$$

Επομένως, για κάθε διαιρέτη d του n, υπάρχει ακριβώς μία κυκλική υποομάδα της G τάξης d. Ιδιαίτερα, υπάρχει μια κυκλική υποομάδα τάξης n και έτσι η ομάδα G είναι κυκλική. ■

4.2.3 Εφαρμογή στην Πολλαπλασιαστική Ομάδα ενός Σώματος

Θα δούμε τώρα μια σημαντική εφαρμογή των παραπάνω αποτελεσμάτων στην πολλαπλασιαστική ομάδα των μη μηδενικών στοιχείων ενός σώματος. Η θεωρία σωμάτων θα αναπτυχθεί σε μεταγενέστερο κεφάλαιο ως μέρος της γενικής θεωρίας δακτυλίων.

Για τους σκοπούς της παρούσας παραγράφου σημειώνουμε μόνο ότι μια τριάδα $(\mathbb{K}, +, \cdot)$ αποτελούμενη από ένα σύνολο $\mathbb{K}$ και δύο διμελείς πράξεις: την πράξη της *πρόσθεσης* «+» και την πράξη του *πολλαπλασιασμού* «·» ορισμένες επί του $\mathbb{K}$, καλείται **σώμα**, αν το ζεύγος $(\mathbb{K}, +)$ είναι μια αβελιανή ομάδα με ουδέτερο στοιχείο 0, το ζεύγος $(\mathbb{K}, \cdot)$ είναι ένα μεταθετικό μονοειδές με ουδέτερο στοιχείο 1, ισχύει η επιμεριστική ιδιότητα της πράξης πρόσθεσης «+» ως προς την πράξη πολλαπλασιασμού «·», δηλαδή: $x \cdot (y+z) = x \cdot y + x \cdot z$ και $(x+y) \cdot z = x \cdot z + y \cdot z$, και επιπλέον κάθε μη μηδενικό στοιχείο του $\mathbb{K}$ είναι αντιστρέψιμο ως προς την πράξη «·». Σημαντικά παραδείγματα σωμάτων είναι τα γνωστά μας σύνολα $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ τα οποία θεωρούνται εφοδιασμένα με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού.

Στην παρούσα υποενότητα υποθέτουμε ότι είναι γνωστά στοιχειώδη αποτελέσματα της θεωρίας σωμάτων. Ιδιαίτερα θεωρούμε γνωστές τις ακόλουθες ιδιότητες, οι οποίες μας είναι οικείες από τα σώματα $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$:

(α) Το σύνολο των μη μηδενικών στοιχείων $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ ενός σώματος $\mathbb{K}$, εφοδιασμένο με την πράξη του πολλαπλασιασμού «·», αποτελεί μια (αβελιανή) ομάδα.

(β) Κάθε μη μηδενικό πολυώνυμο $f(x)$ βαθμού n με συντελεστές από ένα σώμα $\mathbb{K}$, έχει το πολύ n ρίζες στο σώμα $\mathbb{K}$, βλέπε το Θεώρημα 9.1.10.

Τώρα μπορούμε να αποδείξουμε το ακόλουθο χρήσιμο αποτέλεσμα.

Θεώρημα 4.2.9. *Έστω $\mathbb{K}$ ένα σώμα και $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ η πολλαπλασιαστική ομάδα τού $\mathbb{K}$. Τότε κάθε πεπερασμένη υποομάδα G της $\mathbb{K}^*$ είναι κυκλική.*

Απόδειξη. Ας υποθέσουμε ότι $|G| = n$ και ότι $d \mid n$. Αν C είναι μια κυκλική υποομάδα της G με τάξη d, τότε από το Θεώρημα του Lagrange προκύπτει ότι $x^d = 1$, για καθένα από τα d στοιχεία $x \in \mathsf{C}$. Αν τώρα υπήρχε ακόμα μία κυκλική υποομάδα τάξης d, τότε αυτή θα περιείχε τουλάχιστον ένα στοιχείο που δεν θα ήταν συγχρόνως και στοιχείο της C, και έτσι η ομάδα G θα διέθετε τουλάχιστον $d+1$ στοιχεία x, τέτοια ώστε $x^d = 1$. Αλλά σε κάθε σώμα, το πολυώνυμο $x^d - 1$ έχει το πολύ d θέσεις μηδενισμού (ρίζες), βλέπε το Θεώρημα 9.1.10. Επομένως η G έχει το πολύ μία κυκλική υποομάδα τάξης d. Έτσι από το Θεώρημα 4.2.8 προκύπτει ότι η G είναι κυκλική. ■

Πόρισμα 4.2.10. *Έστω $\mathbb{K}$ ένα πεπερασμένο σώμα. Τότε η πολλαπλασιαστική ομάδα $\mathbb{K}^*$ του $\mathbb{K}$ είναι κυκλική.*

Για μια διαφορετική απόδειξη του παραπάνω πορίσματος παραπέμπουμε στο Θεώρημα 9.1.13.

4.3 Ασκήσεις

Άσκηση 4.3.1. *Να σχεδιαστεί το διάγραμμα Hasse των υποομάδων των κυκλικών ομάδων:*

1. $\mathbb{Z}_{12}$.
2. $\mathbb{Z}_{16}$.
3. $\mathbb{Z}_{24}$.
4. $\mathbb{Z}_{28}$.
5. $\mathbb{Z}_{36}$.

Για καθεμία από τις παραπάνω κυκλικές ομάδες, να βρεθούν οι γεννήτορες τους.

Άσκηση 4.3.2. *Έστω G μια πεπερασμένη ομάδα τάξης n και υποθέτουμε ότι η G περιέχει ένα στοιχείο a έτσι ώστε $a^{\frac{n}{p}} \neq e$, για κάθε πρώτο διαιρέτη p του n. Να δειχθεί ότι $G = \langle a \rangle$.*

Άσκηση 4.3.3. *Έστω ότι n, m και r είναι ακέραιοι έτσι ώστε $n, m > 0$. Να δειχθεί ότι ορίζοντας*

$$f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_m, \quad f([k]_n) = [rk]_m$$

αποκτούμε έναν ομομορφισμό προσθετικών ομάδων αν και μόνο αν $m \mid nr$.

Άσκηση 4.3.4. *Να δειχθεί ότι μια ομάδα άπειρης τάξης είναι κυκλική αν και μόνο αν είναι ισόμορφη με κάθε μη τετριμμένη υποομάδα της.*

Άσκηση 4.3.5. *Να δειχθεί ότι ο δείκτης $[G : H]$ κάθε γνήσιας υποομάδας H μιας άπειρης κυκλικής ομάδας G είναι πεπερασμένος. Επιπλέον να δειχθεί ότι για κάθε θετικό ακέραιο n, υπάρχει υποομάδα H της G με δείκτη $[G : H]$ ίσο με n.*

Άσκηση 4.3.6. *Έστω ότι G είναι μια αβελιανή ομάδα με τάξη pq, όπου p q είναι διακεκριμένοι πρώτοι αριθμοί. Να δειχθεί ότι η ομάδα G είναι κυκλική.*

Άσκηση 4.3.7. *Έστω G μια κυκλική ομάδα η οποία έχει ακριβώς οκτώ υποομάδες, τρεις εκ των οποίων έχουν τάξη 2, 19 και 53. Να βρεθεί (με ποια γνωστή σας ομάδα είναι ισόμορφη) η G.*

Άσκηση 4.3.8. *Να δειχθεί ότι η προσθετική ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών δεν είναι κυκλική. Είναι οι προσθετικές ομάδες $(\mathbb{R}, +)$ και $(\mathbb{C}, +)$ των πραγματικών και μιγαδικών αριθμών αντίστοιχα κυκλικές;*

Άσκηση 4.3.9. **1.** *Να δειχθεί ότι, αν μια αβελιανή ομάδα G περιέχει δύο στοιχεία a, b τάξης 2 με $a \neq b$, τότε η G περιέχει και μια μη κυκλική υποομάδα H τάξης 4. Δείξτε ότι η H είναι ισόμορφη με την ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$.*

2. *Δείξτε ότι δεν υπάρχει αβελιανή ομάδα, η οποία να διαθέτει ακριβώς δύο στοιχεία τάξης 2.*

Άσκηση 4.3.10. *Θεωρούμε την ομάδα ευθύ γινόμενο $G = \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ των κυκλικών ομάδων $\mathbb{Z}_{n_i}$, $1 \leq i \leq k$. Να δειχθεί ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα G είναι κυκλική.*
2. $1 \leq i \neq j \leq k \implies (n_i, n_j) = 1$.

Άσκηση 4.3.11. *Έστω G μια ομάδα η οποία έχει ακριβώς τρεις υποομάδες. Να δειχθεί ότι η G είναι κυκλική τάξης p^2, όπου p είναι ένας πρώτος αριθμός.*

Άσκηση 4.3.12. *Έστω ότι G είναι μια ομάδα η οποία έχει ακριβώς (α) τέσσερις, (β) πέντε, και (γ) έξι υποομάδες. Τι μπορείτε να πείτε σε κάθε περίπτωση για την τάξη και τη δομή της G;*

Άσκηση 4.3.13. *Θεωρούμε μια κυκλική ομάδα G τάξης n. Να βρεθεί το πλήθος των γεννητόρων της G, καθώς και το διάγραμμα Hasse των υποομάδων της G στις ακόλουθες περιπτώσεις:*

(a) *$n = pq$, όπου p και q είναι διακεκριμένοι πρώτοι αριθμοί.*

(a) *$n = pqr$, όπου p, q και r είναι διακεκριμένοι πρώτοι αριθμοί.*

(b) $n = p^n$, *όπου* p *είναι ένας πρώτος αριθμός και* $n \geq 1$ *είναι ένας φυσικός αριθμός.*

Άσκηση 4.3.14. (a) *Να δοθεί παράδειγμα μιας πεπερασμένης ομάδας* G *τάξης* $\gneqq 3$ *έτσι ώστε οι μόνες υποομάδες της* G *να είναι οι* $\{e_G\}$ *και* G*. Υπάρχει μη αβελιανή ομάδα με αυτή την ιδιότητα;*

(b) *Υπάρχει ομάδα με την προηγούμενη ιδιότητα η οποία να έχει άπειρη τάξη;*

Άσκηση 4.3.15. *Έστω* G *μια πεπερασμένη ομάδα με τάξη* pq*, όπου* p *και* q *είναι διαφορετικοί πρώτοι αριθμοί. Αν η ομάδα* G *έχει μια κανονική υποομάδα τάξης* p *και μια κανονική υποομάδα τάξης* q*, να δειχθεί ότι η ομάδα* G *είναι κυκλική.*

Άσκηση 4.3.16. *Να προσδιοριστούν όλες οι κυκλικές ομάδες οι οποίες διαθέτουν ακριβώς δύο γεννήτορες.*

Κεφάλαιο 5

Ομάδες Μεταθέσεων

Στο παρόν Κεφάλαιο θα μελετήσουμε τη βασική θεωρία μεταθέσεων, κυρίως επί πεπερασμένων συνόλων, με άλλα λόγια θα μελετήσουμε τις βασικές ιδιότητες των συμμετρικών ομάδων S_n, $n \geq 1$. Στις τρεις πρώτες παραγράφους του παρόντος Κεφαλαίου ακολουθούμε στενά την προσέγγιση του [25].

Υπενθυμίζουμε πρώτα κάποιες βασικές έννοιες περί μεταθέσεων από την υποενότητα 2.2.6.

Αν X είναι ένα μη κενό σύνολο, τότε ορίζεται το μονοειδές $(\mathsf{Map}(X), \circ)$, όπου $\mathsf{Map}(X) = \{f : X \longrightarrow X \mid f : \text{απεικόνιση}\}$ είναι το σύνολο των απεικονίσεων του X, και «$\circ$» είναι η πράξη της σύνθεσης απεικονίσεων:

$$\circ : \mathsf{Map}(X) \times \mathsf{Map}(X) \longrightarrow \mathsf{Map}(X), \quad (f, g) \longmapsto f \circ g$$

Από την Πρόταση 0.2.8, η ομάδα των αντιστρέψιμων στοιχείων του μονοειδούς $(\mathsf{Map}(X), \circ)$ είναι

$$\mathsf{U}(\mathsf{Map}(X), \circ) = \{f : X \longrightarrow X \mid f : \text{απεικόνιση «1-1» και «επί»}\} = \mathsf{S}(X)$$

και άρα αποκτούμε την ομάδα $(\mathsf{S}(X), \circ)$ η οποία καλείται η **ομάδα των μεταθέσεων** ή η **συμμετρική ομάδα** του συνόλου X.

Υπενθυμίζουμε ότι η συμμετρική ομάδα $\mathsf{S}(X)$ επί ενός συνόλου X καθορίζεται με ακρίβεια ισομορφισμού μόνο από το πλήθος των στοιχείων του συνόλου X: αν X και Y είναι δύο μη κενά σύνολα με το ίδιο πλήθος στοιχείων, $|X| = |Y|$, τότε οι συμμετρικές ομάδες $\mathsf{S}(X)$ και $\mathsf{S}(Y)$ επί των X και Y είναι ισόμορφες: $\mathsf{S}(X) \cong \mathsf{S}(Y)$. Έτσι, χρησιμοποιώντας ως μοντέλο ενός συνόλου με n το πλήθος στοιχεία το σύνολο $\mathbb{N}_n = \{1, 2, \cdots, n\}$, ορίζουμε την n-**οστή συμμετρική ομάδα** ως την συμμετρική ομάδα επί του συνόλου $\mathbb{N}_n$. Τέλος, σημειώνουμε ότι, σύμφωνα με τις Προτάσεις 2.2.7 και 1.3.23, η συμμετρική ομάδα $\mathsf{S}(X)$ επί ενός συνόλου X είναι αβελιανή αν και μόνο αν $|X| \leq 2$, και αν $|X| = n < \infty$, τότε: $\mathsf{o}(\mathsf{S}(X)) = n!$. Έτσι η n-οστή συμμετρική ομάδα S_n έχει τάξη $n!$ και είναι αβελιανή αν και μόνο αν $n \leq 2$.

Υπενθυμίζουμε ότι τα στοιχεία της S_n, δηλαδή οι «1-1» και «επί» απεικόνισεις

$$\sigma : \{1, 2, \cdots, n\} \longrightarrow \{1, 2, \cdots, n\}, \quad i \longmapsto \sigma(i)$$

παριστώνται, χάριν εποπτείας, με έναν $2 \times n$ πίνακα

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

του οποίου η πρώτη γραμμή περιέχει τα στοιχεία του συνόλου $\mathbb{N}_n$ και η δεύτερη γραμμή περιέχει τις εικόνες των στοιχείων αυτών μέσω της μετάθεσης σ. Μερικές φορές μια μετάθεση σ παριστάται και αναγράφοντας πλήρως τη δράση της στα στοιχεία του συνόλου $\mathbb{N}_n$ ως εξής $i \xrightarrow{\sigma} \sigma(i)$, $1 \leq i \leq n$, για παράδειγμα η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 5 & 7 & 6 & 1 & 4 & 8 \end{pmatrix}$$

γράφεται με αυτόν τον τρόπο ως εξής:

$$1 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1, \qquad 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2, \qquad 6 \xrightarrow{\sigma} 6$$

Αν $\sigma, \tau \in \mathsf{S}_n$, τότε για το γινόμενο $\sigma \cdot \tau$ των μεταθέσεων σ και τ, δηλαδή για τη σύνθεση των απεικονίσεων σ και τ, όπου πρώτα εφαρμόζουμε τη συνάρτηση τ, θα έχουμε

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \tau(1) & \tau(2) & \cdots & \tau(n-1) & \tau(n) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n-1)) & \sigma(\tau(n)) \end{pmatrix}$$

Η ταυτοτική μετάθεση, δηλαδή η ταυτοτική απεικόνιση $\mathrm{Id}_{\mathbb{N}_n}$, συμβολίζεται συνήθως με ι και είναι

$$\iota = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ 1 & 2 & \cdots & n-1 & n \end{pmatrix}$$

Η αντίστροφη σ^{-1} της μετάθεσης $\sigma = \begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}$ είναι η αντίστροφη απεικόνιση σ^{-1} της σ και μπορεί να υπολογιστεί ως εξής:

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(i) & \cdots & \sigma(n-1) & \sigma(n) \\ 1 & 2 & \cdots & i & \cdots & n-1 & n \end{pmatrix}$$

Παράδειγμα 5.0.1. Θεωρούμε την συμμετρική ομάδα S_{13} και τα στοιχεία της

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 1 & 4 & 5 & 7 & 3 & 6 & 10 & 2 & 8 & 13 & 11 & 12 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 7 & 3 & 5 & 13 & 8 & 1 & 2 & 9 & 11 & 4 & 10 & 12 & 6 \end{pmatrix}$$

Με βάση τις παραπάνω παρατηρήσεις, θα υπολογίσουμε τα στοιχεία $\sigma \circ \tau$, $\tau \circ \sigma$ και σ^{-1}, τ^{-1}. Θα έχουμε:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 6 & 4 & 7 & 12 & 10 & 9 & 1 & 2 & 13 & 5 & 8 & 11 & 3 \end{pmatrix}$$

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 11 & 7 & 13 & 8 & 2 & 5 & 1 & 4 & 3 & 9 & 6 & 10 & 12 \end{pmatrix}$$

$$\begin{aligned} \sigma^{-1} &= \begin{pmatrix} \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \sigma(5) & \sigma(6) & \sigma(7) & \sigma(8) & \sigma(9) & \sigma(10) & \sigma(11) & \sigma(12) & \sigma(13) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 9 & 1 & 4 & 5 & 7 & 3 & 6 & 10 & 2 & 8 & 13 & 11 & 12 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 2 & 9 & 6 & 3 & 4 & 7 & 5 & 10 & 1 & 8 & 12 & 13 & 11 \end{pmatrix} \end{aligned}$$

$$\begin{aligned} \tau^{-1} &= \begin{pmatrix} \tau(1) & \tau(2) & \tau(3) & \tau(4) & \tau(5) & \tau(6) & \tau(7) & \tau(8) & \tau(9) & \tau(10) & \tau(11) & \tau(12) & \tau(13) \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 3 & 5 & 13 & 8 & 1 & 2 & 9 & 11 & 4 & 10 & 12 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 6 & 7 & 2 & 10 & 3 & 13 & 1 & 5 & 8 & 11 & 9 & 12 & 14 \end{pmatrix} \quad \surd \end{aligned}$$

5.1 Τροχιές και ανάλυση σε κύκλους

Οι ομάδες μεταθέσεων S_n έχουν το πλεονέκτημα ότι τα στοιχεία τους είναι πολύ συγκεκριμένα και μπορούμε να κάνουμε εύκολα υπολογισμούς με αυτά, ιδιαίτερα όταν το n είναι μικρό. Για περαιτέρω διευκόλυνση στους υπολογισμούς μας αλλά και για ισχυρούς θεωρητικούς λόγους είναι αναγκαίο να μπορούμε να αναλύσουμε μια τυχούσα μετάθεση σε απλούστερες μεταθέσεις, αν είναι δυνατόν με μοναδικό τρόπο. Ποιες είναι όμως οι απλούστερες μεταθέσεις; Είναι φανερό ότι μεταθέσεις $\sigma \in S_n$ οι οποίες εναλλάσσουν με κυκλικό τρόπο κάποια στοιχεία, όσο το δυνατόν λιγότερα, του συνόλου $\mathbb{N}_n$ και αφήνουν σταθερά τα υπόλοιπα, έχουν απλούστερη δομή από μια τυχούσα μετάθεση. Έτσι, με βάση αυτή την παρατήρηση, ο σκοπός μας είναι να αναλύσουμε μια μετάθεση σε γινόμενο τέτοιων απλούστερων μεταθέσεων με μοναδικό τρόπο.

Για να το πετύχουμε αυτό εργαζόμαστε ως εξής:

Έστω $\sigma \in S_n$ μια τυχούσα μετάθεση. Με βάση την σ, ορίζουμε μια σχέση «$\sim_\sigma$» επί του συνόλου $\mathbb{N}_n$, ως εξής:

$$\forall i, j \in \mathbb{N}_n: \quad i \sim_\sigma j \quad \Longleftrightarrow \quad \exists z \in \mathbb{Z}: \ \sigma^z(i) = j$$

Η ακόλουθη βοηθητική πρόταση πιστοποιεί ότι η σχέση «$\sim_\sigma$» είναι μια σχέση ισοδυναμίας επί του συνόλου $\mathbb{N}_n$.

Λήμμα 5.1.1. *Ας είναι $\sigma \in S_n$ μια μετάθεση του συνόλου $\mathbb{N}_n = \{1, 2, \ldots, n\}$, τότε η σχέση «$\sim_\sigma$» είναι μια σχέση ισοδυναμίας επί του $\mathbb{N}_n$.*

Απόδειξη.

1. Αν $i \in \mathbb{N}_n$, τότε $i \sim_\sigma i$, διότι $\sigma^0(i) = i$. Ώστε η σχέση «$\sim_\sigma$» ικανοποιεί την ανακλαστική ιδιότητα.

2. Αν $i, j \in \mathbb{N}_n$ και ισχύει $i \sim_\sigma j$, τότε $\exists z \in \mathbb{Z}$ με $\sigma^z(i) = j$. Συνεπώς, $\sigma^{-z}(j) = i$ και γι' αυτό $j \sim_\sigma i$. Ώστε η σχέση «$\sim_\sigma$» ικανοποιεί τη συμμετρική ιδιότητα.

3. Αν $i, j, k \in \mathbb{N}_n$ με $i \sim_\sigma j$ και $j \sim_\sigma k$, τότε $\exists z, w \in \mathbb{Z}$ με $\sigma^z(i) = j$ και $\sigma^w(j) = k$. Συνεπώς, $\sigma^{w+z}(i) = \sigma^w(\sigma^z(i)) = \sigma^w(j) = k$ και γι' αυτό $i \sim_\sigma k$. Άρα η σχέση «$\sim_\sigma$» ικανοποιεί τη μεταβατική ιδιότητα.

Επομένως η σχέση «$\sim_\sigma$» είναι μια σχέση ισοδυναμίας επί του συνόλου $\mathbb{N}_n$. ■

Τώρα, για κάθε μετάθεση $\sigma \in S_n$, το σύνολο $\mathbb{N}_n$ διαμερίζεται στις κλάσεις ισοδυναμίας της σχέσης ισοδυναμίας «$\sim_\sigma$», τις οποίες ονομάζουμε τροχιές της σ:

Ορισμός 5.1.2. *Η σ-**τροχιά** του στοιχείου $i \in \mathbb{N}_n$ ορίζεται να είναι η κλάση ισοδυναμίας του i ως προς τη σχέση ισοδυναμίας «$\sim_\sigma$».*

Συνήθως, η *σ-τροχιά* του στοιχείου $i \in \mathbb{N}_n$ συμβολίζεται με $\mathcal{O}_\sigma(i)$ ή $[i]_\sigma$. Έτσι θα έχουμε:

$$\mathcal{O}_\sigma(i) = \{j \in \mathbb{N}_n \mid j \sim_\sigma i\} = \{j \in \mathbb{N}_n \mid \exists z \in \mathbb{Z}: \sigma^z(j) = i\} = \{\sigma^z(i) \in \mathbb{N}_n \mid z \in \mathbb{Z}\}$$

Παράδειγμα 5.1.3. Θα προσδιορίσουμε τις τροχιές των στοιχείων του $\mathbb{N}_n = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ για καθεμία από τις επόμενες μεταθέσεις της S_9:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 5 & 7 & 6 & 1 & 4 & 8 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 3 & 2 & 1 & 4 & 5 & 6 & 9 & 7 \end{pmatrix},$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix},$$

- Παρατηρούμε ότι

$$1 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1, \qquad 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2, \qquad 6 \xrightarrow{\sigma} 6$$

Σύμφωνα με τον ορισμό, η σ διαθέτει τρεις τροχιές, τις ακόλουθες:

$$\mathcal{O}_\sigma(1) = \{1, 9, 8, 4, 5, 7\}, \qquad \mathcal{O}_\sigma(2) = \{2, 3\}, \qquad \mathcal{O}_\sigma(6) = \{6\}$$

- Παρατηρούμε ότι

$$1 \xrightarrow{\tau} 8 \xrightarrow{\tau} 9 \xrightarrow{\tau} 7 \xrightarrow{\tau} 6 \xrightarrow{\tau} 5 \xrightarrow{\tau} 4 \xrightarrow{\tau} 1, \qquad 2 \xrightarrow{\tau} 3 \xrightarrow{\tau} 2.$$

Σύμφωνα με τον ορισμό, η τ διαθέτει τρεις τροχιές, τις ακόλουθες:

$$\mathcal{O}_\tau(1) = \{1,8,9,7,6,5,4\}, \qquad \mathcal{O}_\tau(2) = \{2,3\}$$

- Παρατηρούμε ότι

$$1 \xrightarrow{\rho} 9 \xrightarrow{\rho} 1, \;\; 2 \xrightarrow{\rho} 3 \xrightarrow{\rho} 2, \;\; 4 \xrightarrow{\rho} 4, \;\; 5 \xrightarrow{\rho} 5, \;\; 6 \xrightarrow{\rho} 6, \;\; 7 \xrightarrow{\rho} 7, \;\; 8 \xrightarrow{\rho} 8.$$

Σύμφωνα με τον ορισμό, η ρ διαθέτει τρεις τροχιές, τις ακόλουθες:

$$\mathcal{O}_\rho(1) = \{1,9\}, \quad \mathcal{O}_\rho(2) = \{2,3\}, \quad \mathcal{O}_\rho(4) = \{4\}, \quad \mathcal{O}_\rho(5) = \{5\}, \quad \mathcal{O}_\rho(6) = \{6\}, \quad \mathcal{O}_\rho(7) = \{7\}, \quad \mathcal{O}_\rho(8) = \{8\} \;\; \surd$$

Σταθεροποιούμε μια μετάθεση $\sigma \in \mathsf{S}_n$. Για κάθε στοιχείο $i \in \mathbb{N}_n = \{1,2,\cdots,n\}$, θεωρούμε την σ-τροχιά $\mathcal{O}_\sigma(i) = \{\sigma^z(i) \mid z \in \mathbb{Z}\}$ του i. Επειδή $\mathcal{O}_\sigma(i) \subseteq \mathbb{N}_n$, έπεται ότι το πλήθος των στοιχείων της σ-τροχιάς $\mathcal{O}_\sigma(i)$ είναι πεπερασμένο και μάλιστα είναι $\leq n = |\mathbb{N}_n|$. Προφανώς τότε δεν είναι δυνατόν όλες οι ακέραιες δυνάμεις $\sigma^z(i)$ να είναι διαφορετικές μεταξύ τους, αφού τότε το πλήθος των στοιχείων της τροχιάς $\mathcal{O}_\sigma(i)$ θα ήταν άπειρο. Επομένως υπάρχουν $z, w \in \mathbb{Z}$ με $z \neq w$, ας πούμε $z > w$ και $\sigma^z(i) = \sigma^w(i)$. Επομένως, $\sigma^{z-w}(i) = i$ με $z - w \in \mathbb{N}$. Έτσι συμπεραίνουμε ότι το σύνολο

$$\mathcal{M}_\sigma(i) = \{m \in \mathbb{N} \mid \sigma^m(i) = i\}$$

δεν είναι κενό σύνολο και γι' αυτό διαθέτει ελάχιστο στοιχείο, έστω

$$s := \min \mathcal{M}_\sigma(i)$$

δηλαδή s είναι ο ελάχιστος φυσικός αριθμός με $\sigma^s(i) = i$.

Ισχυρισμός: Είναι

$$\mathcal{O}_\sigma(i) = \{i, \sigma(i), \sigma^2(i), \cdots, \sigma^k(i), \sigma^{k+1}(i), \cdots, \sigma^{s-1}(i)\}$$

Πράγματι, τα στοιχεία $\sigma^k(i), 0 \leq k \leq s-1$ είναι ανά δύο διαφορετικά, διότι, αν, $\sigma^k(i) = \sigma^l(i)$, όπου $0 \leq k, l \leq s-1$ με $k \neq l$, ας πούμε $k > l$, τότε $\sigma^{(k-l)}(i) = i$. Αυτό όμως είναι άτοπο διότι το s είναι το ελάχιστο στοιχείο του συνόλου $\mathcal{M}_\sigma(i)$, διότι $k - l \in \mathbb{N}$, $k - l < s$ και $\sigma^{k-l}(i) = i$. Για την απόδειξη του ισχυρισμού, αρκεί να δείξουμε ότι για κάθε στοιχείο $\sigma^m(i)$, $m \in \mathbb{Z}$, της σ-τροχιάς του i, έχουμε $\sigma^m(i) = \sigma^k(i)$, όπου $0 \leq k \leq s-1$. Πράγματι από την Ευκλείδεια διαίρεση του m με το s θα έχουμε:

$$m = qs + k, \qquad q \in \mathbb{Z}, \quad \text{και} \quad 0 \leq k \leq s-1$$

Πράγματι, αν $q = 0$, τότε $m = k$ και $\sigma^m(i) = \sigma^k(i)$. Αν $q \geq 1$, τότε, χρησιμοποιώντας ότι $\sigma^s(i) = i$, θα έχουμε:

$$\sigma^m(i) = \sigma^{qs+k}(i) = \sigma^k(\sigma^{qs}(i)) = \sigma^k((\sigma^s)^q(i))) = \sigma^k((\underbrace{\sigma^s \circ \sigma^s \circ \cdots \circ \sigma^s}_{q-\text{φορές}})(i)) = \sigma^k(i)$$

Αν $q \leq -1$, έστω $q = -r$, όπου $r \geq 1$, τότε, χρησιμοποιώντας ότι $\sigma^{-s}(i) = i$, θα έχουμε:

$$\sigma^m(i) = \sigma^{qs+k}(i) = \sigma^k(\sigma^{qs}(i)) = \sigma^k((\sigma^s)^q(i))) = \sigma^k((\sigma^s)^{-r}(i))) = \sigma^k((\sigma^{-s})^r(i))) = \sigma^k((\underbrace{\sigma^{-s} \circ \sigma^{-s} \circ \cdots \circ \sigma^{-s}}_{r-\text{φορές}})(i)) = \sigma^k(i)$$

Άρα σε κάθε περίπτωση ισχύει ότι για κάθε $m \in \mathbb{Z}$, υπάρχει k με $0 \leq k \leq s-1$ έτσι ώστε: $\sigma^m(i) = \sigma^k(i)$.

Παρατήρηση 5.1.4. Έστω ότι $\mathcal{O}_\sigma(i)$ και $\mathcal{O}_\sigma(j)$ είναι σ-τροχιές δύο στοιχείων $i, j \in \mathbb{N}_n = \{1,2,\cdots,n\}$ της μετάθεσης $\sigma \in \mathsf{S}_n$. Αν $j \in \mathcal{O}_\sigma(i)$, τότε:

$$\text{είτε} \quad \mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(j) \qquad \text{είτε} \qquad \mathcal{O}_\sigma(i) \cap \mathcal{O}_\sigma(j) = \emptyset$$

Πράγματι, αυτό προκύπτει από το ότι οι τροχιές $\mathcal{O}_\sigma(i)$ και $\mathcal{O}_\sigma(j)$ είναι κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας «$\sim_\sigma$», και άρα είτε θα συμπίπτουν, δηλαδή $\mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(j)$, ή θα είναι ξένες, δηλαδή $\mathcal{O}_\sigma(i) \cap \mathcal{O}_\sigma(j) = \emptyset$.

Ιδιαίτερα αν $j \in \mathcal{O}_\sigma(i)$, δηλαδή αν $j = \sigma^k(i)$ για κάποιον ακέραιο k, τότε: $\mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(j)$. Για παράδειγμα, ας υποθέσουμε ότι

$$\mathcal{O}_\sigma(i) = \left\{i,\ \sigma(i),\ \cdots,\ \sigma^{s-1}(i)\right\}$$

Αν $j = \sigma^k(i)$ για κάποιον ακέραιο k με $1 \le k \le s-1$, τότε

$$\mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(j) = \mathcal{O}_\sigma(\sigma^k(i)) = \left\{j,\ \sigma(j),\ \cdots,\ \sigma^{s-1}(j)\right\}$$

Σημειώνουμε ότι στην περιγραφή των τροχιών παίζει ρόλο και πρέπει να διατηρείται η σειρά με την οποία εμφανίζονται τα στοιχεία της τροχιάς, ως εικόνες μέσω της μετάθεσης σ, διότι καθένα στοιχείο στην τροχιά είναι εικόνα, μέσω της σ, του προηγούμενου. Έτσι, αν και ως σύνολα $\left\{i,\ \sigma(i),\ \sigma^2(i),\ \cdots,\ \sigma^{s-1}(i)\right\} = \left\{\sigma^2(i),\ \sigma(i),\ i,\ \cdots,\ \sigma^{s-1}(i)\right\}$, το δεύτερο σύνολο δεν περιγράφει αναγκαστικά τροχιά της σ, διότι, για παράδειγμα, γενικά $\sigma(\sigma^2(i)) = \sigma^3(i) \neq \sigma(i)$. ▲

Παρατήρηση 5.1.5. Θέλοντας να προσδιορίσουμε τις τροχιές μιας μετάθεσης $\sigma \in \mathsf{S}_n$, εργαζόμαστε ως εξής: ξεκινάμε από ένα τυχόν στοιχείο i_1 του συνόλου $\mathbb{N}_n$ και προσδιορίζουμε τον ελάχιστο θετικό ακέραιο s_1 έτσι ώστε $\sigma^{s_1}(i_1) = i_1$. Τότε η σ τροχιά του i_1 θα είναι το σύνολο

$$\mathcal{O}_\sigma(i_1) = \left\{i_1,\ \sigma(i_1),\ \cdots,\ \sigma^{s_1-1}(i_1)\right\}$$

Κατόπιν επιλέγουμε ένα στοιχείο, αν υπάρχει, στο σύνολο $\mathbb{N}_n \setminus \mathcal{O}_\sigma(i_1)$, χάριν ευκολίας ας υποθέσουμε ότι αυτό είναι το i_2. Προσδιορίζουμε τον ελάχιστο θετικό ακέραιο s_2 έτσι ώστε $\sigma^{s_2}(i_2) = i_2$. Τότε η σ τροχιά του i_2 θα είναι το σύνολο

$$\mathcal{O}_\sigma(i_2) = \left\{i_2,\ \sigma(i_2),\ \cdots,\ \sigma^{s_2-1}(i_2)\right\}$$

Παρατηρούμε ότι οι τροχιές $\mathcal{O}_\sigma(i_1)$ και $\mathcal{O}_\sigma(i_2)$ είναι ξένες, $\mathcal{O}_\sigma(i_1) \cap \mathcal{O}_\sigma(i_2) = \emptyset$, ως διακεκριμένες κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας «$\sim_\sigma$».

Κατόπιν επιλέγουμε ένα στοιχείο, αν υπάρχει, στο σύνολο $\mathbb{N}_n \setminus (\mathcal{O}_\sigma(i_1) \cup \mathcal{O}_\sigma(i_2))$, χάριν ευκολίας ας υποθέσουμε ότι αυτό είναι το i_3. Προσδιορίζουμε τον ελάχιστο θετικό ακέραιο s_3 έτσι ώστε $\sigma^{s_3}(i_3) = i_3$. Τότε η σ τροχιά του i_3 θα είναι το σύνολο

$$\mathcal{O}_\sigma(i_3) = \left\{i_3,\ \sigma(i_3),\ \cdots,\ \sigma^{s_3-1}(i_3)\right\}$$

Παρατηρούμε ότι οι τροχιές $\mathcal{O}_\sigma(i_t), 1 \le t \le 3$, είναι ανα δύο ξένες μεταξύ τους $\mathcal{O}_\sigma(i_k) \cap \mathcal{O}_\sigma(i_l) = \emptyset$, $1 \le k \neq l \le 3$, ως διακεκριμένες κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας «$\sim_\sigma$».

Συνεχίζοντας αυτή τη διαδικασία, επειδή το σύνολο $\mathbb{N}_n$ είναι πεπερασμένο, έπεται ότι υπάρχει θετικός ακέραιος r έτσι ώστε να έχουμε:

$$\mathbb{N}_n = \{1, 2, \cdots, n\} = \mathcal{O}_\sigma(i_1) \bigcup \mathcal{O}_\sigma(i_2) \bigcup \cdots \bigcup \mathcal{O}_\sigma(i_r)$$

Επειδή οι τροχιές, ως κλάσεις ισοδυναμίας ως προς τη σχέση ισοδυναμίας «$\sim_\sigma$» είναι ξένες ανα δύο, $\mathcal{O}_\sigma(i_k) \cap \mathcal{O}_\sigma(i_l) = \emptyset$, $1 \le k \neq l \le r$, έπεται ότι η παραπάνω ένωση είναι ξένη ένωση συνόλων. Επομένως θα έχουμε:

$$n = |\mathbb{N}_n| = \sum_{k=1}^{r} |\mathcal{O}_\sigma(i_k)| = s_1 + s_2 + \cdots + s_r \quad ▲$$

Παρατήρηση 5.1.6. Παρατηρούμε ότι κάθε τροχιά $\mathcal{O}_\sigma(i)$, $i \in \mathbb{N}_n$, μιας μετάθεσης σ μπορεί να αναπαρασταθεί με τη βοήθεια ενός προσανατολισμένου γραφήματος. Το γράφημα αυτό αποτελείται από κορυφές και προσανατολισμένα βέλη.[1] Κορυφές του γραφήματος είναι τα στοιχεία της τροχιάς $\mathcal{O}_\sigma(i) \subseteq \mathbb{N}_n$. Υπάρχει ένα προσανατολισμένο βέλος με αρχή την κορυφή k και τέλος την κορυφή l, ακριβώς όταν $l = \sigma(k)$. Επομένως οι κορυφές του γραφήματος της τροχιάς $\mathcal{O}_\sigma(i)$ είναι τα στοιχεία $i, \sigma(i), \cdots, \sigma^{s-1}(a)$, όπου όπως παραπάνω s είναι ο μικρότερος μη αρνητικός ακέραιος έτσι ώστε $\sigma^s(i) = i$. Κάθε κορυφή $\sigma^k(i)$ συνδέεται με μια προσανατολισμένη ακμή με την κορυφή $\sigma^{k+1}(i)$, όταν $0 \le k \le s-2$ και επιπλέον η κορυφή $\sigma^{(s-1)}(i)$ συνδέεται με την κορυφή $\sigma^s(i) = i$. Συνεπώς, το γράφημα είναι κυκλικό. ▲

[1] Δηλαδή, τμήματα γραμμών ή τόξα κύκλου που το ένα σημείο τους θεωρείται η αρχή και το άλλο το τέλος.

Η παρατήρηση μας οδηγεί φυσιολογικά στους ακόλουθους ορισμούς.

Ορισμός 5.1.7. *Έστω σ μια μετάθεση στη συμμετρική ομάδα S_n.*

1. *Η μετάθεση της σ καλείται* **κύκλος** *της S_n, αν διαθέτει το πολύ μια τροχιά με περισσότερα του ενός στοιχεία.*
2. ***Μήκος** ενός κύκλου σ ονομάζουμε το πλήθος των στοιχείων εκείνης της τροχιάς του, που έχει το μεγαλύτερο πλήθος στοιχείων.*

   *Αν το μήκος ενός κύκλου είναι s, τότε ο κύκλος καλείται s-**κύκλος**.*
3. *Ένας 2-κύκλος σ, δηλαδή ένας κύκλος μήκους 2, καλείται **αντιμετάθεση**.*

Με βάση τον παραπάνω ορισμό, καμία από τις μεταθέσεις του παραδείγματος 5.1.3 δεν είναι κύκλος. Για παράδειγμα, η μετάθεση σ δεν είναι κύκλος διότι διαθέτει δύο τροχιές με περισσότερα απόμ ένα στοιχεία: την τροχιά του 1 η οποία έχει 6 στοιχεία, τα $1,9,8,4,5,7$ και την τροχιά του 2 η οποία έχει 2 στοιχεία, τα $2,3$.

Παράδειγμα 5.1.8. Η μετάθεση

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix} \in \mathsf{S}_8$$

είναι ένας κύκλος της S_8 αφού $\mathcal{O}_\mu(1) = \{1,2,3,4,5,6,7,8\}$. Το μήκος του κύκλου μ είναι 8.

Η μετάθεση

$$\nu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 2 & 4 & 5 & 6 & 7 & 3 \end{pmatrix} \in \mathsf{S}_8$$

είναι επίσης ένας κύκλος της S_8 αφού $\mathcal{O}_\nu(1) = \{1\}$, $\mathcal{O}_\nu(2) = \{2,8,3\}$, $\mathcal{O}_\nu(4) = \{4\}$, $\mathcal{O}_\nu(5) = \{5\}$, $\mathcal{O}_\nu(6) = \{6\}$ και $\mathcal{O}_\nu(7) = \{7\}$. Το μήκος του κύκλου ν είναι 3.

Η μετάθεση

$$\zeta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 4 & 5 & 6 & 3 & 8 \end{pmatrix} \in \mathsf{S}_8$$

είναι ένας κύκλος της S_8 αφού $\mathcal{O}_\zeta(1) = \{1\}$, $\mathcal{O}_\zeta(2) = \{2\}$, $\mathcal{O}_\zeta(3) = \{3,7\}$, $\mathcal{O}_\zeta(4) = \{4\}$, $\mathcal{O}_\zeta(5) = \{5\}$, $\mathcal{O}_\zeta(6) = \{6\}$, και $\mathcal{O}_\zeta(8) = \{8\}$. Το μήκος του κύκλου ν είναι 2, δηλαδή ο κύκλος ζ είναι μια αντιμετάθεση της S_8.

Η μετάθεση

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 8 \end{pmatrix} \in \mathsf{S}_8$$

δεν είναι ένας κύκλος της S_8, αφού έχει περισσότερες από μία τροχιές με περισσότερα του ενός στοιχεία. Πράγματι, $\mathcal{O}_\xi(1) = \{1,2\}$ και $\mathcal{O}_\xi(3) = \{3,4\}$. Επειδή η μετάθεση ξ δεν είναι κύκλος, δεν έχει νόημα να μιλήσουμε για το μήκος της ξ. $\surd$

Παρατήρηση 5.1.9. 1. Το ταυτοτικό στοιχείο της S_n, δηλαδή η μετάθεση

$$\iota = \begin{pmatrix} 1 & 2 & \cdots & i & i+1 & \cdots & n \\ 1 & 2 & \cdots & i & i+1 & \cdots & n \end{pmatrix}$$

είναι ένας κύκλος μήκους 1 αφού κάθε τροχιά του αποτελείται από ακριβώς ένα στοιχείο: $\mathcal{O}_\iota(i) = \{i\}$, $\forall i \in \mathbb{N}_n$. Αλλά και αντίστροφα, αν κάθε τροχιά μιας μεταθεσης $\sigma \in \mathsf{S}_n$ αποτελείται από ακριβώς ένα στοιχείο, τότε η σ διαθέτει n το πλήθος διαφορετικές τροχιές οι οποίες θα είναι $\mathcal{O}_\sigma(i) = \{i\}$, $1 \le i \le n$, και τότε προφανώς η σ συμπίπτει με την ταυτοτική μετάθεση ι.

2. Αν μια μετάθεση $\sigma \in \mathsf{S}_n$ είναι ένας κύκλος, ο οποίος δεν συμπίπτει με την ταυτοτική μετάθεση ι, τότε υπάρχει κάποιο στοιχείο $j \in \mathbb{N}_n = \{1,2,\ldots,n\}$ με $\sigma(j) \neq j$. Έτσι η σ-τροχιά του j θα περιέχει περισσότερα του ενός στοιχεία. Επειδή η μετάθεση σ είναι κύκλος, έπεται ότι η τροχιά $\mathscr{O}_\sigma(j)$ είναι η μοναδική τροχιά του σ η οποία αποτελείται από περισσότερα του ενός στοιχεία και μάλιστα

$$\mathscr{O}_\sigma(j) = \{j, \sigma(j), \sigma^2(j), \cdots, \sigma^i(j), \sigma^{i+1}(j), \cdots, \sigma^{s-1}(j)\}$$

όπου s είναι ο μικρότερος φυσικός με $\sigma^s(j) = j$. Επειδή αναγκαστικά οι υπόλοιπες τροχιές του κύκλου σ θα αποτελούνται ακριβώς από ένα στοιχείο, και άρα για κάθε $i \neq \mathscr{O}_\sigma(j)$, θα έχουμε $\mathscr{O}_\sigma(i) = \{i\}$, και επομένως: $\sigma(i) = i$. Επομένως μπορούμε να περιγράψουμε έναν κύκλο σ μήκους s ως εξής:

$$\exists j \in \mathbb{N}_n : \sigma(j) \neq j, \quad \text{και τότε:} \quad \mathscr{O}_\sigma(j) = \{j, \sigma(j), \sigma^2(j), \cdots, \sigma^{s-1}(j)\} \quad \text{και} \quad \sigma(i) = i, \ \forall i \notin \mathscr{O}_\sigma(j)$$

Συνεπώς:

«Το μήκος ενός κύκλου $\sigma \neq \iota$ ισούται με τον μικρότερο φυσικό s με $\sigma^s(i) = i$, όπου i είναι ένα οποιοδήποτε στοιχείο της τροχιάς του σ που έχει περισσότερα από ένα στοιχεία. Ο κύκλος σ εναλλάσσει κυκλικά τα στοιχεία της τροχιάς $\mathscr{O}_\sigma(i)$ και αφήνει σταθερά τα υπόλοιπα στοιχεία του $\mathbb{N}_n$». ▲

Χαρη στην Παρατήρηση 5.1.9 μπορούμε να παραστήσουμε έναν κύκλο σ που διαθέτει μια τροχιά με περισσότερα από ένα στοιχεία, ας πούμε την

$$\mathscr{O}_\sigma(i) = \{i, \sigma(i), \sigma^2(i), \cdots, \sigma^{s-1}(i)\}, \quad s \geq 2, \quad \text{για κάποιο} \quad i \in \mathbb{N}_n = \{1,2,\cdots,n\}$$

ως εξής:

$$\sigma = \begin{pmatrix} i & \sigma(i) & \sigma^2(i) & \cdots & \sigma^k(i) & \sigma^{k+1}(i) & \cdots & \sigma^{s-1}(i) \end{pmatrix} \tag{5.1}$$

ερμηνεύοντας την ανωτέρω σημειογραφία κατά τον εξής τρόπο:
Έστω $x \in \mathbb{N}_n = \{1,2,\ldots,n\}$, τότε:

$$\sigma(x) = \begin{cases} x, & \text{αν} \quad x \neq \sigma^k(i), \quad 0 \leq k \leq s-1, \quad \text{δηλαδή όταν} \quad x \notin \mathscr{O}_\sigma(i) \\ \sigma^{k+1}(i), & \text{αν} \quad x = \sigma^k(i), \quad 0 \leq k \leq s-2 \\ i, & \text{αν} \quad x = \sigma^{s-1}(i) \quad \surd \end{cases} \tag{5.2}$$

Δηλαδή η μετάθεση του δεύτερου μέλους της (5.1) η οποία περιγράφεται στην σχέση (5.2) συμπίπτει με την μετάθεση σ.

Στην παράσταση (5.1) ενός κύκλου μήκους s είναι απολύτως απαραίτητο να γνωρίζουμε σε ποια συμμετρική ομάδα ανήκει ο κύκλος σ. Για παράδειγμα, ο κύκλος $\sigma = (1\ 2\ 3)$ μήκους 3 μπορεί να είναι στοιχείο της συμμετρικής ομάδας S_3 αλλά και της συμμετρικής ομάδας S_4 η της συμμετρικής ομάδας S_5 κλπ.

Παράδειγμα 5.1.10. 1. Θεωρούμε τη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 2 \end{pmatrix} \in \mathsf{S}_{12}$$

Η σ είναι κύκλος, αφού έχει ακριβώς μια τροχιά με περισσότερα του ενός στοιχεία, πρόκειται για την τροχιά

$$\mathscr{O}_\sigma(2) = \{2, \ \sigma^1(2) = 4, \ \sigma^2(2) = 6, \ \sigma^3(2) = 8, \ \sigma^4(2) = 10, \ \sigma^5(2) = 12\}$$

Το μήκος του κύκλου σ είναι 6, και χρησιμοποιώντας τη νέα σημειογραφία που εισαγάγαμε προηγουμένως, έχουμε:

$$\sigma = \begin{pmatrix} 2 & 4 & 6 & 8 & 10 & 12 \end{pmatrix}$$

Προσέξτε ότι θα μπορούσαμε να είχαμε κατασκευάσει την προηγούμενη τροχιά αρχίζοντας από κάποιο άλλο στοιχείο της, ας πούμε το 10. Τώρα έχουμε:

$$\mathscr{O}_\sigma(10) = \{10, \ \sigma^1(10) = 12, \ \sigma^2(10) = 2, \ \sigma^3(10) = 4, \ \sigma^4(10) = 6, \ \sigma^5(10) = 8\}$$

και ο κύκλος γράφεται

$$\sigma = \begin{pmatrix} 10 & 12 & 2 & 4 & 6 & 8 \end{pmatrix}$$

Όπως προκύπτει και από την Παρατήρηση 5.1.4, η σειρά εμφάνισης των στοιχείων στις δύο προηγούμενες παραστάσεις είναι διαφορετική, ωστόσο αυτές ορίζουν το ίδιο στοιχείο της S_{12}, δηλαδή το σ.

2. Ας δούμε ποιο στοιχείο σ της S_{12} παριστάνει το

$$\begin{pmatrix} 8 & 5 & 11 & 3 \end{pmatrix}$$

Σύμφωνα με την ερμηνεία της σημειογραφίας που δόθηκε στην σχέση (5.2) της Παρατήρησης 5.1.9 έχουμε:

$$\begin{aligned} &\sigma(i) = i, \qquad \forall i \in \{1,2,\ldots,11,12\} \setminus \{8,5,11,3\}, \\ &\sigma(8) = 5, \qquad \sigma^2(8) = \sigma(5) = 11, \quad \sigma^3(8) = \sigma(11) = 3, \quad \sigma^4(8) = \sigma(3) = 8. \end{aligned}$$

Συνεπώς, η συγκεκριμένη μετάθεση σ είναι η

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 8 & 6 & 11 & 8 & 7 & 5 & 9 & 12 & 3 & 2 \end{pmatrix} \quad \surd$$

Παρατήρηση 5.1.11. 1. Κάθε 1-κύκλος της S_n παριστάνει το ταυτοτικό στοιχείο ι. Πράγματι, ας είναι $i \in \mathbb{N}_n = \{1,2,\ldots,n\}$ και ας θεωρήσουμε τον 1-κύκλο $\tau = (i)$.

Σύμφωνα με τη σχέση 5.2 έχουμε:

$$\tau(x) = \begin{cases} x, & \text{αν } \ x \in x \in \mathbb{N}_n \setminus \{i\} \\ i, & \text{αν } \ x = i \end{cases}$$

Προφανώς $\sigma = \iota$ και άρα στην S_n όλοι οι 1-κύκλοι είναι ίσοι μεταξύ τους αφού είναι όλοι ίσοι με την ταυτοτική μετάθεση ι.

2. Όπως είδαμε, ένας κύκλος μήκους 2 ονομάζεται αντιμετάθεση. Η ορολογία προκύπτει επειδή μια τέτοια μετάθεση εναλλάσσει δύο διαφορετικά στοιχεία του συνόλου $\mathbb{N}_n = \{1,2,\ldots,n\}$ και διατηρεί σταθερά τα υπόλοιπα στοιχεία.

Πράγματι, αν $\tau = (i \ \ j)$, όπου $i, j \in \mathbb{N}_n = \{1,2,\ldots,n\}$, όπου $i \neq j$, τότε:

$$\tau(x) = \begin{cases} x, & \text{αν } \ x \in \mathbb{N}_n \setminus \{i,j\} \\ j, & \text{αν } \ x = i \\ i, & \text{αν } \ x = j \end{cases} \qquad \blacktriangle$$

Ορισμός 5.1.12. *Δύο κύκλοι της* $(\mathsf{S}_n, \circ)$ *ονομάζονται* ***ξένοι κύκλοι****, αν οι τροχιές τους με το μεγαλύτερο πλήθος στοιχείων δεν έχουν κοινά στοιχεία. Έτσι, αν:*

$$\sigma = (i_1 \ i_2 \ \cdots \ i_s) \qquad \textit{και} \qquad \tau = (j_1 \ j_2 \ \cdots \ j_r)$$

είναι κύκλοι μήκους s και r αντίστοιχα, τότε οι κύκλοι σ και τ είναι ξένοι αν:

$$\{i_1, \ i_2, \ \cdots, \ i_s\} \cap \{j_1, \ j_2, \ \cdots, \ j_r\} = \emptyset$$

Παρατήρηση 5.1.13. Από τον προηγούμενο ορισμό προκύπτει ότι, για να είναι δύο κύκλοι της S_n ξένοι, πρέπει να έχουν και οι δύο μήκος ≥ 2, αφού, αν ένας από τους δύο έχει μήκος 1, τότε αυτός είναι το ταυτοτικό στοιχείο ι της S_n. Αλλά τώρα κάθε τροχιά του ι έχει μήκος 1, δηλαδή είναι μια τροχιά που έχει το μεγαλύτερο πλήθος στοιχείων, και είναι σαφές ότι, όποιος και αν είναι ο άλλος κύκλος, η τροχιά του με το μεγαλύτερο πλήθος στοιχείων έχει μη κενή τομή με κάποια από τις τροχιές του ι. $\blacktriangle$

Παράδειγμα 5.1.14. Οι κύκλοι $\sigma = (1\ 9\ 8)$ και $\tau = (11\ 1\ 12)$ της S_{12} δεν είναι ξένοι διότι $\{1,9,8\} \cap \{11,1,12\} = \{1\}$. Η μοναδική τροχιά του σ με μήκος > 1 είναι η $\mathcal{O}_{\sigma,1} = \{1,9,8\}$.

Αντίθετα, οι κύκλοι $\sigma = (1\ 9\ 8)$ και $\rho = (6\ 3\ 7)$ της S_{12} είναι ξένοι διότι $\{1,9,8\} \cap \{6,3,7\} = \emptyset$. $\surd$

Θα δούμε τώρα ένα σημαντικό αποτέλεσμα το οποίο πιστοποιεί ότι κάθε μετάθεση της S_n είναι γινόμενο πεπερασμένου πλήθους ξένων κύκλων. Με άλλα λόγια, το σύνολο των κύκλων είναι ένα σύνολο γεννητόρων της S_n.

Πρόταση 5.1.15. *Κάθε μετάθεση της συμμετρικής ομάδας* $(\mathsf{S}_n, \circ)$ *ή είναι ένας κύκλος ή είναι μια σύνθεση κύκλων ξένων ανά δύο, όπου το μήκος εκάστου είναι* ≥ 2.

Απόδειξη. Έστω σ μια τυχούσα μετάθεση της S_n. Αν η σ είναι κύκλος δεν χρειάζεται να αποδειχθεί τίποτα.

Ας υποθέσουμε ότι η σ δεν είναι κύκλος. Τότε εξ ορισμού η σ διαθέτει τουλάχιστον δύο τροχιές με περισσότερα του ενός στοιχεία. Έστω ότι οι τροχιές της σ με περισσότερα του ενός στοιχεία είναι οι εξής:

$$\mathcal{O}_1 = \mathcal{O}_\sigma(a_{11}) = \{a_{11}, a_{12}, \cdots, a_{1t_1}\}, \quad \mathcal{O}_2 = \mathcal{O}_\sigma(a_{21}) = \{a_{21}, a_{22}, \cdots, a_{2t_2}\}, \quad \cdots,$$
$$\mathcal{O}_i = \mathcal{O}_\sigma(a_{i1}) = \{a_{i1}, a_{i2}, \cdots, a_{it_i}\}, \quad \cdots, \quad \mathcal{O}_s = \mathcal{O}_\sigma(a_{s1}) = \{a_{s1}, a_{s2}, \ldots a_{st_s}\}.$$

Για κάθε i όπου $1 \leq i \leq s$, ορίζουμε τη μετάθεση σ_i ως εξής

$$\sigma_i(a) = \begin{cases} \sigma(a), & \text{αν } a \in \mathcal{O}_i \\ a, & \text{αν } a \notin \mathcal{O}_i \end{cases}$$

Εξ ορισμού τότε, για κάθε i, όπου $1 \leq i \leq s$, η μετάθεση σ_i συμπίπτει με τον κύκλο $(a_{i1}\ a_{i2}\ \cdots\ a_{it_i})$ μήκους $|\mathcal{O}_i| = t_i \geq 2$.

Ισχυρισμός: $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_i \circ \cdots \circ \sigma_s$.

- Αν το a είναι ένα στοιχείο του συνόλου $\{1,2,\ldots,n\} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s)$, τότε προφανώς $\sigma(a) = a$ και $(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s)(a) = a$, διότι το a δεν εμφανίζεται σε κανέναν από τους κύκλους σ_i.

- Αν το a είναι ένα στοιχείο από το σύνολο $\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s$, τότε το a ανήκει σε ακριβώς μία τροχιά, ας πούμε την $\mathcal{O}_i$, αφού τα σύνολα $\mathcal{O}_1, \mathcal{O}_2, \cdots, \mathcal{O}_s$ είναι ανά δύο ξένα. Από τον ορισμό των μεταθέσεων σ_i, θα έχουμε $\sigma_s(a) = a$, $\sigma_{s-1}(a) = a$, $\cdots$, $\sigma_{i+1}(a) = a$, και:

$$(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_i \circ \cdots \circ \sigma_s)(a) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_i \circ \cdots \circ \sigma_{s-1})(a) = \cdots = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_i)(a)$$

Από τον ορισμό της μετάθεσης σ_i, επειδή το στοιχείο a ανήκει στην τροχιά $\mathcal{O}_i$, έπεται ότι το στοιχείο $\sigma_i(a)$ είναι ίσο με $\sigma(a)$, το οποίο επίσης ανήκει στην τροχιά $\mathcal{O}_i$ και γι' αυτό το $\sigma(a)$ δεν ανήκει σε καμιά από τις τροχιές $\mathcal{O}_{i-1}$, $\cdots$, $\mathcal{O}_2$, $\mathcal{O}_1$. Αυτό σημαίνει ότι το στοιχείο $\sigma(a)$ παραμένει σταθερό από τις μεταθέσεις σ_1, σ_2, $\cdots$, σ_{i-1}, δηλαδή: $\sigma_{i-1}(\sigma(a)) = \sigma(a)$, $\sigma_{i-2}(\sigma(a)) = \sigma(a)$, $\cdots$, $\sigma_2(\sigma(a)) = \sigma(a)$, $\sigma_1(\sigma(a)) = \sigma(a)$. Επομένως θα έχουμε:

$$(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_i)(a) = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1})(\sigma(a)) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-2})(\sigma(a)) = \cdots = \sigma_1(\sigma(a)) = \sigma(a)$$

δηλαδή:

$$(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_{i-1} \circ \sigma_i \circ \cdots \circ \sigma_s)(a) = \sigma(a)$$

Αποδείξαμε λοιπόν ότι $\forall a \in \mathbb{N}_n = \{1,2,\ldots,n\}$: $\sigma(a) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_i \circ \cdots \circ \sigma_s)(a)$. Συνεπώς θα έχουμε $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_i \circ \cdots \circ \sigma_s$, όπου για κάθε i με $1 \leq i \leq s$ το μήκος του κύκλου σ_i είναι $t_i \geq 2$. ■

Σύμφωνα με την Πρόταση 5.1.15, κάθε μετάθεση μπορεί να γραφεί ως γινόμενο ξένων κύκλων, καθένας απο τους οποίους έχει μήκος ≥ 2. Σημειώνουμε ότι η ταυτοτική μετάθεση λογίζεται ως κύκλος μήκους 1, δεν την γράφουμε και δεν την λαμβάνουμε υπόψη στην παραπάνω ανάλυση. Με βάση τα παραπάνω τίθεται φυσιολογικά το ερώτημα: *μπορεί μια μετάθεση να γραφεί με δύο διαφορετικούς τρόπους ως γινόμενο ξένων κύκλων;* Την απάντηση δίνει η ακόλουθη πρόταση.

Πρόταση 5.1.16. *Η ανάλυση μιας μετάθεσης $\sigma \in \mathsf{S}_n$ ως γινόμενο ξένων κύκλων, καθένας εκ των οποίων έχει μήκος ≥ 2, είναι μοναδική. Δηλαδή αν*

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \delta_1 \circ \delta_2 \circ \cdots \circ \delta_r$$

τότε $r = s$ και υπάρχει μια αναδιάταξη $i_1, i_2, \cdots, i_s$ των δεικτών $1, 2, \cdots, s$ έτσι ώστε: $\gamma_k = \delta_{i_k}$, $1 \leq k \leq s$.

Απόδειξη. Έστω $\mathscr{O}_1$, $\mathscr{O}_2$, $\cdots$, $\mathscr{O}_s$ της σ οι τροχιές οι οποίες αντιστοιχούν στους ξένους κύκλους γ_1, γ_2, $\cdots$, γ_s. Ανάλογα, έστω $\mathscr{O}'_1$, $\mathscr{O}'_2$, $\cdots$, $\mathscr{O}'_r$ της σ οι τροχιές οι οποίες αντιστοιχούν στους ξένους κύκλους δ_1, δ_2, $\cdots$, δ_r. Υπάρχουν s το πλήθος διακεκριμένα στοιχεία x_i του συνόλου $\{1, 2, \cdots, n\}$ έτσι ώστε: $x_i \in \mathscr{O}_i$, $1 \leq i \leq s$. Επειδή τα στοιχεία x_i η μετάθεση σ δεν τα αφήνει σταθερά και ανήκουν σε διαφορετικές τροχιές της σ, έπεται ότι καθένα από αυτά ανήκει ακριβώς σε μια από τις τροχιές $\mathscr{O}'_1$, $\mathscr{O}'_2$, $\cdots$, $\mathscr{O}'_r$ και επομένως $s \leq r$. Ακριβώς ανάλογα δείχνουμε ότι $r \leq s$. Άρα $r = s$. Έστω ότι το στοιχείο $x_1 \in \mathscr{O}_1$ ανήκει τροχιά $\mathscr{O}'_{i_1}$. Τότε προφανώς $\mathscr{O}_1 = \{x_1, \sigma(x_1), \cdots, \sigma^{\ell(\gamma_1)}\}$ και, επειδή $x_1 \in \mathscr{O}'_{i_1}$, προφανώς θα έχουμε $\mathscr{O}_1 \subseteq \mathscr{O}'_{i_1}$. Ακριβώς ανάλογα, επειδή $x_1 \in \mathscr{O}'_{i_1} = \{x_1, \sigma(x_1), \cdots, \sigma^{\ell(\delta_1)}\}$ θα έχουμε $\mathscr{O}'_{i_1} \subseteq \mathscr{O}_1$. Έτσι τελικά $\mathscr{O}_1 = \mathscr{O}'_{i_1}$, και αυτό σημαίνει ότι $\gamma_1 = \delta_{i_1}$. Με παρόμοιο τρόπο δείχνουμε ότι και $\mathscr{O}_k = \mathscr{O}'_k$, $2 \leq k \leq s = r$, και αυτό σημαίνει ότι $\gamma_k = \delta_{i_k}$, $2 \leq k \leq s = r$. ■

Επομένως, από τις Προτάσεις 5.1.15 και 5.1.16, προκύπτει οτι η ανάλυση σε ξένους κύκλους μιας μετάθεσης είμαι μοναδική αν δεν λάβουμε υπόψη μας τη σειρά εμφάνισης των ξένων κύκλων στην ανάλυση, και την εισαγωγή ή αφαίρεση κύκλων μήκους 1 (οι οποίοι συμπίπτουν με την ταυτοτική μετάθεση).

Όπως γνωρίζουμε, η ομάδα S_n δεν είναι αβελιανή, όταν $n \geq 3$, και άρα γενικά δύο μεταθέσεις της S_n δεν μετατίθενται μεταξύ τους. Η επόμενη βοηθητική πρόταση δείχνει ότι μεταθέσεις ειδικού τύπου μετατίθενται:

Λήμμα 5.1.17. *Έστω ότι γ και δ είναι δύο ξένοι κύκλοι της συμμετρικής ομάδας $(\mathsf{S}_n, \circ)$, τότε οι κύκλοι μετατίθενται μεταξύ τους, δηλαδή*

$$\gamma \circ \delta = \delta \circ \gamma$$

Απόδειξη. Σύμφωνα με την Παρατήρηση 5.1.13, οι κύκλοι γ και δ έχουν μήκος ≥ 2. Έστω ότι

$$\gamma = (c_1\ c_2\ \cdots\ c_r) \qquad \text{και} \qquad \delta = (d_1\ d_2\ \cdots\ d_t)$$

όπου $r, t \geq 2$, και τότε θα έχουμε $\{c_1, c_2, \cdots, c_r\} \cap \{d_1, d_2, \cdots, d_r\} = \emptyset$, διότι οι κύκλοι γ και δ είναι ξένοι.

- Για κάθε $a \in \{1, 2, \ldots, n\} \setminus (\{c_1, c_2, \ldots, c_r\} \cup \{d_1, d_2, \ldots, d_t\})$ θα έχουμε προφανώς:

$$(\gamma \circ \delta)(a) = a = (\delta \circ \gamma)(a)$$

- Για κάθε $a \in \{c_1, c_2, \ldots, c_r\}$ θα έχουμε:

$$(\gamma \circ \delta)(a) = \gamma(\delta(a)) = \gamma(a) = \delta(\gamma(a)) = (\delta \circ \gamma)(a)$$

διότι, επειδή $a \in \{c_1, c_2, \cdots, c_r\}$, έπεται ότι $\gamma(a) \in \{c_1, c_2, \cdots, c_r\}$ και γι' αυτό τα στοιχεία a και $\gamma(a)$ δεν ανήκουν στο σύνολο $\{d_1, d_2, \cdots, d_t\}$, επειδή οι γ και δ είναι ξένοι κύκλοι. Έτσι $\delta(a) = a$ και $\delta(\gamma(a)) = \gamma(a)$.

- Ακριβώς ανάλογα αποδεικνύεται ότι, για κάθε $a \in \{d_1, d_2, \cdots, d_t\}$ είναι

$$(\gamma \circ \delta)(a) = \gamma(\delta(a)) = \delta(a) = \delta(\gamma(a)) = (\delta \circ \gamma)(a),$$

αφού $a = \gamma(a)$ και $\delta(a) = \gamma(\delta(a))$.

Άρα τελικά θα έχουμε: $\gamma \circ \delta = \delta \circ \gamma$. ■

Με χρήση της Αρχής Μαθηματικής Επαγωγής, εύκολα προκύπτει από το Λήμμα 5.1.17 το ακόλουθο αποτέλεσμα.

Πόρισμα 5.1.18. *Αν $\gamma_1, \gamma_2, \ldots, \gamma_s$ είναι κύκλοι της $(\mathsf{S}_n, \circ)$ ανά δύο ξένοι, τότε:*

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \gamma_{i_1} \circ \gamma_{i_2} \circ \cdots \circ \gamma_{i_s}$$

όπου $i_1, i_2, \ldots, i_s$ είναι μια οποιαδήποτε αναδιάταξη των $1, 2, \ldots, s$.

Θα αποδείξουμε τώρα ένα ασημαντικό αποτέλεσμα το οποίο επιτρέπει τον υπολογισμό της τάξης μιας μετάθεσης, ως στοιχείου της συμμετρικής ομάδας, αν γνωρίζουμε την ανάλυσή της σε γινόμενο ξένων κύκλων.

Πρόταση 5.1.19. *Έστω ότι σ είναι μια μετάθεση της συμμετρικής ομάδας $(\mathsf{S}_n, \circ)$.*

1. *Αν η μετάθεση σ είναι κύκλος της S_n μήκους $\ell(\sigma)$, τότε η τάξη $\mathsf{o}(\sigma)$ της σ είναι ίση με*

$$\mathsf{o}(\sigma) = \ell(\sigma)$$

2. *Αν η μετάθεση σ είναι γινόμενο $s \geq 2$ το πλήθος ξένων ανά δύο κύκλων γ_i μήκους $\ell(\gamma_i) \geq 2$, $1 \leq i \leq s$:*

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$$

τότε η τάξη $\mathsf{o}(\sigma)$ της σ είναι ίση με το ελάχιστο κοινό πολλαπλάσιο των μηκών $\ell(\gamma_i)$, $1 \leq i \leq s$:

$$\mathsf{o}(\sigma) = \left[\ell(\gamma_1),\ \ell(\gamma_2),\ \cdots,\ \ell(\gamma_s)\right]$$

Απόδειξη. 1. Αν η μετάθεση σ είναι ένας κύκλος μήκους $\ell(\sigma) = 1$, τότε $\sigma = \iota$ και συνεπώς, $\mathsf{o}(\sigma) = 1 = \ell(\sigma)$. Έστω ότι ο κύκλος $\sigma = (a_1\ a_2\ \cdots\ a_t)$ είναι ένας κύκλος μήκους $\ell(\sigma) = t \geq 2$.

Παρατηρούμε ότι

$$\forall i,\ 1 \leq i \leq t-1: \quad \sigma^i(a_1) = a_{i+1} \quad \text{και} \quad \sigma^t(a_1) = a_1 \tag{*}$$

Επομένως δεν υπάρχει $i \in \mathbb{N}$, όπου $1 \leq i \leq t-1$, με $\sigma^i = \mathrm{Id}_n$, διότι από τις παραπάνω σχέσεις έχουμε $\sigma^i(a_1) \neq a_1$. Θα δείξουμε ότι $\sigma^t = \iota$ και τότε επειδή ο αριθμός $t = \ell(\sigma)$ είναι ο μικρότερος φυσικός με αυτήν την ιδιότητα, συμπεραίνουμε ότι $t = \mathsf{o}(\sigma)$.

Γνωρίζουμε από την σχέση $(*)$ ότι $\sigma^t(a_1) = a_1$. Θα δείξουμε ότι $\forall i$, με $2 \leq i \leq t$ είναι: $\sigma^t(a_i) = a_i$. Επειδή $i \geq 2$ έχουμε, λόγω της $(*)$, ότι $a_i = \sigma^{i-1}(a_1)$. Επομένως:

$$\sigma^t(a_i) = \sigma^t(\sigma^{i-1}(a_1)) = \sigma^{i-1}(\sigma^t(a_1)) = \sigma^{i-1}(a_1) = a_i$$

Ώστε, $\sigma^t = \iota$ και επομένως $\mathsf{o}(\sigma) = t = \ell(\sigma)$.

2. Έστω $m = \left[\ell(\gamma_1), \ell(\gamma_2), \cdots, \ell(\gamma_s)\right]$ το ελάχιστο κοινό πολλαπλάσιο των μηκών των ξένων κύκλων στην ανάλυση της μετάθεσης σ. Θα δείξουμε ότι $\mathsf{o}(\sigma) = m$.

Τότε προφανώς $m = \ell(\gamma_1)\cdot k_1 = \ell(\gamma_2)\cdot k_2 = \cdots = \ell(\gamma_s)\cdot k_s$, για κάποιους θετικούς ακεραίους $k_1, k_2, \cdots, k_s$. Για κάθε i, όπου $1 \leq i \leq s$, θα έχουμε $(\gamma_i)^m = (\gamma_i)^{\ell(\gamma_i)\cdot k_i)} = (\gamma_i)^{\ell(\gamma_i)})^{k_i} = \iota^{k_i} = \iota$. Χρησιμοποιώντας αυτές τις σχέσεις και το γεγονός ότι ξένοι κύκλοι αντιμετατίθενται, θα έχουμε:

$$\sigma^m = (\gamma_1\circ\gamma_2\circ\cdots\circ\gamma_i\circ\cdots\circ\gamma_s)^m = (\gamma_1)^m\circ(\gamma_2)^m\circ\cdots\circ(\gamma_i)^m\circ\cdots\circ(\gamma_s)^m = (\gamma_1)^m\circ(\gamma_2)^m\circ\cdots\circ(\gamma_i)^m\circ\cdots\circ(\gamma_s)^m = \iota$$

Επομένως θα έχουμε:

$$\mathsf{o}(\sigma) \mid m = \left[\ell(\gamma_1), \ell(\gamma_2), \cdots, \ell(\gamma_s)\right] \tag{*}$$

Μένει να δείξουμε ότι ισχύει και $m \mid \mathsf{o}(\sigma)$. Για να το αποδείξουμε αυτό, εργαζόμαστε ως εξής. Έστω

$$\gamma_i = (a_{i1}\ a_{i2}\ \cdots\ a_{ir_i}), \quad 1 \leq i \leq s$$

και έστω ότι $\mathscr{O}_i = \left\{a_{i1}, a_{i2}, \cdots, a_{ir_i}\right\}$, $1 \leq i \leq s$, είναι οι ανά δύο ξένες τροχιές οι οποίες αντιστοιχούν στους κύκλους γ_1, γ_2, $\cdots$, γ_{s-1}, και γ_s αντίστοιχα. Θεωρούμε την ένωσή τους

$$\mathscr{O} = \mathscr{O}_1 \cup \mathscr{O}_2 \cup \cdots \cup \mathscr{O}_{s-1} \cup \mathscr{O}_s$$

Αν $a \in \left\{1, 2, \cdots, n\right\} \setminus \mathscr{O}$, τότε για κάθε θετικό ακέραιο k, ισχύει προφανώς ότι:

$$\forall i = 1, 2, \cdots, s: \quad \gamma_i^k(a) = a$$

Από την άλλη πλευρά, για κάθε $i = 1,2,\cdots,s$, η μετάθεση σ μεταθέτει κυκλικά τα στοιχεία $\{a_{i1}, a_{i2},\cdots, a_{ir_i}\}$ της τροχιάς $\mathcal{O}_i$, και επομένως το ίδιο συμβαίνει και με κάθε ακεραία δύναμη σ^k της σ. Επιπλέον ο περιορισμός $\sigma|_{\mathcal{O}_i}$ της μετάθεσης σ στα στοιχεία της τροχιάς $\mathcal{O}_i$ συμπίπτει με τον κύκλο γ_i. Ως συνέπεια, αν για μια ακέραια δύναμη k ισχύει $\sigma^k = \iota$, τότε θα έχουμε και $\gamma_i^k = \iota$. Επομένως, επειδή $\sigma^{o(\sigma)} = \iota$, για κάθε $i = 1,2,\cdots,s$, θα έχουμε $o(\gamma_i) = \ell(\gamma_i) \mid o(\sigma)$ και αυτό σημαίνει ότι

$$m = [\ell(\gamma_1), \ell(\gamma_2),\cdots,\ell(\gamma_s)] \mid o(\sigma) \qquad (**)$$

Από τις σχέσεις (*) και (**) έπεται το ζητούμενο: $o(\sigma) = [\ell(\gamma_1), \ell(\gamma_2),\cdots,\ell(\gamma_s)]$. ■

Παράδειγμα 5.1.20. – Θεωρούμε τη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 3 & 4 & 5 & 1 & 10 & 9 & 2 & 8 \end{pmatrix} \in S_{10}$$

Επειδή όπως μπορούμε εύκολα να υπολογίσουμε

$$\sigma = (1 \quad 7 \quad 10 \quad 8 \quad 9 \quad 2 \quad 6)$$

η σ είναι ένας κύκλος μήκους 7. Επομένως η τάξη του κύκλου σ είναι όσο και το μήκος του: $o(\sigma) = 7$.

– Θεωρούμε τη μετάθεση

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 4 & 5 & 3 & 7 & 6 & 10 & 2 & 8 \end{pmatrix} \in S_{10}$$

Όπως μπορούμε να υπολογίσουμε εύκολα, η ανάλυση της τ σε ξένους κύκλους είναι:

$$\tau = (1 \quad 9 \quad 2) \circ (3 \quad 4 \quad 5) \circ (6 \quad 7) \circ (8 \quad 10)$$

Επομένως η τάξη της τ είναι το ελάχιστο κοινό πολλαπλάσιο των μηκών των ξένων κύκλων που εμφανίζονται στην ανάλυση της τ:

$$o(\tau) = [3,3,2,2] = 6$$

– Υπολογίζουμε το γινόμενο, δηλαδή τη σύνθεση, $\sigma \circ \tau$, και την ανάλυσή της σε ξένους κύκλους:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 7 & 4 & 5 & 3 & 10 & 1 & 8 & 6 & 9 \end{pmatrix} = (1 \quad 2 \quad 7) \circ (3 \quad 4 \quad 5) \circ (6 \quad 10 \quad 9)$$

Επομένως η τάξη της μετάθεσης $\sigma \circ \tau$ είναι $o(\sigma \circ \tau) = [3,3,3] = 3 \neq 7 \cdot 6 = o(\sigma) \cdot o(\tau)$. √

Παράδειγμα 5.1.21. Θεωρούμε τη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 9 & 1 & 4 & 5 & 7 & 3 & 6 & 10 & 2 & 8 & 13 & 11 & 12 \end{pmatrix} \in S_{13}$$

Υπολογίζουμε την ανάλυση της σ σε ξένους κύκλους:

$$\sigma = (1 \quad 9 \quad 2) \circ (3 \quad 4 \quad 5 \quad 7 \quad 6) \circ (8 \quad 10) \circ (11 \quad 13 \quad 12)$$

Επομένως

$$o(\sigma) = [3,5,2,3] = 30$$

Θα υπολογίσουμε τη μετάθεση σ^{2015}. Επειδή $o(\sigma) = 30$, έπεται ότι $\sigma^{30} = \iota$. Εκτελούμε την Ευκλείδεια διαίρεση του 2015 με το 30: $2015 = 67 \cdot 30 + 5$, και θα έχουμε:

$$\sigma^{2015} = \sigma^{30\cdot 67+5} = \sigma^{30\cdot 67} \circ \sigma^5 = (\sigma^{30})^{67} \circ \sigma^5 = \iota^{67} \circ \sigma^5 = \sigma^5$$

Εκμεταλευόμενοι ότι ξένοι κύκλοι μετατίθενται, θα υπολογίσουμε τη μετάθεση σ^5:

$$\begin{aligned}\sigma^5 &= \big((1\ \ 9\ \ 2)\circ(3\ \ 4\ \ 5\ \ 7\ \ 6)\circ(8\ \ 10)\circ(11\ \ 13\ \ 12)\big)^5\\ &= (1\ \ 9\ \ 2)^5\circ(3\ \ 4\ \ 5\ \ 7\ \ 6)^5\circ(8\ \ 10)^5\circ(11\ \ 13\ \ 12)^5\end{aligned}$$

Επειδή η τάξη ενός κύκλου μήκους k είναι ίση k, θα έχουμε:

$$(1\ \ 9\ \ 2)^5=(1\ \ 9\ \ 2)^{3+2}=(1\ \ 9\ \ 2)^3\circ(1\ \ 9\ \ 2)^2=\iota\circ(1\ \ 9\ \ 2)^2=(1\ \ 9\ \ 2)^2=(1\ \ 2\ \ 9)$$

$$(3\ \ 4\ \ 5\ \ 7\ \ 6)^5=\iota$$

$$(8\ \ 10)^5=(8\ \ 10)^4\circ(8\ \ 10)=\big((8\ \ 10)^2\big)^2\circ(8\ \ 10)=\iota^2\circ(8\ \ 10)=\iota\circ(8\ \ 10)=(8\ \ 10)$$

$$(11\ \ 13\ \ 12)^5=(11\ \ 13\ \ 12)^{3+2}=(11\ \ 13\ \ 12)^3\circ(11\ \ 13\ \ 12)^2=\iota\circ(11\ \ 13\ \ 12)^2=$$

$$=(11\ \ 13\ \ 12)^2=(11\ \ 12\ \ 13)$$

Επομένως τελικά θα έχουμε

$$\sigma^{2015}=\sigma^5=(1\ \ 2\ \ 9)\circ\iota\circ(8\ \ 10)\circ(11\ \ 12\ \ 13)=\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13\\2&9&3&4&5&6&7&10&1&8&12&13&11\end{pmatrix}$$

η οποία είναι μια μετάθεση με τάξη $\mathrm{o}(\sigma^{2015})=[3,2,3]=6$. Διαφορετικά θα μπορούσαμε να υπολογίσουμε την τάξη της σ^{2015} με βάση το Θεώρημα 3.2.2:

$$\mathrm{o}(\sigma^{2015})=\mathrm{o}(\sigma^5)=\frac{\mathrm{o}(\sigma)}{(\mathrm{o}(\sigma),5)}=\frac{30}{(30,5)}=\frac{30}{5}=6\quad\surd$$

Συμπληρώνουμε την παρούσα υποενότητα με τα ακόλουθα χρήσιμα αποτελέσματα:

Πρόταση 5.1.22. *Η αντίστροφη μετάθεση δ ενός k-κύκλου $\gamma\in\mathsf{S}_n$ είναι k-κύκλος, και μάλιστα ισχύει ότι:*

$$(a_1\ \ a_2\ \ \cdots\ \ a_k)^{-1}=(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)$$

Απόδειξη. Θέτοντας $\gamma=(a_1\ \ a_2\ \ \cdots\ \ a_k)$ και $\delta=(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)$, είναι αρκετό να αποδείξουμε ότι $\gamma\circ\delta=\iota$, αφού τότε έχουμε

$$\gamma^{-1}\circ(\gamma\circ\delta)=\gamma^{-1}\circ\iota\quad\Longrightarrow\quad\iota\circ\delta=\gamma^{-1}\quad\Longrightarrow\quad\delta=\gamma^{-1}$$

Έτσι πρέπει να δείξουμε ότι $\forall x\in\mathbb{N}_n=\{1,2,\cdots,n\}$ ισχύει: $(\gamma\circ\delta)(x)=x$. Αν $x\in\{1,2,\cdots,n\}\setminus\{a_1,a_2,\cdots,a_k\}$, τότε

$$(\gamma\circ\delta)(x)=\big((a_1\ \ a_2\ \ \cdots\ \ a_k)\circ(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)\big)(x)=(a_1\ \ a_2\ \ \cdots\ \ a_k)(x)=x$$

Αν $x\in\{a_1,a_2,\cdots,a_k\}$, τότε

$$(\gamma\circ\delta)(x)=\begin{cases}\big((a_1\ \ a_2\ \ \cdots\ \ a_k)\circ(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)\big)(a_i)=(a_1\ \ a_2\ \ \cdots\ \ a_k)(a_{i-1})=a_i, & \text{αν: } i\neq1\\ \big((a_1\ \ a_2\ \ \cdots\ \ a_k)\circ(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)\big)(a_1)=(a_1\ \ a_2\ \ \cdots\ \ a_k)(a_k)=a_1, & \text{αν: } i=1\end{cases}$$

Άρα ισχύει ότι $(\gamma\circ\delta)(x)=x$, $\forall x\in\mathbb{N}_n$, και επομένως $\delta=(a_k\ \ a_{k-1}\ \ \cdots\ \ a_1)=\gamma^{-1}$. ■

Πρόταση 5.1.23. *Για κάθε μετάθεση $\sigma\in\mathsf{S}_n$ και για κάθε κύκλο $\gamma=(a_1\ \ a_2\ \ \cdots\ \ a_k)\in\mathsf{S}_n$ μήκους k ισχύει ότι:*

$$\sigma\circ\gamma\circ\sigma^{-1}=\sigma\circ(a_1\ \ a_2\ \ \cdots\ \ a_k)\circ\sigma^{-1}=\big(\sigma(a_1)\ \ \sigma(a_2)\ \ \cdots\ \ \sigma(a_k)\big)$$

Απόδειξη. Είναι αρκετό να δείξουμε ισοδύναμα ότι:

$$\sigma \circ \gamma = \big(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)\big) \circ \sigma$$

Έστω $a \in \{1,2,\ldots,n\}$. Αν $a \notin \{a_1,a_2,\ldots,a_k\}$, τότε, επειδή $\sigma \in \mathsf{S}_n$, έχουμε $\sigma(a) \notin \{\sigma(a_1),\sigma(a_2),\ldots,\sigma(a_k)\}$, και άρα

$$(\sigma\circ\gamma)(a) = \sigma(a) \qquad \text{και} \qquad \big(\big(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)\big) \circ \sigma\big)(a) = \sigma(a)$$

Αν $a \in \{a_1,a_2,\ldots,a_k\}$, δηλαδή $a = a_i$, $1 \le i \le k$, το οποίο είναι ισοδύναμο με ότι $\sigma(a) = \sigma(a_i)$, $1 \le i \le k$, αφού $\sigma \in \mathsf{S}_n$, τότε θα έχουμε

$$(\sigma\circ\gamma)(a) = \begin{cases} \sigma(a_{i+1}), & \text{αν, } i = 1,2,\ldots,k-1, \text{ αφού } \gamma(a_i) = a_{i+1} \\ \sigma(a_1), & \text{αν } i = k, \text{ αφού } \gamma(a_k) = a_1 \end{cases}$$

και

$$\big(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)\big) \circ \sigma(a) = \begin{cases} \sigma(a_{i+1}), & \text{αν, } i = 1,2,\cdots,k-1 \\ \sigma(a_1), & \text{αν, } i = k \end{cases}$$

Ώστε, $(\sigma\circ\gamma)(a) = \big(\big(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)\big) \circ \sigma\big)(a)$, $1 \le a \le n$, και άρα: $\sigma\circ\gamma = \big(\sigma(a_1)\ \sigma(a_2)\ \cdots\ \sigma(a_k)\big)\circ\sigma$. ■

Παρατήρηση 5.1.24. Η παραπάνω Πρόταση μπορεί να χρησιμοποιηθεί για την εύρεση της συζυγούς μετάθεσης $\sigma\circ\tau\circ\sigma^{-1}$ μιας τυχούσας μετάθεσης τ.

Πράγματι, θεωρούμε την ανάλυση σε ξένους κύκλους $\tau = \tau_1\circ\tau_2\circ\cdots\circ\tau_k$ της μετάθεσης τ. Τότε θα έχουμε:

$$\sigma\circ\tau\circ\sigma^{-1} = \sigma\circ(\tau_1\circ\tau_2\circ\cdots\circ\tau_k)\circ\sigma^{-1} = \sigma\circ\tau_1\circ\tau_2\circ\cdots\circ\tau_k\circ\sigma^{-1} = \sigma\circ\tau_1\circ\iota\circ\tau_2\circ\iota\circ\cdots\circ\iota\circ\tau_k\circ\sigma^{-1} =$$

$$= \sigma\circ\tau_1\circ\sigma^{-1}\circ\sigma\circ\tau_2\circ\sigma^{-1}\circ\sigma\circ\cdots\circ\sigma^{-1}\circ\sigma\circ\tau_k\circ\sigma^{-1} = (\sigma\circ\tau_1\circ\sigma^{-1})\circ(\sigma\circ\tau_2\circ\sigma^{-1})\circ\cdots\circ(\sigma\circ\tau_k\circ\sigma^{-1})$$

Επομένως αν $\tau_r = (a_{r1}\ a_{r2}\ \cdots\ a_{rk_r})$, $1 \le r \le s$, θα έχουμε:

$$\sigma\circ\tau\circ\sigma^{-1} = \big(\sigma(a_{11})\ \sigma(a_{12})\ \cdots\ \sigma(a_{1k_1})\big) \circ \big(\sigma(a_{21})\ \sigma(a_{22})\ \cdots\ \sigma(a_{2k_2})\big) \circ \cdots \circ \big(\sigma(a_{s1})\ \sigma(a_{s2})\ \cdots\ \sigma(a_{sk_s})\big)$$

Σημειώνουμε ότι ο παραπάνω υπολογισμός είναι αρκετός και για τον υπολογισμό της μετάθεσης $\sigma^{-1}\circ\tau\circ\sigma$, διότι $\sigma^{-1}\circ\tau\circ\sigma = \sigma^{-1}\circ\tau\circ(\sigma^{-1})^{-1}$ και άρα:

$$\sigma^{-1}\circ\tau\circ\sigma = \big(\sigma^{-1}(a_{11})\ \sigma^{-1}(a_{12})\ \cdots\ \sigma^{-1}(a_{1k_1})\big)\ \circ\ \cdots\circ\big(\sigma^{-1}(a_{s1})\ \sigma^{-1}(a_{s2})\ \cdots\ \sigma^{-1}(a_{sk_s})\big)$$ ▲

5.2 Ο Κυκλικός Τύπος μιας Μετάθεσης

Όπως είδαμε στις Προτάσεις 5.1.15 και 5.1.16, κάθε μετάθεση $\sigma \in \mathsf{S}_n$ μπορεί να γραφεί μοναδικά ως γινόμενο ξένων κύκλων. Επίσης από την Παρατήρηση 5.1.24 προκύπτει ότι η συζυγής μιας μετάθεσης έχει ανάλογη ανάλυση σε ξένους κύκλους. Λαμβάνοντας υπόψη ότι συζυγή στοιχεία σε μια ομάδα έχουν πολλές κοινές ιδιότητες, για παράδειγμα έχουν την ίδια τάξη, τίθεται φυσιολογικά το ερώτημα:

«Ποιες μεταθέσεις είναι συζυγείς στη συμμετρική ομάδα S_n;»

Για να απαντήσουμε σ' αυτό το ερώτημα, θα χρειαστούμε τον ακόλουθο ορισμό.

Ορισμός 5.2.1. *Έστω $\sigma \in \mathsf{S}_n$ μια μετάθεση. Γράφουμε τη σ ως γινόμενο ξένων κύκλων*

$$\sigma = \sigma_1\circ\sigma_2\circ\cdots\circ\sigma_s$$

όπου επιτρέπουμε και κύκλους μήκους 1, δηλαδή την ταυτοτική μετάθεση, και διατάσσουμε τους ξένους κύκλους κατά αύξουσα σειρά ανάλογα με το μήκος τους, δηλαδή:

$$\ell(\sigma_1) \le \ell(\sigma_2) \le \cdots \le \ell(\sigma_{s-1}) \le \ell(\sigma_s)$$

Ο **κυκλικός τύπος** *της μετάθεσης σ ορίζεται να είναι η ακολουθία θετικών ακέραιων αριθμών*

$$\big(\ell(\sigma_1),\ \ell(\sigma_2),\ \cdots,\ \ell(\sigma_{s-1}),\ \ell(\sigma_s)\big)$$

Παράδειγμα 5.2.2. Θεωρούμε τη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 7 & 3 & 12 & 5 & 6 & 9 & 4 & 11 & 10 & 2 & 8 \end{pmatrix} \in \mathsf{S}_{12}$$

Επιτρέποντας κύκλους μήκους 1 και διατάσσοντας τους κύκλους ανάλογα με το μήκος τους κατά αύξουσα σειρα, όπως στον Ορισμό 5.2.1, θα έχουμε ότι: η ανάλυση της σ σε ξένους κύκλους είναι

$$\sigma = (1) \circ (3) \circ (5) \circ (6) \circ (10) \circ (4 \quad 12 \quad 8) \circ (2 \quad 7 \quad 9 \quad 11).$$

Επομένως ο κυκλικός τύπος της σ είναι ο

$$(1,\ 1,\ 1,\ 1,\ 1,\ 3,\ 4) \quad \surd$$

Παρατήρηση 5.2.3. Αν $(k_1, k_2, \cdots, k_s)$ είναι ο κυκλικός τύπος μιας μετάθεσης $\sigma \in \mathsf{S}_n$, τότε:

$$n = \sum_{i=1}^{s} k_i \qquad \text{και} \qquad k_1 \le k_2 \le \cdots \le k_s \tag{5.3}$$

Αντίστροφα, αν ικανοποιούνται οι παραπάνω σχέσεις, τότε η s-άδα αριθμών $(k_1, k_2, \cdots, k_s)$ είναι ο κυκλικός τύπος μιας μετάθεσης, όχι απαραίτητα μοναδικής, της συμμετρικής ομάδας S_n. Πράγματι, έστω χωρίς βλάβη της γενικότητας ότι $k_1 = k_2 = \cdots = k_r = 1$, όπου $r \le s$, οπότε θεωρούμε κύκλους $\sigma_k = (i_k) = \iota$ μήκους 1, όπου $1 \le k \le r$ και $\{i_1, i_2, \cdots, i_r\} \subseteq \mathbb{N}_n$. Θεωρούμε το υποσύνολο $\mathbb{N}_n \setminus \{i_1, i_2, \cdots, i_r\}$ το οποίο περιέχει $n-r$ στοιχεία. Λόγω των σχέσεων (5.3), το σύνολο αυτό μπορούμε να το διαμερίσουμε σε $s-r$ το πλήθος ξένα ανά δύο υποσύνολα $\mathscr{O}_{r+1}$, $\mathscr{O}_{r+2}$, $\cdots$, $\mathscr{O}_s$, καθένα εκ των οποίων έχει k_{r+1}, k_{r+2}, $\cdots$, k_s, στοιχεία αντίστοιχα. Θεωρούμε (ξένους) κύκλους σ_i μήκους $k_i \ge 2$, $r+1 \le i \le s$, των οποίων οι τροχιές είναι ακριβώς τα ξένα σύνολα $\mathscr{O}_i$, $r+1 \le i \le s$. Τότε προφανώς η μετάθεση $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r \circ \sigma_{r+1} \circ \cdots \circ \sigma_s$ έχει κυκλικό τύπο $(k_1, k_2, \cdots, k_s)$.

Για παράδειγμα, έστω $n = 7$, και θεωρούμε την ακολουθία αριθμών $(1,1,2,3)$ η οποία ικανοποεί τις σχέσεις (5.3). Τότε στη συμμετρική ομάδα S_6 θεωρούμε τους κύκλους $\sigma_1 = (1)$ και $\sigma_2 = (3)$, μήκους 1, και τους ξένους κύκλους $\sigma_3 = (2\ 5)$ και $\sigma_4 = (4\ 6\ 7)$ μήκους 2 και 3 αντίστοιχα. Τότε η μετάθεση

$$\sigma = \sigma_1 \circ \sigma_2 \circ \sigma_3 \circ \sigma_4 = (1) \circ (3) \circ (2\ 5) \circ (4\ 6\ 7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 6 & 2 & 7 & 4 \end{pmatrix}$$

έχει κυκλικό τύπο $(1,1,2,3)$.

Παρατηρούμε ότι και η μετάθεση

$$\tau = \tau_1 \circ \tau_2 \circ \tau_3 \circ \tau_4 = (2) \circ (7) \circ (4\ 6) \circ (1\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 6 & 1 & 4 & 7 \end{pmatrix}$$

έχει τον ίδιο κυκλικό τύπο $(1,1,2,3)$ με τη σ. Αυτό, όπως θα δούμε γενικά σε λίγο, δεν είναι τυχαίο: οι ματαθέσεις σ και τ είναι συζυγείς. Πράγματι, θεωρούμε τη μετάθεση

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix}$$

Τότε θα έχουμε $\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & 1 & 6 & 3 & 5 \end{pmatrix}$ και:

$$\begin{aligned} \rho \circ \tau \circ \rho^{-1} &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 6 & 2 & 7 & 5 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 6 & 1 & 4 & 7 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 7 & 1 & 6 & 3 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 3 & 6 & 2 & 7 & 4 \end{pmatrix} \\ &= \sigma \end{aligned}$$

Σε επόμενο αποτέλεσμα θα δείξουμε ότι η παραπάνω παρατήρηση ισχύει γενικά. ▲

Γενικά, αν $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s$ είναι μια ανάλυση της $\sigma \in \mathsf{S}_n$ ως γινόμενο ξένων κύκλων

$$\sigma_i = \big(a_{i1}\ \ a_{i2}\ \ \cdots\ \ a_{ik_i}\big), \quad 1 \le i \le s, \qquad \text{και} \qquad \ell(\gamma_i) = t_i \ge 2$$

τότε μπορούμε να συμπληρώσουμε την ανάλυση με $m = [n - (k_1 + k_2 + \cdots + k_s)]$ το πλήθος 1–κύκλους

$$\tau_1 = \big(j_1\big), \quad \tau_2 = \big(j_2\big), \quad \cdots, \quad \tau_m = \big(j_m\big),$$

όπου

$$j_r \in \{1, 2, \cdots, n\} \setminus \bigcup_{i=1}^{s} \{a_{i1}, a_{i2}, \cdots, a_{ik_i}\}, \qquad 1 \le r \le m$$

και συνεπώς

$$\sigma = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_m \circ \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s = \big(j_1\big) \circ \big(j_2\big) \circ \cdots \big(j_m\big) \circ \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s$$

Παρατηρούμε ότι το άθροισμα όλων των μηκών των κύκλων της παραπάνω ανάλυσης είναι ισο με n. Επειδή ξένοι κύκλοι μετατίθενται, βλέπε το Πόρισμα 5.1.18, μπορούμε επιπλέον να δεχθούμε ότι οι κύκλοι $\sigma_i, 1 \le i \le s$ είναι διατεταγμένοι με αύξουσα σειρά ως προς τα μήκη τους, δηλαδή αν $i < j$, τότε $\ell(\sigma_i) = k_i \le k_j = \ell(\sigma_j)$, και τότε έχουμε:

$$n = \underbrace{1 + 1 + \cdots + 1}_{m-\text{φορές}} + k_1 + k_2 + \cdots + k_s =$$

Θέτοντας $l_1 = l_2 = \cdots = l_m = 1$, θα έχουμε:

$$n = \sum_{i=1}^{m} l_i + \sum_{i=1}^{s} k_i \qquad \text{και} \qquad l_1 \le l_2 \le \cdots \le l_m \le k_1 \le k_2 \le \cdots \le k_s$$

Η ακολουθία αριθμών $(l_1, l_2, \cdots, l_m, k_1, k_2, \cdots, k_s)$ είναι επομένως μια διαμέριση του n με την έννοια του ακόλουθου ορισμου:

Ορισμός 5.2.4. *Μια ακολουθία φυσικών αριθμών $(n_1, n_2, \cdots, n_r)$ καλείται* **διαμέριση** *του φυσικού αριθμού n, αν:*

$$n_1 \le n_2 \le \cdots \le n_r \qquad \text{και} \qquad n_1 + n_2 + \cdots + n_r = n$$

Πρόταση 5.2.5. *Έστω $\sigma \in \mathsf{S}_n$ μια μετάθεση με κυκλικό τύπο $(n_1, n_2, \ldots, n_t)$. Τότε η τάξη της είναι το ελάχιστο κοινό πολλαπλάσιο των αριθμών $n_1, n_2, \cdots, n_t$:*

$$\mathsf{o}(\sigma) = [n_1, n_2, \cdots, n_t]$$

Απόδειξη. Από την Πρόταση 5.1.19 η τάξη της σ είναι το ελάχιστο κοινό πολλαπλάσιο των μηκών των ξένων κύκλων στην ανάλυση της σ. Όσοι από τους αριθμούς n_i, $1 \le i \le t$, είναι μεγαλύτεροι ή ίσοι του 2, αν υπάρχουν τέτοιοι αριθμοί, αντιπροσωπεύουν μήκη κύκλων οι οποίοι είναι ξένοι ανά δύο, και όσοι από τους αριθμούς n_i, $1 \le i \le t$, είναι ίσοι με 1, αν υπάρχουν τέτοιοι αριθμοί, αντιπροσωπεύουν μήκη κύκλων μήκους 1 οι οποίοι δεν επηρεάζουν το ελάχιστο κοινό πολλαπλάσιο των αριθμών $n_1, n_2, \cdots, n_t$. Έτσι από την Πρόταση 5.1.19 έπεται ότι η τάξη της σ είναι το ελάχιστο κοινό πολλαπλάσιο των $n_1, n_2, \cdots, n_t$. ■

Είμαστε τώρα σε θέση να δούμε ποιες μεταθέσεις της συμμετρικής ομάδα S_n έχουν τον ίδιο κυκλικό τύπο.

Θεώρημα 5.2.6. *Αν σ και τ είναι δύο μεταθέσεις της S_n, τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Οι μεταθέσεις σ και τ είναι συζυγείς.*
2. *Οι μεταθέσεις σ και τ έχουν τον ίδιο κυκλικό τύπο.*

Απόδειξη. Υποθέτουμε ότι

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_s \quad \text{και} \quad \tau = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_t$$

είναι οι κυκλικές αναλύσεις των σ και τ, όπου

$$\sigma_i = (a_{i1}\ a_{i2}\ \cdots\ a_{ik_i}),\quad 1 \le i \le s \quad \text{και} \quad \tau_j = (b_{j1}\ b_{j2}\ \cdots\ b_{jl_j}),\quad 1 \le j \le t$$

Έτσι ο κυκλικός τύπος των σ και τ είναι $(k_1, k_2, \cdots, k_s)$ και $(l_1, l_2, \cdots, l_t)$ αντίστοιχα.

1. $\Longrightarrow$ 2. Υποθέτουμε ότι οι μεταθέσεις σ και τ είναι συζυγείς. Τότε υπάρχει μια μετάθεση $\rho \in \mathsf{S}_n$ έτσι ώστε $\rho \circ \sigma \circ \rho^{-1} = \tau$. Από την Παρατήρηση 5.1.24, έπεται ότι η κυκλική ανάλυση της μετάθεσης $\rho \circ \sigma \circ \rho^{-1}$ είναι:

$$\tau = \rho\circ\sigma\circ\rho^{-1} = \big(\rho(a_{11})\ \rho(a_{12})\ \cdots\ \rho(a_{1k_1})\big) \circ \big(\rho(a_{21})\ \rho(a_{22})\ \cdots\ \rho(a_{2k_2})\big) \circ \cdots \circ \big(\rho(a_{s1})\ \rho(a_{s2})\ \cdots\ \rho(a_{sk_s})\big)$$

Άρα ο κυκλικός τύπος $(l_1, l_2, \cdots, l_t)$ της μετάθεσης τ αναγκαστικά συμπίπτει με τον κυκλικό τύπο $(k_1, k_2, \cdots, k_s)$ της μετάθεσης σ.

2. $\Longrightarrow$ 1. Υποθέτουμε ότι οι μεταθέσεις σ και τ έχουν τον ίδιο κυκλικό τύπο και άρα $(k_1, k_2, \cdots, k_s) = (l_1, l_2, \cdots, l_t)$, δηλαδή $s = t$ και $k_i = l_i$, $1 \le i \le s$. Θεωρούμε την μετάθεση

$$\rho = \begin{pmatrix} a_{11} & \cdots & a_{1k_1} & a_{21} & \cdots & a_{2k_2} & \cdots\cdots & a_{s1} & \cdots & a_{sk_s} \\ b_{11} & \cdots & b_{1k_1} & b_{21} & \cdots & b_{2k_2} & \cdots\cdots & b_{s1} & \cdots & b_{sk_s} \end{pmatrix}$$

Τότε, με βάση την Παρατήρηση 5.1.24, εύκολα υπολογίζουμε ότι

$$\rho\circ\sigma\circ\rho^{-1} = \big(\rho(a_{11})\ \rho(a_{12})\ \cdots\ \rho(a_{1k_1})\big) \circ \big(\rho(a_{21})\ \rho(a_{22})\ \cdots\ \rho(a_{2k_2})\big) \circ \cdots \circ \big(\rho(a_{s1})\ \rho(a_{s2})\ \cdots\ \rho(a_{sk_s})\big) =$$

$$= \big(b_{11}\ b_{12}\ \cdots\ b_{1k_1}\big) \circ \big(b_{21}\ b_{22}\ \cdots\ b_{2k_2}\big) \circ \cdots \circ \big(b_{s1}\ b_{s2}\ \cdots\ b_{sk_s}\big) = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_s = \tau$$

Επομένως οι μεταθέσεις σ και τ είναι συζυγείς. ■

Υπενθυμίζουμε ότι η σχέση συζυγίας σε μια ομάδα G ορίζεται να είναι η ακόλουθη σχέση

$$\forall g_1, g_2 \in G\colon \quad g_1 \ \sim\ g_2 \quad \Longleftrightarrow \quad \exists h \in G\colon \quad h \cdot g_1 \cdot h^{-1} = g_2$$

Η σχέση συζυγίας είναι μια σχέση ισοδυναμίας επί του συνόλου G. Πράγματι, για κάθε στοιχείο $g \in G$ έχουμε $g \sim g$ διότι $e \cdot g \cdot e^{-1} = g$. Αν $g_1 \sim g_2$, τότε $h \cdot g_1 \cdot h^{-1} = g_2$ για κάποιο $h \in G$, και τότε $g_1 = h^{-1} \cdot g_2 \cdot h = h^{-1} \cdot g_2 \cdot (h^{-1})^{-1}$, δηλαδή $g_2 \sim g_1$. Τέλος, αν $g_1 \sim g_2$ και $g_2 \sim g_3$, τότε θα έχουμε $h \cdot g_1 \cdot h^{-1} = g_2$ και $k \cdot g_2 \cdot k^{-1} = g_3$. Επομένως θα έχουμε $g_3 = k \cdot g_2 \cdot k^{-1} = k \cdot (h \cdot g_1 \cdot h^{-1}) \cdot k^{-1} = (k \cdot h) \cdot g_1 \cdot (k \cdot h)^{-1}$ και άρα $g_1 \sim g_3$.

Η σχέση συζυγίας, ως σχέση ισοδυναμίας, διαμερίζει την ομάδα G σε κλάσεις ισοδυναμίας, τις **κλάσεις συζυγίας**.

Πόρισμα 5.2.7. *Η κλάση συζυγίας μιας μετάθεσης $\sigma \in \mathsf{S}_n$ αποτελείται από όλες τις μεταθέσεις της S_n οι οποίες έχουν τον ίδιο κυκλικό τύπο με τη σ.*

Το Θεώρημα 5.2.6 μας επιτρέπει να προσδιορίσουμε το πλήθος των κλάσεων συζυγίας της συμμετρικής ομάδας S_n.

Η συνάρτηση p η οποία υπολογίζει το πλήθος των διαμερίσεων ενός φυσικού αριθμού ορίζεται ως εξής:

$$\mathsf{p}\colon \mathbb{N} \longrightarrow \mathbb{N}, \quad \mathsf{p}(n) = \text{ πλήθος διαμερίσεων του } n$$

Πόρισμα 5.2.8. *Το πλήθος των κλάσεων συζυγίας των στοιχείων της S_n συμπίπτει με το πλήθος $\mathsf{p}(n)$ των διαμερίσεων του n. Δηλαδή*

$$\mathsf{p}(n) = |\mathsf{S}_n / \sim|$$

όπου «$\sim$» είναι η σχέση συζυγίας στην S_n και $\mathsf{S}_n / \sim$ είναι το σύνολο πηλίκο των διακεκριμένων κλάσεων συζυγίας της S_n.

Παρατήρηση 5.2.9. Ας προσδιορίσουμε κάποιες από τις τιμές της συνάρτησης $\mathsf{p}(n)$:[2]

1. Προφανώς $\mathsf{p}(1) = 1$.
2. Είναι $\mathsf{p}(2) = 2$ διότι έχουμε τις διαμερίσεις $(1,1)$ και (2).
3. Είναι $\mathsf{p}(3) = 3$ διότι έχουμε τις διαμερίσεις $(1,1,1)$, $(1,2)$, και (3).
4. Είναι $\mathsf{p}(4) = 5$ διότι έχουμε τις διαμερίσεις $(1,1,1,1)$, $(1,1,2)$, $(2,2)$, $(1,3)$, και (4).
5. Είναι $\mathsf{p}(5) = 7$ διότι έχουμε τις διαμερίσεις $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,2,2)$, $(1,1,3)$, $(2,3)$, $(1,4)$, και (5).

Έτσι το πλήθος των κλάσεων συζυγίας των στοιχείων των συμμετρικών ομάδων S_1, S_2, S_3, S_4 και S_5, είναι αντίστοιχα: 1, 2, 3, 5, και 7.

Γενικά, όταν ο αριθμός n είναι μεγάλος, η συνάρτηση παίρνει αντίστοιχα γρήγορα πολύ μεγάλες τιμές. Αναφέρουμε ενδεικτικά κάποιες τιμές της συνάρτησης p καθώς ο φυσικός αριθμός n αυξάνει:

$$\mathsf{p}(10) = 42, \quad \mathsf{p}(20) = 627, \quad \mathsf{p}(30) = 5604, \quad \mathsf{p}(100) = 190,569,292$$

$$\mathsf{p}(1000) = 24,061,467,864,032,622,473,692,149,727,991$$

Παρατήρηση 5.2.10. *Ποια είναι η μεγαλύτερη τάξη την οποία μπορεί να έχει ένα στοιχείο της συμμετρικής ομάδας S_n; Ποια στοιχεία έχουν τη μεγαλύτερη δυνατή τάξη;*

Σύμφωνα με την Πρόταση 5.1.19 και το Θεώρημα 5.2.6, σε συνδυασμό με το γεγονός ότι συζυγή στοιχεία σε μια ομάδα έχουν την ίδια τάξη, για να προσδιορίσουμε ποια είναι η μεγαλύτερη τάξη στοιχείων της S_n και ποια στοιχεία έχουν αυτή την τάξη, αρκεί να προσδιορίσουμε την διαμέριση $(n_1, n_2, \cdots, n_k)$ του n για την οποία το ελάχιστο κοινό πολλαπλάσιο $[n_1, n_2, \cdots, n_k]$ παίρνει τη μεγαλύτερη τιμή.

Για παράδειγμα, όπως είδαμε, οι διαμερίσεις του 5 είναι 7 οι εξής: $(1,1,1,1,1)$, $(1,1,1,2)$, $(1,2,2)$, $(1,1,3)$, $(2,3)$, $(1,4)$, και (5). Από αυτές τις διαμερίσεις, εκείνη η οποία δίνει το μεγαλύτερο ελάχιστο κοινό πολλαπλάσιο είναι η διαμέριση $(2,3)$: $[2,3] = 6$. Άρα η μεγαλύτερη τάξη την οποία μορεί να έχει ένα στοιχείο της S_5 είναι 6, και ένα στοιχείο με τάξη 6 είναι το γινόμενο δύο ξένων κύκλων, ενός μήκους 2 και ενός μήκους 3, για παράδειγμα η μετάθεση $\sigma = \begin{pmatrix} 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 4 & 5 \end{pmatrix}$ έχει τάξη 6.

Η συνάρτηση

$$g : \mathbb{N} \longrightarrow \mathbb{N}, \quad g(n) = \max\left\{\mathsf{o}(\sigma) \in \mathbb{N} \mid \sigma \in \mathsf{S}_n\right\}$$

δηλαδή $g(n)$ είναι η μεγαλύτερη δυνατή τάξη στοιχείου της συμμετρικής ομάδας S_n, καλείται συνάρτηση του Landau,[3] και είναι γνωστό ότι:

$$\lim_{n\to\infty} \frac{\ln(g(n))}{\sqrt{n\ln(n)}} = 1 \qquad \text{και} \qquad g(n) \leq e^{\frac{n}{e}} \quad \blacktriangle$$

5.3 Άρτιες και Περιττές Μεταθέσεις - Η Εναλλάσσουσα Ομάδα

Όπως είδαμε στην προηγούμενη υποενότητα, κάθε μετάθεση μπορεί να γραφεί ως γινόμενο ξένων κύκλων. Οι κύκλοι είναι απλούστερες μεταθέσεις, και προφανώς η απλούστερη μη ταυτοτική μετάθεση είναι ένας κύκλος μήκους 2, δηλαδή μια αντιμετάθεση. Μια αντιμετάθεση εναλλάσσει δύο στοιχεία και αφήνει σταθερά τα υπόλοιπα. Είναι εύλογο να αναρωτηθούμε αν κάθε μετάθεση μπορεί να γραφεί ως γινόμενο αντιμεταθέσεων.

Λήμμα 5.3.1. *Κάθε κύκλος $\gamma = \begin{pmatrix} a_1 & a_2 & \cdots & a_k \end{pmatrix}$ της S_n, $n \geq 2$, είναι γινόμενο αντιμεταθέσεων. Αν $k \geq 2$, τότε ο κύκλος γ είναι γινόμενο $(k-1)$ το πλήθος αντιμεταθέσων.*

[2] Για περισσότερες πληροφορίες και λεπτομέρειες για τη συνάρτηση p παραπέμπουμε στον ιστότοπο *The On-Line Encyclopedia of Integer Sequences*: https://oeis.org/A000041.

[3] Edmund Landau (14 Φεβρουαρίου 1877 - 19 Φεβρουαρίου 1938) [https://en.wikipedia.org/wiki/Edmund_Landau]: Γερμανός μαθηματικός, με συμβολή στη Θεωρία Αριθμών και στη Μιγαδική Ανάλυση.

Απόδειξη. Αν ο κύκλος γ έχει μήκος $k=1$, τότε ο γ συμπίπτει με την ταυτοτική μετάθεση ι και, επειδή $n\geq 2$, μπορούμε να γράψουμε $\gamma=(1\ 2)\circ(2\ 1)$.

Υποθέτουμε ότι ο κύκλος γ έχει μήκος $k\geq 2$. Τότε ισχύει ότι:

$$\gamma=(a_1\ a_2\ \cdots\ a_k)=(a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\circ(a_1\ a_i)\circ\cdots\circ(a_1\ a_3)\circ(a_1\ a_2) \tag{5.4}$$

Πράγματι, αν $x\in\{1,2,\cdots,n\}\setminus\{a_1,a_2\ldots,a_k\}$, τότε προφανώς $\gamma(x)=x$ και

$$\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ \ ,a_{i+1})\circ(a_1\ a_i)\circ\cdots\circ(a_1\ a_3)\circ(a_1\ a_2)\Big)(x)=x$$

Αν $x\in\{a_1,a_2\ldots,a_k\}$, όπου $x=a_i$ με $i\neq k$, τότε $\gamma(a_i)=a_{i+1}$ και

$$\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\circ(a_1\ a_i)\circ\cdots\circ(a_1\ a_3)\circ(a_1\ a_2)\Big)(a_i)=$$
$$\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\circ(a_1\ a_i)\Big)(a_i)=$$
$$\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\Big)(a_1)=\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+2})\Big)(a_{i+1})=a_{i+1}=\gamma(a_i)$$

Τέλος, αν $x=a_k$, τότε $\gamma(a_k)=a_1$ και

$$\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\circ(a_1\ a_i)\circ\cdots\circ(a_1\ a_3)\circ(a_1\ a_2)\Big)(a_k)=(a_1\ a_k)(a_k)=a_1=\gamma(a_k)$$

Επομένως, $\forall a\in\{1,2,\ldots,n\}$:

$$\gamma(a)=\Big((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\cdots\circ(a_1\ a_{i+1})\circ(a_1\ a_i)\circ\cdots\circ(a_1\ a_3)\circ(a_1\ a_2)\Big)(a)$$

Συνεπώς η (5.4) ισχύει, και προφανώς το πλήθος των αντιμεταθέσεων είναι $(k-1)$. ■

Πρόταση 5.3.2. *Κάθε μετάθεση $\sigma\in\mathsf{S}_n$, $n\geq 2$, είναι γινόμενο αντιμεταθέσεων.*

Απόδειξη. Σύμφωνα με την Πρόταση 5.1.19, κάθε μετάθεση είναι γινόμενο (ξένων) κύκλων και, σύμφωνα με το Λήμμα 5.3.1, κάθε κύκλος είναι γινόμενο αντιμεταθέσεων. Επομένως, κάθε μετάθεση είναι γινόμενο αντιμεταθέσεων. ■

Παρατήρηση 5.3.3. Σε αντίθεση με τη γραφή μιας μετάθεσης ως γινόμενο ξένων κύκλων μήκους ≥ 2, η οποία είναι μοναδική αν δεν λάβουμε υπόψη μας τη σειρά των παραγόντων στο γινόμενο, η ανάλυση μιας μετάθεσης ως γινόμενο αντιμεταθέσεων δεν είναι μοναδική. Για παράδειγμα, για την μετάθεση

$$\sigma=\begin{pmatrix}1&2&3&4&5&6&7\\7&2&6&4&3&1&5\end{pmatrix}$$

εύκολα υπολογίζουμε ότι:

$$\sigma\ =\ (1\ 5)\circ(1\ 2)\circ(1\ 7)\circ(3\ 5)\circ(3\ 6)\circ(3\ 7)\circ(2\ 7)\circ(2\ 3)\ =\ (1\ 6)\circ(1\ 3)\circ(1\ 5)\circ(1\ 7)$$

Άρα η σ γράφεται με δύο διαφορετικούς τρόπους ως γινόμενο αντιμεταθέσεων, η πρώτη ανάλυση περιέχει 8 αντιμεταθέσεις και η δεύτερη ανάλυση περιέχει 4 αντιμεταθέσεις. Παρατηρούμε, ότι και στις δύο αναλύσεις, το πλήθος των αντιμεταθέσεων είναι άρτιο. Όπως θα δούμε σε λίγο, αυτό δεν είναι τυχαίο, δηλαδή θα δείξουμε ότι κάθε μετάθεση της S_n, $n\geq 2$, δεν μπορεί να γραφεί ταυτόχρονα ως γινόμενο άρτιου πλήθους αντιμεταθέσεων και ως γινόμενο περιττού πλήθους αντιμεταθέσεων. ▲

Για την απόδειξη του επόμενου θεωρήματος είναι απαραίτητο να υπενθυμίσουμε την έννοια της ορίζουσας $\mathsf{Det}(A)$ ενός $n\times n$ πίνακα πραγματικών αριθμών A, καθώς και ότι η ορίζουσα ενός πίνακα A αλλάζει πρόσημο όταν εναλλάξουμε αμοιβαία δύο γραμμές της.

Η συμμετρική ομάδα S_n δρα με φυσικο τρόπο στο σύνολο $\mathsf{M}_n(\mathbb{R})$ των $n\times n$ πινάκων με στοιχεία πραγματικούς αριθμούς, δηλαδή υπάρχει μια απεικόνιση

$$\star:\mathsf{S}_n\times\mathsf{M}_n(\mathbb{R})\longrightarrow\mathsf{M}_n(\mathbb{R}),\qquad(\sigma,A)\longmapsto\sigma\star A:=\sigma(A)$$

η οποία ικανοποιεί τις ακόλουθες δύο ιδιότητες, $\forall\sigma,\tau\in\mathsf{S}_n$, $\forall A\in\mathsf{M}_n(\mathbb{R})$:

1. $\iota \star A = \iota(A) = A$.
2. $(\sigma \circ \tau) \star A = \sigma \star (\tau \star A) = \sigma(\tau(A))$.

Ο πίνακας $\sigma(A)$ ορίζεται ως εξής: αν $A_1, A_2, \cdots, A_n$ είναι οι γραμμές του πίνακα A, δηλαδή:

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{pmatrix} \quad \text{και} \quad A_i = \begin{pmatrix} a_{i1} & a_{i2} & \cdots & a_{in} \end{pmatrix}, \qquad 1 \le i \le n$$

τότε ο πίνακας $\sigma(A)$ ορίζεται να είναι ο $n \times n$ πίνακας του οποίου η $\sigma(i)$-γραμμή $A_{\sigma(i)}$ είναι η i-οστή γραμμή A_i του πίνακα A ή ισοδύναμα i-οστή γραμμή τού $\sigma(A)$ είναι η $\sigma^{-1}(i)$-οστή γραμμή του A, δηλαδή:

$$\sigma(A)_{\sigma(i)} = A_i \quad \text{ή ισοδύναμα} \quad \sigma(A)_i = A_{\sigma^{-1}(A)}$$

Προφανώς για κάθε $i = 1, 2, \cdots, n$, ισχύει

$$\iota(A)_i = A_{\iota^{-1}(i)} = A_i \quad \Longrightarrow \quad \iota(A) = A$$

Επιπλέον $\forall \sigma, \tau \in \mathsf{S}_n$:

$$(\sigma \circ \tau)(A)_{(\sigma\circ\tau)(i)} = A_i, \quad \tau(A)_{\tau(i)} = A_i \quad \text{και} \quad (\sigma(\tau(A))_{\sigma(\tau(i))}$$

Παράδειγμα 5.3.4. Για παράδειγμα, θεωρούμε την μετάθεση

$$\sigma = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 \end{pmatrix} \in \mathsf{S}_5$$

και τον 5×5-πίνακα

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{pmatrix}$$

Τότε:

$$\sigma(A) = \begin{pmatrix} 21 & 22 & 23 & 24 & 25 \\ 16 & 17 & 18 & 19 & 20 \\ 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{pmatrix} \quad \surd$$

Παρατηρούμε ότι:

«*Αν σ, τ είναι δύο στοιχεία της S_n και A είναι ένας $n \times n$ πίνακας, τότε $\sigma \circ \tau(A) = \sigma(\tau(A))$,* διότι, $\forall i \in \{1, 2, \ldots, n\}$:

$$(\sigma \circ \tau)(A)_i = A_{(\sigma\circ\tau)^{-1}(i)} = A_{(\tau^{-1}\circ\sigma^{-1})(i)} = A_{\tau^{-1}(\sigma^{-1}(i))} \quad \text{και} \quad (\sigma(\tau(A))_i = \tau(A)_{\sigma^{-1}(i)} = A_{\tau^{-1}(\sigma^{-1}(i))}$$»

Επομένως, πράγματι η απεικόνιση $\star \colon \mathsf{S}_n \times \mathsf{M}_n(\mathbb{R}) \longrightarrow \mathsf{M}_n(\mathbb{R}), \quad (\sigma, A) \longmapsto \sigma \star A := \sigma(A)$ είναι μια δράση, δηλαδή ικανοποιεί τις ιδιότητες 1. και 2.

Θεώρημα 5.3.5. *Δεν υπάρχει μετάθεση $\sigma \in \mathsf{S}_n$, $n \ge 2$, το οποίο να είναι ταυτόχρονα γινόμενο και άρτιου και περιττού πλήθους αντιμεταθέσεων.*

Απόδειξη. Υποθέτουμε ότι υπάρχει μετάθεση $\sigma \in \mathsf{S}_n$ η οποία είναι γινόμενο 2κ αντιμεταθέσεων μ_i, $1 \le i \le 2\kappa$ και επίσης γινόμενο $2\lambda+1$, αντιμεταθέσεων ν_j, $1 \le j \le 2\lambda+1$, όπου $\kappa, \lambda \in \mathbb{N}$:

$$\sigma = \mu_1 \circ \cdots \circ \mu_{2\kappa} = \nu_1 \circ \cdots \circ \nu_{2\lambda+1}$$

Θεωρούμε τον μοναδιαίο $n \times n$ πίνακα $I_n = (\delta_{ij})$, όπου δ_{ij}, $1 \le i, j \le n$ είναι το σύμβολο του Kronecker.[4] Υπενθυμίζουμε ότι: $\delta_{ij} = 1$, όταν $i = j$ και $\delta_{ij} = 0$, όταν $i \ne j$. Παρατηρούμε ότι για οποιαδήποτε αντιμετάθεση $\tau = (s\ \ t)$, $1 \le s, t \le n$, $s \ne t$, η ορίζουσα $\mathsf{Det}(\tau(I_n))$ του πίνακα $\tau(I_n)$ ισούται με $-\mathsf{Det}(I_n) = -1$, διότι ο πίνακας $\tau(I_n)$ προκύπτει από τον μοναδιαίο πίνακα I_n κατόπιν εναλλαγής της s–οστής με την t–οστή γραμμή.

Συνεπώς:

$$\sigma = \mu_1 \circ \cdots \circ \mu_{2\kappa} \quad \Longrightarrow \quad \mathsf{Det}(\sigma(I_n)) = \mathsf{Det}((\mu_1 \circ \cdots \circ \mu_{2\kappa})(I_n)) = (-1)^{2\kappa} = 1$$

$$\sigma = \nu_1 \circ \cdots \circ \nu_{2\lambda+1} \quad \Longrightarrow \quad \mathsf{Det}(\sigma(I_n)) = \mathsf{Det}((\nu_1 \circ \cdots \circ \nu_{2\lambda+1})(I_n)) = (-1)^{2\lambda+1} = -1$$

Έτσι καταλήγουμε στην αντίφαση $1 = \mathsf{Det}(\sigma(I_n)) = -1$.

Ώστε, οποιοδήποτε στοιχείο $\sigma \in \mathsf{S}_n$ είναι σύνθεση ή μόνο από άρτιου πλήθους ή μόνο από περιττού πλήθους αντιμεταθέσεις. ■

Το Θεώρημα 5.3.5 μας επιτρέπει να δώσουμε τον ακόλουθο ορισμό.

Ορισμός 5.3.6. *Μια μετάθεση σ της συμμετρικής ομάδας S_n, $n \ge 2$ καλείται* ***άρτια****, αντίστοιχα* ***περιττή****, αν είναι γινόμενο άρτιου, αντίστοιχα περιττού, πλήθους αντιμεταθέσεων.*

Παράδειγμα 5.3.7. Η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 4 & 5 & 3 & 7 & 6 & 10 & 2 & 8 \end{pmatrix} \in \mathsf{S}_{10}$$

είναι άρτια, αφού

$$\sigma \ = \ (1\ 9\ 2) \circ (3\ 4\ 5) \circ (6\ 7) \circ (8\ 10) \ = \ (1\ 2) \circ (1\ 9) \circ (3\ 5) \circ (3\ 4) \circ (6\ 7) \circ (8\ 10)$$

Η μετάθεση

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 7 & 4 & 5 & 3 & 10 & 1 & 8 & 9 & 6 \end{pmatrix} \in \mathsf{S}_{10}$$

είναι περιττή, αφού

$$\tau \ = \ (1\ 2\ 7) \circ (3\ 4\ 5) \circ (6\ 10) \circ (1\ 7) \ = \ (1\ 7) \circ (1\ 2) \circ (3\ 5) \circ (3\ 4) \circ (6\ 10) \quad \surd$$

Παρατήρηση 5.3.8. Ένας κύκλος $\gamma = (a_1\ a_2\ \cdots\ a_k)$ μήκους $k \ge 2$ είναι άρτια, αντίστοιχα περιττή, μετάθεση, όταν το μήκος του k είναι περιττό, αντίστοιχα άρτιο:

Αυτό προκύπτει άμεσα από το Λήμμα 5.3.1 σύμφωνα με το οποίο ένας κύκλος μήκους k είναι γινόμενο $(k-1)$ το πλήθος αντιμεταθέσεων.

Αλλά και κάθε κύκλος της S_n, $n \ge 2$, μήκους 1, δηλαδή η ταυτοτική μετάθεση ι, είναι μια άρτια μετάθεση, διότι $\iota = (1\ 2) \circ (1\ 2)$.

Τέλος, αν $n = 1$, τότε $\mathsf{S}_1 = \{\iota\}$, και θεωρούμε την ταυτοτική μετάθεση ι της S_1 ως άρτια μετάθεση. ▲

Η ακόλουθη σημαντική πρόταση πιστοποιεί ότι το σύνολο των άρτιων μεταθέσεων της συμμετρικής ομάδας αποτελεί μια υποομάδα της.

[4] Leopold Kronecker (7 Δεκεμβρίου 1823 - 29 Δεκεμβρίου 1891) [https://en.wikipedia.org/wiki/Leopold_Kronecker]: Γερμανός μαθηματικός με σημαντική συμβολή στην Άλγεβρα και στη Θεωρία Αριθμών.

Πρόταση 5.3.9. *Το υποσύνολο*

$$\mathsf{A}_n = \{\sigma \in \mathsf{S}_n \mid \sigma : \textit{ άρτια μετάθεση}\} \subseteq \mathsf{S}_n$$

αποτελεί μια υποομάδα της S_n.

Απόδειξη. Επειδή η συμμετρική ομαδα S_n είναι πεπερασμένη και προφανώς το σύνολο A_n δεν είναι το κενό, αφού περιέχει πάντα την ταυτοτική μετάθεση ι, σύμφωνα με την Πρόταση 2.4.8, αρκεί να δείξουμε ότι το υποσύνολο A_n είναι κλειστό στην πράξη της ομάδας S_n. Αλλά, όταν οι μεταθέσεις σ και τ είναι στοιχεία του υποσυνόλου A_n, τότε και η σύνθεσή τους $\sigma\circ\tau$ ανήκει επίσης στο υποσύνολο A_n, αφού, όταν δύο μεταθέσεις σ και τ είναι σύνθεση άρτιου πλήθους αντιμεταθέσεων, ας πούμε αντίστοιχα 2κ και 2λ, τότε η μετάθεση $\sigma\circ\tau$ είναι σύνθεση $2\kappa+2\lambda = 2(\kappa+\lambda)$ πλήθους αντιμεταθέσεων, δηλαδή είναι επίσης μια άρτια μετάθεση. Επομένως, η A_n είναι μια υποομάδα της S_n. ■

Ορισμός 5.3.10. *Η υποομάδα* A_n *της* S_n *η οποία αποτελείται από τις άρτιες μεταθέσεις της* S_n *καλείται η* ***εναλλάσσουσα υποομάδα*** *της* S_n.

Στην απόδειξη της Πρότασης 5.3.9 διαπιστώσαμε πολύ εύκολα ότι η σύνθεση δύο άρτιων μεταθέσεων είναι μια άρτια μετάθεση. Διαπιστώνεται επίσης πολύ εύκολα, μετρώντας το πλήθος των αντιμεταθέσεων, ότι η σύνθεση μιας περιττής μετάθεσης με μια άρτια, καθώς και η σύνθεση μιας άρτιας με μια περιττή δίνει μια περιττή μετάθεση. Τέλος, η σύνθεση μιας περιττής μετάθεσης με μια περιττή, δίνει μια άρτια μετάθεση.

Τα προηγούμενα εκφράζονται συνοπτικά αντιστοιχώντας σε κάθε μετάθεση $\sigma \in \mathsf{S}_n$ έναν αριθμό $\epsilon(\sigma) \in \{1,-1\} \subset \mathbb{Z}$ της σ ως εξής:

$$\epsilon(\sigma) = \begin{cases} 1, & \text{αν η } \sigma \text{ είναι άρτια μετάθεση} \\ -1, & \text{αν η } \sigma \text{ είναι περιττή μετάθεση} \end{cases}$$

Ισοδύναμα μπορούμε να ορίσουμε την απεικόνιση $\sigma \longmapsto \epsilon(\sigma)$ ως εξής:

$$\epsilon : \mathsf{S}_n \longrightarrow \{1,-1\}, \qquad \epsilon(\sigma) = \mathsf{Det}(\sigma(I_n))$$

Η παραπάνω ανάλυση δείχνει ότι, για οποιεσδήποτε δύο μεταθέσεις $\sigma,\tau \in \mathsf{S}_n$ είναι:

$$\epsilon(\sigma\circ\tau) = \epsilon(\sigma)\cdot\epsilon(\tau)$$

Λαμβάνοντας υπόψη ότι το σύνολο $\{1,-1\}$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό «$\cdot$» ακέραιων αριθμών, πρόκειται για την ομάδα των αντιστρέψιμων στοιχείων του μονοειδούς $(\mathbb{Z},\cdot)$, η παραπάνω σχέση δείχνει ότι η απεικόνιση ϵ είναι ένας ομομορφισμός ομάδων. Ιδιαίτερα, θα έχουμε:

$$\epsilon(\tau_1\circ\tau_2\circ\cdots\circ\tau_k) = \epsilon(\tau_1)\cdot\epsilon(\tau_2)\ \cdots\ \epsilon(\tau_k) \qquad \text{και} \qquad \epsilon(\rho^{-1}) = \epsilon(\rho)^{-1}$$

Ορισμός 5.3.11. *Το* **πρόσημο** *μιας μετάθεσης* σ *ορίζεται να είναι ο αριθμός* $\epsilon(\sigma) \in \{1,-1\}$, *όπου* $\epsilon(\sigma) = 1$, *αν η μετάθεση* σ *είναι άρτια, και* $\epsilon(\sigma) = -1$, *αν η μετάθεση* σ *είναι περιττή.*

Σύμφωνα με τα παραπάνω, έχουμε την ακόλουθη περιγραφή της εναλλάσσουσας υποομάδας:

$$\mathsf{A}_n = \{\sigma \in \mathsf{S}_n \mid \epsilon(\sigma) = 1\}$$

Μπορούμε τώρα να προσδιορίσουμε την τάξη της εναλλάσουσσας ομάδας.[5]

Πρόταση 5.3.12. *Η τάξη της εναλλάσσουσας υποομάδας* A_n *της* S_n, $n \geq 2$, *είναι ίση με:*

$$\mathsf{o}(\mathsf{A}_n) = \frac{n!}{2}$$

[5] Αν σ' αυτό το σημείο γνωρίζαμε το Πρώτο Θεώρημα Ισομορφισμών Ομάδων, τότε η απόδειξη της Πρότασης 5.3.12 θα ήταν απλούστερη και θα μας εφοδίαζε με περισσότερες πληροφορίες, βλέπε το Πόρισμα 6.2.4 και το Θεώρημα 6.3.1, σύμφωνα με τα οποία η εναλλάσσουσα ομάδα A_n είναι κανονική υποομάδα της συμμετρικής ομάδας S_n και το σύνολο πηλίκο $\mathsf{S}_n/\mathsf{A}_n$ των (αριστερών πλευρικών κλάσεων της A_n στην S_n) είναι ομάδα ισόμορφη με την πολλαπλασιαστική ομάδα $\mathbb{Z}_2 \cong (\{1,-1\},\cdot)$.

Απόδειξη. Επειδή κάθε μετάθεση S_n είναι είτε άρτια είτε περιττή αλλά όχι και τα δύο, έπεται ότι το σύνολο S_n είναι ξένη ένωση του συνόλου A_n και του συνόλου $\mathsf{S}_n \setminus \mathsf{A}_n$ των περιττών μεταθέσεων:

$$\mathsf{S}_n = \mathsf{A}_n \bigcup (\mathsf{S}_n \setminus \mathsf{A}_n)$$

Άρα θα έχουμε

$$n! = |\mathsf{S}_n| = |\mathsf{A}_n \cup (\mathsf{S}_n \setminus \mathsf{A}_n)| = |\mathsf{A}_n| + |\mathsf{S}_n \setminus \mathsf{A}_n| \qquad (*)$$

και αρκεί να δείξουμε ότι: $|\mathsf{A}_n| = |\mathsf{S}_n \setminus \mathsf{A}_n|$.

Θεωρούμε την αντιμετάθεση $\mu = (1\ 2) \in \mathsf{S}_n \setminus \mathsf{A}_n$. Επειδή η σύνθεση μιας περιττής μετάθεσης με μια άρτια δίνει μια περιττή μετάθεση, ορίζεται με τη βοήθεια της μ η απεικόνιση

$$\varphi : \mathsf{A}_n \longrightarrow \mathsf{S}_n \setminus \mathsf{A}_n, \quad \sigma \longmapsto \varphi(\sigma) = \mu \circ \sigma$$

Επειδή η σύνθεση μιας περιττής μετάθεσης με μια περιττή δίνει μια άρτια μετάθεση, ορίζεται με τη βοήθεια της μ και η απεικόνιση

$$\psi : \mathsf{S}_n \setminus \mathsf{A}_n \longrightarrow \mathsf{A}_n, \quad \tau \longmapsto \psi(\tau) = \mu \circ \tau$$

Αλλά οι $\varphi \circ \psi$ και $\psi \circ \varphi$ είναι οι ταυτοτικές απεικονίσεις των συνόλων $(\mathsf{S}_n \setminus \mathsf{A}_n)$ και A_n, διότι:

$$\forall \tau \in \mathsf{S}_n \setminus \mathsf{A}_n: \qquad (\varphi \circ \psi)(\tau) = \varphi(\mu \circ \tau) = \mu \circ (\mu \circ \tau) = \mu^2 \circ \tau = (1\ 2)^2 \circ \tau = \iota \circ \tau = \tau$$

και

$$\forall \sigma \in \mathsf{A}_n: \qquad (\psi \circ \varphi)(\sigma) = \psi(\mu \circ \sigma) = \mu \circ (\mu \circ \sigma) = \mu^2 \circ \sigma = (1\ 2)^2 \circ \sigma = \iota \circ \sigma = \sigma$$

Επομένως, η φ είναι μια «1-1» και «επί» απεικόνιση και γι' αυτό $|\mathsf{A}_n| = |\mathsf{S}_n \setminus \mathsf{A}_n|$.

Τώρα η σχέση $(*)$ δίνει

$$n! = |\mathsf{S}_n| = |\mathsf{A}_n \cup (\mathsf{S}_n \setminus \mathsf{A}_n)| = |\mathsf{A}_n| + |\mathsf{S}_n \setminus \mathsf{A}_n| = 2|\mathsf{A}_n| \qquad \Longrightarrow \qquad |\mathsf{A}_n| = \frac{n!}{2}$$

■

Παράδειγμα 5.3.13. Θα περιγράψουμε τα στοιχεία της εναλλάσσουσας υποομάδας A_n, όταν $1 \le n \le 4$.

1. Προφανώς $\mathsf{A}_1 = \{\iota\}$.
2. Επειδή $\mathsf{S}_2 = \{\iota,\ (1\ 2)\}$ και η μετάθεση $(1\ 2)$ είναι περιττή, έπεται ότι $\mathsf{A}_2 = \{\iota\}$.
3. Για την A_3 θα έχουμε:
$$\mathsf{A}_3 = \{\iota,\ (1\ 2\ 3)),\ (1\ 3\ 2)\}$$
4. Για την A_4 θα έχουμε:
$$\mathsf{A}_4 = \Big\{\iota,\ (1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4),\ (1\ 3\ 2),\ (1\ 4\ 2),\ (1\ 4{,}3),\ (2\ 4\ 3),\ (1\ 2)\circ(3\ 4),\ (1\ 3)\circ(2\ 4),\ (1\ 4)\circ(2\ 3)\Big\}$$
Σημειώνουμε ότι ο πίνακας Cayley της A_4 σχεδιάστηκε στην υποενότητα 3.5.2. √

Πόρισμα 5.3.14. *Η εναλλάσσουσα υποομάδα A_n, μαζί με κάθε στοιχείο της σ, περιέχει και όλα τα συζυγή του στοιχεία:*

$$\forall \rho \in \mathsf{S}_n: \quad \sigma \in \mathsf{A}_n \qquad \Longrightarrow \qquad \rho \circ \sigma \circ \rho^{-1} \in \mathsf{A}_n$$

Δηλαδή $\forall \rho \in \mathsf{S}_n$: $\rho \circ \mathsf{A}_n \circ \rho^{-1} \subseteq \mathsf{A}_n$. Με άλλα λόγια η A_n είναι μια κανονική υποομάδα της S_n.

Απόδειξη. Επειδή μια μετάθεση τ της S_n ανήκει στην υποομάδα A_n αν και μόνο αν $\epsilon(\tau) = 1$, θα έχουμε:

$$\epsilon(\rho \circ \sigma \circ \rho^{-1}) = \epsilon(\rho) \cdot \epsilon(\sigma) \cdot \epsilon(\rho^{-1}) = \epsilon(\rho) \cdot 1 \cdot \epsilon(\rho)^{-1}) = 1$$

και επομένως $\rho \circ \sigma \circ \rho^{-1} \in \mathsf{A}_n$. ■

Με τη βοήθεια της έννοιας της διαμέρισης ενός φυσικού n, όπως στην υποενότητα 5.2, μπορούμε να περιγράψουμε τον κυκλικό τύπο των στοιχείων της S_n που ανήκουν στην υποομάδα A_n.

Έστω σ μια μετάθεση της S_n και η ανάλυσή της

$$\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \gamma_s$$

σε γινόμενο ξένων κύκλων. Επειδή

$$\epsilon(\sigma) = \epsilon(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s) = \epsilon(\gamma_1) \cdot \epsilon(\gamma_2) \cdots \epsilon(\gamma_s)$$

μπορεί κανείς να υπολογίσει το αν η σ είναι άρτια η περιττή, υπολογίζοντας τα $\epsilon(\gamma_i)$, $1 \le i \le s$, όπου υπενθυμίζουμε ότι ένας κύκλος με άρτιο μήκος (αντίστοιχα περιττό) είναι περιττή (αντίστοιχα άρτια) μετάθεση.

Δηλαδή, αν $(n_1, n_2, \cdots, n_l, n_{l+1}, n_{l+2}, \cdots, n_k) = (1, 1, \cdots, 1, n_{l+1}, n_{l+2}, \cdots, n_k)$ είναι ο κυκλικός τύπος μιας μετάθεσης σ, όπου $n_1 = n_2 \cdots = n_l = 1$ και $n_i \ge 2$ αν $l+1 \le i \le k$, τότε η μετάθεση σ είναι άρτια, αν το γινόμενο $(n_{l+1} - 1) + (n_{l+2} - 1) + \cdots + (n_k - 1)$ είναι άρτιος αριθμός.

Επιπλέον, αν η μετάθεση σ γράφεται ως γινόμενο $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$ ξένων κύκλων μήκους ≥ 2, τότε:

$$\epsilon(\sigma) = \prod_{i=1}^{k} (-1)^{\ell(\sigma_i)-1}$$

Αν η μετάθεση σ είναι γινόμενο k το πλήθος αντιμεταθέσεων, τότε: $\epsilon(\sigma) = (-1)^k$.

Παράδειγμα 5.3.15. Θα προσδιορίσουμε τον κυκλικό τύπο και τις τάξεις των στοιχείων της A_7.

Οι διαμερίσεις του 7 είναι 15, οι εξής:

$$1111111,\quad 111112,\quad 11122,\quad 1222,\quad 11113,\quad 1123,\quad 133,\quad 1114,\quad 115,\quad 16,\quad 124,\quad 223,\quad 25,\quad 34,\quad 7$$

Οι μεταθέσεις της S_7 οι οποίες ανήκουν στην εναλλάσσουσα υποομάδα A_7 είναι οι μεταθέσεις της S_7 που έχουν κυκλικό τύπο

$$(1,1,1,1,1,1,1),\quad (1,1,1,2,2),\quad (1,1,1,1,3),\quad (1,3,3),\quad (1,1,5),\quad (1,2,4),\quad (2,2,3),\quad (3,4),\quad (7)$$

Μεταθέσεις με αντίστοιχο κυκλικό τύπο είναι:

$$\iota,\quad (1\ 2)\circ(3\ 4),\quad (1\ 2\ 3),\quad (1\ 2\ 3)\circ(4\ 5\ 6),\quad (1\ 2\ 3\ 4\ 5),\quad (1\ 2)\circ(3\ 4\ 5\ 6),\quad (1\ 2)\circ(3\ 4)\circ(5\ 6\ 7),\quad (1\ 2\ 3\ 4\ 5\ 6\ 7)$$

Όλα τα στοιχεία της A_7, τα οποία είναι σε πλήθος 2520, είναι όλα τα συζυγή στοιχεία των παραπάνω στοιχείων της A_7.

Γι' αυτό οι αντίστοιχες τάξεις των στοιχείων της A_7 είναι:

$$[1,1,1,1,1,1,1] = 1,\quad [1,1,1,2,2] = 2,\quad [1,1,1,1,3] = 3,$$
$$[1,3,3] = 3,\quad [1,1,5] = 5,\quad [1,2,4] = 4,\quad [2,2,3] = 6,\quad [7] = 7 \quad \surd$$

5.4 Σύνολα γεννητόρων της S_n και της A_n

Γνωρίζουμε ότι κάθε μετάθεση της συμμετρικής ομάδας S_n είναι γινόμενο ξένων κύκλων. Επομένως το σύνολο των κύκλων παράγει τη συμμετρική ομάδα. Επιπλέον, επειδή κάθε κύκλος στην S_n είναι γινόμενο αντιμεταθέσεων, έπεται ότι το σύνολο όλων των αντιμεταθέσεων, το πλήθος των οποίων είναι $\frac{n(n-1)}{2}$, είναι επίσης ένα σύνολο γεννητόρων της S_n. Πράγματι, οι αντιμεταθέσεις της S_n είναι οι εξής:

$$\begin{array}{cccccc} (1\ 2), & (1\ 3), & (1\ 4), & \cdots, & (1\ n) \\ & (2\ 3), & (2\ 4), & \cdots, & (2\ n) \\ & & (3\ 4), & \cdots, & (3\ n) \\ & & & & \vdots \\ & & & & (n-1\ n) \end{array}$$

και είναι σε πλήθος:

$$(n-1)+(n-2)+\cdots+3+2+1=\frac{n(n-1)}{2}$$

Υπενθυμίζουμε ότι ένα υποσύνολο $S\subseteq G$ μιας ομάδας G καλείται *σύνολο γεννητόρων* της G, αν $G=\langle S\rangle$, όπου $\langle S\rangle$ είναι η υποομάδα της G η οποία παράγεται από το S, δηλαδή κάθε στοιχείο της G γράφεται ως γινόμενο στοιχείων από το σύνολο S. Ένα σύνολο γεννητόρων $S\subseteq G$ μιας ομάδας G καλείται *ελάχιστο σύνολο γεννητόρων* αν δεν υπάρχει γνήσιο υποσύνολο του S το οποίο να είναι σύνολο γεννητόρων της G, ή ισοδύναμα, για κάθε στοιχείο $g\in S$, το σύνολο $S\setminus\{g\}$ δεν είναι σύνολο γεννητόρων της G.

Προφανώς όμως το παραπάνω σύνολο γεννητόρων δεν είναι ελάχιστο, και, όπως θα δούμε, υπάρχουν (ελάχιστα) σύνολα γεννητόρων τα οποία αποτελούνται από αντιμεταθέσεις και περιέχουν πολύ λιγότερα στοιχεία.

Έτσι στην παρούσα ενότητα θα παρουσιάσουμε κάποια *ελάχιστα* σύνολα γεννητόρων της συμμετρικής ομάδας S_n και της εναλλάσσουσας υποομάδας A_n.

Θεώρημα 5.4.1. *Τα ακόλουθα σύνολα αντιμεταθέσεων είναι ελάχιστα σύνολα γεννητόρων της* S_n*:*

$$\mathscr{S}=\Big\{(1\ 2),\quad (1\ 3),\quad (1\ 4),\quad \cdots,\quad (1\ n)\Big\}$$

$$\mathscr{T}=\Big\{(1\ 2),\quad (2\ 3),\quad (3\ 4),\quad \cdots,\quad (n-1\ n)\Big\}$$

$$\mathscr{R}=\Big\{(1\ 2),\quad (1\ 2\ 3\ \cdots\ n)\Big\}\qquad (n\geq 3)$$

Απόδειξη. 1. Θεωρούμε μια αντιμετάθεση $(i\ \ j)$, όπου $1\leq i\neq j\leq n$. Τότε, όπως μπορούμε να υπολογίσουμε εύκολα:

$$(i\ \ j)=(1\ \ i)\circ(1\ \ j)\circ(1\ \ i)$$

και επομένως κάθε αντιμετάθεση είναι γινόμενο αντιμεταθέσεων από το σύνολο $\mathscr{S}$. Επειδή η συμμετρική ομάδα S_n παράγεται από το σύνολο όλων των αντιμεταθέσεων, έπεται ότι το σύνολο $\mathscr{S}$ είναι ένα σύνολο γεννητόρων της S_n. Αν αφαιρέσουμε μια αντιμετάθεση, για παράδειγμα την $(1,\ i)$, όπου $2\leq i\leq n$, από το σύνολο $\mathscr{S}$, τότε το σύνολο $\mathscr{S}\setminus\{(1,\ i)\}$ δεν παράγει την S_n διότι κάθε μετάθεση της S_n η οποία ανήκει στην υποομάδα $\langle\mathscr{S}\setminus\{(1,\ i)\}\rangle$ αφήνει προφανώς το στοιχείο i σταθερό και επομένως $(1,\ i)\notin\langle\mathscr{S}\setminus\{(1,\ i)\}\rangle$. Άρα $\langle\mathscr{S}\setminus\{(1,\ i)\}\rangle\neq\mathsf{S}_n$ και επομένως το σύνολο γεννητόρων S_n είναι ελάχιστο.

2. Θεωρούμε μια τυχούσα αντιμετάθεση $(1\ \ j)$, όπου $j\geq 3$, από το σύνολο $\mathscr{S}$. Θα δείξουμε ότι η αντιμετάθεση $(1\ \ j)$ ανήκει στην υποομάδα $\langle\mathscr{T}\rangle$, δηλαδή είναι γινόμενο αντιμεταθέσεων από το σύνολο $\mathscr{T}$. Πράγματι, θα έχουμε:

$$\begin{aligned}
(1\ \ j) &= (1\ \ j-1)\circ(j-1\ \ j)\circ(1\ \ j-1)\\
&= (1\ \ j-2)\circ(j-2\ \ j-1)\circ(1\ \ j-2)\circ(j-1\ \ j)\circ(1\ \ j-2)\circ(j-2\ \ j-1)\circ(1\ \ j-2)\\
&= (1\ \ j-2)\circ(j-2\ \ j-1)\circ(j-1\ \ j)\circ(1\ \ j-2)^2\circ(j-2\ \ j-1)\circ(1\ \ j-2)\\
&= (1\ \ j-2)\circ(j-2\ \ j-1)\circ(j-1\ \ j)\circ(j-2\ \ j-1)\circ(1\ \ j-2)\\
&\ \ \vdots\\
&= (1\ 2)\circ(2\ 3)\circ(3\ 4)\circ\cdots\circ(j-2\ \ j-1)\circ(j-1\ \ j)\circ(j-2\ \ j-1)\circ\cdots\circ(3\ 4)\circ(2\ 3)\circ(1\ 2)
\end{aligned}$$

Άρα η μετάθεση $(1\ \ j)$ γράφεται ως γινόμενο αντιμεταθέσεων του συνόλου $\mathscr{T}$ και επομένως $(1\ \ j)\in\langle\mathscr{T}\rangle$. Επειδή το υποσύνολο $\langle\mathscr{T}\rangle$ είναι υποομάδα της S_n, έπεται ότι $\langle\mathscr{S}\rangle\leq\langle\mathscr{T}\rangle$. Επειδή από το μέρος 1. έχουμε $\mathsf{S}_n=\langle\mathscr{S}\rangle$, θα έχουμε $\mathsf{S}_n=\langle\mathscr{T}\rangle$ και επομένως το σύνολο $\mathscr{T}$ είναι ένα σύνολο γεννητόρων της S_n. Το ότι το σύνολο γεννητόρων $\mathscr{T}$ είναι ελάχιστο αποδεικνύεται με ανάλογο επιχείρημα όπως στο μέρος 1., και αφήνεται ως Άσκηση, βλέπε την Άσκηση 5.6.14.

3. Επειδή από το μέρος 2. το σύνολο $\mathscr{T}$ είναι σύνολο γεννητόρων της S_n και $(1\ 2) \in \mathscr{T}$, αρκεί να δείξουμε ότι τα υπόλοιπα στοιχεία $(2\ 3)$, $(3\ 4)$, $\cdots$, $(n-1\ n)$ του συνόλου $\mathscr{T}$ ανήκουν στην υποομάδα $H := \langle (1\ 2),\ (1\ 2\ 3\ \cdots\ n)\rangle$. Θα έχουμε διαδοχικά:

$$\begin{aligned}
(1\ 2\ 3\ \cdots\ n)\circ(1\ 2)\circ(1\ 2\ 3\ \cdots\ n)^{-1} &= (2\ 3) \in H\\
(1\ 2\ 3\ \cdots\ n)\circ(2\ 3)\circ(1\ 2\ 3\ \cdots\ n)^{-1} &= (3\ 4) \in H\\
&\vdots\\
(1\ 2\ 3\ \cdots\ n)\circ(n-2\ n-1)\circ(1\ 2\ 3\ \cdots\ n)^{-1} &= (n-1\ n) \in H
\end{aligned}$$

Άρα πράγματι $\mathscr{T} \subseteq H$ και επομένως $\mathsf{S}_n = \langle \mathscr{T}\rangle \leq H$. Δηλαδή $\mathsf{S}_n = H = \langle (1\ 2),\ (1\ 2\ 3\ \cdots\ n)\rangle$ και άρα το σύνολο $\mathscr{R}$ είναι ένα σύνολο γεννητόρων της S_n. Προφανώς το σύνολο γεννητόρων $\mathscr{R}$ είναι ελάχιστο διότι τα σύνολα $\mathscr{R}\setminus\{(1\ 2)\}$ και $\mathscr{R}\setminus\{(1\ 2\ 3\ \cdots\ n)\}$ παράγουν κυκλική υποομάδα τάξης 2 και n αντίστοιχα, και αυτή η κυκλική υποοομάδα δεν μπορεί να είναι η S_n, διότι η S_n δεν είναι κυκλική, αν $n \geq 3$. ■

Θεώρημα 5.4.2. *Τα ακόλουθα σύνολα αντιμεταθέσεων είναι σύνολα γεννητόρων της* A_n, $n \geq 3$*:*

$$\mathscr{A} = \Big\{\sigma \in \mathsf{S}_n \mid \sigma \text{ } \textit{είναι κύκλος μήκους } 3\Big\}$$

$$\mathscr{B}_{r,s} = \Big\{(r\ \ s\ \ i) \in \mathsf{S}_n \mid 1 \leq i \neq r, s \leq n\Big\} \qquad (r \neq s)$$

$$\mathscr{C} = \Big\{(1\ 2\ 3),\ \ (1\ 2\ 4),\ \cdots,\ (1\ 2\ n)\Big\}$$

$$\mathscr{D} = \Big\{(i\ \ j)\circ(k\ \ l) \in \mathsf{A}_n \mid 1 \leq i \neq j \leq n \ \ \textit{και}\ \ 1 \leq k \neq l \leq n\Big\} \qquad (n \geq 5)$$

Απόδειξη. 1. Γνωρίζουμε ότι η εναλλάσσουσα υποομάδα A_n αποτελείται από τις άρτιες μεταθέσεις, και κάθε άρτια μετάθεση είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων. Επομένως, για να δείξουμε ότι το σύνολο των κύκλων μήκους 3 είναι ένα σύνολο γεννητόρων της A_n, αρκεί να δείξουμε ότι το γινόμενο $(i\ \ j)\circ(k\ \ l)$ δύο τυχαίων αντιμεταθέσεων $(i\ \ j)$ και $(k\ \ l)$ είναι γινόμενο κύκλων μήκους 3.

Αυτό πράγματι ισχύει διότι:

(α') Αν $\{i,j\}\cap\{k,l\} = \emptyset$, τότε υπολογίζουμε εύκολα ότι:

$$(i\ \ j)\circ(k\ \ l) = (i\ \ k\ \ j)\circ(i\ \ k\ \ l)$$

(β') Αν $i = k$, τότε:

$$(i\ \ j)\circ(i\ \ l) = (i\ \ l\ \ j)$$

(γ') Αν $i = l$, τότε:

$$(i\ \ j)\circ(k\ \ i) = (i\ \ k\ \ j)$$

(δ') Αν $j = k$, τότε:

$$(i\ \ j)\circ(j\ \ l) = (i\ \ j\ \ l)$$

(ε') Αν $j = l$, τότε:

$$(i\ \ j)\circ(k\ \ j) = (i\ \ j\ \ k)$$

Επομένως το γινόμενο δύο αντιμεταθέσεων είναι γινόμενο κύκλων μήκους 3, και άρα, επειδή κάθε στοιχείο της A_n είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων, έπεται οτι κάθε στοιχείο της A_n είναι γινόμενο κύκλων μήκους 3. Έτσι το σύνολο $\mathscr{A}$ όλων των κύκλων μήκους 3 είναι σύνολο γεννητόρων της A_n, δηλαδή $\mathsf{A}_n = \langle \mathscr{A}\rangle$.

2. Έστω $1 \le r \ne s \le n$ σταθεροί διαφορετικοί ακέραιοι, και έστω $H = \langle \mathscr{B}_{r,s} \rangle$ η υποομάδα της A_n η οποία παράγεται από το σύνολο $\mathscr{B}_{r,s}$ των κύκλων της μορφής $(r\ s\ i)$ μήκους 3, όπου $1 \le i \ne r,s \le n$. Τότε $H \le \mathsf{A}_n$, και επειδή από το μέρος 1. η εναλλάσσουσα υποομάδα παράγεται από το σύνολο όλων των κύκλων μήκους 3, αρκεί να δείξουμε ότι κάθε κύκλος $(i\ j\ k)$ μήκους 3 είναι γινόμενο κύκλων από το σύνολο $\mathscr{B}_{r,s}$. Πράγματι θα έχουμε:

$$(i\ j\ k) = (r\ s\ i)\circ(r\ s\ i)\circ(r\ s\ k)\circ(r\ s\ j)\circ(r\ s\ i)$$

Επομένως κάθε κύκλος μήκους 3 είναι γινόμενο κύκλων από το σύνολο $\mathscr{B}_{r,s}$, και αυτό σημαίνει ότι $\mathsf{A}_n = \langle \mathscr{B}_{r,s} \rangle$.

3. Προκύπτει άμεσα από το μέρος 2. διότι $\mathscr{C} = \mathscr{B}_{1,2}$.

4. Επειδή η A_n παράγεται από τους κύκλους μήκους 3, αρκεί να δείξουμε ότι κάθε κύκλος μήκους 3 είναι γινόμενο μεταθέσεων με κυκλικό τύπο $(2,2)$. Έστω $(i_1\ i_2\ i_3)$ ένας τυχαίος κύκλος μήκους 3. Επειδή $n \ge 5$, μπορούμε να επιλέξουμε $i_4 \ne i_5$, όπου $i_4, i_5 \in \{i_1, i_2, i_3\}$, και τότε θα έχουμε:

$$(i_1\ i_2\ i_3) = (i_1\ i_2)\circ(i_4\ i_5)\circ(i_4\ i_5)\circ(i_2\ i_3)$$

από όπου προκύπτει το ζητούμενο. ■

5.5 Η εναλλάσσουσα υποομάδα A_n είναι απλή αν και μόνο αν $n \ne 4$

Η παρούσα υποενότητα είναι αφιερώμενη στην απόδειξη ενος σημαντικού Θεωρήματος, η αρχική μορφή του οποίου οφείλεται στον Camille Jordan.[6] Συγκεκριμένα ο Jordan απέδειξε ότι η εναλλάσσουσα υποομάδα A_n είναι **απλή**, δηλαδή δεν περιέχει καμία γνήσια μη τετριμμένη κανονική υποομάδα, όταν $n \ne 4$. Αυτό το αποτέλεσμα έχει σημαντικές συνέπειες στη Θεωρία Galois αναφορικά με την επιλυσιμότητα εξισώσεων.

Λήμμα 5.5.1. *1. Αν $n = 4$, τότε υπάρχουν κύκλοι μήκους 3 στην A_4 οι οποίοι είναι συζυγείς ως στοιχεία της S_4 αλλά δεν είναι συζυγείς ως στοιχεία της A_4.*

2. Αν $n \ge 5$, τότε δύο τυχόντες κύκλοι μήκους 3 στην A_n είναι συζυγείς ως στοιχεία της A_n.

3. Αν $n \ge 5$ και $\{\iota\} \ne N \trianglelefteq \mathsf{A}_n$ είναι μια κανονική υποομάδα της A_n η οποία περιέχει έναν κύκλο μήκους 3, τότε $N = \mathsf{A}_n$.

Απόδειξη. 1. Σύμφωνα με το Θεώρημα 5.2.6 όλοι οι κύκλοι μήκους 3 είναι συζυγείς στην S_4, αλλά οι κύκλοι $(1\ 2\ 3)$ και $(1\ 3\ 2)$ δεν είναι συζυγείς ως στοιχεία της A_4. Πράγματι, αν υπάρχει μετάθεση $\sigma \in \mathsf{A}_4$ έτσι ώστε: $\sigma\circ(1\ 2\ 3)\circ\sigma^{-1} = (1\ 3\ 2)$, τότε:

$$\sigma\circ(1\ 2\ 3)\circ\sigma^{-1} = (1\ 3\ 2) \implies (\sigma(1)\ \sigma(2)\ \sigma(3)) = (1\ 3\ 2) \implies \sigma(1)=1,\ \sigma(2)=3,\ \sigma(3)=2$$

Επομένως $\sigma = (2\ 3)$ η οποία δεν είναι άρτια μετάθεση, δηλαδή $\sigma \notin \mathsf{A}_4$. Αυτό είναι άτοπο και άρα οι κύκλοι $(1\ 2\ 3)$ και $(1\ 3\ 2)$ δεν είναι συζυγείς ως στοιχεία της A_4.

2. Έστω σ ένας κύκλος μήκους 3 στην A_n. Σύμφωνα με το Θεώρημα 5.2.6, ο σ είναι συζυγής στην S_n με τον κύκλο $(1\ 2\ 3)$, δηλαδή υπάρχει $\tau \in \mathsf{S}_n$ έτσι ώστε

$$\tau\circ\sigma\circ\tau^{-1} = (1\ 2\ 3)$$

Αν $\tau \in \mathsf{A}_n$, τότε οι σ και $(1\ 2\ 3)$ είναι συζυγείς στην A_n. Αν $\sigma \notin \mathsf{A}_n$, θεωρούμε την μετάθεση $\rho = (4\ 5)\circ\tau$, αυτό μπορεί να γίνει διότι $n \ge 5$, η οποία είναι προφανώς άρτια, και τότε:

$$\rho\circ\sigma\circ\rho^{-1} = (4\ 5)\circ\tau\circ\sigma\circ\tau^{-1}\circ(4\ 5) = (4\ 5)\circ(1\ 2\ 3)\circ(4\ 5) = (1\ 2\ 3)$$

Δηλαδή σε κάθε περίπτωση κάθε κύκλος μήκους 3 είναι συζυγής στην A_n με τον κύκλο $(1\ 2\ 3)$. Ιδιαίτερα όλοι οι κύκλοι μήκους 3 είναι συζυγείς στην A_n.

[6] Camille Jordan (5 Ιανουαρίου 1838 - 22 Ιανουαρίου 1922) [https://en.wikipedia.org/wiki/Camille_Jordan]: Γάλλος μαθηματικός με σημαντική συμβολή στη Θεωρία Ομάδων, στην Άλγεβρα, στη Τοπολογία, και στη Μαθηματική Ανάλυση.

3. Αν η υποομάδα N περιέχει έναν κύκλο μήκους 3, τότε επειδή, από το μέρος 2., όλοι οι κύκλοι μήκους 3 είναι συζυγείς ως στοιχεία της A_n, και επειδή η N είναι κανονική υποομάδα της A_n, έπεται ότι η N περιέχει όλους τους κύκλους μήκους 3. Επειδή το σύνολο των κύκλων μήκους 3 παράγει την A_n, έπεται ότι $N = \mathsf{A}_n$. ■

Θεώρημα 5.5.2 (C. Jordan, 1870)**.** *Η εναλλάσσουσα υποομάδα A_n είναι απλή για κάθε $n \neq 4$.*

Απόδειξη. Θα χωρίσουμε την απόδειξη σε αρκετά βήματα.

1. Αν $1 \leq n \leq 3$, τότε η A_n είναι είτε η τετριμμένη, όταν $n = 1$ και $n = 2$, είτε είναι (ισόμορφη με την) κυκλική τάξης 3, όταν $n = 3$: $\mathsf{A}_3 = \langle (1\ 2\ 3) \rangle = \{\iota,\ (1\ 2\ 3),\ (1\ 3\ 2)\}$. Η τελευταία προφανώς είναι απλή.

2. Αν $n = 4$, τότε η εναλλάσσουσα υποομάδα A_4 δεν είναι απλή διότι περιέχει ως κανονική υποομάδα το ακόλουθο ισόμορφο αντίγραφο της ομάδας $\mathcal{V}_4$ του Klein:

$$\mathcal{V}_4 = \{\iota,\ (1\ 2)\circ(3\ 4),\ (1\ 3)\circ(2\ 4),\ (14)\circ(23)\}$$

   Αυτό προκύπτει εύκολα, υπολογίζοντας ότι τα στοιχεία $\rho\circ\sigma\circ\rho^{-1}$, όπου $\rho \in \mathsf{A}_4$ και $\sigma \in \mathcal{V}_4$, ανήκουν στην $\mathcal{V}_4$, λαμβάνοντας υπόψη τον πίνακα Cayley της ομάδας

$$\mathsf{A}_4 = \Big\{\iota,\ (1\ 2\ 3),\ (1\ 2\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4),\ (1\ 3\ 2),\ (1\ 4\ 2),\ (1\ 4{,}3),\ (2\ 4\ 3),\ (1\ 2)\circ(3\ 4),\ (1\ 3)\circ(2\ 4),\ (1\ 4)\circ(2\ 3)\Big\}$$

   βλέπε τον πίνακα πριν από την Πρόταση 3.5.1. Ας κάνουμε ενδεικτικά κάποιους υπολογισμούς. Αρκεί να θεωρήσουμε ρ να είναι ένας από τους 8 κύκλους μήκους 3. Εδώ $\rho = (1\ 2\ 3)$.

$$(1\ 2\ 3)\circ(1\ 2)\circ(3\ 4)\circ(1\ 2\ 3)^{-1} = (1\ 2\ 3)\circ(1\ 2)\circ(3\ 4)\circ(1\ 3\ 2) = (1\ 4)\circ(2\ 3) \in \mathcal{V}_4$$

$$(1\ 2\ 3)\circ(1\ 3)\circ(2\ 4)\circ(1\ 2\ 3)^{-1} = (1\ 2\ 3)\circ(1\ 3)\circ(2\ 4)\circ(1\ 3\ 2) = (1\ 2)\circ(3\ 4) \in \mathcal{V}_4$$

$$(1\ 2\ 3)\circ(1\ 4)\circ(2\ 3)\circ(1\ 2\ 3)^{-1} = (1\ 2\ 3)\circ(1\ 3)\circ(2\ 3)\circ(1\ 3\ 2) = (1\ 3)\circ(2\ 4) \in \mathcal{V}_4$$

   Η επαλήθευση ότι $\rho\circ\sigma\circ\rho^{-1} \in \mathcal{V}_4$, για κάθε $\sigma \in \mathcal{V}_4$, όπου ρ είναι ένας από τους υπόλοιπους 7 κύκλους μήκους 3 της A_4 είναι παρόμοια και αφήνεται ως Άσκηση, βλέπε την Άσκηση 5.6.25.

3. Υποθέτουμε ότι $n \geq 5$. Έστω $\{\iota\} \neq K \trianglelefteq \mathsf{A}_n$ μια μη τετριμμένη κανονική υποομάδα της A_n. Θα δείξουμε σε μια σειρά βημάτων ότι $K = \mathsf{A}_n$. Σύμφωνα με το Λήμμα 5.5.1, για να το δείξουμε αυτό, αρκεί να δείξουμε ότι η K περιέχει έναν κύκλο μήκους 3.

   Έστω ότι $\iota \neq \sigma \in K$ είναι μια τυχούσα μετάθεση στην υποομάδα K την οποία τη γράφουμε ως γινόμενο ξένων κύκλων μήκους ≥ 2:

$$\sigma = \sigma_1\circ\sigma_2\circ\cdots\circ\sigma_k$$

   (α') Υποθέτουμε ότι για κάποιο $i = 1, 2\cdots, k$, ο κύκλος σ_i έχει μήκος $\ell(\sigma_i) \geq 4$. Επειδή ξένοι κύκλοι μετατίθενται, χωρίς βλάβη της γενικότητας, εν ανάγκη μετά από κάποια αναδιάταξη, μπορούμε να υποθέσουμε ότι $i = 1$ και τότε:

$$\sigma_1 = (i_1\ \ i_2\ \ \cdots\ \ i_r), \qquad r \geq 4$$

   Θεωρούμε τον κύκλο $\rho = (i_1\ \ i_2\ \ i_3)$ μήκους 3. Επειδή η υποομάδα K είναι κανονική υποομάδα της A_4, θα έχουμε ότι $\rho\circ\sigma\circ\rho^{-1} \in K$. Χρησιμοποιώντας ότι $\rho\circ\sigma\circ\rho^{-1} = \rho\circ\sigma_1\circ\rho^{-1}\circ\rho\circ\sigma_2\circ\rho^{-1}\circ\cdots\circ\rho\circ\sigma_n\circ\rho^{-1}$, ότι οι κύκλοι σ_s, $2 \leq s \leq k$ δεν περιέχουν τα στοιχεία i_1, i_2, i_3, και ότι $\sigma_2\circ\cdots\circ\sigma_k = \sigma_1^{-1}\circ\sigma$, θα έχουμε:

$$\begin{aligned}
\rho\circ\sigma\circ\rho^{-1} &= \rho\circ\sigma_1\circ\rho^{-1}\circ\sigma_2\circ\cdots\circ\sigma_k \\
&= \rho\circ\sigma_1\circ\rho^{-1}\circ\sigma_1^{-1}\circ\sigma \\
&= (i_1\ \ i_2\ \ i_3)\circ(i_1\ \ i_2\ \ \cdots\ \ i_r)\circ(i_1\ \ i_3\ \ i_2)\circ(i_r\ \ i_{r-1}\ \ \cdots\ \ i_1)\circ\sigma \\
&= (i_1\ \ i_2\ \ i_4)\circ\sigma
\end{aligned}$$

και άρα:

$$\rho\circ\sigma\circ\rho^{-1}=(i_1\ i_2\ i_4)\circ\sigma \implies (i_1\ i_2\ i_4)=\rho\circ\sigma\circ\rho^{-1}\circ\sigma^{-1}\in K$$

Επομένως η K περιέχει τον κύκλο $(i_1\ i_2\ i_4)$ μήκους 3.

(β΄) Υποθέτουμε ότι όλοι οι κύκλοι σ_i έχουν μήκος ≤ 3 και τουλάχιστον δύο από τους κύκλους σ_i έχουν μήκος 3. Σ΄ αυτή την περίπτωση προφανώς θα έχουμε ότι $n\ge 6$. Έτσι υποθέτουμε ότι για κάποια $i,j=1,2\cdots,k$, οι κύκλοι σ_i και σ_j είναι ξένοι και έχουν μήκος $\ell(\sigma_i)=3=\ell(\sigma_j)$. Επειδή ξένοι κύκλοι μετατίθενται, χωρίς βλάβη της γενικότητας, εν ανάγκη μετά από κάποια αναδιάταξη, μπορούμε να υποθέσουμε ότι $i=1$ και $j=2$, και τότε:

$$\sigma_1=(i_1\ i_2\ i_3)\qquad\text{και}\qquad\sigma_2=(i_4\ i_5\ i_6)$$

Θεωρούμε τον κύκλο $\rho=(i_1\ i_2\ i_4)$ μήκους 3. Όπως και στην περίπτωση (α΄), θα έχουμε:

$$\begin{aligned}\rho\circ\sigma\circ\rho^{-1} &= \rho\circ\sigma_1\circ\sigma_2\circ\rho^{-1}\circ\sigma_3\circ\sigma_4\circ\cdots\circ\sigma_k\\ &= \rho\circ\sigma_1\circ\sigma_2\circ\rho^{-1}\circ\sigma_2^{-1}\circ\sigma_1^{-1}\circ\sigma\\ &= (i_1\ i_2\ i_4)\circ(i_1\ i_2\ i_3)\circ(i_4\ i_5\ i_6)\circ(i_1\ i_4\ i_2)\circ(i_4\ i_6\ i_5)\circ(i_1\ i_3\ i_2)\circ\sigma\\ &= (i_1\ i_2\ i_5\ i_3\ i_4)\circ\sigma\end{aligned}$$

και άρα:

$$\rho\circ\sigma\circ\rho^{-1}=(i_1\ i_2\ i_5\ i_3\ i_4)\circ\sigma \implies (i_1\ i_2\ i_5\ i_3\ i_4)=\rho\circ\sigma\circ\rho^{-1}\circ\sigma^{-1}\in K$$

Επομένως η K περιέχει τον κύκλο $(i_1\ i_2\ i_5\ i_3\ i_4)$ μήκους 5. Τότε μπορούμε να εφαρμόσουμε την περίπτωση (α΄) γι΄ αυτόν τον κύκλο και να συμπεράνουμε ότι η K περιέχει έναν κύκλο μήκους 3.

(γ΄) Υποθέτουμε ότι ακριβώς ένας κύκλος σ_i έχει μήκος ≤ 3 και οι υπόλοιποι κύκλοι έχουν μήκος ≤ 2. Όπως και στις παραπάνω περιπτώσεις, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι ο μοναδικός κύκλος μήκους 3 είναι ο $\sigma_1=(i_1\ i_2\ i_3)$, και οι κύκλοι σ_i, $2\le i\le k$, είναι αντιμεταθέσεις. Χρησιμοποιώντας ότι ξένοι κύκλοι μετατίθενται, θα έχουμε:

$$K\ni\sigma^2=(\sigma_1\circ\sigma_2\circ\cdots\circ\sigma_k)^2=\sigma_1^2\circ\sigma_2^2\circ\cdots\circ\sigma_k^2=\sigma_1^2=(i_1\ i_2\ i_3)^2=(i_1\ i_3\ i_2)$$

Επομένως η K περιέχει τον κύκλο $(i_1\ i_3\ i_2)$ μήκους 3.

(δ΄) Όλοι οι ξένοι κύκλοι σ_i, $1\le i\le k$, είναι μήκους 2, δηλαδή είναι αντιμεταθέσεις. Σ΄ αυτή την περίπτωση προφανώς θα έχουμε $k\ge 2$, διότι η μετάθεση σ είναι άρτια. Όπως και στις παραπάνω περιπτώσεις, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $\sigma_1=(i_1\ i_2)$ και $\sigma_2=(i_3,i_4)$. Θεωρούμε την μετάθεση $\rho=(i_1\ i_2\ i_3)$. Τότε θα έχουμε:

$$\begin{aligned}\rho\circ\sigma\circ\rho^{-1} &= \rho\circ\sigma_1\circ\sigma_2\circ\rho^{-1}\circ\sigma_3\circ\sigma_4\circ\cdots\circ\sigma_k\\ &= \rho\circ\sigma_1\circ\sigma_2\circ\rho^{-1}\circ\sigma_2^{-1}\circ\sigma_1^{-1}\circ\sigma\\ &= (i_1\ i_2\ i_3)\circ(i_1\ i_2)\circ(i_3\ i_4)\circ(i_1\ i_3\ i_2)\circ(i_3\ i_4)\circ(i_1\ i_2)\circ\sigma\\ &= (i_1\ i_3)\circ(i_2\ i_4)\circ\sigma\end{aligned}$$

και άρα:

$$\rho\circ\sigma\circ\rho^{-1}=(i_1\ i_3)\circ(i_2\ i_4)\circ\sigma \implies (i_1\ i_3)\circ(i_2\ i_4)=\rho\circ\sigma\circ\rho^{-1}\circ\sigma^{-1}\in K$$

Θεωρούμε τον κύκλο $\tau=(i_1\ i_3\ i_5)$ μήκους 3. Τότε θα έχουμε:

$$\begin{aligned}K\ni\rho\circ\sigma\circ\rho^{-1}\circ\sigma^{-1}\circ\tau\circ\rho\circ\sigma\circ\rho^{-1}\circ\sigma^{-1}\circ\tau^{-1} &= (i_1\ i_3)\circ(i_2\ i_4)\circ(i_1\ i_3\ i_5)\circ(i_1\ i_3)\circ(i_2\ i_4)\circ(i_1\ i_5\ i_3)\\ &= (i_1\ i_3)\circ(i_1\ i_3\ i_5)\circ(i_1\ i_3)\circ(i_1\ i_5\ i_3)\\ &= (i_1\ i_3\ i_5)\end{aligned}$$

Επομένως η K περιέχει τον κύκλο $(i_1\ i_3\ i_5)$ μήκους 3.

Άρα σε κάθε περίπτωση η κανονική υποομάδα K περιέχει έναν κύκλο μήκους 3, και επομένως $K = \mathsf{A}_4$.

Επομένως δείξαμε ότι η εναλλάσσουσα υποομάδα A_4 είναι απλή αν $n \neq 4$ και δεν είναι απλή αν $n = 4$. ■

Πρόταση 5.5.3. *Αν $n \geq 5$, τότε η μοναδική μη τετριμμένη γνήσια κανονική υποομάδα της S_n είναι η A_n.*

Απόδειξη. Έστω ότι $\{\iota\} \leq N \leq \mathsf{S}_n$ είναι μια κανονική υποομάδα της S_n και υποθέτουμε ότι $\{\iota\} \neq N \neq \mathsf{S}_n$. Επειδή $N \neq \{\iota\}$, έπεται ότι υπάρχει $N \ni \sigma \neq \iota$, και άρα $\sigma(i) \neq i$ για κάποιο $i \in \mathbb{N}_n$. Επειδή $n \geq 5$, μπορούμε να επιλέξουμε ένα στοιχείο $j \in \mathbb{N}_n$ έτσι ώστε: $i \neq j \neq \sigma(i)$. Αν η σ είναι αντιμετάθεση, τότε, επειδή η N είναι κανονική υποομάδα της S_n, έπεται ότι η N θα περιέχει και όλες τις αντιμεταθέσεις. Επειδή το σύνολο των αντιμεταθέσεων παράγει την S_n, έπεται ότι $N = \mathsf{S}_n$ και αυτό είναι άτοπο από την υπόθεση που κάναμε. Άρα η μετάθεση σ δεν μπορεί να είναι αντιμετάθεση. Θεωρούμε την αντιμετάθεση $\mu = (i\ \ j)$. Επειδή η N είναι κανονική υποομάδα, θα έχουμε $\mu \circ \sigma^{-1} \circ \mu^{-1} \in N$ και επομένως $\sigma \circ \mu \circ \sigma^{-1} \circ \mu^{-1} \in N$. Όμως

$$N \ni \sigma \circ \mu \circ \sigma^{-1} \circ \mu^{-1} = \sigma \circ (i\ \ j) \circ \sigma^{-1} \circ (i\ \ j) = (\sigma(i)\ \ \sigma(j)) \circ (i\ \ j)$$

και η τελευταία μετάθεση δεν είναι η ταυτοτική διότι διαφορετικά θα είχαμε $(\sigma(i)\ \ \sigma(j)) \circ (i\ \ j) = \iota \implies (\sigma(i)\ \ \sigma(j)) = (i\ \ j)^{-1} = (i\ \ j)$, και αυτό είναι άτοπο διότι $i \neq \sigma(i) \neq j$ και $\sigma(i) \neq \sigma(j)$. Αν επιπρόσθετα $\sigma(j) \neq i$ και $\sigma(j) \neq j$, τότε οι αντιμεταθέσεις $(\sigma(i)\ \ \sigma(j))$ και $(i\ \ j)$ είναι ξένες, και άρα ο κυκλικός τύπος της μετάθεσης $(\sigma(i)\ \ \sigma(j)) \circ (i\ \ j)$ είναι $(2,2)$. Αν $\sigma(j) = i$ ή $\sigma(j) = j$, τότε θα έχουμε: $(\sigma(i)\ \ i) \circ (i\ \ j) = (\sigma(i)\ \ i\ \ j)$ ή $(\sigma(i)\ \ j) \circ (i\ \ j) = (\sigma(i)\ \ j\ \ i)$ αντίστοιχα, δηλαδή είναι ένας κύκλος μήκους 3. Επομένως η υποομάδα N περιέχει είτε μια μετάθεση με κυκλικό τύπο $(2,2)$ είτε έναν κύκλο μήκους 3. Επειδή N είναι κανονική υποομάδα της S_n, έπεται ότι η N θα περιέχει και όλες τις μεταθέσεις με κυκλικό τύπο $(2,2)$ ή αντίστοιχα όλους τους κύκλους μήκους 3. Επειδή αυτού του τύπου οι μεταθέσεις παράγουν την A_n, έπεται ότι η N θα περιέχει την A_n και επομένως $N = \mathsf{A}_n$. ■

Πόρισμα 5.5.4. *Αν $n \geq 2$, τότε η μοναδική υποομάδα της S_n με δείκτη 2 είναι η A_n.*

Απόδειξη. Έστω ότι $H \leq \mathsf{S}_n$ είναι μια υποομάδα της S_n με δείκτη 2. Τότε από την Πρόταση 3.4.13, η H είναι κανονική και η τάξη της είναι $\mathsf{o}(H) = \frac{n!}{2}$.

1. Αν $n = 2$ ή $n = 3$, τότε προφανώς $H = \mathsf{A}_n$. Πράγματι, αν $n = 2$, τότε $\mathsf{A}_2 = \{\iota\}$ είναι η μοναδική υποομάδα της S_2 με δείκτη 2. Αν $n = 3$, τότε επίσης η μοναδική υποομάδα της S_3 με τάξη 3, και άρα με δείκτη 2, είναι η A_3.

2. Αν $n \geq 5$, τότε, επειδή η H είναι κανονική και επειδή η H είναι προφανώς γνήσια και μη τετριμμένη, η προηγούμενη Πρόταση 5.5.3 μας εξασφαλίζει ότι $H = \mathsf{A}_n$.

3. Έστω ότι $n = 4$ και $H \neq \mathsf{A}_4$. Αν η H περιέχει έναν κύκλο μήκους 2 ή έναν κύκλο μήκους 3, τότε, επειδή η H είναι κανονική, η H θα περιέχει όλους τους κύκλους μήκους 2 ή όλους τους κύκλους μήκους 3 αντίστοιχα. Επειδή το σύνολο των κύκλων μήκους 2 παράγει την S_4 και το σύνολο των κύκλων μήκους 3 παράγει την A_4, έπεται στην πρώτη περίπτωση ότι η H περιέχει την S_4 και στην δεύτερη περίπτωση την A_4. Και οι δύο περιπτώσεις μάς οδηγούν σε άτοπο: $\mathsf{S}_4 \neq H$, διότι η H είναι δείκτη 2, και από την υπόθεσή μας $\mathsf{A}_4 \neq H$. Επειδή το σύνολο των αντιμεταθέσεων της S_4 είναι 6 και το σύνολο των κύκλων μήκους 3 είναι 8, έπεται ότι το πλήθος των στοιχείων της H είναι μικρότερο ή ίσο του $24 = \mathsf{o}(\mathsf{S}_4) - (8 + 6) = 10$, και αυτό είναι άτοπο διότι, επειδή η H είναι δείκτη 2, θα έχουμε $\mathsf{o}(H) = 12$. Στο άτοπο καταλήξαμε διότι υποθέσαμε ότι $H \neq \mathsf{A}_4$. Άρα $H = \mathsf{A}_4$. ■

Χάριν ευκολίας και για μελλοντική χρήση καταγράφουμε τα στοιχεία των συμμετρικών ομάδων S_3 και S_4 αν ανάλογα με τον κυκλικό τους τύπο:

1. Τα στοιχεία της S_3:

   (α') Η ταυτοτική μετάθεση ι.

(β') Οι ακόλουθοι 3 κύκλοι μήκους 2 (αντιμεταθέσεις):

$$(1\ 2),\quad (1\ 3),\quad (2\ 3)$$

(γ') Οι ακόλουθοι 2 κύκλοι μήκους 3:

$$(1\ 2\ 3),\quad (1\ 3\ 2)$$

Η εναλλάσσουσα υποομάδα A_3 αποτελείται από την ταυτοτική μετάθεση, και τους 2 κύκλους μήκους 3.

2. Τα στοιχεία της S_4:

(α') Η ταυτοτική μετάθεση ι.

(β') Οι ακόλουθοι 6 κύκλοι μήκους 2 (αντιμεταθέσεις):

$$(1\ 2),\quad (1\ 3),\quad (1\ 4),\quad (2\ 3),\quad (2\ 4),\quad (3\ 4)$$

(γ') Οι ακόλουθοι 8 κύκλοι μήκους 3:

$$(1\ 2\ 3),\quad (1\ 2\ 4),\quad (1\ 3\ 4),\quad (2\ 3\ 4),\quad (1\ 3\ 2),\quad (1\ 4\ 2),\quad (1\ 4{,}3),\quad (2\ 4\ 3),$$

(δ') Οι ακόλουθες μεταθέσεις με κυκλικό τύπο $(2,2)$:

$$(1\ 2)\circ(3\ 4),\quad (1\ 3)\circ(2\ 4),\quad (1\ 4)\circ(2\ 3)$$

(ε') Οι ακόλουθοι 6 κύκλοι μήκους 4:

$$(1\ 2\ 3\ 4),\quad (1\ 3\ 4\ 2),\quad (1\ 4\ 2\ 3),\quad (1\ 2\ 4\ 3),\quad (1\ 3\ 2\ 4),\quad (1\ 4\ 3\ 2)$$

Η εναλλάσσουσα υποομάδα A_4 αποτελείται από την ταυτοτική μετάθεση, τους 8 κύκλους μήκους 3, και τα 3 γινόμενα ξένων αντιμεταθέσεων.

5.6 Ασκήσεις

Άσκηση 5.6.1. *Να γραφεί η μετάθεση*

$$\sigma = (4\ 5\ 6)\circ(5\ 6\ 7)\circ(6\ 7\ 1)\circ(1\ 2\ 3)\circ(2\ 3\ 4)\circ(3\ 4\ 5)$$

της S_7 *ως γινόμενο ξένων κύκλων και ως γινόμενο αντιμεταθέσεων. Είναι η* σ *άρτια ή περιττή;*

Άσκηση 5.6.2. *Να δειχθεί ότι η εναλλάσσουσα υποομάδα* A_8 *έχει ένα στοιχείο τάξης* 15.

Άσκηση 5.6.3. *Θεωρούμε τις μεταθέσεις της συμμετρικής ομάδας* S_8*:*

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 5 & 3 & 7 & 8 & 6 \end{pmatrix} \quad \textit{και} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 6 & 8 & 7 & 1 & 5 & 2 \end{pmatrix}$$

(a) *Να γραφούν οι μεταθέσεις* σ *και* τ *ως γινόμενα ξένων κύκλων.*

(b) *Να προσδιοριστούν οι τάξεις των μεταθέσεων* τ *και* σ*.*

(c) *Να υπολογιστούν οι μεταθέσεις* σ^{2013} *και* τ^{2015}*.*

(d) *Να εξεταστεί αν, υπάρχει μετάθεση $\rho \in \mathsf{S}_8$ τέτοια, ώστε: $\rho \circ \tau \circ \rho^{-1} = \sigma$.*
Αν υπάρχει, να βρείτε μια τέτοια μετάθεση.

Άσκηση 5.6.4. *Θεωρούμε τη συμμετρική ομάδα $(\mathsf{S}_4, \circ)$ και ένα υποσύνολο $A = \{\sigma, \tau\}$ της S_4 όπου οι σ και τ είναι δύο ξένες αντιμεταθέσεις. Να δειχθεί ότι:*

(a) *το σύνολο $\langle A \rangle = \{\sigma^i \tau^j \mid i, j \in \mathbb{Z}\}$ είναι μια υποομάδα της S_4,*

(b) *η τάξη της υποομάδας $\langle A \rangle$ είναι ίση με 4, και*

(c) *η ομάδα $\langle A \rangle$ είναι ισόμορφη με το ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ της ομάδας $(\mathbb{Z}_2, +)$ με τον εαυτό της.*

Άσκηση 5.6.5. *Θεωρούμε τη συμμετρική ομάδα S_n, $n \geq 2$.*

1. *Ποια στοιχεία της S_n έχουν τάξη 2;*
2. *Αν σ, τ είναι στοιχεία της S_n, να εξετάσετε αν, και υπό ποιες προϋποθέσεις, τα στοιχεία $\sigma\tau\sigma^{-1}\tau^{-1}$ και $\sigma\tau\sigma^{-1}$ ανήκουν στην εναλλάσσουσα ομάδα A_n.*
3. *Να γραφεί η μετάθεση $\mu = (1234) \circ (4357) \circ (1234)^{-1} \circ (12345678)^4$ της S_8 ως γινόμενο ξένων κύκλων και ως γινόμενο αντιμεταθέσεων, και να βρεθεί η τάξη της. Είναι η μ περιττή μετάθεση;*
4. *Αν γνωρίζουμε ότι η μετάθεση*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & i & j & 7 & 8 & 9 & 6 \end{pmatrix} \in \mathsf{S}_9$$

είναι άρτια, να βρεθούν τα i, j.

Άσκηση 5.6.6. *Να βρεθεί το διάγραμμα Hasse των υποομάδων της κυκλικής υποομάδας $\langle \rho \rangle$ της συμμετρικής S_9 η οποία παράγεται από τη μετάθεση*

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 6 & 5 & 8 & 3 & 1 & 2 & 9 & 4 \end{pmatrix}$$

Άσκηση 5.6.7. *Θεωρούμε τη μετάθεση*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 5 & 2 & 6 & 1 & 4 & 10 & 3 & 8 & 7 \end{pmatrix} \in \mathsf{S}_{10}$$

Να γραφεί η σ ως γινόμενο ξένων κύκλων, ως γινόμενο αντιμεταθέσεων, και να προσδιοριστεί το πρόσημό της. Είναι η σ άρτια ή περιττή; Να προσδιοριστεί η τάξη της μετάθεσης σ^{2015}.

Άσκηση 5.6.8. *Να εξεταστεί αν η συμμετρική ομάδα S_7 περιέχει στοιχεία τάξης 5, 10, και 15. Ποια είναι η μέγιστη δυνατή τιμή την οποία μπορεί να έχει ως τάξη ένα στοιχείο της S_7;*

Άσκηση 5.6.9. *Έστω η συμμετρική ομάδα $(\mathsf{S}_n, \circ)$ και H οποιαδήποτε υποομάδα της. Να δειχθεί ότι το πλήθος των στοιχείων της H που είναι άρτιες μεταθέσεις, είναι ίσο είτε με την τάξη $\mathsf{o}(H)$ της H είτε ίσο με $\mathsf{o}(H)/2$.*

Άσκηση 5.6.10. *Θεωρούμε τη συμμετρική ομάδα S_n, $n \geq 3$. Να δειχθούν τα εξής:*

1. *Κάθε κύκλος στην S_n μπορεί να γραφεί ως γινόμενο το πολύ $n-1$ αντιμεταθέσεων.*
2. *Κάθε μετάθεση στην S_n η οποία δεν είναι κύκλος μπορεί να γραφεί ως γινόμενο το πολύ $n-2$ αντιμεταθέσεων.*

3. *Κάθε περιττή μετάθεση στην* S_n *μπορεί να γραφεί ως γινόμενο* $2n+3$ *αντιμεταθέσεων.*

4. *Κάθε άρτια μετάθεση στην* S_n *μπορεί να γραφεί ως γινόμενο* $2n+8$ *αντιμεταθέσεων.*

Άσκηση 5.6.11. *Θεωρούμε τα ακόλουθα στοιχεία της συμμετρικής ομάδας* S_9*:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 4 & 2 & 6 & 1 & 9 & 8 & 7 \end{pmatrix} \quad \text{και} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 9 & 2 & 7 & 8 & 4 & 6 & 3 \end{pmatrix}$$

1. *Να γραφούν οι μεταθέσεις* σ *και* τ *ως γινόμενα ξένων κύκλων και αντιμεταθέσεων.*

2. *Να υπολογιστούν οι τάξεις των στοιχείων* σ^{2014} *και* τ^{2013}*.*

3. *Να υπολογιστεί η τάξη της κυκλικής υποομάδας* $\langle \sigma \circ \tau \circ \sigma^{-1} \rangle$*.*

4. *Να εξεταστεί αν υπάρχει* $\rho \in S_7$ *έτσι ώστε:* $\rho\,\sigma\,\rho^{-1} = \tau$*.*

5. *Να υπολογιστεί η τάξη της τομής* $\langle \sigma \rangle \cap \langle \tau \rangle$*.*

Άσκηση 5.6.12. 1. *Έστω* $\sigma \in \mathsf{S}_n$ *ένα στοιχείο της συμμετρικής ομάδας* S_n*,* $n \geq 2$*. Να δειχθεί ότι η τάξη του* σ *είναι* 2 *αν και μόνο αν η μετάθεση* σ *είναι γινόμενο αντιμεταθέσεων ξένων ανά δύο.*

2. *Έστω* $\tau \in \mathsf{S}_7$ *ένα στοιχείο της συμμετρικής ομάδας* S_7 *για το οποίο γνωρίζουμε ότι:* $\tau^4 = (2\,1\,4\,3\,5\,6\,7)$*. Να βρεθεί η μετάθεση* τ *και να γραφεί ως γινόμενο ξένων κύκλων και αντιμεταθέσεων.*

Άσκηση 5.6.13. *Να σχεδιαστεί το διάγραμμα Hasse των υποομάδων της συμμετρικής ομάδας* S_3*.*

Άσκηση 5.6.14. *Να δειχθεί ότι το σύνολο γεννητόρων*

$$\mathscr{T} = \{(1\ 2),\ \ (2\ 3),\ \ (3\ 4),\ \ \cdots,\ \ (n-1\ \ n)\}$$

της S_n *είναι ελάχιστο.*

Άσκηση 5.6.15. *Να προσδιοριστεί αν η μετάθεση*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

είναι άρτια ή περιττή.

Άσκηση 5.6.16. *Να βρεθεί η κυκλική δομή όλων των δυνάμεων* τ^n*,* $n \in \mathbb{Z}$*, της μετάθεσης* $\tau = (1\,2\,3\,4\,5\,6\,7\,8) \in \mathsf{S}_8$*.*

Άσκηση 5.6.17. *Έστω* τ *ένας* m*-κύκλος στη συμμετρική ομάδα* S_n*. Να βρεθούν οι τιμές του* m *για τις οποίες η μετάθεση* τ *είναι άρτια.*

Άσκηση 5.6.18. 1. *Να βρεθεί ο κεντροποιητής της μετάθεσης* $(1\ 2)$ *στην* S_4 *και στην* S_5*.*

2. *Να προσδιοριστούν όλες οι υποομάδες τάξης* 4 *στη συμμετρική ομάδα* S_4*.*

Άσκηση 5.6.19. *Να βρεθεί ο κεντροποιητής του στοιχείου* $\tau = (1\,2 \cdots k) \in \mathsf{S}_n$*, όπου* $1 \leq k \leq n$*.*
Ποιο είναι το πλήθος των συζυγών στοιχείων του τ *στην* S_n*;*

Άσκηση 5.6.20. *Θεωρούμε τη μετάθεση* $\sigma = (1\ 2) \circ (3\ 4) \in \mathsf{S}_n$, $n \geq 4$.

1. *Να βρεθεί το πλήθος των συζυγών στοιχείων της* σ *στην* S_n.
2. *Να βρεθεί ο κεντροποιητής της* σ *στην* S_n.
3. *Να βρεθεί ο κεντροποιητής της* σ *στην* A_n.

Άσκηση 5.6.21. *Θεωρούμε τη μετάθεση* $\sigma \in \mathsf{S}_n$ *η οποία ως «1-1» και «επί» απεικόνιση ορίζεται ως εξής* $\sigma(i) = n - i$, $1 \leq i \leq n-1$ *και* $\sigma(n) = n$. *Να βρεθεί η ανάλυση σε ξένους κύκλους της* σ.

Άσκηση 5.6.22. *Να εξεταστεί αν οι μεταθέσεις της* S_9

$$\sigma_1 = (1\,2\,3) \circ (4\,5\,6) \circ (6\,8), \quad \sigma_2 = (6\,7\,8) \circ (8\,9) \circ (1\,2\,3\,4), \quad \sigma_3 = (1\,2\,3\,4) \circ (5\,6) \circ (7\,8\,9), \quad \sigma_4 = (1\,4\,5) \circ (2\,3) \circ (6\,7\,8\,9)$$

είναι συζυγείς (ανά δύο). Αν οι μεταθέσεις σ_i *και* σ_j *είναι συζυγείς,* $1 \leq i \neq j \leq 4$, *να βρεθεί μετάθεση* τ *έτσι ώστε* $\tau \circ \sigma_i \circ \tau^{-1} = \sigma_j$.

Άσκηση 5.6.23. *Να βρεθούν οι κυκλικοί τύποι των μεταθέσεων των ομάδων* S_5 *και* A_5, *και για κάθε κυκλικό τύπο να δοθεί αντίστοιχο παράδειγμα μετάθεσης.*

Άσκηση 5.6.24. *Έστω* $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_k$ *η ανάλυση μιας μετάθεσης* σ *σε γινόμενο ξένων κύκλων. Να βρεθούν αναγκαίες και ικανές συνθήκες έτσι ώστε* $\sigma = \sigma^{-1}$.

Άσκηση 5.6.25. *Να επαληθευθεί ότι για την ομάδα του Klein*

$$\mathcal{V}_4 = \{\iota,\ (1\ 2) \circ (3\ 4),\ (1\ 3) \circ (2\ 4),\ (1\,4) \circ (2\,3)\}$$

θεωρούμενης ως υποομάδας της A_4, *ισχύει ότι:* $\rho \circ \sigma \circ \rho^{-1} \in \mathcal{V}_4$, *για κάθε* $\rho \in \mathsf{A}_4$ *και για κάθε* $\sigma \in \mathcal{V}_4$.

Άσκηση 5.6.26. *Να βρεθεί το διάγραμμα Hasse των υποομάδων των εναλλασσουσών ομάδων* A_n, $1 \leq n \leq 4$.

Άσκηση 5.6.27. *Να βρεθούν οι κλάσεις συζυγίας της συμμετρικής ομάδας* S_3 *και της εναλλάσσουσας ομάδας* A_4.

Άσκηση 5.6.28. *Να δειχθεί ότι ο ομομορφισμός* $\epsilon \colon \mathsf{S}_n \longrightarrow \{1,-1\}$ *του οποίου ορίζει το πρόσημο μιας μετάθεσης είναι ο μοναδικός ομομορφισμός ομάδων από την* S_n *στην ομάδα* $\{1,-1\}$, *ο οποίος είναι «επί», δηλαδή αν*

$$f \colon \mathsf{S}_n \longrightarrow \{1,-1\}$$

είναι ένας επιμορφισμός ομάδων, τότε $f = \epsilon$.

Άσκηση 5.6.29. *Να δειχθεί ότι η απεικόνιση*

$$f \colon \mathsf{S}_n \longrightarrow \{1,-1\}, \quad f(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

είναι ένας επιμορφισμός ομάδων. Να συμπεράνετε από την Άσκηση 5.6.28 ότι για κάθε μετάθεση $\sigma \in \mathsf{S}_n$:

$$\epsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$$

Άσκηση 5.6.30. *Να προσδιοριστεί το πρόσημο ενός k-κύκλου $\sigma \in \mathsf{S}_n$ συναρτήσει του θετικού ακεραίου k.*

Άσκηση 5.6.31. *Να προσδιοριστούν τα κέντρα $\mathsf{Z}(\mathsf{S}_n)$ και $\mathsf{Z}(\mathsf{A}_n)$ των ομάδων S_n και A_n, $\forall n \geq 1$.*

Άσκηση 5.6.32. *Να δειχθεί ότι τα ακόλουθα σύνολα είναι (ελάχιστα) σύνολα γεννητόρων της εναλλάσσουσας ομάδας A_n:*

$$\{(1\ 2\ 3),\ \ (1\ 2\ 3\ \cdots\ n)\} \quad \textit{αν } n\textit{: περιττός,} \qquad \textit{και} \qquad \{(1\ 2\ 3),\ \ (2\ 3\ \cdots\ n)\} \quad \textit{αν } n\textit{: άρτιος}$$

Άσκηση 5.6.33. *Να δειχθεί ότι η συμμετρική ομάδα S_4 έχει 6 κύκλους μήκους 2, 8 κύκλους μήκους 3, και 6 κύκλους μήκους 4, και τα υπόλοιπα στοιχεία σχηματίζουν H μια υποομάδα της S_4. Είναι η H κυκλική; Είναι η H κανονική υποομάδα;*

Άσκηση 5.6.34. *Έστω n ένας θετικός ακέραιος και $d \mid n$ ένας διαιρέτης του n. Αν σ είναι ένας n-κύκλος στη συμμετρική ομάδα S_n, να δειχθεί ότι η μετάθεση σ^d είναι το γινόμενο d το πλήθος ξένων ανά δύο $\frac{n}{d}$-κύκλων.*

Άσκηση 5.6.35. *Να δειχθεί ότι ο κανονικοποιητής $N_{\mathsf{S}_n}(H)$ της κυκλικής υποομάδας $H = \langle(1\ 2\ 3\ \cdots\ n)\rangle$ της συμμετρικής ομάδας S_n έχει τάξη $n\phi(n)$, όπου ϕ είναι η συνάρτηση του Euler.*

Κεφάλαιο 6

Ομάδες Πηλίκα και τα Θεωρήματα Ισομορφισμών

Στο παρόν Κεφάλαιο θα μελετήσουμε τις βασικές ιδιότητες της ομάδας πηλίκο μιας ομάδας ως προς μια κανονική υπομάδα, θα αποδείξουμε τα βασικά θεωρήματα ισομορφισμών τα οποία αποτελούν θεμελιώδη εργαλεία στη Θεωρία Ομάδων, και θα δώσουμε εφαρμογές. Επιπρόσθετα θα δούμε διάφορες εκδοχές του θεωρήματος του Cayley, το οποίο πιστοποιεί ότι κάθε ομάδα είναι ισόμορφη με μια υποομάδα της ομάδας μεταθέσεων ενός κατάλληλου συνόλου. Ιδιαίτερα, έπεται ότι κάθε πεπερασμένη ομάδα τάξης n μπορεί να υλοποιηθεί ως υποομάδα της συμμετρικής ομάδας S_n.

6.1 Κανονικές Υποομάδες και Ομάδες Πηλίκα

Από τώρα και στο εξής σταθεροποιούμε μια (πολλαπλασιαστική) ομάδα $(G,\cdot)$.

Υπενθυμίζουμε ότι μια υποομάδα H της G καλείται **κανονική υποομάδα** αν ικανοποιείται μια από τις ακόλουθες ισοδύναμες συνθήκες:

1. $\mathsf{N}_G(H) = G$, δηλαδή $G = \{x \in G \mid xHx^{-1} = H\}$.
2. $\forall x \in G\colon \quad xHx^{-1} \subseteq H$.
3. $\forall x \in G,\ \forall h \in H\colon \quad x \cdot h \cdot x^{-1} \in H$.
4. $\forall x \in G\colon \quad xH = Hx$.

και τότε θα γράφουμε: $H \trianglelefteq G$.

6.1.1 Κανονικές Υποομάδες και Σχέσεις Ισοδυναμίας

Έστω ότι G είναι μια ομάδα και ότι H είναι μια υποομάδα της G. Τότε, όπως είδαμε στην υποενότητα 3.3, ορίζοντας

$$\forall x, y \in G\colon \ x \sim_{\mathscr{R}_H} y \quad \Longleftrightarrow \quad x^{-1}y \ \in \ H \tag{6.1}$$

αποκτούμε μια σχέση ισοδυναμίας $\mathscr{R}_H$ επί του συνόλου G.

Η ακόλουθη Πρόταση δίνει έναν ακόμα χαρακτηρισμό κανονικών υποομάδων ο οποίος, όπως θα δούμε, είναι απαραίτητος στην κατασκευή της ομάδας πηλίκο. Με βάση αυτόν τον χαρακτηρισμό οι κανονικές υποομάδες είναι ακριβώς εκείνες οι υποομάδες $H \leq G$ της G για τις οποίες η επαγόμενη σχέση ισοδυναμίας $\mathscr{R}_H$, ή ισοδύναμα η σχέση ισοδυναμίας $\mathscr{R}^H$, είναι συμβιβαστή με την πράξη της G.

Υπενθυμίζουμε, βλέπε τον Ορισμό 1.3.36, ότι: η σχέση ισοδυναμίας $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη «$\cdot$» της ομάδας G, αν και μόνο αν ισχύει:

$$\forall x, y, z, w \in G\colon \quad x \sim_{\mathscr{R}_H} z \quad \text{και} \quad y \sim_{\mathscr{R}_H} w \quad \Longrightarrow \quad xy \ \sim_{\mathscr{R}_H} \ zw \tag{6.2}$$

Με άλλα λόγια, αν και μόνο αν:

$$\forall x,y,z,w\in G:\quad x^{-1}z\ \in\ H\quad\text{και}\quad y^{-1}w\ \in\ H\quad\Longrightarrow\quad (xy)^{-1}zw=y^{-1}x^{-1}zw\ \in\ H \tag{6.3}$$

Ισοδύναμα:

$$\forall x,y,z,w\in G:\quad z\ \in\ xH\quad\text{και}\quad w\ \in\ yH\quad\Longrightarrow\quad zw\ \in\ (xy)H \tag{6.4}$$

Λαμβάνοντας υπόψη, ότι η κλάση ισοδυναμίας ενός στοιχείου x ως προς τη σχέση $\mathscr{R}_H$ συμπίπτει με το αριστερό σύμπλοκο (αριστερή πλευρική κλάση) του x στην H:

$$[x]_H=xH=\{xh\in G\mid h\in H\}$$

η τελευταία σχέση γράφεται ισοδύναμα:

$$\forall x,y,z,w\in G:\quad z\ \in\ [x]_H\quad\text{και}\quad w\ \in\ [y]_H\quad\Longrightarrow\quad zw\ \in\ [xy]_H \tag{6.5}$$

Πρόταση 6.1.1. *Για μια υποομάδα $H\leq G$ μιας ομάδας $(G,\cdot)$, οι ακόλουθες συνθήκες είναι ισοδύναμες:*

1. *Η υποομάδα H είναι κανονική.*
2. *Η σχέση ισοδυναμίας $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη της ομάδας G.*

Απόδειξη. 1. $\Longrightarrow$ 2. Υποθέτουμε ότι η H είναι μια κανονική υποομάδα της G. Για να δείξουμε ότι η σχέση ισοδυναμίας $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη «$\cdot$» της G, αρκεί να δείξουμε ότι:

$$\forall x,y,z,w\in G:\quad z\ \in\ xH\quad\text{και}\quad w\ \in\ yH\quad\Longrightarrow\quad zw\ \in\ (xy)H$$

Έστω $z\in xH$ και $w\in yH$. Επειδή H είναι κανονική, θα έχουμε $xH=Hx$ και άρα υπάρχουν $h_1,h_2\in H$ έτσι ώστε:

$$z=h_1x\quad\text{και}\quad w=yh_2\quad\Longrightarrow\quad zw=h_1xyh_2\in(h_1xy)H\quad\overset{(5)}{\Longrightarrow}\quad zw\in H(h_1xy)$$

Επειδή προφανώς

$$H(h_1xy)=(Hh_1)(xy)\quad\text{και}\quad Hh_1=H\quad\text{διότι}\quad h_1\in H$$

θα έχουμε:

$$zw\in H(h_1xy)=H(xy)\quad\Longrightarrow\quad zw\ \in\ (xy)H$$

Επομένως δείξαμε ότι ισχύει η συνεπαγωγή στη σχέση (6.4), και άρα η σχέση ισοδυναμίας $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη της G.

2. $\Longrightarrow$ 1. Επειδή η σχέση $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη της G, έπεται ότι θα ισχύει η σχέση (6.2). Έστω $g\in G$ και $h\in H$. Τότε

$$g^{-1}hg=g^{-1}ehg=g^{-1}e^{-1}hg=(eg)^{-1}hg$$

Έτσι, θέτοντας $x=e$, $y=g$, $z=h$ και $w=g$, στη σχέση (6.3), θα έχουμε:

$$x^{-1}z=e^{-1}h=h\in H\quad\text{και}\quad y^{-1}w=g^{-1}g=e\in H\quad\Longrightarrow\quad y^{-1}x^{-1}zw=g^{-1}e^{-1}hg=g^{-1}hg\ \in\ H$$

Επομένως δείξαμε ότι: $g^{-1}hg\ \in\ H$, $\forall g\in G$, $\forall h\in H$. Άρα η υποομάδα H είναι μια κανονική υποομάδα της G. ■

Είδαμε ότι, αν $H\trianglelefteq G$ είναι μια κανονική υποομάδα της G, τότε η σχέση ισοδυναμίας $\mathscr{R}_H$ επί του συνόλου G είναι συμβιβαστή με την πράξη της G.

Απο την άλλη πλευρά αν $\mathscr{R}$ είναι τυχούσα σχέση ισοδυναμίας επί του συνόλου G η οποία είναι συμβιβαστή με την πράξη της G, τότε το επόμενο βασικό Θεώρημα δείχνει ότι, αντίστροφα, το υποσύνολο

$$[e]_{\mathscr{R}}=\{x\in G\mid x\sim_{\mathscr{R}}e\}$$

είναι μια κανονική υποομάδα $H=[e]_{\mathscr{R}}$ η οποία επάγει την αρχική σχέση ισοδυναμίας $\mathscr{R}$ στην G, δηλαδή: $\mathscr{R}=\mathscr{R}_H$.

Ιδιαίτερα το επόμενο Θεώρημα δείχνει ότι υπάρχουν τόσες κανονικές υποομάδες σε μια ομάδα G όσες και οι σχέσεις ισοδυναμίας επί του συνόλου G οι οποίες είναι συμβιβαστές με την πράξη της ομάδας.

Θεώρημα 6.1.2. *Έστω ότι G είναι μια ομάδα, και έστω τα ακόλουθα σύνολα:*

$$\mathbf{R} = \{\mathscr{R} \subseteq G \times G \mid \eta\ \mathscr{R}\ \text{είναι σχέση ισοδυναμίας επί του}\ G\ \text{συμβιβαστή με την πράξη της}\ G\}$$

$$\mathbf{K} = \{H \subseteq G \mid \eta\ H\ \text{είναι κανονική υποομάδα της}\ G\}$$

Τότε οι απεικονίσεις

$$\Psi : \mathbf{R} \longrightarrow \mathbf{K}, \quad \Psi(\mathscr{R}) = [e]_{\mathscr{R}}$$

$$\Phi : \mathbf{K} \longrightarrow \mathbf{R}, \quad \Phi(H) = \mathscr{R}_H$$

είναι «1-1» και «επί» και επιπλέον: $\Psi = \Phi^{-1}$.

Απόδειξη. • Έχουμε ήδη αποδείξει ότι, αν H είναι μια κανονική υποομάδα της G, τότε η σχέση $\mathscr{R}_H$ είναι μια σχέση ισοδυναμίας επί του συνόλου G. Δηλαδή έχουμε δείξει ότι $\forall H \in \mathbf{K}$: $\Phi(H) = \mathscr{R}_H \in \mathbf{R}$. Επιπλέον θα δείξουμε ότι:

$$H = \Psi\Phi(H) \qquad \text{δηλαδή} \qquad H = [e]_{\mathscr{R}_H} = \{g \in G \mid g \sim_{\mathscr{R}_H} e\}$$

Πράγματι:

$$[e]_{\mathscr{R}_H} = \{g \in G \mid g \sim_{\mathscr{R}_H} e\} = \{g \in G \mid e \sim_{\mathscr{R}_H} g\} = \{g \in G \mid e^{-1}g \in H\} = \{g \in G \mid eg \in H\} = \{g \in G \mid g \in H\} = H$$

• Έστω $\mathscr{R} \in \mathbf{R}$, μια σχέση ισοδυναμίας επί του G η οποία είναι συμβιβαστή με την πράξη της G. Θα δείξουμε ότι:

$$\Psi(\mathscr{R}) = [e]_{\mathscr{R}} \in \mathbf{K} \qquad \text{και} \qquad \Phi\Psi(\mathscr{R}) = \mathscr{R}$$

Δηλαδή θα δείξουμε ότι:

$$[e]_{\mathscr{R}} = \{g \in G \mid g \sim_{\mathscr{R}} e\} \trianglelefteq G \qquad \text{και} \qquad \mathscr{R} = \mathscr{R}_{[e]_{\mathscr{R}}}$$

– Δείχνουμε πρώτα ότι το υποσύνολο $[e]_{\mathscr{R}}$ είναι υποομάδα της G. Προφανώς $[e]_{\mathscr{R}} \neq \emptyset$ διότι $e \in [e]_{\mathscr{R}}$ (επειδή η σχέση $\mathscr{R}$ είναι σχέση ισοδυναμίας επί του συνόλου G θα έχουμε $e \sim_{\mathscr{R}} e$). Έστω $g, g_1, g_2 \in [e]_{\mathscr{R}}$. Τότε, χρησιμοποιώντας ότι η σχέση ισοδυναμίας $\mathscr{R}$ είναι συμβιβαστή με την πράξη της G, θα έχουμε:

$$g_1 \sim_{\mathscr{R}} e \ \text{ και } \ g_2 \sim_{\mathscr{R}} e \quad \Longrightarrow \quad g_1 g_2 \sim_{\mathscr{R}} ee = e \quad \Longrightarrow \quad g_1 g_2 \in [e]_{\mathscr{R}}$$

$$g \sim_{\mathscr{R}} e \ \text{ και } \ g^{-1} \sim_{\mathscr{R}} g^{-1} \quad \Longrightarrow \quad gg^{-1} \sim_{\mathscr{R}} eg^{-1} = g^{-1} \quad \Longrightarrow \quad e \sim_{\mathscr{R}} g^{-1} \quad \Longrightarrow$$
$$\Longrightarrow \quad g^{-1} \sim_{\mathscr{R}} e \quad \Longrightarrow \quad g^{-1} \in [e]_{\mathscr{R}}$$

Οι τελευταίες σχέσεις δείχνουν ότι το υποσύνολο $[e]_{\mathscr{R}}$ είναι μια υποομάδα της G.

– Στη συνέχεια δείχνουμε ότι η υποομάδα $[e]_{\mathscr{R}}$ είναι κανονική: έστω $g \in G$ και $h \in [e]_{\mathscr{R}}$, δηλαδή $h \sim_{\mathscr{R}} e$. Επειδή η $\mathscr{R}$ είναι συμβιβαστή με την πράξη της ομάδας G, θα έχουμε:

$$g^{-1} \sim_{\mathscr{R}} g^{-1} \ \text{ και } \ h \sim_{\mathscr{R}} e \quad \Longrightarrow \quad g^{-1}h \sim_{\mathscr{R}} g^{-1}e \quad \Longrightarrow \quad g^{-1}h \sim_{\mathscr{R}} g^{-1}$$

παρόμοια

$$g^{-1}h \sim_{\mathscr{R}} g^{-1} \ \text{ και } \ g \sim_{\mathscr{R}} g \quad \Longrightarrow \quad g^{-1}hg \sim_{\mathscr{R}} g^{-1}g \quad \Longrightarrow \quad g^{-1}hg \sim_{\mathscr{R}} e \quad \Longrightarrow \quad g^{-1}hg \in [e]_{\mathscr{R}}$$

Η τελευταία σχέση δείχνει ότι η υποομάδα $[e]_{\mathscr{R}}$ της G είναι κανονική.

– Τέλος, δείχνουμε ότι $\mathscr{R} = \mathscr{R}_{[e]_{\mathscr{R}}}$. Θα έχουμε $\forall g_1, g_2 \in G$:

$$g_1 \sim_{\mathscr{R}_{[e]_{\mathscr{R}}}} g_2 \iff g^{-1}g_2 \in [e]_{\mathscr{R}} \iff g^{-1}g_2 \sim_{\mathscr{R}} e$$

Επομένως, αν ισχύει η τελευταία σχέση, επειδή η $\mathscr{R}$ είναι συμβιβαστή με την πράξη της ομάδας, θα έχουμε:

$$g_1 \sim_{\mathscr{R}} g_1 \ \text{ και } \ g^{-1}g_2 \sim_{\mathscr{R}} e \quad \Longrightarrow \quad g_1 g^{-1} g_2 \sim_{\mathscr{R}} g_1 e \quad \Longrightarrow \quad eg_2 \sim_{\mathscr{R}} g_1 \quad \Longrightarrow \quad g_2 \sim_{\mathscr{R}} g_1 \quad \Longrightarrow \quad g_1 \sim_{\mathscr{R}} g_2$$

Δηλαδή:

$$\forall g_1, g_2 \in G: \ g_1 \sim_{\mathscr{R}_{[e]_{\mathscr{R}}}} g_2 \quad \Longrightarrow \quad g_1 \sim_{\mathscr{R}} g_2 \qquad \text{και επομένως:} \qquad \mathscr{R}_{[e]_{\mathscr{R}}} \subseteq \mathscr{R} \qquad (*)$$

Αντίστροφα, αν $g_1 \sim_{\mathscr{R}} g_2$, τότε χρησιμοποιώντας ότι η $\mathscr{R}$ είναι συμβιβαστή με την πράξη της G θα έχουμε:

$$g_1^{-1} \sim_{\mathscr{R}} g_1^{-1} \quad \text{και} \quad g_1 \sim_{\mathscr{R}} g_2 \implies g_1^{-1} g_1 \sim_{\mathscr{R}} g_1^{-1} g_2 \implies e \sim_{\mathscr{R}} g^{-1} g_2 \implies$$
$$\implies g^{-1} g_2 \sim_{\mathscr{R}} e \implies g^{-1} g_2 \in [e]_{\mathscr{R}}$$

Αυτό όμως σημαίνει ότι:

$$g_1 \sim_{\mathscr{R}_{[e]_{\mathscr{R}}}} g_2$$

Άρα θα έχουμε

$$\forall g_1, g_2 \in G: \ g_1 \sim_{\mathscr{R}} g_2 \implies g_1 \sim_{\mathscr{R}_{[e]_{\mathscr{R}}}} g_2 \qquad \text{και επομένως:} \qquad \mathscr{R} \subseteq \mathscr{R}_{[e]_{\mathscr{R}}} \qquad (**)$$

Από τις σχέσεις $(*)$ και $(**)$ θα έχουμε ότι $\mathscr{R} \subseteq \mathscr{R}_{[e]_{\mathscr{R}}}$. Έτσι $\mathscr{R} = \mathscr{R}_{[e]_{\mathscr{R}}}$ και συνεπώς: $\Phi\Psi(\mathscr{R}) = \mathscr{R}$. ■

6.1.2 Τρία Χαρακτηριστικά (Αντι-)Παραδείγματα

Στην παρούσα υποενότητα θα δούμε ότι υπάρχουν μη αβελιανές ομάδες με την ιδιότητα ότι όλες οι υποομάδες τους είναι κανονικές. Επίσης θα δούμε ότι, γενικά, η σχέση κανονικότητας στο σύνολο των υποομάδων μιας ομάδας δεν ικανοποιεί την μεταβατική ιδιότητα.

1. Έχουμε δει ότι όλες οι υποομάδες μιας αβελιανής ομάδας είναι κανονικές. Το αντίστροφο δεν ισχύει:

«Υπάρχει μια μη αβελιανή ομάδα Q τάξης 8 όλες οι υποομάδες της οποίας είναι κανονικές.»

Πράγματι θεωρούμε την ομάδα Q των τετρανίων του Hamilton:

$$Q = \left\{ \pm I_2, \ \pm I, \ \pm J, \ \pm K \right\}$$

όπου

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Όπως γνωρίζουμε από το Παράδειγμα 2.4.20, η ομάδα Q είναι μια μη-αβελιανή ομάδα τάξης 8, και

$$Q \leq \mathsf{SL}_2(\mathbb{C}) \leq \mathsf{GL}_2(\mathbb{C})$$

Τα στοιχεία $\pm I, \pm J, \pm K$ έχουν τάξη 4, και το στοιχείο $-I_2$ έχει τάξη 2.

Θα δειξουμε ότι **όλες οι υποομάδες της Q είναι κανονικές**.

Έστω H μια υποομάδα της Q. Τότε έχουμε τις ακόλουθες περιπτώσεις:

1. $\mathsf{o}(H) = 1$. Τότε $H = \{I_2\}$ η οποία προφανώς είναι κανονική υπομάδα της Q.
2. $\mathsf{o}(H) = 8$. Τότε $H = Q$ η οποία προφανώς είναι κανονική υπομάδα της Q.
3. $\mathsf{o}(H) = 4$. Τότε $[Q : H] = 2$ και άρα από την Πρόταση 3.4.13 η H είναι κανονική υπομάδα της Q.
4. $\mathsf{o}(H) = 2$. Τότε η H είναι μια κυκλική υποομάδα τάξης 2 της Q. Επομένως θα είναι της μορφής:

$$H = \{I_2, X\} \qquad \text{όπου} \qquad X^2 = I_2$$

Όμως εύκολα βλέπουμε, με χρήση των σχέσεων $I^2 = J^2 = K^2 = IJK = -I_2$, ότι το μόνο στοιχείο τάξης 2 της Q είναι το στοιχείο

$$-I_2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

Έτσι $H = \{I_2, -I_2\}$ και τότε, $\forall X \in Q$:

$$X^{-1}(-I_2)X = -(X^{-1} I_2 X) = -I_2 \in H \qquad \text{και} \qquad X^{-1} I_2 X = X^{-1} I_2 X = I_2 \in H$$

Άρα $\forall X \in Q$: $X^{-1} H X \subseteq H$, και επομένως η H είναι κανονική υπομάδα της Q.[1]

[1] Προκύπτει εύκολα ότι η υποομάδα H συμπίπτει με το κέντρο $\mathsf{Z}(Q)$ και άρα είναι κανονική υποομάδα της Q.

Μια ομάδα G καλείται **ομάδα Hamilton** αν η G δεν είναι αβελιανή και κάθε υποομάδα της G είναι κανονική. Η ομάδα τετρανίων Q είναι η μικρότερη ομάδα Hamilton.

Παρατήρηση 6.1.3. Με χρήση περισσότερο προχωρημένων εργαλείων από όσα μπορούμε να αναπτύξουμε εδώ, αποδεικνύεται[2] ότι για μια ομάδα G τα ακόλουθα είναι ισοδύναμα, για μια απόδειξη βλέπε το βιβλίο [32]:

1. Η ομάδα είναι ομάδα Hamilton.
2. Η G είναι ισόμορφη με την ομάδα ευθύ γινόμενο

$$Q \times \mathbb{Z}_2^r \times H$$

όπου Q είναι η ομάδα τετρανίων, $\mathbb{Z}_2^r$ είναι η ομάδα ευθύ γινόμενο $\mathbb{Z}_2^r = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2$ (r παράγοντες), και H είναι μια αβελιανή ομάδα κάθε στοιχείο της οποίας έχει περιττή τάξη.

Επομένως η δομή όλων των ομάδων Hamilton είναι γνωστή. ▲

2. Θα δούμε ότι η ιδιότητα του να είναι η κανονικότητα υποομάδων μιας ομάδας μεταβατική ιδιότητα δεν ισχύει γενικά.

Παράδειγμα 6.1.4. Υπάρχει μια ομάδα G και υποομάδες H και K της G, έτσι ώστε:

1. $H \leq K \leq G$.
2. Η υποομάδα H **είναι** κανονική υποομάδα της K: $H \trianglelefteq K$.
3. Η υποομάδα K **είναι** κανονική υποομάδα της G: $K \trianglelefteq G$.
4. Η υποομάδα H **δεν είναι** κανονική υποομάδα της G: $H \not\trianglelefteq G$.

Θέτουμε:

1. $G = \mathsf{S}_4$.
2. $K = \{(1),\ (12)(34),\ (13)(24),\ (23)(41)\}$.
3. $H = \langle (12)(34) \rangle = \{(1), (12)(34)\}$.

Τότε προφανώς θα έχουμε $H \subseteq K \subseteq G$ και η H **είναι κανονική υποομάδα** της K διότι είναι δείκτη $[K : H] = 2$.
Επίσης η K **είναι κανονική υποομάδα** της S_4, διότι, όπως μπορούμε να δούμε εύκολα:

$$\forall \sigma \in \mathsf{S}_4 : \ \sigma^{-1}(12)(34)\sigma \in K, \quad \sigma^{-1}(13)(24)\sigma \in K, \quad \sigma^{-1}(23)(41)\sigma \in K$$

Όμως η H **δεν είναι κανονική** στην S_4, διότι:

$$\text{αν } \ \sigma = (123) \quad \text{τότε:} \quad \sigma^{-1}(12)(34)\sigma = (321)\,(12)(34)\,(123) = (13)(24) \notin H$$

3. Η ομάδα G με την μικρότερη δυνατή τάξη για την οποία $H \trianglelefteq K \trianglelefteq G$, αλλά η H δεν είναι κανονική υποομάδα της G, είναι η διεδρική ομάδα D_4 τάξης 8:

[2] Το αποτέλεσμα αυτό οφείλεται στον:
Reinhold Baer (22 Ιουλίου 1902 - 22 Οκτωβρίου 1979) [https://en.wikipedia.org/wiki/Reinhold_Baer]: Γερμανός μαθηματικός με σημαντική συμβολή στην Άλγεβρα. Εισήγαγε την έννοια του ενριπτικού προτύπου (injective module) και απέδειξε βασικά αποτελέσματα που τα αφορούν. Είναι επίσης γνωστός για τις έννοιες των δακτυλίων και ομάδων που φέρουν το όνομά του.

Παράδειγμα 6.1.5. Θεωρούμε τους αντιστρέψιμους πίνακες πραγματικών αριθμών (στοιχεία της πολλαπλασιαστικής ομάδας $\mathsf{GL}(2,\mathbb{R})$ των αντιστρέψιμων 2×2 πινάκων πραγματικών αριθμών):

$$A=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad \text{και} \qquad B=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

Εύκολα βλέπουμε ότι:

$$A^2=I_2, \quad B^4=I_2, \quad AB=B^{-1}A \tag{$*$}$$

Επίσης εύκολα βλέπουμε ότι τα στοιχεία του συνόλου

$$\mathsf{D}_4=\left\{I_2,\ A,\ B,\ B^2,\ B^3,\ AB,\ AB^2,\ AB^3\right\}$$

είναι διακεκριμένα. Χρησιμοποιώντας τις σχέσεις $(*)$, βλέπουμε ότι το σύνολο D_4 είναι κλειστό στην πράξη του πολλαπλασιασμού πινάκων, και άρα το σύνολο D_4 είναι μια υποομάδα τάξης 8 της (άπειρης) ομάδας $\mathsf{GL}(2,\mathbb{R})$ η οποία είναι ισόμορφη με την τέταρτη διεδρική ομάδα D_4, βλέπε 2.2.

Η ομάδα D_4 **δεν είναι αβελιανή** διότι:

$$AB=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\neq\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=BA$$

Θέτουμε:

1. $G=\mathsf{D}_4$.
2. $K=\left\{I_2,\ A,\ B^2,\ AB^2\right\}$.
3. $H=\left\langle AB^2\right\rangle=\left\{I_2, AB^2\right\}$.

Τότε προφανώς θα έχουμε $H\subseteq K\subseteq G$ και η H **είναι κανονική υποομάδα** της K και η K **είναι κανονική υποομάδα** της G (ως υποομάδες δείκτη 2).

Όμως η H **δεν είναι κανονική υποομάδα** της G. Πραγματικά, επειδή $A^2=I_4$, θα έχουμε $A=A^{-1}$, και τότε από την $(*)$, θα έχουμε:

$$(AB)^{-1}AB^2AB=B^{-1}A^{-1}AB^2AB=B^{-1}I_2B^2AB=BAB=BB^{-1}A=A\notin H \quad \surd$$

Παρατήρηση 6.1.6. Στα παραπάνω παραδείγματα είδαμε δύο μη αβελιανές ομάδες τάξης 8, την ομάδα των τετρανίων Q και την διεδρική ομάδα D_4. Παρατηρούμε ότι:

1. Η Q περιέχει ακριβώς ένα στοιχείο τάξης 2. Τον πίνακα
$$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$
2. Η D_4 περιέχει τουλάχιστον δύο στοιχεία τάξης 2. Τα εξής:
$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad \text{και} \qquad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$$

Επομένως:

Οι (μη αβελιανές) ομάδες Q και D_4 τάξης 8 δεν είναι ισόμορφες ▲

Παρατήρηση 6.1.7. Αποδεικνύεται ότι, με ακρίβεια ισομορφισμού, οι μόνες (ανά δύο μη ισόμορφες) ομάδες τάξης 8 είναι οι εξής:

$$\text{Αβελιανές:}\quad \mathbb{Z}_8, \qquad \mathbb{Z}_4\times\mathbb{Z}_2, \qquad \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$
$$\text{Μη Αβελιανές:}\quad Q, \qquad \mathsf{D}_4$$

Βλέπε το Παράδειγμα 4.1.24. ▲

6.1.3 Η Ομάδα Πηλίκο

Έστω $(G,\cdot)$ μια ομάδα και $H \trianglelefteq G$ μια κανονική υποομάδα της G. Τότε, όπως είδαμε, η σχέση ισοδυναμίας $\mathscr{R}_H$ είναι συμβιβαστή με την πράξη της ομάδας G, και επομένως απο την Πρόταση 1.3.37 έπεται ότι το σύνολο πηλίκο

$$G/H = G/\mathscr{R}_H = \{[x]_H \subseteq G \mid x \in G\} = \{xH \subseteq G \mid x \in G\}$$

είναι εφοδιασμένο με την επαγόμενη πράξη

$$\cdot : G/H \times G/H \longrightarrow G/H, \qquad ([x]_H, [y]_H) := [x]_H \cdot [y]_H = [xy]_H$$

δηλαδή

$$\cdot : G/H \times G/H \longrightarrow G/H, \qquad xH \cdot yH := (xy)H$$

Πρόταση 6.1.8. *Έστω ότι $H \trianglelefteq G$ είναι μια κανονική υποομάδα μιας ομάδας G. Τότε:*

1. *Το σύνολο πηλίκο G/H αποτελεί ομάδα με πράξη:*

$$xH \cdot yH := (xy)H$$

Το ουδέτερο στοιχείο της ομάδας G/H είναι το σύμπλοκο $eH = H$ και το αντίστροφο του στοιχείου xH είναι το σύμπλοκο $x^{-1}H$:

$$e_{G/H} = e_G H = H \qquad \text{και} \qquad (xH)^{-1} = x^{-1}H$$

Η ομάδα G/H καλείται η **ομάδα πηλίκο** *της G ως προς την κανονική υποομάδα H.*

2. *Αν η ομάδα G είναι αβελιανή, τότε και η ομάδα πηλίκο G/H είναι αβελιανή.*

3. *Αν η ομάδα G είναι πεπερασμένη, τότε και η ομάδα πηλίκο G/H είναι πεπερασμένη και ισχύει:*

$$o(G/H) = \frac{o(G)}{o(H)} = [G : H]$$

Απόδειξη. Η απόδειξη προκύπτει άμεσα από τις παραπάνω παρατηρήσεις σε συνδυασμό με την Πρόταση 1.3.37. ■

Παρατήρηση 6.1.9. Έστω ότι H είναι μια κανονική υποομάδα μιας ομάδας G.
Ως άμεση συνέπεια της Πρότασης 6.1.8, θα έχουμε τα ακόλουθα:

1.
$$\forall x_1H, x_2H \cdots, x_nH \in G/H: \qquad x_1Hx_2H \cdots x_nH = (x_1x_2 \cdots x_n)H$$

2.
$$\forall k \in \mathbb{Z}, \quad \forall xH \in G/H: \qquad (xH)^k = x^kH$$

3. Αν $g \in G$ είναι ένα στοιχείο πεπερασμένης τάξης. Τότε:

$$o(gH) \mid o(g)$$

Πράγματι, αν $o(g) = n$, τότε $g^n = e$ και θα έχουμε: $(gH)^n = g^nH = eH = H$. Επομένως $o(gH) \mid n$. ▲

Γνωρίζουμε ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική. Το ακόλουθο αποτέλεσμα πιστοποιεί ότι κάθε ομάδα πηλίκο μιας κυκλικής ομάδας είναι επίσης κυκλική ομάδα. Σημειώνουμε ότι επειδή κάθε κυκλική ομάδα είναι αβελιανή, έπεται ότι κάθε υποομάδα H μιας κυκλικής ομάδας G είναι κανονική και επομένως ορίζεται η ομάδα πηλίκο G/H.

Πρόταση 6.1.10. *Έστω ότι G είναι μια κυκλική ομάδα. Τότε για κάθε υποομάδα H της G η ομάδα πηλίκο G/H είναι κυκλική.*

Απόδειξη. Έστω $G = \langle g \rangle$. Θα δείξουμε ότι

$$G/H = \langle gH \rangle$$

Έστω xH ένα τυχόν στοιχείο της G/H. Τότε $x \in G = \langle g \rangle$ και άρα $x = g^k$ για κάποιο $k \in \mathbb{Z}$. Τότε όμως θα έχουμε:

$$xH = g^k H = (gH)k \implies xH \in \langle gH \rangle$$

Επομένως $G/H = \langle gH \rangle$ και η G/H είναι κυκλική. ■

Γενικότερα ισχύει η ακόλουθη Πρόταση:

Πρόταση 6.1.11. *Έστω $H \trianglelefteq G$ μια κανονική υποομάδα μιας ομάδας $(G, \cdot)$. Αν η ομάδα G είναι πεπερασμένα παραγόμενη, τότε η ομάδα πηλίκο G/H είναι πεπερασμένα παραγόμενη.*

Απόδειξη. Επειδή η G είναι πεπερασμένα παραγόμενη, έπεται ότι η G περιέχει ένα πεπερασμένο σύνολο γεννητόρων $S = \{s_1, s_2, \cdots, s_k\} \subseteq G$. Τότε το σύνολο $S \cdot H = \{sH \in G/H \mid s \in S\}$ είναι ένα σύνολο γεννητόρων της ομάδας πηλίκου G/H. Πράγματι, αν $xH \in G/H$ είναι ένα τυχόν στοιχείο της G/H, τότε, επειδή το S είναι σύνολο γεννητόρων θα έχουμε $x = s_1^{n_1} \cdot s_2^{n_2} \cdots s_k^{n_k}$, για κάποιους ακέραιους $n_1, n_2, \cdots, n_k$. Τότε θα έχουμε

$$xH = (s_1^{n_1} \cdot s_2^{n_2} \cdots s_k^{n_k})H = (s_1^{n_1} H) \cdot (s_2^{n_2} H) \cdots (s_k^{n_k} H) = (s_1 H)^{n_1} \cdot (s_2 H)^{n_2} \cdots (s_k H)^{n_k}$$

Επομένως το σύνολο $S \cdot H = \{s_1 H, s_2 H, \cdots, s_k H\}$ είναι ένα σύνολο γεννητόρων της G/H και, επειδή το σύνολο SH είναι προφανώς πεπερασμένο, έπεται ότι η ομάδα πηλίκο G/H είναι πεπερασμένα παραγόμενη. ■

Από την Πρόταση 6.1.8 έπεται ότι η ομάδα πηλίκο μιας αβελιανής ομάδας ως προς τυχούσα υποομάδα (η οποία είναι πάντα κανονική) είναι αβελιανή. Το αντίστροφο δεν ισχύει. Δηλαδή υπάρχει μη αβελιανή ομάδα G και μια αβελιανή κανονική υποομάδα H της G με την ιδιότητα η ομάδα πηλίκο G/H είναι αβελιανή:

Παράδειγμα 6.1.12. Θεωρούμε τη συμμετρική ομάδα S_3 η οποία είναι μια μη αβελιανή ομάδα τάξης 6, και έστω $H = \langle (123) \rangle$ η κυκλική υποομάδα της S_3 η οποία παράγεται από τον 3-κύκλο (123). Τότε η H είναι μια αβελιανή ομάδα τάξης 3 και άρα είναι δείκτη 2 στην S_3. Επομένως $H \trianglelefteq S_3$, και τότε η ομάδα πηλίκο S_3/H έχει τάξη 2, και άρα είναι αβελιανή διότι όλες οι ομάδες τάξης ≤ 5 είναι αβελιανές. √

Από την Πρόταση 6.1.8 έπεται ότι η ομάδα πηλίκο μιας κυκλικής ομάδας ως προς τυχούσα υποομάδα (η οποία είναι πάντα κανονική) είναι κυκλική. Το παραπάνω παράδειγμα δείχνει ότι το αντίστροφο δεν ισχύει. Δηλαδή υπάρχει μη κυκλική ομάδα G, στο παράδειγμα η S_3, και μια (κυκλική) κανονική υποομάδα H της G, στο παράδειγμα η $H = \langle (123) \rangle$, με την ιδιότητα η ομάδα πηλίκο G/H να είναι κυκλική.

Η επόμενη Προταση χαρακτηρίζει πότε μια σημαντική ομάδα πηλίκο είναι κυκλική. Υπενθυμίζουμε ότι το κέντρο $Z(G)$ είναι πάντα κανονική υποομάδα μιας ομάδας G και άρα ορίζεται πάντα η ομάδα πηλίκο $G/Z(G)$.

Πρόταση 6.1.13. *Αν G είναι μια ομάδα, τότε:*

$$\textit{η ομάδα πηλίκο } G/Z(G) \textit{ είναι κυκλική} \iff \textit{η ομάδα } G \textit{ είναι αβελιανή} \quad (\textit{και τότε } G = Z(G))$$

Απόδειξη. Αν η ομάδα G είναι αβελιανή, τότε θα έχουμε $G = Z(G)$. Έτσι η ομάδα πηλίκο $G/Z(G)$ θα είναι η τετριμμένη, και ιδιαίτερα θα είναι κυκλική.

Αντίστροφα, υποθέτουμε ότι η ομάδα πηλίκο $G/Z(G)$ είναι κυκλική με γεννήτορα την πλευρική κλάση $gZ(G)$:

$$G/Z(G) = \langle gZ(G) \rangle$$

Τότε για κάθε στοιχείο $x \in G$, θα έχουμε $xZ(G) \in \langle gZ(G) \rangle$ και άρα $xZ(G) = (gZ(G))^n = g^n Z(G)$. Τότε όμως $x(g^n)^{-1} \in Z(G)$, δηλαδή $xg^{-n} = z_x$, για κάποιο $z_x \in Z(G)$. Επομένως, για κάθε στοιχείο $x \in G$, υπάρχει ακέραιος $n \in \mathbb{Z}$ και στοιχείο $z_x \in Z(G)$, έτσι ώστε: $x = g^n z_x$. Έτσι, αν y είναι ένα άλλο στοιχείο της G, τότε θα έχουμε $y = g^m z_y$, όπου $m \in \mathbb{Z}$ και $z_y \in Z(G)$. Τότε, εκμεταλευόμενοι ότι τα στοιχεία z_x και z_y μετατίθενται με όλα τα στοιχεία της G, θα έχουμε:

$$xy = g^n z_x g^m z_y = g^n g^m z_x z_y = g^{n+m} z_x z_y \quad \text{και} \quad yx = g^m z_y g^n z_x = g^m g^n z_y z_x = g^{m+n} z_y z_x = g^{n+m} z_x z_y$$

Άρα $xy = yx$, $\forall x, y \in G$ και επομένως η ομάδα G είναι αβελιανή. Προφανώς τότε $G = Z(G)$. ■

Παρατήρηση 6.1.14. Η απόδειξη της Πρότασης 6.1.13 δείχνει γενικότερα ότι, αν $N \leq \mathsf{Z}(G)$ είναι μια υποομάδα της G η οποία περιέχεται στο κέντρο της G, οπότε η υποομάδα N είναι κανονική υποομάδα της G, τότε: *η ομάδα πηλίκο G/N είναι κυκλική αν και μόνο αν η G είναι αβελιανή.* ▲

6.1.4 Το Θεώρημα του Cauchy για Αβελιανές Ομάδες

Το Θεώρημα του Cauchy πιστοποιεί ότι, αν ένας πρώτος διαιρεί την τάξη μιας ομάδας, τότε η ομάδα περιέχει ένα στοιχείο με τάξη τον πρώτο αριθμό. Εδώ θα αποδείξουμε το Θεώρημα του Cauchy για αβελιανές ομάδες.

Θεώρημα 6.1.15 (Θεώρημα Cauchy για αβελιανές ομάδες)**.** *Έστω G μια πεπερασμένη αβελιανή ομάδα τάξης > 1 και p ένας πρώτος διαιρέτης της τάξης $\mathsf{o}(G)$ της ομάδας. Τότε η G έχει (τουλάχιστον) ένα στοιχείο τάξης p.*

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στην τάξη $\mathsf{o}(G) = n \geq 2$ της ομάδας.

1. Αν $\mathsf{o}(G) = 2$, τότε προφανώς κάθε στοιχείο της G εκτός του ταυτοτικού έχει τάξη 2 και το Θεώρημα ισχύει κατά τετριμμένο τρόπο.

2. Επαγωγικη Υποθεση: Υποθέτουμε ότι, για κάθε πεπερασμένη αβελιανή ομάδα K τάξης $< \mathsf{o}(G)$ και για κάθε πρώτο διαιρέτη p της τάξης της ομάδας K, η K έχει (τουλάχιστον) ένα στοιχείο τάξης p.

3. Υποθέτουμε ότι η τάξη της G είναι $n \geq 3$.

   (α') Αν οι μόνες υποομάδες της G είναι η τετριμμένη $\{e\}$ και η ίδια η G, τότε, όπως γνωρίζουμε, η G είναι κυκλική με τάξη έναν πρώτο αριθμό, οποίος αναγκαστικά είναι ο πρώτος διαιρέτης p. Τότε ο γεννήτορας της G έχει προφανώς τάξη p, και άρα η G έχει ένα στοιχείο τάξης p.

   (β') Υποθέτουμε ότι η G έχει μια μη τετριμμένη γνήσια υποομάδα N. Διακρίνουμε περιπτώσεις:

   i. $p \mid \mathsf{o}(N)$.
   Τότε, επειδή $G \neq N \neq \{e\}$, έπεται ότι $\mathsf{o}(N) < \mathsf{o}(G)$. Επειδή η N είναι αβελιανή ως υποομάδα αβελιανής ομάδας, από την Επαγωγική Υπόθεση έπεται ότι η N έχει ένα στοιχείο τάξης p. Τότε όμως και η G έχει ένα στοιχείο τάξης p.

   ii. $p \nmid \mathsf{o}(N)$.
   Επειδή η G είναι αβελιανή, η υποομάδα N είναι κανονική υποομάδα της G. Επομένως ορίζεται η ομάδα πηλίκο G/N, η οποία όπως γνωρίζουμε είναι αβελιανή. Επιπλέον η τάξη της είναι
   $$1 \;<\; \mathsf{o}(G/N) = \frac{\mathsf{o}(G)}{\mathsf{o}(N)} \;<\; \mathsf{o}(G)$$
   διότι, αν $\mathsf{o}(G/N) = 1$, τότε $\mathsf{o}(G) = \mathsf{o}(N)$ από όπου $G = N$, το οποίο είναι άτοπο, και $\frac{\mathsf{o}(G)}{\mathsf{o}(N)} = \mathsf{o}(G)$, τότε $\mathsf{o}(N) = 1$ από όπου $N = \{e\}$, το οποίο είναι άτοπο. Επειδή ο αριθμός p είναι πρώτος, θα έχουμε:
   $$p \mid \mathsf{o}(G) = \frac{\mathsf{o}(G)}{\mathsf{o}(N)} \cdot \mathsf{o}(N) \quad \text{και} \quad p \nmid \mathsf{o}(N) \quad \Longrightarrow \quad p \mid \frac{\mathsf{o}(G)}{\mathsf{o}(N)} = \mathsf{o}(G/N)$$
   Επειδή η ομάδα πηλίκο G/N είναι αβελιανή και $p \mid \mathsf{o}(G/N) < \mathsf{o}(G)$, από την Επαγωγική Υπόθεση, έπεται ότι η ομάδα G/N) έχει ένα στοιχείο xN τάξης p, και ιδιαίτερα $(xN)^p = N$. Επομένως υπάρχει ένα στοιχείο $e \neq x \in G$: $x^p \in N$. Έστω $m = \mathsf{o}(N)$. Τότε
   $$(x^p)^m = (x^m)^p = e^p = e$$
   Θέτουμε $y = x^m$. Τότε $y^p = e$, και άρα $\mathsf{o}(y) \mid p$. Επειδή p είναι πρώτος, είτε $\mathsf{o}(y) = 1$ ή $\mathsf{o}(y) = p$. Όμως, αν $\mathsf{o}(y) = 1$, τότε $y = x^m = e$ και άρα $(xN)^m = N$, το οποίο σημαίνει ότι $p = \mathsf{o}(xN) \mid m = \mathsf{o}(N)$. Αυτό όμως είναι άτοπο διότι $p \nmid \mathsf{o}(N)$. Επομένως $\mathsf{o}(y) = p$, και άρα η G έχει ένα στοιχείο τάξης p. ■

6.2 Στοιχειώδεις Ιδιότητες Ομομορφισμών

Στην παρούσα ενότητα, αφού υπενθυμίσουμε κάποιες από τις βασικές ιδιότητες ομομορφισμών ομάδων, θα αναλύσουμε εν συντομία την αλληλεπίδραση μεταξύ ομομορφισμών ομάδων και υποομάδων μιας ομάδας.

Υπενθυμίζουμε ότι μια απεικόνιση $f: G \longrightarrow G'$ μεταξύ ομάδων $(G,\cdot)$ και $(G',\cdot)$ καλείται **ομομορφισμός ομάδων** αν:

$$\forall x, y \in G: \quad f(xy) = f(x)f(y)$$

Ένας **ενδομορφισμός** της ομάδας G είναι ένας ομομορφισμός ομάδων $f: G \longrightarrow G$. Σημειώνουμε ότι, χάριν ευκολίας του συμβολισμού, συμβολίζουμε με το ίδιο σύμβολο την πράξη στις ομάδες G και G'. Γενικά, αν «$\star$» είναι η πράξη της G και «$\circ$» η πράξη της G', τότε η παραπάνω σχέση γράφεται: $f(x \star y) = f(x) \circ f(y)$. Επίσης σημειώνουμε ότι για κάθε ομάδα G, η ταυτοτική απεικόνιση $\mathrm{Id}_G: G \longrightarrow G$, $\mathrm{Id}_G(x) = x$, είναι ένας ενδομορφισμός της G, ο οποίος καλείται ο **ταυτοτικός ενδομορφισμός** της G, και, αν G, G' είναι ομάδες, τότε η απεικόνιση $f: G \longrightarrow G'$, $f(x) = e_{G'}$, $\forall x \in G$, είναι προφανώς ένας ομομορφισμός, ο οποίος καλείται ο **τετριμμένος ομομορφισμός** (από την G στην G').

Οι στοιχειώδεις ιδιότητες τις οποίες ικανοποιεί ένας ομομορφισμός ομάδων περιγράφονται στην ακόλουθη Πρόταση.

Πρόταση 6.2.1. *(Πρόταση 2.8.8). Έστω $(G,\cdot)$ και $(G',\cdot)$ δύο ομάδες.*

1. *Έστω ότι $f: G \longrightarrow G'$ είναι ένας ομομορφισμός ομάδων. Τότε:*
   - *(α΄)* $f(e_G) = e_{G'}$.
   - *(β΄)* $\forall a \in G_1$: $f(a^{-1}) = f(a)^{-1}$.
   - *(γ΄)* *Αν* $a_1, \cdots, a_n \in G$, $n \geq 1$, *τότε:* $f(a_1 \cdot \cdots \cdot a_n) = f(a_1) \cdot \cdots \cdot f(a_n)$.
   - *(δ)* $\forall a \in G_1$, $\forall n \in \mathbb{Z}$: $f(a^n) = f(a)^n$.
2. *Η σύνθεση ομομορφισμών (ισομορφισμών) ομάδων ομάδων είναι (ομομορφισμός) ισομορφισμός ομάδων.*
3. *(α΄) Αν ο ομομορφισμός ομάδων $f: G \longrightarrow G'$ είναι ισομορφισμός, τότε η αντίστροφη απεικόνιση $f^{-1}: G' \longrightarrow G$ είναι ισομορφισμός ομάδων.*
   (β΄) Ένας ομομορφισμός ομάδων $f: G, \star) \longrightarrow G'$ είναι ισομορφισμός αν και μόνο αν υπάρχει ομομορφισμός ομάδων $g: G' \longrightarrow G$, (και τότε $g = f^{-1}$), έτσι ώστε:

$$f \circ g = \mathrm{Id}_{G'} \quad \text{και} \quad g \circ f = \mathrm{Id}_G \quad \blacksquare$$

Θα δούμε τώρα ότι ομομορφισμοί ομάδων συμπεριφέρονται ομαλά ως προς τις υποομάδες.

Πρόταση 6.2.2. *Έστω $f: G \longrightarrow G'$ ένας ομομορφισμός ομάδων.*

1. *Για κάθε υποομάδα H της G, το σύνολο $f(H)$ είναι υποομάδα της G':*

$$H \leq G \implies f(H) \leq G'$$

2. *Για κάθε υποομάδα K της G', το σύνολο $f^{-1}(K)$ είναι υποομάδα της G:*

$$K \leq G' \implies f^{-1}(K) \leq G$$

Απόδειξη. 1. Επειδή $H \leq G$, θα έχουμε ότι $e_G \in H$ και άρα από την Πρόταση 2.8.8 θα έχουμε $e_{G'} = f(e_G) \in f(H)$. Έστω $z, w \in f(H)$. Τότε $z = f(x)$ και $w = f(y)$, όπου $x, y \in H$. Επειδή $H \leq G$, θα έχουμε: $xy^{-1} \in H$, και άρα χρησιμοποιώντας την Πρόταση 2.8.8 θα έχουμε:

$$xy^{-1} \in H \implies f(xy^{-1}) \in f(H) \implies f(x)f(y^{-1}) \in f(H) \implies f(x)f(y)^{-1} \in f(H) \implies zw^{-1} \in H$$

Επομένως το υποσύνολο $f(H)$ είναι υποομάδα της G'.

2. Επειδή $K \leq G'$, έπεται ότι $e_{G'} \in K$ και άρα επειδή $e_{G'} = f(e_G)$, θα έχουμε ότι $e_G \in f^{-1}(K)$. Έστω $z, w \in f^{-1}(K)$. Τότε $f(z) \in K$ και $f(w) \in K$. Επειδή $K \leq G'$, θα έχουμε $f(z)f(w)^{-1} \in K$. Όμως από την Πρόταση 2.8.8 θα έχουμε:

$$K \ni f(z)f(w)^{-1} = f(z)f(w^{-1}) = f(zw^{-1}) \implies zw^{-1} \in f^{-1}(K)$$

Επομένως το υποσύνολο $f^{-1}(K)$ είναι υποομάδα της G. ■

Επειδή κάθε ομάδα H έχει τουλάχιστον δύο υποομάδες: την τετριμμένη $\{e_H\}$ και την ίδια την ομάδα H, κάθε ομομορφισμός ομάδων $f: G \longrightarrow G'$ ορίζει δύο υποομάδες: την $f^{-1}(\{e_{G'}\}) \leq G$ και την $f(G) \leq G'$. Έτσι οδηγούμαστε στον ακόλουθο ορισμό.

Ορισμός 6.2.3. *Έστω $f: G \longrightarrow G'$ ένας ομομορφισμός ομάδων.*

1. *Ο* **πυρήνας του** *f είναι το υποσύνολο του συνόλου G το οποίο ορίζεται ως:*

$$\mathsf{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\}$$

2. *Η* **εικόνα του** *f είναι το υποσύνολο του συνόλου G' το οποίο ορίζεται ως:*

$$\mathsf{Im}(f) = \{f(x) \in G' \mid x \in G\}$$

Η επόμενη Πρόταση δείχνει ιδιαίτερα ότι ο πυρήνας ενός ομομορφισμού ομάδων είναι κανονική υποομάδα, και επίσης δίνει χαρακτηρισμούς μονομορφισμών, επιμορφισμών και ισομορφισμών.

Πόρισμα 6.2.4. *Έστω $f: G \longrightarrow G'$ ένας ομομορφισμός ομάδων.*

1. *Ο πυρήνας $\mathsf{Ker}(f)$ του f είναι μια κανονική υποομάδα της G.*

   Επιπλέον ο f είναι μονομορφισμός αν και μόνο αν $\mathsf{Ker}(f) = \{e_G\}$.

2. *Η εικόνα $\mathsf{Im}(f)$ του f είναι μια υποομάδα της G.*

   Επιπλέον ο f είναι επιμορφισμός αν και μόνο αν $\mathsf{Im}(f) = G'$.

Απόδειξη. 1. Επειδή

$$\mathsf{Ker}(f) = \{x \in G \mid f(x) = e_{G'}\} = f^{-1}(\{e_{G'}\})$$

από την Πρόταση 6.2.2 έπεται ότι ο πυρήνας $\mathsf{Ker}(f)$ είναι υποομάδα της G.

Έστω $x \in G$ και $h \in \mathsf{Ker}(f)$. Τότε

$$f(x \cdot h \cdot x^{-1}) = f(x) \cdot f(h) \cdot f(x^{-1}) = f(x) \cdot e \cdot f(x)^{-1} = f(x) \cdot f(x)^{-1} = e \implies x \cdot h \cdot x^{-1} \in \mathsf{Ker}(f)$$

Επομένως $\mathsf{Ker}(f) \trianglelefteq G$.

Έστω ότι η f είναι μονομορφισμός, δηλαδή «1-1», και έστω $x \in \mathsf{Ker}(f)$. Τότε $f(x) = e_{G'}$. Από την Πρόταση 2.8.8 γνωρίζουμε ότι $f(e_G) = e_{G'}$. Επειδή $f(x) = e_{G'} = f(e_G)$ και η f είναι «1-1», έπεται ότι $x = e_G$. Επομένως $\mathsf{Ker}(f) \subseteq \{e_G\}$, και άρα $\mathsf{Ker}(f) = \{e_G\}$, καθώς πάντα έχουμε $e_G \in \mathsf{Ker}(f)$ διότι $\mathsf{Ker}(f) \leq G$.

Αντίστροφα, έστω $\mathsf{Ker}(f) = \{e_G\}$ και έστω $f(x) = f(y)$. Τότε

$$f(x) = f(y) \implies f(x)f(y)^{-1} = e_{G'} \implies f(x)f(y^{-1}) = e_{G'} \implies f(xy^{-1}) = e_{G'} \implies$$

$$xy^{-1} \in \mathsf{Ker}(f) = \{e_G\} \implies xy^{-1} = e_G \implies x = y$$

και επομένως η f είναι «1-1».

2. Παρόμοια θα έχουμε

$$\mathsf{Im}(f) = \{f(x) \in G' \mid x \in G\} = f(G) \leq G'$$

και προφανώς η f είναι επιμορφισμός αν και μόνο αν $\mathsf{Im}(f) = G'$. ■

Είδαμε ότι ο πυρήνας $\mathsf{Ker}(f)$ ενός ομομορφισμού ομάδων $f\colon G \longrightarrow H$ είναι μια κανονική υποομάδα της ομάδας G. Η κατασκευή της ομάδας πηλίκου μας επιτρέπει να δείξουμε ότι κάθε κανονική υποομάδα μιας ομάδας είναι ο πυρήνας κατάλληλου ομομορφισμού ομάδων. Πράγματι, αν $H \trianglelefteq G$ είναι μια κανονική υποομάδα μιας ομάδας G, τότε οι ομάδα G και η ομάδα πηλίκο G/H συνδέονται μέσω της απεικόνισης κανονική προβολής:

$$\pi : G \longrightarrow G/H, \quad \pi(x) = xH$$

Πρόταση 6.2.5. *Η απεικόνιση κανονικής προβολής*

$$\pi\colon G \longrightarrow G/H, \quad \pi(x) = xH$$

είναι ένας επιμορφισμός ομάδων και $\mathsf{Ker}(\pi) = H$.

Απόδειξη. Για τυχόντα στοιχεία $xH, yH \in G/H$, θα έχουμε:

$$\pi(x \cdot y) = (xy)H = (xH) \cdot (yH) = \pi(x) \cdot \pi(y)$$

Άρα η απεικόνιση π είναι ομομορφισμός, και, επειδή προφανώς είναι απεικόνιση «επί», έπεται ότι η π είναι επιμορφισμός ομάδων. Επιπλέον θα έχουμε:

$$\mathsf{Ker}(\pi) = \{x \in G \mid \pi(x) = e_{G/H}\} = \{x \in G \mid xH = H\} = \{x \in G \mid x \in H\} = H$$ ■

6.3 Τα Θεωρήματα Ισομορφισμών και οι Εφαρμογές τους

Στην παρούσα ενότητα θα αποδείξουμε τα τρία βασικά Θεωρήματα Ισομορφισμών ομάδων, καθώς και το Θεώρημα αντιστοιχίας υποομάδων, και θα αναλύσουμε κάποιες από τις άμεσες εφαρμογές τους.

6.3.1 Το Πρώτο Θεώρημα Ισομορφισμών

Έστω $f\colon G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων. Τότε ο πυρήνας $\mathsf{Ker}(f)$ του ομομορφισμού f είναι μια κανονική υποομάδα της G_1, και άρα ορίζεται η ομάδα πηλίκο $G_1/\mathsf{Ker}(f)$. Από την άλλη πλευρά, όπως έχουμε δει, η εικόνα $\mathsf{Im}(f)$ του ομομορφισμού f είναι μια υποομάδα, όχι απαραίτητα κανονική, της G_2. Το πρώτο Θεώρημα Ισομορφισμών πιστοποιεί ότι οι ομάδες $G_1/\mathsf{Ker}(f)$ και $\mathsf{Im}(f)$ είναι ισόμορφες και μας επιτρέπει να αναλύσουμε κάθε ομομορφισμό ομάδων ως σύνθεση ενός επιμορφισμού, ενός ισομορφισμού και ενός μονομορφισμού.

Θεώρημα 6.3.1 (1ο Θεώρημα Ισομορφισμών)**.** *Έστω $f\colon G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων. Τότε η απεικόνιση*

$$\widetilde{f}\colon G_1/\mathsf{Ker}(f) \longrightarrow \mathsf{Im}(f), \quad \widetilde{f}(x\mathsf{Ker}(f)) = f(x)$$

ορίζει έναν ισομορφισμό ομάδων

$$\widetilde{f}\colon G_1/\mathsf{Ker}\, f \xrightarrow{\cong} \mathsf{Im}(f)$$

Απόδειξη. Γνωρίζουμε ότι ο πυρήνας $\mathsf{Ker}(f)$ του ομομορφισμού f είναι μια κανονική υποομάδα της G_1, και άρα ορίζεται η ομάδα πηλίκο $G_1/\mathsf{Ker}(f)$, και η εικόνα $\mathsf{Im}(f)$ του ομομορφισμού f είναι μια υποομάδα, όχι απαραίτητα κανονική, της G_2. Θέτουμε για ευκολία $H = \mathsf{Ker}(f)$, και ορίζουμε απεικόνιση

$$\widetilde{f}\colon G_1/H \longrightarrow \mathsf{Im}(f), \quad \widetilde{f}(xH) = f(x)$$

Θα δείξουμε ότι η $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση η οποία είναι ισομορφισμός ομάδων.

1. Η $\widetilde{f}$ ΕΙΝΑΙ ΚΑΛΑ ΟΡΙΣΜΕΝΗ: Έστω $xH = yH$, όπου $x, y \in G_1$. Τότε θα έχουμε:

$$xH = yH \implies x^{-1}y \in H = \mathsf{Ker}(f) \implies f(x^{-1}y) = e_{G_2} \implies$$
$$\implies f(x^{-1})f(y) = e_{G_2} \implies f(x)^{-1}f(y) = e_{G_2} \implies f(x) = f(y) \implies \widetilde{f}(xH) = \widetilde{f}(yH)$$

   Επομένως η $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση.

2. Η $\widetilde{f}$ ΕΙΝΑΙ ΟΜΟΜΟΡΦΙΣΜΟΣ: Έστω $xH, yH \in G_1/H$. Τότε θα έχουμε:

$$\widetilde{f}(xH \cdot yH) = \widetilde{f}((x \cdot y)H) = f(x \cdot y) = f(x) \cdot f(y) = \widetilde{f}(xH) \cdot \widetilde{f}(yH)$$

   Επομένως η $\widetilde{f}(xH)$ είναι ένας ομομορφισμός ομάδων.

3. Η $\widetilde{f}$ ΕΙΝΑΙ ΕΠΙΜΟΡΦΙΣΜΟΣ: Έστω $z \in \mathsf{Im}(f)$. Τότε υπάρχει $x \in G_1$ έτσι ώστε $f(x) = z$. Επειδή $\widetilde{f}(xH) = f(x) = z$, έπεται ότι η απεικόνιση $\widetilde{f}$ είναι επιμορφισμός.

4. Η $\widetilde{f}$ ΕΙΝΑΙ ΜΟΝΟΜΟΡΦΙΣΜΟΣ: Θα υπολογίσουμε τον πυρήνα του ομομορφισμού $\widetilde{f}$:

$$\mathsf{Ker}(\widetilde{f}) = \left\{xH \in G_1/H \mid \widetilde{f}(xH) = e_{G_2}\right\} = \left\{xH \in G_1/H \mid f(x) = e_{G_2}\right\} = \left\{xH \in G_1/H \mid x \in \mathsf{Ker}(f) = H\right\} = H$$

   Επειδή το αριστερό σύμπλοκο H είναι το ουδέτερο στοιχείο της ομάδας πηλίκου G_1/H: $H = e_{G_1/H}$, έπεται ότι ο πυρήνας του ομομορφισμού $\widetilde{f}$ αποτελείται μόνο από το ταυτοτικό στοιχείο της ομάδας G_1/H. Αυτό, όπως γνωρίζουμε, δείχνει ότι ο ομομορφσιμός $\widetilde{f}$ είναι μονομορφισμός.

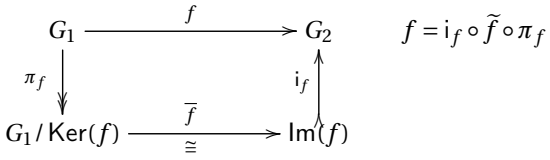
Συνδυάζοντας τα παραπάνω, βλέπουμε ότι η καλά ορισμένη απεικόνιση $\widetilde{f}$ είναι ένας ισομορφισμός ομάδων. ■

Τα ακόλουθα Πορίσματα είναι άμεσες συνέπειες του Θεωρήματος 6.3.1.

Πόρισμα 6.3.2. *Κάθε ομομορφισμός ομάδων $f: G_1 \longrightarrow G_2$ είναι σύνθεση $f = \mathsf{i}_f \circ \widetilde{f} \circ \pi_f$:*

1. *του μονομορφισμού $\mathsf{i}_f: \mathsf{Im}(f) \longrightarrow G_2$, $\mathsf{i}_f(y) = y$,*
2. *του ισομορφισμού $\widetilde{f}: G_1/\mathsf{Ker}(f) \longrightarrow \mathsf{Im}(f)$, $\widetilde{f}(x\mathsf{Ker}(f)) = f(x)$,*
3. *του επιμορφισμού $\pi_f: G_1 \longrightarrow G_1/\mathsf{Ker}(f)$, $\pi_f(x) = x\mathsf{Ker}(f)$.*

Δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό



Απόδειξη. Στο Θεώρημα 6.3.1 δείξαμε ότι η απεικόνιση $\widetilde{f}$ είναι ισομορφισμός ομάδων. Από την Πρόταση 6.2.5 έπεται ότι η απεικόνιση π_f είναι επομορφισμός ομάδων με πυρήνα $\mathsf{Ker}(\pi_f) = \mathsf{Ker}(f)$. Προφανώς η κανονική έγκλειση i_f είναι ένας μονομορφισμός ομάδων. Τέλος:

$$\forall x \in G_1: \quad (\mathsf{i}_f \circ \widetilde{f} \circ \pi_f)(x) = \mathsf{i}_f(\widetilde{f}(\pi_f(x))) = \mathsf{i}_f(\widetilde{f}(xH)) = \mathsf{i}_f(f(x)) = f(x)$$

Επομένως $\mathsf{i}_f \circ \widetilde{f} \circ \pi_f = f$. ■

Πόρισμα 6.3.3. *Έστω $f: G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων.*

1. *Αν ο f είναι μονομορφισμός, τότε ο ομομορφισμός $f\colon G_1 \longrightarrow G_2$ ορίζει έναν ισομορφισμό*

$$f'\colon G_1 \xrightarrow{\cong} \mathsf{Im}(f) \leq G_2, \quad f'(x) = f(x)$$

Δηλαδή η G_1 είναι ισόμορφη με μια υποομάδα της G_2.

2. *Αν ο f είναι επιμορφισμός, τότε ο ομομορφισμός $f\colon G_1 \longrightarrow G_2$ επάγει έναν ισομορφισμό*

$$G_1/\mathsf{Ker}(f) \xrightarrow{\cong} G_2$$

Δηλαδή η G_2 είναι ισόμορφη με μια ομάδα πηλίκο της G_1.

Απόδειξη. 1. Αν ο ομομορφισμός f είναι μονομορφισμός, τότε $\mathsf{Ker}(f) = \{e_{G_1}\}$ και τότε προφανώς θα έχουμε έναν ισομορφισμό $G_1/\mathsf{Ker}(f) = G_1$ και άρα ο μονομορφισμός $f\colon G_1 \longrightarrow G_2$ ορίζει έναν ισομορφισμό $f'\colon G_1 \longrightarrow \mathsf{Im}(f)$, $f'(x) = f(x)$.

2. Αν ο ομομορφισμός f είναι επιμορφισμός, τότε $\mathsf{Im}(f) = G_2$ και ο ισχυρισμός προκύπτει από το Θεώρημα 6.3.1. ■

Το ακόλουθο αποτέλεσμα παρουσιάζει μια περισσότερο γενική μορφή του Πρώτου Θεωρήματος Ισομορφισμών:

Θεώρημα 6.3.4 (1ο Θεώρημα Ισομορφισμών - Γενικευμένη Μορφή)**.** *Έστω $H \trianglelefteq G_1$ μια κανονική υποομάδα μιας ομάδας G_1 και $f\colon G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων. Αν $H \leq G_1$, τότε τα ακόλουθα είναι ισοδύναμα:*

1. *$H \leq \mathsf{Ker}(f)$.*

2. *Υπάρχει μοναδικός ομομορφισμός ομάδων:*

$$\widetilde{f}\colon G_1/H \longrightarrow G_2 \quad \text{έτσι ώστε:} \quad \widetilde{f} \circ \pi_H = f \tag{†}$$

όπου $\pi_H\colon G_1 \longrightarrow G_1/H$ είναι ο φυσικός επιμορφισμός.

Επιπλέον:

(*a*) *Ο ομομορφισμός ομάδων $\widetilde{f}$ είναι επιμορφισμός αν και μόνο αν ο ομομορφισμός ομάδων f είναι επιμορφισμός.*

(*b*) *Ο ομομορφισμός ομάδων $\widetilde{f}$ είναι μονομορφισμός αν και μόνο αν $H = \mathsf{Ker}(f)$.*

(*c*) *Ο ομομορφισμός ομάδων $\widetilde{f}$ είναι ισομορφισμός αν και μόνο αν ο ομομορφισμός f είναι επιμορφισμός και $H = \mathsf{Ker}(f)$.*

Απόδειξη. 1. $\Longrightarrow$ 2. Υποθέτουμε ότι $H \subseteq \mathsf{Ker}(f)$, και ορίζουμε μια απεικόνιση

$$\widetilde{f}\colon G_1/H \longrightarrow G_2 \quad f(xH) = f(x)$$

Δείχνουμε ότι η απεικόνιση $\widetilde{f}$ είναι καλά ορισμένη. Έστω $xH, yH \in G_1/H$. Τότε θα έχουμε:

$$xH = yH \implies x^{-1}y \in H \leq \mathsf{Ker}(f) \implies f(x^{-1}y) = e_{G_2} \implies f(x)^{-1}f(y) = e_{G_2} \implies f(x) = f(y) \implies$$

$$\widetilde{f}(xH) = \widetilde{f}(yH)$$

και, επομένως, πράγματι η απεικόνιση $\widetilde{f}$ είναι καλά ορισμένη. Όπως στην απόδειξη του Θεωρήματος 6.3.1, βλέπουμε ότι η $\widetilde{f}$ είναι ομομορφισμός ομάδων, και

$$\forall x \in G_1\colon \quad (\widetilde{f} \circ \pi_H)(x) = \widetilde{f}(\pi_H(x))\widetilde{f}(xH) = f(x)$$

και επομένως $f = \widetilde{f} \circ \pi_H$.

Αν $g\colon G_1/H \longrightarrow G_2$ είναι ένας άλλος ομομορφισμός ομάδων έτσι ώστε $f = g\circ\pi_H$. Τότε:

$$\forall xH \in G_1/H\colon \quad g(xH) = g(\pi_H(x)) = (g\circ\pi_H)(x) = (\widetilde{f}\circ\pi_H)(x) = \widetilde{f}(\pi_H(x)) = \widetilde{f}(xH)$$

Άρα $g = \widetilde{f}$.

2. $\Longrightarrow$ 1. Υποθέτουμε ότι η απεικόνιση (†) είναι ένας ομομορφισμός ομάδων με την ιδιότητα $\widetilde{f}\circ\pi_H = f$. Τότε επειδή η $\widetilde{f}$ είναι ομομορφισμός, επειδή το αριστερό σύμπλοκο H είναι το ουδέτερο στοιχείο της ομάδας πηλίκου G_1/H, και επειδή ένας ομομορφισμός ομάδων στέλνει το ουδέτερο στοιχείο στο ουδέτερο στοιχείο, θα έχουμε:

$$f(H) = (\widetilde{f}\circ\pi_H)(H) = \widetilde{f}(\pi_H(H)) = \widetilde{f}(H) = e_{G_2}$$

Αυτό σημαίνει ότι ο ομομορφισμός f στέλνει κάθε στοιχείο της υποομάδας H στο ουδέτερο στοιχείο e_{G_2} της ομάδας G_2. Επομένως $H \leq \mathsf{Ker}(f)$.

(*a*) Υποθέτουμε ότι ο ομομορφισμός $\widetilde{f}$ είναι επιμορφισμός. Επειδή $f = \widetilde{f}\circ\pi_H$, επειδή ο ομομορφισμός π_H είναι επιμορφισμός, και επειδή σύνθεση επιμορφισμών είναι επιμορφισμός, έπεται ότι ο ομομορφισμός f είναι επιμορφισμός.

Αντίστροφα, έστω ότι ο ομομορφισμός f είναι επιμορφισμός, και έστω $y \in G_2$. Τότε υπάρχει στοιχείο $x \in G_1$ έτσι ώστε $f(x) = y$. Τότε $\widetilde{f}(xH) = f(x) = y$ και επομένως ο ομομορφισμός $\widetilde{f}$ είναι επιμορφισμός.

(*b*) Υποθέτουμε πρώτα ότι ο ομομορφισμός $\widetilde{f}$ είναι μονομορφισμός, και έστω $x \in \mathsf{Ker}(f)$. Τότε $\widetilde{f}(\pi_H(x)) = (\widetilde{f}\circ\pi_H)(x) = f(x) = e_{G_2}$. Επειδή η $\widetilde{f}$ είναι μονομορφισμός, θα έχουμε $\pi_H(x) = xH = e_{G_1/H} = H$ και άρα $x \in H$. Δηλαδή $\mathsf{Ker}(f) \subseteq H$ και επομένως $H = \mathsf{Ker}(f)$.

Αντίστροφα, αν $H = \mathsf{Ker}(f)$, τότε έστω $xH \in \mathsf{Ker}(\widetilde{f})$. Τότε $\widetilde{f}(xH) = f(x) = e_{G_2}$ και άρα $x \in \mathsf{Ker}(f) = H$. Αυτό δείχνει ότι $xH = H = e_{G_1/H}$ και επομένως ο ομομορφισμός $\widetilde{f}$ είναι μονομορφισμός.

(*c*) Συνδυάζοντας τα (*a*) και (*b*) θα έχουμε: ο ομομορφισμός $\widetilde{f}$ είναι ισομορφισμός αν και ο μόνο αν ο ομομορφισμός f είναι επιμορφισμός και $H = \mathsf{Ker}(f)$. ■

Παρατήρηση 6.3.5. Με ακρίβεια ισομορφισμού, η αντιστοιχία

$$\Phi\ :\ \{\text{κανονικές υποομάδες}\ \ H\ \ \text{της}\ \ G\} \longrightarrow \{\text{επιμορφισμοί}\ \ f\colon G \longrightarrow G'\}$$

$$\Phi(H) = \pi_H\colon G \longrightarrow G/H$$

είναι «1-1» και «επί», με αντίστροφη την αντιστοιχία

$$\Psi\ :\ \{\text{επιμορφισμοί}\ \ f\colon G \longrightarrow G'\} \longrightarrow \{\text{κανονικές υποομάδες}\ \ H\ \ \text{της}\ \ G\}$$

$$\Psi(f) = \mathsf{Ker}(f)$$

Δηλαδή:

1. αν $H \trianglelefteq G$ είναι μια κανονική υποομάδα της G, τότε η κανονική προβολή $\pi_H\colon G \longrightarrow G/H$ είναι επιμορφισμός και $\mathsf{Ker}(\pi_H) = H$.

2. αν $f\colon G \longrightarrow G'$ είναι ένας επιμορφισμός ομάδων, τότε ο πυρήνας $\mathsf{Ker}(f)$ είναι μια κανονική υποομάδα της G και, χρησιμοποιώντας τον ισομορφισμό $G/\mathsf{Ker}(f) \cong G'$ του Πρώτου Θεωρήματος Ισομορφισμών 6.3.1, ο επιμορφισμός f «συμπίπτει» με τον φυσικό επιμορφισμό $\pi_f\colon G \longrightarrow G/\mathsf{Ker}(f)$ με την έννοια ότι $\pi_f\circ\widetilde{f} = f$ και ο ομομορφισμός $\widetilde{f}$ είναι ισομορφισμός.

Επομένως, υπό αυτή την οπτική γωνία, κανονικές υποομάδες της G, και επιμορφισμοί οι οποίοι εκκινούν από την G, είναι ισοδύναμες έννοιες. ▲

6.3.2 Το Δεύτερο Θεώρημα Ισομορφισμών

Αν H και N είναι υποομάδες μιας ομάδας G, τότε, υποθέτοντας ότι η N είναι κανονική υποομάδα της G, το υποσύνολο HN είναι μια υποομάδα της G η οποία περιέχει ως κανονική υποομάδα την N και η τομή $H \cap N$ είναι κανονική υποομάδα της H. Το Δεύτερο Θεώρημα Ισομορφισμών εξετάζει τη σχέση μεταξύ των ομάδων πηλίκων HN/N και $H/H \cap N$:

Θεώρημα 6.3.6 (2ο Θεώρημα Ισομορφισμών)**.** *Έστω G μια ομάδα, $H \leq G$ μια υποομάδα της G, και $N \trianglelefteq G$ μια κανονική υποομάδα της G. Τότε:*

1. *Το υποσύνολο $HN = \{hn \in G \mid h \in H \ \& \ n \in N\}$ είναι μια υποομάδα της G και $N \trianglelefteq HN$.*
2. *$H \cap N \trianglelefteq H$, και υπάρχει ένας ισομορφισμός ομάδων:*

$$HN \big/ N \ \cong \ H \big/ (H \cap N)$$

Αν η ομάδα G είναι προσθετική, τότε ο παραπάνω ισομορφισμός έχει την ακόλουθη μορφή:

$$H + N \big/ N \ \cong \ H \big/ (H \cap N)$$

Απόδειξη. 1. Προφανώς $e = ee \in HN$.

Έστω $g_1, g_2 \in HN$. Τότε $g_1 = h_1 n_1$ και $g_2 = h_2 n_2$, και επομένως:

$$g_1 g_2^{-1} = h_1 n_1 (h_2 n_2)^{-1} = h_1 n_1 n_2^{-1} h_2^{-1} = h_1 n_1 e n_2^{-1} h_2^{-1} = h_1 n_1 h_2^{-1} h_2 n_2^{-1} h_2^{-1} = h_1 n_1 h_2^{-1} n'$$

$$\text{όπου} \quad n' = h_2 n_2^{-1} h_2^{-1} = (h_2^{-1})^{-1} n_2^{-1} h_2^{-1} \in N \quad \text{διότι} \quad N \trianglelefteq G$$

Παρόμοια:

$$h_1 n_1 h_2^{-1} n' = h_1 e n_1 h_2^{-1} n' = h_1 h_2^{-1} h_2 n_1 h_2^{-1} n' = h_1 h_2^{-1} n'' n' \in HN$$

$$\text{όπου} \quad n'' = h_2 n_1 h_2^{-1} = (h_2^{-1})^{-1} n_1 h_2^{-1} \in N \quad \text{διότι} \quad N \trianglelefteq G$$

Επομένως θα έχουμε:

$$g_1 g_2^{-1} \in HN \quad \text{και άρα} \quad HN \leq G$$

Έστω τώρα $hn \in HN$ και $n' \in N$. Τότε, χρησιμοποιώντας ότι $n^{-1} \in N$ και $N \trianglelefteq G$, έπεται ότι $h^{-1} n' h \in N$ και θα έχουμε ότι:

$$(hn)^{-1} n' (hn) = n^{-1} h^{-1} n' h n = n^{-1} (h^{-1} n' h) n \in N$$

Άρα $N \trianglelefteq HN$.

2. Ορίζουμε απεικόνιση

$$f : H \longrightarrow HN/N, \qquad f(h) = hN$$

θεωρώντας το στοιχείο $h \in H \subseteq HN$.

Η f είναι προφανώς ομομορφισμός ομάδων. Ο πυρήνας της f είναι:

$$\mathsf{Ker}(f) = \{h \in H \mid f(h) = N\} = \{h \in H \mid hN = N\} = \{h \in H \mid h \in N\} = H \cap N$$

και επομένως η υποομάδα $H \cap N$ είναι κανονική υποομάδα της H.

Η απεικόνιση f είναι επιμορφισμός, διότι:

$$\forall (hn)N \in HN/N: \quad (hn)N = hN \quad \text{διότι} \quad h^{-1}(hn) = (h^{-1}h)n = en = n \in N \quad \text{και άρα}$$

$$f(h) = hN = (hn)N$$

Από το Πρώτο Θεώρημα Ισομορφισμών 6.3.1 θα έχουμε ότι ο επιμορφισμός f ορίζει έναν ισομορφισμό

$$\overline{f} : H/H \cap N \xrightarrow{\cong} HN/N, \qquad \overline{f}(h(H \cap N)) = hN$$

■

6.3.3 Το Τρίτο Θεώρημα Ισομορφισμών

Αν H είναι μια κανονική υποομάδα μιας ομάδας G, τότε το Τρίτο Θεώρημα Ισομορφισμών περιγράφει τις ομάδες πηλίκα των κανονικών υποομάδων της ομάδας πηλίκου G/H.

Θεώρημα 6.3.7 (3ο Θεώρημα Ισομορφισμών). *Έστω $H \trianglelefteq G$ και $N \trianglelefteq G$ κανονικές υποομάδες μιας ομάδας G, και έστω ότι $N \leq H$. Τότε η ομάδα πηλίκο H/N είναι μια κανονική υποομάδα της ομάδας πηλίκο G/N και υπάρχει ένας ισομορφισμός ομάδων:*

$$G/N \big/ H/N \xrightarrow{\cong} G/H$$

Απόδειξη. Επειδή οι υποομάδες $H \trianglelefteq G$ και $N \trianglelefteq G$ της G είναι κανονικές υποομάδες, ορίζονται οι ομάδες πηλίκα G/H και G/N αντίστοιχα.

Ορίζουμε απεικόνιση

$$f : G/N \longrightarrow G/H, \quad f(xN) = xH$$

Θα δείξουμε ότι η f είναι ένας καλά ορισμένος επιμορφισμός με πυρήνα την υποομάδα H/N.

1. Η f ΕΙΝΑΙ ΚΑΛΑ ΟΡΙΣΜΕΝΗ: Έστω $xN = yN$, όπου $x, y \in G$. Τότε επειδή $N \leq H$, θα έχουμε:

$$xN = yN \implies x^{-1}y \in N \implies x^{-1}y \in H \implies xH = yH \implies f(xN) = f(yN)$$

   Επομένως η f είναι μια καλά ορισμένη απεικόνιση.

2. Η ΑΠΕΙΚΟΝΙΣΗ f ΕΙΝΑΙ ΟΜΟΜΟΡΦΙΣΜΟΣ: Έστω $xN, yN \in G/N$. Τότε θα έχουμε:

$$f(xN \cdot yN) = f((x \cdot y)N) = (x \cdot y)H = xH \cdot yH = f(xN) \cdot f(yN)$$

   Επομένως η f είναι ένας ομομορφισμός ομάδων.

3. Ο ΟΜΟΜΟΡΦΙΣΜΟΣ f ΕΙΝΑΙ ΕΠΙΜΟΡΦΙΣΜΟΣ: Έστω $zH \in G/H$. Τότε υπάρχει το αριστερό σύμπλοκο $xN \in G/N$ είναι τέτοιο ώστε $f(xN) = zH$. Επομένως η απεικόνιση f είναι επιμορφισμός.

4. $\mathsf{Ker}(f) = H/N$: Θα υπολογίσουμε τον πυρήνα του επιμορφισμού f:

$$\mathsf{Ker}(f) = \{xN \in G/N \mid f(xN) = e_{G/H}\} = \{xN \in G/N \mid xH = H\} = \{xN \in G/N \mid x \in H\} = H/N$$

   Άρα $\mathsf{Ker}(f) = H/N$. Επειδή ο πυρήνας ενός ομομορφισμού είναι πάντα κανονική υποομάδα, έπεται ότι $H/N \trianglelefteq G/N$.

Από το Πρώτο Θεώρημα Ισομορφισμών 6.3.1, έπεται ότι υπάρχει ένας ισομορφισμός μεταξύ των ομάδαν $G/N/H/N$ και G/H. ■

6.3.4 Το Θεώρημα Αντιστοιχίας

Κλείνουμε την παρούσα υποενότητα με το ακόλουθο αποτέλεσμα το οποίο, δοθέντος ενός ομομορφισμού ομάδων $f : G_1 \longrightarrow G_2$, μας δίνει μια «1-1» και «επί» αντιστοιχία μεταξύ των υποομάδων της G_1 οι οποίες περιέχουν τον πυρήνα της f, και των υποομάδων της G_2 οι οποίες περιέχονται στην εικόνα του f. Επιπρόσθετα αυτή η αντιστοιχία διατηρεί κανονικές υποομάδες. Το ακόλουθο Θεώρημα αναφέρεται κάποιες φορές στην βιβλιογραφία και ως *Τέταρτο Θεώρημα Ισομορφισμών*.

Θεώρημα 6.3.8 (Θεώρημα Αντιστοιχίας - 4ο Θεώρημα Ισομορφισμών). *Έστω $f : G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων.*

1. *Η απεικόνιση*

$$\Phi:\ \{H\leq G_1 \mid \mathsf{Ker}(f)\leq H\} \ \longrightarrow\ \{K\leq G_2 \mid K\leq \mathsf{Im}(f)\},\quad \Phi(H)=f(H)$$

είναι «1-1» και «επί», με αντίστροφη την απεικόνιση:

$$\Psi:\ \{K\leq G_2 \mid K\leq \mathsf{Im}(f)\} \ \longrightarrow\ \{H\leq G_1 \mid \mathsf{Ker}(f)\leq H\},\quad \Psi(K)=f^{-1}(K)$$

2. *Επιπλέον οι «1-1» και «επί» απεικονίσεις* Φ *και* Ψ *διατηρούν την κανονικότητα, με άλλα λόγια:*

$$\mathsf{Ker}(f)\leq H\trianglelefteq G_1 \iff f(H)\trianglelefteq \mathsf{Im}(f) \quad \textit{και} \quad K\trianglelefteq \mathsf{Im}(f) \iff \mathsf{Ker}(f)\leq f^{-1}(K)\trianglelefteq G_1$$

Απόδειξη. 1. Αν $H\leq G_1$, τότε προφανώς $f(H)\subseteq f(G)=\mathsf{Im}(f)$, και αν $K\leq \mathsf{Im}(f)=f(G)$, τότε $\{e_{G_2}\}\subseteq K$ και άρα $\mathsf{Ker}(f)=f^{-1}(\{e_{G_2}\})\subseteq f^{-1}(K)\subseteq G$. Επομένως από την Πρόταση 6.2.2 έπεται ότι οι απεικονίσεις Φ και Ψ είναι καλά ορισμένες μεταξύ των παραπάνω αναφερομένων συνόλων υποομάδων.

Μένει να δείξουμε ότι:

$$\mathsf{Ker}(f)\leq H\leq G \implies \Psi\Phi(H)=H \quad \text{και} \quad K\leq \mathsf{Im}(f) \implies \Phi\Psi(K)=K$$

Με άλλα λόγια, αρκεί να δείξουμε ότι:

$$\mathsf{Ker}(f)\leq H\leq G \implies f^{-1}(f(H))=H \quad \text{και} \quad K\leq \mathsf{Im}(f) \implies f(f^{-1}(K))=K$$

Παρατηρούμε ότι, με τους παραπάνω συμβολισμούς, θα έχουμε:

$$\mathsf{Ker}(f)\leq H \implies \mathsf{Ker}(f)\cdot H\ \subseteq\ H$$

(*a*) Υποθέτουμε ότι: $\mathsf{Ker}(f)\leq H\leq G$.

Έστω $h\in H$. Τότε $f(h)\in f(H)$ και επομένως $h\in f^{-1}(f(H))$. Άρα: $H\subseteq f^{-1}(f(H))$.

Αντίστροφα, έστω $x\in f^{-1}(f(H))$. Τότε $f(x)\in f(H)$ και άρα $f(x)=f(h)$, όπου $h\in H$. Τότε:

$$f(x)=f(h) \implies f(x)f(h)^{-1}=e_G \implies f(x)f(h^{-1})=e_G \implies f(xh^{-1})=e_G \implies$$

$$xh^{-1}\in \mathsf{Ker}(f) \implies x\in \mathsf{Ker}(f)h\subseteq \mathsf{Ker}(f)\cdot H\subseteq H$$

και επομένως $f^{-1}(f(H))\subseteq H$. Άρα:

$$f^{-1}(f(H))=H$$

(*b*) Υποθέτουμε ότι $K\leq \mathsf{Im}(f)=f(G)$.

Έστω $y\in f(f^{-1}(K))$. Τότε $y=f(x)$, όπου $x\in f^{-1}(K)$ και επομένως $f(x)\in K$. Τότε $y=f(x)\in K$ και άρα $f(f^{-1}(K))\subseteq K$.

Αντίστροφα, έστω $k\in K\leq f(G)$. Τότε $k=f(x)$, για κάποιο $x\in G$ και τότε προφανώς $x\in f^{-1}(K)$ διότι $f(x)=k\in K$. Άρα $k=f(x)\in f(f^{-1}(K))$ και επομένως $K\subseteq f(f^{-1}(K))$. Άρα:

$$K=f(f^{-1}(K))$$

Από τα (α) και (β) έπεται ότι $\Psi\Phi(H)=H$ για κάθε υποομάδα H της G_1 η οποία περιέχει τον πυρήνα της G και $\Phi\Psi(K)=K$, για κάθε υποομάδα K της G_2 η οποία περιέχεται στην εικόνα της f. Επομένως η απεικόνιση Φ είναι «1-1» και «επί» και η Ψ είναι η αντίστροφή της.

2. Θα έχουμε:

(*a*) Αν H είναι μια υποομάδα της G_1, θα δείξουμε ότι: $H \trianglelefteq G_1 \iff f(H) \trianglelefteq \mathsf{Im}(f)$.

«$\Longrightarrow$» Έστω ότι $H \trianglelefteq G_1$, δηλαδή: $ghg^{-1} \in H$, $\forall g \in G_1$, $\forall h \in H$. Αν $g \in \mathsf{Im}(f)$, τότε $g' = f(g)$ για κάποιο $g \in G_1$. Τότε, για κάθε $h \in H$ θα έχουμε: $g'f(h)(g')^{-1} = f(g)f(h)f(g)^{-1} = f(g)f(h)f(g^{-1}) = f(ghg^{-1}) \in f(H)$. Επομένως η υποομάδα $f(H)$ είναι κανονική στην $\mathsf{Im}(f)$.

«$\Longleftarrow$» Έστω ότι $f(H) \trianglelefteq \mathsf{Im}(f)$, δηλαδή $f(g)f(h)f(g)^{-1} \in f(H)$, $\forall h \in H$. Τότε, όπως παραπάνω, $f(ghg^{-1}) \in f(H)$ και άρα $f(ghg^{-1}) = f(h')$, όπου $h' \in H$. Τότε, χρησιμοποιώντας ότι $h' \in H$, θα έχουμε

$$f(ghg^{-1}) = f(h') \implies f(ghg^{-1})f(h')^{-1} = e_{G_2} \implies f(ghg^{-1}(h')^{-1}) = e_{G_2} \implies$$

$$ghg^{-1}(h')^{-1} \in \mathsf{Ker}(f) \leq H \implies ghg^{-1} \in Hh' = H$$

Επομένως $ghg^{-1} \in H$, $\forall g \in G$, $\forall h \in H$, και άρα η H είναι κανονική υποομάδα της G_1.

(*b*) Αν K είναι μια υποομάδα της G_2, θα δείξουμε ότι: $K \trianglelefteq \mathsf{Im}(f) \iff f^{-1}(K) \trianglelefteq G_1$.

«$\Longrightarrow$» Έστω ότι $K \trianglelefteq \mathsf{Im}(f)$, δηλαδή $f(g)kf(g)^{-1} \in K$, $\forall g \in G_1$, $\forall k \in K$. Έστω $g \in G$ και $x \in f^{-1}(K)$. Τότε $f(x) := k \in K$, και, χρησιμοποιώντας ότι $K \trianglelefteq \mathsf{Im}(f)$, θα έχουμε $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)kf(g)^{-1} \in K$. Αυτό σημαίνει ότι $gxg^{-1} \in f^{-1}(K)$ και επομένως η $f^{-1}(K)$ είναι μια κανονική υποομάδα της G_1.

«$\Longleftarrow$» Έστω ότι $f^{-1}(K) \trianglelefteq G_1$, δηλαδή $gxg^{-1} \in f^{-1}(K)$, $\forall g \in G_1$, $\forall x \in f^{-1}(K)$. Έστω $g \in G_1$ και $k \in K$. Τότε $k = f(x)$ για κάποιο $x \in G_1$, όπου προφανώς $x \in f^{-1}(K)$, και θα έχουμε $gxg^{-1} \in f^{-1}(K)$ διότι $f^{-1}(K) \trianglelefteq G_1$. Άρα:

$$f(g)kf(g)^{-1} = f(g)f(x)f(g^{-1}) = f(gxg^{-1}) \in f(f^{-1}(K)) \subseteq K$$

Επομένως η K είναι μια κανονική υποομάδα της $\mathsf{Im}(f)$. ■

Αν ο ομομορφισμός $f: G_1 \longrightarrow G_2$ είναι επιμορφισμός, θα έχουμε το ακόλουθο πόρισμα.

Πόρισμα 6.3.9. *Έστω $f: G_1 \longrightarrow G_2$ ένας επιμορφισμός ομάδων.*

1. *Η απεικόνιση*
$$\Phi: \{H \leq G_1 \mid \mathsf{Ker}(f) \leq H\} \longrightarrow \{K \leq G_2\}, \quad \Phi(H) = f(H)$$
είναι «1-1» και «επί», με αντίστροφη την απεικόνιση:
$$\Psi: \{K \leq G_2\} \longrightarrow \{H \leq G_1 \mid \mathsf{Ker}(f) \leq H\}, \quad \Psi(K) = f^{-1}(K)$$

2. *Επιπλέον οι «1-1» και «επί» απεικονίσεις Φ και Ψ διατηρούν την κανονικότητα, με άλλα λόγια:*
$$H \trianglelefteq G_1 \iff f(H) \trianglelefteq G_2 \quad \text{και} \quad K \trianglelefteq G_2 \iff f^{-1}(K) \trianglelefteq G_1 \quad ■$$

Ισοδύναμα, ως πόρισμα έχουμε τα ακόλουθα πολύ χρήσιμα αποτελέσματα τα οποία περιγράφουν τις (κανονικές) υποομάδες μιας ομάδας πηλίκου.

Πόρισμα 6.3.10. *Έστω $N \trianglelefteq G$ μια κανονική υποομάδα μιας ομάδας G. Τότε η απεικόνιση*

$$\Phi: \{\textit{(κανονικές) υποομάδες } H \textit{ της } G \textit{ έτσι ώστε: } N \leq H\} \longrightarrow \{\textit{(κανονικές) υποομάδες } K \textit{ της } G/N\}$$

$$\Phi(H) = \pi_N(H) = H/N$$

είναι «1-1» και «επί».

Απόδειξη. Η απόδειξη είναι άμεση απόρροια του Θεωρήματος 6.3.8 όταν αυτό εφαρμοστεί στον επιμορφισμό ομάδων $\pi_N: G \longrightarrow G/N$. ■

Ισοδύναμα:

Πόρισμα 6.3.11. *Έστω $H \trianglelefteq G$ μια κανονική υποομάδα μιας ομάδας G.*

1. *Κάθε υποομάδα K της ομάδας πηλίκου G/H είναι της μορφής $K = G/N$, όπου $H \leq N$.*
2. *Αν $H \leq N$, τότε: $N \trianglelefteq G \iff N/H \trianglelefteq G/H$.*

Έστω G μια ομάδα. Μια υποομάδα N της G καλείται **μέγιστη κανονική υποομάδα** της G, αν:

1. Η N είναι κανονική υποομάδα της G.
2. Δεν υπάρχει κανονική υποομάδα H της G έτσι ώστε: $N \lneqq H \lneqq G$.

Προφανώς κάθε κυκλική ομάδα με τάξη έναν πρώτο αριθμό είναι απλή. Το ακόλουθο παράδειγμα δείχνει ότι κάθε υποομάδα N δείκτη 2 σε μια πεπερασμένη ομάδα G είναι μια μέγιστη κανονική υποομάδα της G, ισοδύναμα η ομάδα πηλίκο G/N είναι απλή.

Παράδειγμα 6.3.12. Έστω G μια πεπερασμένη ομάδα τάξης > 2 και N μια υποομάδα της G έτσι ώστε $[G:N] = 2$. Τότε, ως γνωστόν, η υποομάδα N είναι μια κανονική υποομάδα της G η οποία είναι γνήσια (διότι, αν $G = N$, τότε $[G:N] = 1$, το οποίο είναι άτοπο) και μη τετριμμένη (διότι, αν $N = \{e_G\}$, τότε $[G:N] = o(G) = 2$, το οποίο είναι άτοπο). Η ομάδα πηλίκο G/N έχει τάξη $[G:N] = 2$ και άρα δεν έχει γνήσιες μη τετριμμένες (κανονικές) υποομάδες. Επομένως η ομάδα πηλίκο G/N είναι απλή. Ισοδύναμα η υποομάδα N είναι μια μέγιστη κανονική υποομάδα της G.

Για παράδειγμα, αν $N = \langle(123)\rangle$ είναι η κυκλική υποομάδα της συμμετρικής ομάδας S_3 η οποία παράγεται από τον 3-κύκλο (123). Τότε $[S_3 : N] = 2$ και άρα η N είναι μια μέγιστη κανονική υποομάδα της S_3. Διαφορετικά: η υποομάδα N είναι κανονική στην S_3 και η ομάδα πηλίκο είναι ισόμορφη με την κυκλική ομάδα τάξης 2. Άρα η ομάδα πηλίκο S_3/N είναι απλή. $\surd$

Γενικότερα, αν N είναι μια κανονική υποομάδα μιας πεπερασμένης ομάδας G και $[G:N] = p$, όπου p είναι ένας πρώτος αριθμός, τότε η N είναι μέγιστη κανονική υποομάδα της G, βλέπε την Άσκηση 6.6.21.

6.3.5 Εσωτερικοί Αυτομορφισμοί

Υπενθυμίζουμε ότι, αν G είναι μια ομάδα, τότε μια απεικόνιση $f: G \longrightarrow G$ καλείται **αυτομορφισμός** της G, αν η απεικόνιση f είναι ισομορφισμός. Υπενθυμίζουμε επίσης ότι το σύνολο

$$\mathrm{Aut}(G) = \{f : G \longrightarrow G \mid f : \text{αυτομορφισμός της } G\}$$

αποτελεί μια υποομάδα της ομάδας μεταθέσεων $S(G)$ επί του συνόλου G, η οποία καλείται η **ομάδα αυτομορφισμών** της G. Έτσι η πράξη με την οποία το σύνολο $\mathrm{Aut}(G)$ δομείται σε ομάδα είναι η σύνθεση απεικονίσεων, το ουδέτερο στοιχείο της είναι η ταυτοτική απεικόνιση ι_G, και το αντίστροφο στοιχείο του $f \in \mathrm{Aut}(G)$ είναι η αντίστροφη απεικόνιση f^{-1} της f.

Η ακόλουθη βοηθητική πρόταση δείχνει ότι κάθε στοιχείο σε μια ομάδα επάγει με φυσικό τρόπο έναν αυτομορφισμό της G.

Λήμμα 6.3.13. *Για κάθε $g \in G$, η απεικόνιση*

$$\iota_g : G \longrightarrow G, \quad \iota_g(x) = gxg^{-1}$$

είναι ένας αυτομορφισμός της G.

Απόδειξη. Η απεικόνιση ι_g είναι ομομορφισμός, διότι, για τυχόντα στοιχεία $x, y \in G$, έχουμε:

$$\iota_g(xy) = gxyg^{-1} = gxeyg^{-1} = gxg^{-1}gyg^{-1} = \iota_g(x)\iota_g(y)$$

Η απεικόνιση ι_g είναι μονομορφισμός διότι

$$\mathsf{Ker}(\iota_g) = \{x \in G \mid \iota_g(x) = e\} = \{x \in G \mid gxg^{-1} = e\} = \{x \in G \mid x = g^{-1}g = e\} = \{e\}$$

Τέλος, η απεικόνιση ι_g είναι επιμορφισμός, διότι

$$\forall y \in G: \quad \iota_g(g^{-1}yg_{=}g(g^{-1}yg)g^{-1} = (gg^{-1})y(gg^{-1}) = eye = y$$ ■

Το παραπάνω Λήμμα ξεχωρίζει μια ιδιαίτερη κλάση αυτομορφισμών μιας ομάδας, αυτών που επάγονται μέσω συζυγίας από τα στοιχεία της G. Έτσι οδηγούμαστε φυσιολογικά στην ακόλουθη έννοια.

Ορισμός 6.3.14. *Ένας αυτομορφισμός της G καλείται* **εσωτερικός αυτομορφισμός** *αν είναι της μορφής ι_g για κάποιο $g \in G$, δηλαδή αν είναι της μορφής*

$$\iota_g : G \longrightarrow G, \quad \iota_g(x) = gxg^{-1}$$

Το σύνολο όλων των εσωτερικών αυτομορφισμών της G συμβολίζεται με:

$$\mathsf{Inn}(G) = \{f : G \longrightarrow G \mid f : \text{εσωτερικός αυτομορφισμός της } G\} = \{\iota_g \in \mathsf{Aut}(G) \mid g \in G\}$$

Ένας αυτομορφισμός της G καλείται **εξωτερικός αυτομορφισμός** *αν δεν είναι εσωτερικός αυτομορφισμός.*

Θεώρημα 6.3.15. *Το υποσύνολο $\mathsf{Inn}(G)$ είναι μια κανονική υποομάδα της $\mathsf{Aut}(G)$. Επιπλέον η απεικόνιση*

$$\Phi : G \longrightarrow \mathsf{Aut}(G), \quad g \longmapsto \Phi(g) := \iota_g, \quad \text{όπου} \quad \iota_g : G \longrightarrow G, \ \iota_g(x) = gxg^{-1}$$

είναι ένας ομομορφισμός ομάδων, και:

$$\mathsf{Ker}(\iota) = \mathsf{Z}(G) \qquad \text{και} \qquad \mathsf{Im}(\iota) = \mathsf{Inn}(G)$$

Επομένως έχουμε έναν ισομορφισμό ομάδων:

$$G/\mathsf{Z}(G) \xrightarrow{\cong} \mathsf{Inn}(G)$$

Απόδειξη. Προφανώς $\mathsf{Inn}(G) \neq \emptyset$ διότι, για παράδειγμα, $\iota_e = \mathrm{Id}_G \in \mathsf{Inn}(G)$. Έστω ι_{g_1} και ι_{g_2} δύο εσωτερικοί αυτομορφισμοί της G. Τότε για κάθε $x \in G$ θα έχουμε:

$$(\iota_{g_1} \circ \iota_{g_2})(x) = \iota_{g_1}(\iota_{g_2}(x)) = \iota_{g_1}(g_2xg_2^{-1}) = g_1(g_2xg_2^{-1})g_1^{-1} = (g_1g_2)x(g_2^{-1}g_1^{-1}) = (g_1g_2)x(g_1g_2)^{-1} = \iota_{g_1g_2}(x)$$

Επομένως θα έχουμε $\iota_{g_1} \circ \iota_{g_2} = \iota_{g_1g_2} \in \mathsf{Inn}(G)$. Επιπλέον, $\forall g, x \in G$ θα έχουμε:

$$\iota_g^{-1}(x) = y \implies x = \iota_g(y) = gyg^{-1} \implies y = g^{-1}xg = g^{-1}x(g^{-1})^{-1} = \iota_{g^{-1}}(x)$$

Άρα $\iota_g^{-1} = \iota_{g^{-1}} \in \mathsf{Inn}(G)$. Επομένως το υποσύνολο $\mathsf{Inn}(G)$ είναι μια υποομάδα της $\mathsf{Aut}(G)$.

Θα δείξουμε ότι $\mathsf{Inn}(G) \trianglelefteq \mathsf{Aut}(G)$. Δηλαδή θα δείξουμε ότι για κάθε $f \in \mathsf{Aut}(G)$ και για κάθε $\iota_g \in \mathsf{Inn}(G)$, όπου $g \in G$, ο αυτομορφισμός $f \circ \iota_g \circ f^{-1}$ είναι εσωτερικός. Για κάθε στοιχείο $x \in G$ θα έχουμε:

$$(f \circ \iota_g \circ f^{-1})(x) = f(\iota_g(f^{-1}(x)) = f(gf^{-1}(x)g^{-1}) = f(g)f(f^{-1}(x))f(g^{-1}) = f(g)xf(g)^{-1} = \iota_{f(g)}(x)$$

Άρα $f \circ \iota_g \circ f^{-1} = \iota_{f(g)} \in \mathsf{Inn}(G)$, και επομένως $\mathsf{Inn}(G) \trianglelefteq \mathsf{Aut}(G)$.

Θεωρούμε απεικόνιση

$$\Phi : G \longrightarrow \mathsf{Aut}(G), \quad \Phi(g) := \iota_g, \quad \text{όπου} \quad \iota_g : G \longrightarrow G, \ \iota_g(x) = gxg^{-1}$$

της οποίας η εικόνα είναι $\mathsf{Im}(\Phi) = \mathsf{Inn}(G)$. Χρησιμοποιώντας ότι, όπως δείξαμε παραπάνω, $\iota_{g_1} \circ \iota_{g_2} = \iota_{g_1g_2}$, θα έχουμε:

$$\Phi(g_1g_2) = \iota_{g_1g_2} = \iota_{g_1} \circ \iota_{g_2} = \Phi(g_1) \circ \Phi(g_2)$$

και άρα η απεικόνιση Φ είναι ομομορφισμός ομάδων. Για τον πυρήνα της Φ θα έχουμε:

$$\mathsf{Ker}(\Phi) = \{g \in G \mid \Phi(g) = \iota_G\} = \{g \in G \mid \Phi(g)(x) = x\} = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = \mathsf{Z}(G)$$

Τέλος, από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε έναν ισομορφισμό ομάδων:

$$G/\mathsf{Z}(G) \xrightarrow{\cong} \mathsf{Inn}(G)$$ ■

Η ομάδα πηλίκο

$$\mathsf{Aut}(G)/\mathsf{Inn}(G) := \mathsf{Out}(G)$$

καλείται η **ομάδα των εξωτερικών αυτομορφισμών** της G.

Παρατήρηση 6.3.16. Ποιες ομάδες έχουν τετριμμένη ομάδα εσωτερικών αυτομορφισμών; Η απάντηση είναι εύκολη:

$$\mathsf{Inn}(G) = \{\iota_G\} \iff \text{η } G \text{ είναι αβελιανή}$$

Πράγματι, αν η G είναι αβελιανή, τότε $\mathsf{Z}(G) = G$, άρα η ομάδα $G/\mathsf{Z}(G)$ είναι τετριμμένη, και τότε ο ισομορφισμός του Θεωρήματος 6.3.15 δείχνει ότι $\mathsf{Inn}(G) = \{\iota_G\}$. Αντίστροφα, αν αυτό ισχύει, τότε η ομάδα $G/\mathsf{Z}(G)$ είναι τετριμμένη και αυτό σημαίνει ότι $\mathsf{Z}(G) = G$, δηλαδή η ομάδα G είναι αβελιανή. ▲

Πότε η ομάδα εσωτερικών αυτομορφισμών είναι κυκλική; Την απάντηση δίνει το ακόλουθο πόρισμα.

Πόρισμα 6.3.17. *Αν G είναι μια ομάδα, τότε:*

$$\eta\ \mathsf{Inn}(G)\ \textit{είναι κυκλική}\ \big(\textit{και τότε}\ \mathsf{Inn}(G) = \{\iota_G\}\big) \iff \eta\ G\ \textit{είναι αβελιανή}$$

Απόδειξη. Χρησιμοποιούμε τον ισομορφισμό $G/\mathsf{Z}(G) \cong \mathsf{Inn}(G)$. Όπως και πριν, αν η G είναι αβελιανή, τότε $\mathsf{Inn}(G) = \{\iota_G\}$, και άρα η $\mathsf{Inn}(G)$ είναι κυκλική. Αντίστροφα, αν η $\mathsf{Inn}(G)$, ισοδύναμα η $G/\mathsf{Z}(G)$, είναι κυκλική, τότε από την Πρόταση 6.1.13 έπεται ότι η G είναι αβελιανή. ■

6.4 Η Ομάδα Ομομορφισμών μιας Κυκλικής Ομάδας

Στην παρούσα ενότητα θα μελετήσουμε ομομορφισμούς μεταξύ κυκλικών ομάδων και θα περιγράψουμε πλήρως την ομάδα ομομορφισμών μεταξύ δύο κυκλικών ομάδων, καθώς και την ομάδα αυτομορφισμών μιας κυκλικής ομάδας. Λαμβάνοντας υπόψη ότι, όπως αποδεικνύεται με περισσότερο προχωρημένες μεθόδους από όσες μπορούμε να αναλύσουμε εδώ, κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι ισόμορφη με το ευθύ γινόμενο πεπερασμένου πλήθους κυκλικών ομάδων, οι υπολογισμοί μας μπορούν να προσδιορίσουν την ομάδα ομομορφισμών μεταξύ δύο τυχαίων πεπερασμένα παραγόμενων αβελιανών ομάδων.

6.4.1 Ομάδες Ομομορφισμών Κυκλικών Ομάδων

Στην παρούσα υποενότητα θα μελετήσουμε ομομορφισμούς μεταξύ κυκλικών ομάδων και θα περιγράψουμε πλήρως την ομάδα ομομορφισμών μεταξύ δύο κυκλικών ομάδων, πεπερασμένων ή άπειρων.

Πρόταση 6.4.1. *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα, και έστω $f : G \longrightarrow G$ μια απεικόνιση. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η f είναι ένας ενδομορφισμός της G.*
2. *Υπάρχει σταθερός ακέραιος $k \in \mathbb{Z}$:*
$$\forall g \in G: \quad f(g) = g^k$$

Απόδειξη. 2. $\Longrightarrow$ 1. Δείχνουμε ότι η απεικόνιση $f(g) = g^k$ είναι ομομορφισμός. Επειδή η G είναι αβελιανή, θα έχουμε:

$$f(g_1 g_2) = (g_1 g_2)^k = g_1^k g_2^k = f(g_1) f(g_2)$$

και άρα η f είναι ομομορφισμός ομάδων, δηλαδή η f είναι ένας ενδομορφισμός της G.

1. $\Longrightarrow$ 2. Έστω ότι η f είναι ενδομορφισμός. Τότε $f(a) \in G = \langle a \rangle$ και άρα υπάρχει $k \in \mathbb{Z}$ έτσι ώστε: $f(a) = a^k$. Θα δείξουμε ότι $f(g) = g^k$, $\forall g \in G$. Θα έχουμε $g = a^r$ για κάποιο $r \in \mathbb{Z}$. Χρησιμοποιώντας ότι η f είναι ενδομορφισμός, θα έχουμε:

$$f(g) = f(a^r) = f(a)^r = (a^k)^r) = a^{kr} = (a^r)^k = g^k$$ ■

Παρατήρηση 6.4.2. Σημειώνουμε ότι, αν η G είναι άπειρη κυκλική, τότε το $k \in \mathbb{Z}$ στην Πρόταση 6.4.1 είναι μοναδικό διότι, αν $f(a) = a^l$, τότε $a^k = a^l$ και άρα $a^{k-l} = e$ το οποίο σημαίνει ότι $k = l$ διότι το a έχει άπειρη τάξη.

Αν η G είναι πεπερασμένη κυκλική, με τάξη n, τότε θα έχουμε αν $f(a) = a^l = a^k$, τότε $a^{k-l} = e$ και άρα $o(a) = n \mid k-l$ το οποίο σημαίνει ότι $[k]_n = [l]_n$, δηλαδή το k είναι μοναδικό mod n. ▲

Συμβολισμός 6.4.3. Αν G και G' είναι δύο ομάδες, τότε συμβολίζουμε με

$$\mathsf{Hom}(G, G') = \{f : G \longrightarrow G' \mid f : \text{ ομομορφισμός}\}$$

το σύνολο όλων των ομομορφισμών από την G στην G'.

Αν $G = G'$, τότε συμβολίζουμε με:

$$\mathsf{End}(G) = \mathsf{Hom}(G, G)$$

το σύνολο όλων των ενδομορφισμών της G.

Σκοπός μας είναι να προσδιορίσουμε την δομή του συνόλου $\mathsf{Hom}(G, H)$ των ομομορφισμών μεταξύ κυκλικών ομάδων G και H. Γενικά το σύνολο $\mathsf{Hom}(G, H)$ των ομομορφισμών μεταξύ ομάδων G και H δεν έχει δομή ομάδας. Η επόμενη Πρόταση δείχνει ότι, όταν η ομάδα H είναι αβελιανή, τότε το σύνολο $\mathsf{Hom}(G, H)$ μπορεί να εφοδιαστεί με δομή ομάδας.

Πρόταση 6.4.4. *Έστω ότι $(G, \circ)$ και $(G', \cdot)$ είναι δύο ομάδες, και υποθέτουμε ότι η G' είναι αβελιανή.*

1. *Το σύνολο $\mathsf{Hom}(G, G')$ αποτελεί αβελιανή ομάδα με πράξη:*

$$\star : \mathsf{Hom}(G, G') \times \mathsf{Hom}(G, G') \longrightarrow \mathsf{Hom}(G, G'), \quad (f, g) \longmapsto f \star g : G \longrightarrow G', \quad (f \star g)(x) = f(x) \cdot g(x)$$

2. *Το ουδέτερο στοιχείο της $\mathsf{Hom}(G, G')$ είναι ο ομομορφισμός*

$$\epsilon : G \longrightarrow G', \quad x \longmapsto \epsilon(x) = e_{G'}$$

3. *Το αντίστροφο στοιχείο του ομομορφισμού $f \in \mathsf{Hom}(G, G')$ είναι ο ομομορφισμός*

$$\widetilde{f} : G \longrightarrow G, \quad x \longmapsto \widetilde{f}(x) = f(x)^{-1}$$

Απόδειξη. 1. Η πράξη $\star$ είναι καλά ορισμένη, δηλαδή, $\forall f, g \in \mathsf{Hom}(G, G')$: $f \star g \in \mathsf{Hom}(G, G')$.

Πράγματι, έστω $x, y \in G$. Τότε θα έχουμε:

$$(f \star g)(x \circ y) = f(x \circ y) \cdot g(x \circ y) = f(x) \cdot f(y) \cdot g(x) \cdot g(y) = f(x) \cdot g(x) \cdot f(y) \cdot g(y) = (f \star g)(x) \cdot (f \star g)(y)$$

και άρα η απεικόνιση $f \star g$ ανήκει στο σύνολο $\mathsf{Hom}(G, G')$.

2. Προσεταιριστικότητα: Έστω $f, g, h : G \longrightarrow G'$. Τότε $\forall x \in G$:

$$[f \star (g \star h)](x) = f(x) \cdot (g \star h)(x) = f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) = ((f \star g)(x)) \cdot h(x) = [(f \star g) \star h](x)$$

Επομένως $f \star (g \star h) = (f \star g) \star h$ και η πράξη «$\star$» είναι προσεταιριστική στο σύνολο $\mathsf{Hom}(G, G')$.

3. Ύπαρξη Ουδέτερου Στοιχείου: Έστω $f : G \longrightarrow G'$. Τότε $\forall x \in G$:

$$(f \star \epsilon)(x) = f(x) \cdot \epsilon(x) = f(x) \cdot e_{G'} = f(x) = e_{G'} \cdot f(x) = \epsilon(x) \cdot f(x) = (\epsilon \star f)(x)$$

και άρα: $f \star \epsilon = f = \epsilon \star f$. Δηλαδή ο τετριμμένος ομομορφισμός $\epsilon \in \mathsf{Hom}(G, G')$ είναι ουδέτερο στοιχείο για την πράξη «$\star$».

4. Ύπαρξη Αντίστροφου Στοιχείου: Έστω $f: G \longrightarrow G'$. Δείχνουμε πρώτα ότι η απεικόνιση $\widetilde{f}: G \longrightarrow G$, $\widetilde{f}(x) = f(x)^{-1}$, $\forall x \in G$, είναι ομομορφισμός ομάδων. Πραγματικά, χρησιμοποιώντας ότι η f είναι ομομορφισμός και ότι η G' είναι αβελιανή, θα έχουμε:

$$\widetilde{f}(x \circ y) = f(x \circ y)^{-1} = (f(x) \cdot f(y))^{-1} = f(y)^{-1} \cdot f(x)^{-1} = f(x)^{-1} \cdot f(y)^{-1} = \widetilde{f}(x) \cdot \widetilde{f}(y)$$

επομένως η $\widetilde{f}$ είναι ομομορφισμός ομάδων και άρα $\widetilde{f} \in \mathsf{Hom}(G, G')$.

Επιπρόσθετα $\forall x \in G$:

$$(f \star \widetilde{f})(x) = f(x) \cdot \widetilde{f}(x) = f(x) \cdot f(x)^{-1} = e_{G'} = \epsilon(x) = e_{G'} = f(x)^{-1} \cdot f(x) = \widetilde{f}(x) \cdot f(x) = (\widetilde{f} \star f)(x)$$

και επομένως $f \star \widetilde{f} = \epsilon = \widetilde{f} \star f$. Δηλαδή ο ομομορφισμός $\widetilde{f}$ είναι το αντίστροφο στοιχείο του ομομορφισμού f για την πράξη «$\star$» στο σύνολο $\mathsf{Hom}(G, G')$.

5. Μεταθετικότητα: Έστω $f, g \in \mathsf{Hom}(G, G')$. Τότε $\forall x \in G$:

$$(f \star g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \star f)(x)$$

και επομένως $f \star g = g \star f$, δηλαδή η πράξη «$\star$» στο σύνολο $\mathsf{Hom}(G, G')$ είναι μεταθετική. ■

Παράδειγμα 6.4.5. Από την προηγούμενη Πρόταση 6.4.4 έπεται ότι, αν G, H είναι αβελιανές ομάδες, τότε το σύνολο ομομορφισμών $\mathsf{Hom}(G, H)$ αποτελεί μια αβελιανή ομάδα. Επειδή κάθε κυκλική ομάδα είναι αβελιανή, έπεται ιδιαίτερα ότι, $\forall n, m \geq 1$, τα σύνολα:

$$\mathsf{End}(\mathbb{Z}) = \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}), \quad \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}_n), \quad \mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}), \quad \mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$$

είναι αβελιανές ομάδες. Όλες οι παραπάνω ομάδες είναι προσθετικές. Έτσι η δομή αβελιανής ομάδας σε καθένα από τα παραπάνω σύνολα αποκτάται μέσω της ακόλουθης πράξης πρόσθεσης ομομορφισμών

$$(f + g)(x) = f(x) + g(x)$$

όπου f και g είναι ομομορφισμοί οι οποίοι ανήκουν σε ένα από τα παραπάνω τέσσερα σύνολα, και x ανήκει στο πεδίο ορισμού τους. √

Το κεντρικό αποτέλεσμα της παρούσας υποενότητας είναι το ακόλουθο Θεώρημα, το οποίο δείχνει ότι οι ομάδες ομομορφισμών μεταξύ κυκλικών ομάδων είναι κυκλικές και επιπρόσθετα δίνει την ακριβή κλάση ισομορφίας τους.

Θεώρημα 6.4.6. *Υπάρχουν ισομορφισμοί ομάδων:*

1. $$\mathsf{Hom}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{\cong} \mathbb{Z}$$
2. $$G \text{ πεπερασμένη αβελιανή ομάδα } (\text{ιδιαίτερα αν } G = \mathbb{Z}_n) \implies \mathsf{Hom}(G, \mathbb{Z}) \xrightarrow{\cong} \{e\}$$
3. $$\mathsf{Hom}(\mathbb{Z}, \mathbb{Z}_n) \xrightarrow{\cong} \mathbb{Z}_n$$
4. $$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \mathbb{Z}_{(n,m)}$$

Απόδειξη. 1. Ορίζουμε απεικονίσεις

$$\Phi : \mathsf{Hom}(\mathbb{Z},\mathbb{Z}) \longrightarrow \mathbb{Z}, \quad \Phi(f) = f(1)$$

$$\Psi : \mathbb{Z} \longrightarrow \mathsf{Hom}(\mathbb{Z},\mathbb{Z}), \quad \Psi(n) = f_n$$

όπου

$$f_n : \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f_n(m) = nm$$

Από την Πρόταση 6.4.1, έπεται ότι η απεικόνιση f_n είναι ενδομορφισμός της ομάδας $(\mathbb{Z},+)$, $\forall n \in \mathbb{Z}$. Δείχνουμε ότι οι απεικονίσεις Φ και Ψ είναι ισομορφισμοί και $\Psi = \Phi^{-1}$.

(α) Θα έχουμε:

$$\forall n \in \mathbb{Z}: \quad \Phi\Psi(n) = \Phi(f_n) = f_n(1) = n1 = n \implies \Phi\Psi = \mathrm{Id}_{\mathbb{Z}}$$

$$\forall f \in \mathsf{Hom}(\mathbb{Z},\mathbb{Z}): \quad \Psi\Phi(f) = \Psi(f(1)) = f_{f(1)}$$

$$\text{όμως } \forall m \in \mathbb{Z}: \quad f_{f(1)}(m) = f(1)m = mf(1) = f(1m) = f(m) \implies f_{f(1)} = f \implies \Psi\Phi(f) = f$$

Επομένως:

$$\Psi\Phi = \mathrm{Id}_{\mathsf{Hom}(\mathbb{Z},\mathbb{Z})}$$

Άρα οι απεικονίσεις Φ και Ψ είναι «1-1» και «επί» και $\Phi = \Psi^{-1}$.

(β) Δείχνουμε ότι η Φ είναι ομομορφισμός ομάδων:

$$\Phi(f+g) = (f+g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

Άρα η Φ είναι ισομορφισμός αβελιανών ομάδων με αντίστροφο τον ομομορφισμό Ψ.

2. Έστω G μια πεπερασμένη αβελιανή (πολλαπλασιαστική) ομάδα. Τότε κάθε στοιχείο της G θα έχει πεπερασμένη τάξη:

$$\forall a \in G, \ \exists n \geq 1: \quad a^n = e$$

Αν $f \in \mathsf{Hom}(G,\mathbb{Z})$ είναι ένας ομομορφισμός, τότε:

$$\forall a \in G: \ 0 = f(e) = f(a^n) = nf(a) \implies n = 0 \ \text{ή} \ f(a) = 0 \implies f(a) = 0$$

Άρα ο μοναδικός ομομορφισμός $f \in \mathsf{Hom}(G,\mathbb{Z})$ είναι ο τετριμμένος $f = \varepsilon : G \longrightarrow \mathbb{Z}$, $\varepsilon(a) = 0$, ο οποίος είναι το ταυτοτικό στοιχείο της αβελιανής ομάδας $\mathsf{Hom}(G,\mathbb{Z})$. Επομένως

$$\mathsf{Hom}(G,\mathbb{Z}) = \{\varepsilon\} \xrightarrow{\cong} \{e\}$$

3. Ορίζουμε απεικονίσεις

$$\Phi : \mathsf{Hom}(\mathbb{Z},\mathbb{Z}_n) \longrightarrow \mathbb{Z}_n, \quad \Phi(f) = [f(1)]_n$$

Επειδή $\Phi(f+g) = (f+g)(1) = f(1)+g(1) = \Phi(f)+\Phi(g)$, έπεται ότι η Φ είναι ομομορφισμός ομάδων. Επιπλέον η Φ είναι μονομορφισμός διότι:

$$\Phi(f) = [0]_n \implies f(1) = [0]_n \quad \text{και τότε} \quad \forall m \in \mathbb{Z}: \ f(m) = f(m1) = mf(1) = m[0]_n = [m0]_n = [0]_n$$

Επομένως ο ομομορφισμός f είναι ο τετριμμένος $f = \varepsilon : G \longrightarrow \mathbb{Z}$, $\varepsilon(a) = 0$, ο οποίος είναι το ταυτοτικό στοιχείο της αβελιανής ομάδας $\mathsf{Hom}(\mathbb{Z},\mathbb{Z}_n)$. Αυτό σημαίνει ότι ο ομομορφσιμός Φ είναι μονομορφισμός.

Μένει να δείξουμε ότι ο μονομορφισμός Φ είναι επιμορφισμός. Έστω $[k]_n \in \mathbb{Z}_n$. Ορίζουμε μια απεικόνιση

$$f_{[k]_n} : \mathbb{Z} \longrightarrow \mathbb{Z}_n, \quad f_{[k]_n}(m) = [km]_n$$

Τότε η απεικόνιση $f_{[k]_n}$ είναι ομομορφισμός, διότι:

$$f_{[k]_n}(m_1+m_2) = [k(m_1+m_2)]_n = [km_1+km_2]_n = [km_1]_n + [km_2]_n = f_{[k]_n}(m_1) + f_{[k]_n}(m_2)$$

Επιπλέον:

$$\Phi(f_{[k]_n}) = f_{[k]_n}(1) = [k1]_n = [k]_n \implies \Phi: \text{ επιμορφισμός}$$

Άρα η απεικόνιση Φ είναι ισομορφισμός ομάδων και επομένως

$$\mathsf{Hom}(\mathbb{Z}, \mathbb{Z}_n) \xrightarrow{\cong} \mathbb{Z}_n$$

4. Η απόδειξη ύπαρξης ισομορφισμού

$$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \mathbb{Z}_{(n,m)}$$

χρειάζεται αρκετή προεργασία και θα δοθεί μετά την απόδειξη των τεσσάρων παρακάτω προκαταρκτικών αποτελεσμάτων τα οποία είναι ενδιαφέροντα από μόνα τους. ■

Λήμμα 6.4.7. *Έστω $n, m \geq 1$, και υποθέτουμε ότι: $(n, m) = 1$. Τότε υπάρχει ένας ισομορφισμός:*

$$\mathbb{Z}_{nm} \xrightarrow{\cong} \mathbb{Z}_n \times \mathbb{Z}_m$$

Απόδειξη. Από το Θεώρημα 4.1.16 προκύπτει ότι επειδή $(n, m) = 1$, η ομάδα ευθύ γινόμενο $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι κυκλική. Επομένως, επειδή κυκλικές ομάδες με την ίδια τάξη είναι ισόμορφες και επειδή η τάξη της $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι nm, έπεται ότι η ομάδα $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{nm}$. ■

Λήμμα 6.4.8. *Έστω $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ η ανάλυση του φυσικού αριθμού $n > 1$ σε γινόμενο δυνάμεων διακεκριμένων πρώτων αριθμών. Τότε υπάρχει ένας ισομορφισμός ομάδων:*

$$\mathbb{Z}_n \xrightarrow{\cong} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

Απόδειξη. Επειδή $(p_i^{a_i}, p_j^{a_j}) = 1$, $1 \leq i \neq j \leq k$, ο ισχυρισμός έπεται εύκολα από το Λήμμα 6.4.7 με χρήση της Αρχής Μαθηματικής Επαγωγής. ■

Λήμμα 6.4.9. *Έστω p, q δύο διαφορετικοί πρώτοι αριθμοί. Τότε για κάθε $k, l \geq 1$:*

$$\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{q^l}) \xrightarrow{\cong} \{e\}$$

Απόδειξη. Έστω $f: \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{q^l}$ ένας ομομορφισμός. Αν $[x]_{p^k} \in \mathbb{Z}_{p^k}$, τότε $p^k[x]_{p^k} = [0]_{p^k}$ και θα έχουμε $f(p^k[x]_{p^k}) = p^k f([x]_{p^k}) = [0]_{q^l}$. Αυτό σημαίνει ότι $\mathsf{o}(f([x]_{p^k})) \mid p^k$. Όμως ο αριθμός $\mathsf{o}(f([x]_{p^k}))$ θα διαιρεί την τάξη q^l της ομάδας $\mathbb{Z}_{q^l}$ και άρα θα είναι μια δύναμη του q, έστω $\mathsf{o}(f([x]_{p^k})) = q^a$. Τότε $q^a \mid p^k$, και επειδή οι p, q είναι διαφορετικοί πρώτοι αριθμοί, θα έχουμε $q^a = 1 = \mathsf{o}(f([x]_{p^k}))$, δηλαδή $f([x]_{p^k}) = [0]_{q^l}$. Έτσι ο τυχόν ομομορφισμός f στέλνει κάθε στοιχείο της ομάδας $\mathbb{Z}_{p^k}$ στο μηδενικό στοιχείο της ομάδας $\mathbb{Z}_{q^l}$. Αυτό σημαίνει ότι ο f είναι ο τετριμμένος ομομορφισμός και άρα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{q^l}) = \{e\}$. ■

Λήμμα 6.4.10. *Έστω ότι $G = \langle a \rangle$ και $H = \langle b \rangle$ είναι δύο κυκλικές ομάδες, και υποθέτουμε ότι η G είναι πεπερασμένη. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Υπάρχει ομομορφισμός $f: G \longrightarrow H$ έτσι ώστε $f(a) = b$.*
2. *$\mathsf{o}(b) \mid \mathsf{o}(a)$.*

Αν $\mathsf{o}(b) \mid \mathsf{o}(a)$, τότε υπάρχει μοναδικός ομομορφισμός $f: G \longrightarrow H$ έτσι ώστε: $f(a^k) = b^k$, $\forall k \in \mathbb{Z}$.

Απόδειξη. Υποθέτουμε ότι $\mathsf{o}(G) = \mathsf{o}(a) = n$, και άρα $G = \{e, a, a^2, \cdots a^{n-1}\}$.

1. $\Longrightarrow$ 2. Έστω $f : G \longrightarrow H$ ένας ομομορφισμός έτσι ώστε $f(a) = b$. Τότε $a^n = e$ και άρα $b^n = f(a)^n = f(a^n) = f(e) = e$. Επομένως $\mathsf{o}(b) \mid n = \mathsf{o}(a)$.

2. $\Longrightarrow$ 1. Έστω $\mathsf{o}(b) \mid n = \mathsf{o}(a)$, και $n = mk$, όπου $m = \mathsf{o}(b)$. Ορίζουμε απεικόνιση

$$f : \langle a \rangle \longrightarrow \langle b \rangle, \quad f(a^k) = b^k$$

Προφανώς η απεικόνιση f είναι ένας καλά ορισμένος ομομορφισμός και ισχύει $f(a) = b$.

Αν $g : \langle a \rangle \longrightarrow \langle b \rangle$, είναι ένας άλλος ομομορφισμός έτσι ώστε $g(a) = b$, τότε θα έχουμε $g(a^k) = g(a)^k = b^k = f(a)^k = f(a^k)$ και επομένως $f = g$. ■

Λήμμα 6.4.11. *Έστω p ένας πρώτος αριθμός. Τότε για κάθε $k, l \geq 1$:*

$$\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l}) \xrightarrow{\cong} \mathbb{Z}_{p^{\min\{k,l\}}}$$

Απόδειξη. Έστω $a = [1]_{p^k}$ και $b = [1]_{p^l}$. Τότε

$$\mathbb{Z}_{p^k} = \langle a \rangle \quad \text{και} \quad \mathbb{Z}_{p^l} = \langle b \rangle$$

Θα δείξουμε ότι το πλήθος των διακεκριμένων ομομορφισμών $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ είναι $p^{\min\{k,l\}}$.

- Αν $k \geq l$, τότε $p^k \geq p^l$ και προφανώς $\mathsf{o}(b) = p^l \mid p^k = \mathsf{o}(a)$. Τότε από το Λήμμα 6.4.10, έπεται ότι υπάρχει (μοναδικός) ομομορφισμός $f : \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ έτσι ώστε $f(a) = b$. Παρατηρούμε ότι επειδή $k \geq l$, θα έχουμε $\min\{k, l\} = l$ και επομένως υπάρχουν l το πλήθος ομομορφισμοί $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ διότι το πλήθος των διαιρετών του p^k οι οποίοι είναι μικρότεροι ή ίσοι από το p^l και διάφοροι του 1 είναι ακριβώς l: $p, p^2, \cdots, p^l$.
- Αν $k \leq l$, τότε $\min\{k, l\} = k$ και κάθε ομομορφισμός $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ έχει προφανώς εικόνα στην (μοναδική) κυκλική υποομάδα τάξης p^k της $\mathbb{Z}_{p^l}$. Άρα το ζητούμενο πλήθος συμπίπτει με το πλήθος των ομομορφισμών $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^k}$. Από την πρώτη περίπτωση τότε θα έχουμε ότι το πλήθος αυτών των ομομορφισμών είναι ακριβώς $p^k = p^{\min\{k,l\}}$.

Άρα θα έχουμε:

$$\mathsf{o}(\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})) = p^{\min\{k,l\}}$$

Τέλος, από το Λήμμα 6.4.10, έπεται άμεσα ότι η απεικόνιση

$$\psi : \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}, \qquad \psi([r]_{p^k}) = p^{l-\min\{k,l\}}[r]_{p^l}$$

είναι ομομορφισμός ομάδων και μάλιστα επειδή η τάξη της ομάδας $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι $p^{\min\{k,l\}}$, ισχύει:

$$p^{\min\{k,l\}}\psi = \varepsilon \quad \text{όπου} \quad \varepsilon([x]_{p^k}) = [0]_{p^l}$$

δηλαδή ο ομομορφισμός ε είναι το ταυτοτικό στοιχείο της ομάδας $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$. Αν $n\psi = \varepsilon$, τότε θα έχουμε:

$$n\psi = \varepsilon \implies n\psi([1]_{p^k}) = \varepsilon([1]_{p^k}) \implies np^{l-\min\{k,l\}}[1]_{p^l} = [0]_{p^l} \implies [np^{l-\min\{k,l\}}]_{p^l} = [0]_{p^l} \implies$$

$$\implies p^l \mid np^{l-\min\{k,l\}} \implies np^{l-\min\{k,l\}} = p^l m \implies np^l = p^l p^{\min\{k,l\}} m \implies n = p^{\min\{k,l\}} m \implies$$

$$p^{\min\{k,l\}} \leq n$$

Επομένως

$$\mathsf{o}(\psi) = p^{\min\{k,l\}} = \mathsf{o}(\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l}))$$

και άρα η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ τάξης $p^{\min\{k,l\}}$ έχει ένα στοιχείο τάξης $p^{\min\{k,l\}}$. Επομένως η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι κυκλική τάξης $p^{\min\{k,l\}}$. Τότε από το Θεώρημα 4.1.21, η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{p^{\min\{k,l\}}}$. ■

Λήμμα 6.4.12. *Έστω ότι G, G_1, G_2, και H, H_1, H_2, είναι αβελιανές ομάδες.*

1. *Υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{Hom}(G_1 \times G_2, H) \xrightarrow{\cong} \mathsf{Hom}(G_1, H) \times \mathsf{Hom}(G_2, H)$$

2. *Υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{Hom}(G, H_1 \times H_2) \xrightarrow{\cong} \mathsf{Hom}(G, H_1) \times \mathsf{Hom}(G, H_2)$$

3. *Γενικότερα, έστω ότι $\{G_i\}_{i=1}^n$ και $\{H_j\}_{j=1}^m$ είναι αβελιανές ομάδες, και έστω*

$$G = G_1 \times G_2 \times \cdots \times G_n \qquad \text{και} \qquad H = H_1 \times H_2 \times \cdots \times H_m$$

οι αντίστοιχες ομάδες ευθύ γινόμενο. Τότε:

$$\mathsf{Hom}(G, H) \xrightarrow{\cong} \prod_{i=1}^{n} \prod_{j=1}^{m} \mathsf{Hom}(G_i, H_j)$$

δηλαδή:

$$\mathsf{Hom}(G, H) \xrightarrow{\cong} \mathsf{Hom}(G_1, H_1) \times \cdots \times \mathsf{Hom}(G_1, H_m) \times \cdots \times \mathsf{Hom}(G_n, H_1) \times \cdots \times \mathsf{Hom}(G_n, H_m)$$

Απόδειξη. 1. Ορίζουμε απεικόνιση

$$\Phi : \mathsf{Hom}(G_1 \times G_2, H) \longrightarrow \mathsf{Hom}(G_1, H) \times \mathsf{Hom}(G_2, H), \qquad \Phi(f) = (f_1, f_2)$$

όπου

$$f_1 : G_1 \longrightarrow H, \quad f_1(x_1) = f(x_1, e_{G_2}) \qquad \text{και} \qquad f_2 : G_2 \longrightarrow H, \quad f_2(x_2) = f(e_{G_1}, x_2)$$

Επίσης ορίζουμε απεικόνιση

$$\Psi : \mathsf{Hom}(G_1, H) \times \mathsf{Hom}(G_2, H) \longrightarrow \mathsf{Hom}(G_1 \times G_2, H), \qquad \Psi(g_1, g_2) = g$$

όπου

$$g : G_1 \times G_2 \longrightarrow H, \quad g(x_1, x_2) = g_1(x_1) + g_2(x_2)$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύει $\Psi = \Phi^{-1}$.

2. Ορίζουμε απεικόνιση

$$\Phi : \mathsf{Hom}(G, H_1 \times H_2) \longrightarrow \mathsf{Hom}(G, H_1) \times \mathsf{Hom}(G, H_2), \qquad \Phi(f) = (f_1, f_2)$$

όπου

$$f_i : G \longrightarrow H_i, \quad f_i = \pi_i \circ f$$

όπου

$$\pi_1 : H_1 \times H_2 \longrightarrow H_1, \quad \pi(h_1, h_2) = h_1 \qquad \text{και} \qquad \pi_2 : H_1 \times H_2 \longrightarrow H_2, \quad \pi(h_1, h_2) = h_2$$

είναι οι ομομορφισμοί προβολές από την ομάδα ευθύ γινόμενο στις ομάδες παράγοντες.

Επίσης ορίζουμε απεικόνιση

$$\Psi : \mathsf{Hom}(G, H_1) \times \mathsf{Hom}(G, H_2) \longrightarrow \mathsf{Hom}(G, H_1 \times H_2), \qquad \Psi(g_1, g_2) = g$$

όπου

$$g : G \longrightarrow H_1 \times H_2, \quad g(x) = (g_1(x), g_2(x))$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύει $\Psi = \Phi^{-1}$.

3. Υποθέτουμε πρώτα ότι $n=1$. Θα κατασκευάσουμε έναν ισομορφισμό

$$\Phi:\ \mathsf{Hom}(G_1, H_1\times\cdots\times H_m) \ \xrightarrow{\cong}\ \mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)$$

ως εξής:

$$\Phi(f)=(f_1,\cdots,f_m)\quad \text{όπου}\quad f_i=\pi_i\circ f$$

και όπου

$$\pi_i:\ H_1\times\cdots\times H_m\ \longrightarrow\ H_i,\quad \pi_i(h_1,\cdots,h_m)=h_i$$

είναι οι ομομορφισμοί προβολές από την ομάδα ευθύ γινόμενο στις ομάδες παράγοντες.

Αν $(f_1,\cdots,f_m)\in\mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)$, τότε ορίζουμε μια απεικόνιση

$$f:\ G_1\ \longrightarrow\ H_1\times\cdots\times H_m,\qquad f(x)=(f_1(x),\cdots,f_m(x))$$

η οποία με τη σειρά της ορίζει μια απεικόνιση

$$\Psi:\ \mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)\ \longrightarrow\ \mathsf{Hom}(G_1,H_1\times\cdots\times H_m),\quad \Psi(f_1,\cdots,f_m)=f$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύει ότι $\Psi=\Phi^{-1}$.

Άρα ο ισχυρισμός αληθεύει για $n=1$. Η γενική περίπτωση αποδεικνύεται εύκολα με χρήση της Αρχής Μαθηματικής Επαγωγής στο n, χρησιμοποιώντας το μέρος 1, και αφήνεται ως Άσκηση, βλέπε την Άσκηση 6.6.51. ■

Μπορούμε τώρα να ολοκληρώσουμε την απόδειξη του τελευταίου μέρους 4 του Θεωρήματος 6.4.6:

Απόδειξη του Θεωρήματος 6.4.6(4)**:** Αν $n=1$ ή $m=1$, τότε η ομάδα $\mathbb{Z}_n$, αντίστοιχα η $\mathbb{Z}_m$, είναι η τετριμμένη και τότε προφανώς και η ομάδα $\mathsf{Hom}(\mathbb{Z}_n,\mathbb{Z}_m)$ είναι η τετριμμένη. Επειδή $(n,m)=1$, θα έχουμε ότι η ομάδα $\mathbb{Z}_{(n,m)}$ είναι η τετριμμένη, και επομένως θα έχουμε έναν ισομορφισμό ομάδων $\mathsf{Hom}(\mathbb{Z}_n,\mathbb{Z}_m)\cong\mathbb{Z}_{(n,m)}$.

Υποθέτουμε ότι $n,m>1$ και έστω

$$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}\qquad\text{και}\qquad m=p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k}$$

οι αναλύσεις των φυσικών αριθμών n και m σε γινόμενο δυνάμεων διακεκριμένων πρώτων αριθμών. Γνωρίζουμε ότι ο μέγιστος κοινός διαιρέτης των m και n είναι:

$$(m,n)=p_1^{\min\{a_1,b_1\}}\cdot p_2^{\min\{a_1,b_2\}}\ \cdots\ p_k^{\min\{a_k,b_k\}}$$

Από το Λήμμα 6.4.8 υπάρχουν ισομορφισμοί:

$$\mathbb{Z}_n\ \xrightarrow{\cong}\ \mathbb{Z}_{p_1^{a_1}}\times\mathbb{Z}_{p_2^{a_2}}\times\cdots\times\mathbb{Z}_{p_k^{a_k}}\quad\text{και}\quad \mathbb{Z}_m\ \xrightarrow{\cong}\ \mathbb{Z}_{q_1^{b_1}}\times\mathbb{Z}_{p_2^{n_2}}\times\cdots\times\mathbb{Z}_{p_k^{b_k}}$$

Από το Λήμμα 6.4.12, θα έχουμε έναν ισομορφισμό

$$\mathsf{Hom}(\mathbb{Z}_n,\mathbb{Z}_m)\ \xrightarrow{\cong}\ \prod_{i=1}^{k}\prod_{j=1}^{l}\mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}},\mathbb{Z}_{q_j^{b_j}})$$

Από το Λήμμα 6.4.9 θα έχουμε ότι

$$\mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}},\mathbb{Z}_{p_j^{b_j}})=\{e\},\qquad \forall\, i\neq j$$

Επομένως επειδή από το Λήμμα 6.4.11 έχουμε

$$\mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}},\mathbb{Z}_{p_j^{b_j}})\ \xrightarrow{\cong}\ \mathbb{Z}_{p^{\min\{a_i,b_j\}}}$$

θα έχουμε τελικά:

$$\mathsf{Hom}(\mathbb{Z}_n,\mathbb{Z}_m)\ \xrightarrow{\cong}\ \mathsf{Hom}(\mathbb{Z}_{p_1^{a_1}},\mathbb{Z}_{p_1^{b_1}})\times\cdots\times\mathsf{Hom}(\mathbb{Z}_{p_k^{a_k}},\mathbb{Z}_{p_k^{b_k}})\ \xrightarrow{\cong}\ \mathbb{Z}_{p_1^{\min\{a_1,b_1\}}}\times\cdots\times\mathbb{Z}_{p_k^{\min\{a_k,b_k\}}}$$

και άρα μια τελευταία εφαρμογή του Λήμματος 6.4.8 δίνει:

$$\mathsf{Hom}(\mathbb{Z}_n,\mathbb{Z}_m)\ \xrightarrow{\cong}\ \mathbb{Z}_{p_1^{\min\{a_1,b_1\}}}\times\cdots\times\mathbb{Z}_{p_k^{\min\{a_k,b_k\}}}\ \xrightarrow{\cong}\ \mathbb{Z}_{p_1^{\min\{a_1,b_1\}}\cdots p_k^{\min\{a_k,b_k\}}}\ \xrightarrow{\cong}\ \mathbb{Z}_{(m,n)}$$ ■

6.4.2 Η Ομάδα Αυτομορφισμών μιας Κυκλικής Ομάδας

Στην παρούσα υποενότητα θα προσδιορίσουμε την ομάδα αυτομορφισμών μιας κυκλικής ομάδας.

Υπενθυμίζουμε ότι

$$\mathsf{Aut}(G) = \{f : G \longrightarrow G \mid f : \text{ισομορφισμός}\}$$

και το σύνολο $\mathsf{Aut}(G)$ αποτελεί ομάδα με πράξη τη σύνθεση αυτομορφισμών, η οποία είναι υποομάδα της ομάδας μεταθέσεων $\mathsf{S}(G)$.

Θα χρειαστούμε το ακόλουθο απλό βοηθητικό αποτέλεσμα.

Λήμμα 6.4.13. *Έστω G μια ομάδα και $a \in G$. Έστω $f : G \longrightarrow G$ ένας αυτομορφισμός της G.*

1. *Το στοιχείο a είναι γεννήτορας της G αν και μόνο αν το στοιχείο $f(a)$ είναι γεννήτορας της G:*

$$G = \langle a \rangle \quad \Longleftrightarrow \quad G = \langle f(a) \rangle$$

2. $\mathsf{o}(a) = \mathsf{o}(f(a))$.

Απόδειξη. Η απόδειξη είναι εύκολη και αφήνεται ως Άσκηση, βλέπε την Άσκηση 6.6.1. ■

Το ακόλουθο θεώρημα δείχνει ότι η ομάδα αυτομορφισμών μιας άπειρης κυκλικής ομάδας είναι κυκλική τάξης 2.

Θεώρημα 6.4.14. *Έστω $G = \langle a \rangle$ μια άπειρη κυκλική ομάδα. Τότε υπάρχει ένας ισομορφισμός*

$$\phi : \mathsf{Aut}(G) \xrightarrow{\cong} \mathbb{Z}_2$$

Απόδειξη. Έστω $G = \langle a \rangle$ ένας γεννήτορας της G. Τότε για κάθε αυτομορφισμό $f : G \longrightarrow G$ της G, το στοιχείο $f(a)$ είναι επίσης γεννήτορας της G. Επειδή η G είναι άπειρη κυκλική, γνωρίζουμε ότι η G έχει ακριβώς δύο γεννήτορες: το στοιχείο a και το στοιχείο a^{-1}. Έτσι $f(a) = a$ ή $f(a) = a^{-1}$. Επειδή $G = \langle a \rangle$, αν $f(a) = a$, έπεται ότι $f = \mathrm{Id}_G$, και αν $f(a) = a^{-1}$, τότε $f(x) = x^{-1}$, $\forall x \in G$.

Αντίστροφα οι απεικονίσεις Id_G και $\varphi : G \longrightarrow G, \varphi(x) = x^{-1}$ είναι προφανώς αυτομορφισμοί της G. Άρα $\mathsf{Aut}(G) = \{\mathrm{Id}_G, \varphi\}$, όπου άμεσα βλέπουμε ότι $\varphi^2 = \mathrm{Id}_G$. Επομένως η $\mathsf{Aut}(G)$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_2$, μέσω του ισομορφισμού $\mathrm{Id}_G \longmapsto [0]_2$ και $\varphi \longmapsto [1]_2$. ■

Πόρισμα 6.4.15. *Υπάρχει ένας ισομορφισμός ομάδων*

$$\phi : \mathsf{Aut}(\mathbb{Z}) \xrightarrow{\cong} \mathbb{Z}_2$$

Το ακόλουθο θεώρημα δείχνει ότι το πλήθος των αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας τάξης n δίνεται από την τιμή $\varphi(n)$ της συνάρτησης φ του Euler.

Θεώρημα 6.4.16. *Έστω $G = \langle a \rangle$ μια πεπερασμένη κυκλική ομάδα τάξης n. Τότε υπάρχει ένας ισομορφισμός*

$$\Phi : \mathsf{Aut}(G) \xrightarrow{\cong} \mathsf{U}(\mathbb{Z}_n)$$

Ιδιαίτερα: $\mathsf{o}\big(\mathsf{Aut}(G)\big) = \varphi(n)$.

Απόδειξη. Θα έχουμε

$$G = \langle a \rangle = \{e,\ a,\ a^2,\ \cdots,\ a^{n-1}\}$$

Αν $n = 1$, τότε $G = \{e\}$ και $\mathbb{Z}_1 = [0]_1$ και τότε προφανώς $\mathsf{Aut}(G) = \{\mathrm{Id}_G\} \cong \{\mathrm{Id}_{\mathbb{Z}_1}\} \cong \mathsf{U}(\mathbb{Z}_1)$.

Υποθέτουμε ότι $n > 1$. Έστω $f : G \longrightarrow G$ ένας αυτομορφισμός της G. Τότε το στοιχείο $f(a) \in G$ είναι γεννήτορας της G και άρα $f(a) = a^k$, για ένα μοναδικό στοιχείο k, όπου $1 \leq k \leq n-1$ και $(k, n) = 1$ (αν $k = 0$, τότε $f(a) = e$ και άρα $a = e$ διότι η f αυτομορφισμός, δηλαδή $G = \{e\}$, το οποίο είναι άτοπο).

Έτσι θα έχουμε $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, και επομένως μπορούμε να ορίσουμε μια απεικόνιση

$$\Phi\colon \mathsf{Aut}(G) \longrightarrow \mathsf{U}(\mathbb{Z}_n), \quad \Phi(f) = [k]_n, \qquad \text{όπου} \qquad f(a) = a^k$$

- Έστω $f, g \in \mathsf{Aut}(G)$ και έστω ότι $\Phi(f) = \Phi(g)$, δηλαδή: $[k]_n = [l]_n$, όπου $f(a) = a^k$ και $g(a) = a^l$. Τότε $n \mid k-l$ και επειδή $1 \leq k, l \leq n$ και $(k,n) = 1 = (l,n)$, έπεται ότι $k = l$. Επομένως $f(a) = g(a)$ και τότε προφανώς $f = g$, διότι, επειδή οι f, g είναι ομομορφισμοί και $\forall x \in G$, $x = a^m$, θα έχουμε: $f(x) = f(a^m) = f(a)^m = g(a)^m = g(a^m) = g(x)$. Επομένως η απεικόνιση Φ είναι «1-1».
- Έστω $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, δηλαδή $1 \leq k \leq n-1$ και $(k,n) = 1$. Ορίζουμε μια απεικόνιση

$$f_k\colon G \longrightarrow G, \quad f(a^m) = a^{km}$$

Η απεικόνιση f_k είναι ομομορφισμός, διότι:

$$f_k(a^{m_1}a^{m_2}) = f_k(a^{m_1+m_2}) = a^{(m_1+m_2)k} = a^{m_1k+m_2k} = a^{m_1k}a^{m_2k} = f_k(a^{m_1})f(a^{m_2})$$

Αν $f_k(a^m) = e$, τότε $a^{mk} = e$, και άρα $n \mid mk$. Επειδή $(k,n) = 1$, έπεται ότι $n \mid m$. Τότε όμως αναγκαστικά $m = 0$, διότι $0 \leq m \leq n-1$. Άρα $a^m = a^0 = e$ και ο ομομορφισμός f_k είναι μονομορφισμός. Τότε όμως ο ομομορφισμός f_k είναι αυτομορφισμός, διότι $\mathsf{o}(G) = n < \infty$. Τότε εξ ορισμού θα έχουμε $\Phi(f_k) = [k]_n$, διότι $f_k(a) = a^k$. Άρα η απεικόνιση Φ είναι «επί».

- Μένει να δείξουμε ότι η Φ είναι ομομορφισμός ομάδων. Έστω $f, g \in \mathsf{Aut}(G)$. Τότε θα έχουμε $\Phi(f) = a^k$, $g(a) = a^l$, όπου $f(a) = a^k$, $g(a) = a^l$, και $1 \leq k, l \leq n-1$ και $(k,n) = 1 = (l,n)$. Υποθέτουμε ότι $\Phi(f \circ g) = a^m$, όπου $1 \leq m \leq n-1$, $(n,m) = 1$, και $(f \circ g)(a) = a^m$. Όμως $(f \circ g)(a) = f(g(a)) = f(a^l) = f(a)^l = (a^k)^l = a^{kl}$. Τότε: $a^{kl} = a^m$ και επομένως $a^{kl-m} = e$. Επειδή $\mathsf{o}(a) = n$, θα έχουμε $n \mid kl - m$ και επομένως $[kl]_n = [m]_n$, δηλαδή: $[k]_k[l]_n = [m]_n$. Τότε:

$$\Phi(f \circ g) = [m]_n = [kl]_n = [k]_n[l]_n = \Phi(f)\Phi(g)$$

και άρα η απεικόνιση Φ είναι ομομορφισμός. Επομένως η Φ είναι ισομορφισμός ομάδων. ■

Πόρισμα 6.4.17. *Για κάθε $n \geq 1$, υπάρχει ένας ισομορφισμός ομάδων*

$$\phi : \mathsf{Aut}(\mathbb{Z}_n) \xrightarrow{\cong} \mathsf{U}(\mathbb{Z}_n)$$

Σε αντίθεση με την ομάδα αυτομορφισμών μιας άπειρης κυκλικής ομάδας, η οποία είναι κυκλική, η ομάδα αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας δεν είναι πάντα κυκλική.

Παράδειγμα 6.4.18. Θεωρούμε την κυκλική ομάδα $\mathbb{Z}_{12}$ τάξης 12. Τότε η ομάδα $\mathsf{U}(\mathbb{Z}_{12})$ των αντιστρέψιμων κλάσεων ισοτιμίας mod 12 έχει τάξη 4:

$$\mathsf{U}(\mathbb{Z}_{12}) = \{[1]_{12},\ [5]_{12},\ [7]_{12},\ [11]_{12}\}$$

και είναι ισόμορφη με την ομάδα των τεσσάρων στοιχείων του Klein διότι όλα τα μη ταυτοτικά στοιχεία της έχουν τάξη 2. Έτσι θα έχουμε έναν ισομορφισμό

$$\mathsf{U}(\mathbb{Z}_{12}) \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_2$$

Επομένως με βάση το Πόρισμα 6.4.17 θα έχουμε έναν ισομορφισμό

$$\mathsf{Aut}(\mathbb{Z}_{12}) \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_2$$

και άρα η ομάδα αυτομορφισμών $\mathsf{Aut}(\mathbb{Z}_{12})$ δεν είναι κυκλική. √

Παραθέτουμε χωρίς απόδειξη[3] το ακόλουθο βασικό αποτέλεσμα το οποίο περιγράφει την ομάδα αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας ως ευθύ γινόμενο κυκλικών ομάδων:

[3] Για μια απόδειξη βλέπε το βιβλίο [32].

Θεώρημα 6.4.19. *Έστω G μια κυκλική ομάδα τάξης*

$$n = 2^i p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}$$

όπου $p_1, p_2, \cdots, p_r$ είναι διακεκριμένοι περιττοί πρώτοι αριθμοί, και $i, j_1, j_2, \cdots, j_r \geq 0$.

Τότε:

$$\mathsf{Aut}(G) \xrightarrow{\cong} \begin{cases} \mathbb{Z}_1, & i = 0 \\ \mathbb{Z}_{2^{i-1}}, & i = 1 \text{ ή } 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{i-2}}, & i \geq 3 \end{cases} \times \mathbb{Z}_{p_1^{j_1-1}(p_1-1)} \times \mathbb{Z}_{p_2^{j_2-1}(p_2-1)} \times \cdots \times \mathbb{Z}_{p_r^{j_r-1}(p_r-1)} \quad \blacksquare$$

Υπενθυμίζουμε ότι οι γεννήτορες της ομάδας $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρέψιμων κλάσεων mod n, αν υπάρχουν, καλούνται **πρωταρχικές ρίζες** mod n, και διαδραματίζουν σημαντικό ρόλο στη Θεωρία Αριθμών. Επομένως η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ είναι κυκλική αν και μόνο αν υπάρχει μια πρωταρχική ρίζα mod n. Με βάση το Θεώρημα 6.4.19, έπεται το ακόλουθο Πόρισμα:[4]

Πόρισμα 6.4.20. *Έστω $n \geq 1$ ένας θετικός ακέραιος. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρέψιμων κλάσεων mod n είναι κυκλική, ισοδύναμα υπάρχουν πρωταρχικές ρίζες mod n.*
2. *Η ομάδα αυτομορφισμών $\mathsf{Aut}(\mathbb{Z}_n)$ της κυκλικής ομάδας $(\mathbb{Z}_n, +)$ είναι κυκλική.*
3. *$n = 2, 4, p^k, 2p^k$, όπου p είναι περιττός πρώτος.*

Αν ισχύει μια από τις παραπάνω ισοδύναμες συνθήκες, τότε υπάρχουν $\phi(\phi(n))$ πρωταρχικές ρίζες mod n. $\blacksquare$

6.5 Το Θεώρημα του Cayley

Υπενθυμίζουμε ότι για κάθε μη κενό σύνολο A, το σύνολο

$$\mathsf{S}(A) = \{\sigma : A \longrightarrow A \mid \sigma : \text{«1-1» και «επί»}\}$$

των «1-1» και «επί» απεικονίσεων από το σύνολο A στον εαυτό του αποτελεί μια ομάδα με πράξη τη σύνθεση απεικονίσεων. Η ομάδα $\mathsf{S}(A)$ καλείται η *συμμετρική ομάδα* επί του συνόλου A. Αν $A = \{1, 2, \cdots, n\}$, τότε

$$\mathsf{S}(A) = \mathsf{S}(\{1, 2, \cdots, n\}) = \mathsf{S}_n$$

είναι η n-οστή συμμετρική ομάδα.

6.5.1 Το Θεώρημα του Cayley

Το ακόλουθο σημαντικό Θεώρημα, το οποίο οφείλεται στον Cayley, πιστοποιεί ότι κάθε ομάδα G είναι ισόμορφη με μια *ομάδα μεταθέσεων*, δηλαδή με μια υποομάδα μιας συμμετρικής ομάδας. Με βάση το Θεώρημα του Cayley, η θεωρία ομάδων ανάγεται τυπικά στη θεωρία συμμετρικών ομάδων και των υποομάδων τους. Γενικά αυτή η παρατήρηση έχει μόνο θεωρητική σημασία, αλλά πολλές φορές έχει και πρακτική αξία, καθώς υπάρχουν σημαντικά πλεονεκτήματα όταν εργαζόμαστε με μεταθέσεις.

[4] Βλέπε το βιβλίο [28] για μια απόδειξη ότι υπάρχουν πρωταρχικές ρίζες mod n αν και μόνο αν $n = 2, 4, p^k, 2p^k$, όπου p είναι περιττός πρώτος.

Θεώρημα 6.5.1 (Θεώρημα Cayley (1854)). *Κάθε ομάδα $(G,\cdot)$ είναι ισόμορφη με μια υποομάδα μιας κατάλληλης ομάδας μεταθέσεων. Ιδιαίτερα αν η ομάδα G είναι πεπερασμένη με τάξη $|G| = n < \infty$, τότε η G είναι ισόμορφη με μια υποομάδα της συμμετρικής ομάδας S_n.*

Με άλλα λόγια, υπάρχει ένας μονομορφισμός ομάδων

$$\mathsf{L}_G : G \rightarrowtail \mathsf{S}(G)$$

και η ομάδα G είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L}_G) \leq \mathsf{S}(G)$:

$$\mathsf{L}_G : G \xrightarrow{\cong} \mathsf{Im}(\mathsf{L}_G) \leq \mathsf{S}(G)$$

Απόδειξη. Θεωρούμε την ομάδα μεταθέσεων

$$\mathsf{S}(G) = \{\sigma : G \longrightarrow G \mid \sigma : \text{«1 – 1» και «επί» απεικόνιση}\}$$

επί του συνόλου G εφοδιασμένη με την πράξη της σύνθεσης απεικονίσεων, και ορίζουμε απεικόνιση

$$\mathsf{L}_G : G \longrightarrow \mathsf{S}(G), \quad \mathsf{L}_G(g) = \mathsf{l}_g$$

όπου

$$\mathsf{l}_g : G \longrightarrow G, \qquad \mathsf{l}_g(x) = gx$$

Θα δείξουμε τον ισχυρισμό της εκφώνησης σε μια σειρά βημάτων:

1. *Για κάθε $g \in G$, η απεικόνιση $\mathsf{l}_g : G \longrightarrow G$ είναι «1-1» και «επί», δηλαδή είναι μια μετάθεση του συνόλου G:*

   $$\forall g \in G : \ \mathsf{L}_G(g) = \mathsf{l}_g \in \mathsf{S}(G)$$

   Πράγματι θα έχουμε:

   $$\mathsf{l}_g(x) = \mathsf{l}_g(y) \implies gx = gy \implies x = y \implies \mathsf{l}_g : \text{«1-1»}$$

   $$\forall y \in G : \ \mathsf{l}_g(g^{-1}y) = g(g^{-1}y) = gg^{-1}y = e_G y = y \implies \mathsf{l}_g : \text{«επί»}$$

   Επομένως, πράγματι η απεικόνιση L_G στέλνει την G στην ομάδα μεταθέσεων $\mathsf{S}(G)$.

2. *Η απεικόνιση $\mathsf{L}_G : G \longrightarrow \mathsf{S}(G)$ είναι ομομορφισμός ομάδων.*

   Πράγματι, θα έχουμε:

   $$\mathsf{L}_G(g_1 g_2) = \mathsf{l}_{g_1 g_2} \quad \text{και} \quad \mathsf{L}_G(g_1) \circ \mathsf{L}_G(g_2) = \mathsf{l}_{g_1} \circ \mathsf{l}_{g_2}$$

   Έτσι πρέπει να δείξουμε ότι οι απεικονίσεις $\mathsf{l}_{g_1 g_2}$ και $\mathsf{l}_{g_1} \circ \mathsf{l}_{g_2}$ είναι ίσες. Θα έχουμε:

   $$\big(\mathsf{l}_{g_1} \circ \mathsf{l}_{g_2}\big)(x) = \mathsf{l}_{g_1}\big(\mathsf{l}_{g_2}(x)\big) = \mathsf{l}_{g_1}(g_2 x) = g_1(g_2 x) = (g_1 g_2)x = \mathsf{l}_{g_1 g_2}(x)$$

   Άρα $\mathsf{l}_{g_1 g_2} = \mathsf{l}_{g_1} \circ \mathsf{l}_{g_2}$ και άρα

   $$\mathsf{L}_G(g_1 g_2) = \mathsf{l}_{g_1 g_2} = \mathsf{l}_{g_1} \circ \mathsf{l}_{g_2} = \mathsf{L}_G(g_1) \circ \mathsf{L}_G(g_2)$$

   δηλαδή η απεικόνιση L_G είναι ομομορφισμός ομάδων.

3. *Η απεικόνιση $\mathsf{L}_G : G \longrightarrow \mathsf{S}(G)$ είναι μονομορφισμός.*

   Πράγματι, θα έχουμε:

   $$\mathsf{Ker}(\mathsf{L}_G) = \{g \in G \mid \mathsf{L}_G(g) = \mathrm{Id}_G\} = \{g \in G \mid \mathsf{l}_g = \mathrm{Id}_G\} =$$

   $$= \{g \in G \mid \mathsf{l}_g(x) = \mathrm{Id}(x), \quad \forall x \in G\} = \{g \in G \mid gx = x, \quad \forall x \in G\} = \{e_G\}$$

   Επομένως, η απεικόνιση L_G είναι μονομορφισμός ομάδων.

4. Θέτοντας
$$G' = \{\mathsf{l}_g \in \mathsf{S}(G) \mid g \in G\} = \mathsf{Im}(\mathsf{L}_G) \leq \mathsf{S}(G)$$
έχουμε έναν ισομορφισμό $G \cong G' \leq \mathsf{S}(G)$.

Πράγματι, επειδή η απεικόνιση $\mathsf{L}_G \colon G \longrightarrow \mathsf{S}(G)$ είναι ομομορφισμός και «1-1», από το Πρώτο Θεώρημα Ισομορφισμών, έπεται ότι θα επάγει έναν ισομορφισμό ομάδων
$$\mathsf{L}_G : G \longrightarrow \mathsf{Im}(\mathsf{L}_G) \leq \mathsf{S}(G), \qquad \mathsf{L}_G(g) = \mathsf{l}_g$$
όπου $\mathsf{Im}(\mathsf{L}_G)$ είναι η ακόλουθη υποομάδα της $\mathsf{S}(G)$:
$$\mathsf{Im}(\mathsf{L}_G) = \{\mathsf{L}_G(g) \in \mathsf{S}(G) \mid g \in G\} = \{\mathsf{l}_g \in \mathsf{S}(G) \mid g \in G\} \leq \mathsf{S}(G)$$ ■

Παρατήρηση 6.5.2. Μπορούμε να θεωρήσουμε και την απεικόνιση
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}(G), \qquad \mathsf{R}_G(g) = \mathsf{r}_g$$
όπου
$$\mathsf{r}_g : G \longrightarrow G, \qquad \mathsf{r}_g(x) = xg$$
Ακριβώς με τον ίδιο τρόπο όπως στο Θεώρημα του Cayley 6.5.1, αποδεικνύεται ότι υπάρχει μια «1-1» απεικόνιση
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}(G)$$
η οποία όμως *δεν είναι* μονομορφισμός ομάδων, διότι εύκολα βλέπουμε ότι ισχύει:
$$\mathsf{R}_{g_1 g_2} = \mathsf{R}_{g_2} \circ \mathsf{R}_{g_1} \qquad \text{αλλά γενικά} \qquad \mathsf{R}_{g_1 g_2} \neq \mathsf{R}_{g_1} \circ \mathsf{R}_{g_2}$$
και άρα $\mathsf{R}(g_1 g_2) = \mathsf{R}(g_2) \circ \mathsf{R}(g_1)$. Διορθώνουμε το πρόβλημα ως εξής: Έστω η απεικόνιση
$$\cdot^{\mathsf{op}} : G \times G \longrightarrow G, \qquad x \cdot^{\mathsf{op}} y = yx$$
Τότε εύκολα βλέπουμε ότι το ζεύγος $(G, \cdot^{\mathsf{op}})$ είναι μια ομάδα, η οποία καλείται η **αντίθετη ομάδα** της G, και συμβολίζεται με G^{op}. Τότε προφανώς θα έχουμε έναν μονομορφισμό ομάδων
$$\mathsf{R}_G : G^{\mathsf{op}} \rightarrowtail \mathsf{S}(G)$$
και η G^{op} είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{R}_G) \leq \mathsf{S}(G)$:
$$\mathsf{R}_G : G^{\mathsf{op}} \xrightarrow{\cong} \mathsf{Im}(\mathsf{R}_G) \leq \mathsf{S}(G)$$
Θα λέμε ότι η G είναι *αντι-ισόμορφη* με την υποομάδα $\mathsf{Im}(\mathsf{R}_G)$ της $\mathsf{S}(G)$.

Εναλλακτικά, για να αποφύγουμε το πρόβλημα και να μην θεωρήσουμε την αντίθετη ομάδα G^{op} της G, ορίζουμε μια απεικόνιση
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}(G), \qquad \mathsf{R}_G(g) = \mathsf{r}_g$$
όπου
$$\mathsf{r}_g : G \longrightarrow G, \qquad \mathsf{r}_g(x) = xg^{-1}$$
Ακριβώς με τον ίδιο τρόπο, όπως στο Θεώρημα 6.5.1, αποδεικνύεται ότι η R_G είναι μια «1-1» απεικόνιση
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}(G)$$
η οποία είναι μονομορφισμός ομάδων, διότι εύκολα βλέπουμε ότι ισχύει:
$$\mathsf{R}_{g_1 g_2} = \mathsf{R}_{g_1} \circ \mathsf{R}_{g_2}$$ ▲

Έτσι, με βάση την συζήτηση στην Παρατήρηση 6.5.2, προκύπτει ο ακόλουθος ορισμός:

Ορισμός 6.5.3. *Έστω G μια ομάδα.*

1. *Ο μονομορφισμός*
$$\mathsf{L}_G : G \longrightarrow \mathsf{S}(G), \quad g \longmapsto \mathsf{L}_G = \mathsf{l}_g, \quad \text{και} \quad \mathsf{l}_g(x) = gx$$
καλείται η **αριστερή κανονική αναπαράσταση της** G.

2. *Ο μονομορφισμός*
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}(G), \quad g \longmapsto \mathsf{R}_G = \mathsf{r}_g, \quad \text{και} \quad \mathsf{r}_g(x) = xg^{-1}$$
καλείται η **δεξιά κανονική αναπαράσταση της** G.

Πόρισμα 6.5.4. *Έστω G μια πεπερασμένη ομάδα τάξης $\mathsf{o}(G) = n$.*

1. *Η αριστερή κανονική αναπαράσταση L_G της G ορίζει έναν μονομορφισμό*
$$\mathsf{L}_G : G \longrightarrow \mathsf{S}_n, \quad g \longmapsto \mathsf{L}_G = \mathsf{l}_g, \quad \text{και} \quad \mathsf{l}_g(x) = gx$$
και άρα κάθε πεπερασμένη ομάδα τάξης n είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L}_G)$ της S_n.

2. *Η δεξιά κανονική αναπαράσταση R_G της G ορίζει έναν μονομορφισμό*
$$\mathsf{R}_G : G \longrightarrow \mathsf{S}_n, \quad g \longmapsto \mathsf{R}_G = \mathsf{r}_g, \quad \text{και} \quad \mathsf{r}_g(x) = xg^{-1}$$
και άρα κάθε πεπερασμένη ομάδα τάξης n είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{R}_G)$ της S_n.

Παράδειγμα 6.5.5. Θα υπολογίσουμε την αριστερή κανονική αναπαράσταση της κυκλικής ομάδας G τάξης 3:
$$G = \{e,\ a,\ b\} = \{e,\ a,\ a^2\} = \langle a \rangle$$
Επειδή $\mathsf{o}(G) = 3$, έπεται ότι η G θα είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L}_G)$ της S_3, και θα έχουμε:
$$\mathsf{Im}(\mathsf{L}_G) = \{\mathsf{l}_e,\ \mathsf{l}_a,\ \mathsf{l}_b\} \ \leq \ \mathsf{S}_3$$
Οι πίνακες Cayley του πολλαπλασιασμού των ομάδων G και $\mathsf{Im}(\mathsf{L}_G)$ είναι:

$G = \{e,\ a,\ b\}$:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

και

$\mathsf{Im}\,\mathsf{L}_G = \{\mathsf{l}_e,\ \mathsf{l}_a,\ \mathsf{l}_b\}$:

$\cdot$	l_e	l_a	l_b
l_e	l_e	l_a	l_b
l_a	l_a	l_b	l_e
l_b	l_b	l_e	l_a

Θα προσδιορίσουμε τις μεταθέσεις l_e, l_a, l_b:

1. Η μετάθεση
$$\mathsf{l}_e : G \longrightarrow G, \quad \mathsf{l}_e(x) = ex$$
Άρα:
$$\mathsf{l}_e(e) = ee = e^2 = e, \qquad \mathsf{l}_e(a) = ea = a, \qquad \mathsf{l}_e(b) = e = b$$
Επομένως η απεικόνιση l_e είναι η ταυτοτική μετάθεση του συνόλου $G = \{e, a, b\}$:
$$\mathsf{l}_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$$

2. Η μετάθεση
$$\mathsf{l}_a : G \longrightarrow G, \quad \mathsf{l}_a(x) = ax$$
Άρα:
$$\mathsf{l}_a(e) = ae = a, \quad \mathsf{l}_a(a) = aa = a^2 = b, \quad \mathsf{l}_a(b) = ab = e$$
Επομένως η απεικόνιση l_a είναι η ακόλουθη μετάθεση του συνόλου $G = \{e, a, b\}$:
$$\mathsf{l}_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix} = (e\,a\,b)$$

3. Η μετάθεση
$$\mathsf{l}_b : G \longrightarrow G, \quad \mathsf{l}_b(x) = bx$$
Άρα:
$$\mathsf{l}_b(e) = be = b, \quad \mathsf{l}_b(a) = ba = e, \quad \mathsf{l}_b(b) = bb = b^2 = a$$
Επομένως η απεικόνιση l_a είναι η ακόλουθη μετάθεση του συνόλου $G = \{e, a, b\}$:
$$\mathsf{l}_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix} = (e\,b\,a)$$

Επομένως η G είναι ισόμορφη με την ακόλουθη ομάδα μεταθέσεων (υποομάδα της $\mathsf{S}(G)$):
$$\mathsf{Im}(\mathsf{L}_G) = \big\{(e),\ (eab),\ (eba)\big\}$$
Χρησιμοποιώντας την «1-1» και «επί» απεικόνιση $G = \{e, a, b\} \longrightarrow \{1, 2, 3\}$, όπου $e \leftrightarrows 1$, $a \leftrightarrows 2$, $b \leftrightarrows 3$, θα έχουμε ότι η $\mathsf{S}(G)$ είναι ισόμορφη με την S_3.

Επομένως η G είναι ισόμορφη με τη ακόλουθη ομάδα μεταθέσεων (υποομάδα της S_3):
$$\mathsf{Im}(\mathsf{L}_G) = \big\{\iota,\ (1\ 2\ 3),\ (1\ 3\ 2)\big\}$$
η οποία συμπίπτει με την εναλλάσσουσα ομάδα A_3. Άρα:
$$\mathsf{L}_G : G \xrightarrow{\ \cong\ } \mathsf{A}_3 \leq \mathsf{S}_3$$
Παρόμοια δουλεύουμε για την εύρεση της δεξιάς κανονικής αναπαράστασης της G. $\surd$

Κλείνουμε την παρούσα ενότητα με το ακόλουθο, σημαντικό απο θεωρητικής πλευράς, αποτέλεσμα.

Θεώρημα 6.5.6. *Για κάθε $n \geq 1$, το πλήθος των κλάσεων ισομορφίας των πεπερασμένων ομάδων τάξης n είναι πεπερασμένο.*

Απόδειξη. Από το Θεώρημα του Cayley 6.5.1 έπεται ότι κάθε ομάδα G τάξης n είναι ισόμορφη με μια υποομάδα της συμμετρικης ομάδας S_n. Επειδή η S_n είναι μια πεπερασμένη ομάδα (τάξης $n!$), έπεται ότι το σύνολο των υποομάδων της είναι πεπερασμένο. Συμπεραίνουμε ότι το πλήθος των κλάσεων ισομορφίας των ομάδων τάξης n είναι ίσο με το σύνολο των υποομάδων της S_n και επομένως είναι πεπερασμένο. ■

6.5.2 Μια σχετική εκδοχή του Θεωρήματος του Cayley

Έστω G μια ομάδα και $H \leq G$ μια υποομάδα της G. Θεωρούμε το σύνολο $G/H = \big\{Hx \subseteq G \mid x \in G\big\}$ των δεξιών πλευρικών κλάσεων της H στην G (το σύνολο G/H δεν είναι απαραίτητα ομάδα, διότι δεν υποθέτουμε ότι η υποομάδα H είναι κανονική στην G). Ορίζουμε μια απεικόνιση
$$\Phi\colon G \longrightarrow \mathsf{S}(G/H), \quad g \longmapsto \Phi(g) := \Phi_g \quad \text{όπου} \quad \Phi_g\colon G/H \longrightarrow G/H, \quad \Phi_g(Hx) = Hgx$$

Πρόταση 6.5.7. *Η απεικόνιση Φ είναι ένας καλά ορισμένος ομομορφισμός ομάδων και*

$$\mathsf{Ker}(\Phi) = \{g \in G \mid x^{-1}gx \in H,\ \forall x \in G\} = \bigcap_{x\in G} xHx^{-1} \trianglelefteq G$$

είναι η μεγαλύτερη κανονική υποομάδα της G η οποία περιέχεται στην H.

Απόδειξη. Δείχνουμε πρώτα ότι, για κάθε $g \in G$, η απεικόνιση $\Phi_g \colon G/H \longrightarrow G/H$ είναι στοιχείο της ομάδας μεταθέσεων $\mathsf{S}(G/H)$, δηλαδή είναι «1-1» και «επί». Πράγματι, αν $\Phi_g(Hx) = \Phi(Hy)$, τότε $Hgx = Hgy$. Όπως γνωρίζουμε, αυτό είναι ισοδύναμο με το ότι $(gy)^{-1}gx \in H$, δηλαδή $y^{-1}g^{-1}gx \in H$ και άρα $y^{-1}x \in H$. Τότε όμως $Hx = Hy$ και επομένως η Φ_g είναι «1-1». Αν $Hy \in G/H$, τότε $\Phi_g(g^{-1}y) = Hgg^{-1}y = Hy$ και άρα η Φ_g είναι «επί». Επομένως $\Phi_g \in \mathsf{S}(G/H)$, $\forall g \in G$.

Δείχνουμε ότι η απεικόνιση Φ είναι ομομορφισμός ομάδων, δηλαδή ότι ισχύει $\Phi_{g_1\circ g_2} = \Phi_{g_1} \circ \Phi_{g_2}$. Αυτή η σχέση ισχύει αν και μόνο αν $\Phi_{g_1\circ g_2}(Hx) = (\Phi_{g_1} \circ \Phi_{g_2})(Hx)$, $\forall x \in G$. Θα έχουμε:

$$\Phi_{g_1\circ g_2}(Hx) = H((g_1g_2)x) \quad \text{και} \quad (\Phi_{g_1} \circ \Phi_{g_2})(Hx) = \Phi_{g_1}(\Phi_{g_2}(Hx)) = \Phi_{g_1}(Hg_2x) = H(g_1(g_2x)) = H((g_1g_2)x)$$

Επομένως η ζητούμενη ισότητα ισχύει για κάθε $x \in G$ και επομένως η απεικόνιση Φ είναι ομομορφισμός ομάδων. Για τον πυρήνα του ομομορφισμού Φ θα έχουμε $\mathsf{Ker}(\Phi) = \{g \in G \mid \Phi_g = \iota\}$ και επομένως:

$$\mathsf{Ker}(\Phi) = \{g \in G \mid \Phi_g(Hx) = Hx,\ \forall x \in G\} = \{g \in G \mid Hgx = Hx,\ \forall x \in G\} = \{g \in G \mid x^{-1}gx \in H,\ \forall x \in G\}$$

Η υποομάδα $\mathsf{Ker}(\Phi)$ ως πυρήνας ομομορφισμού Φ είναι μια κανονική υποομάδα της G η οποία περιέχεται στην H διότι, αν $g \in \mathsf{Ker}(\Phi)$, τότε από την παραπάνω περιγραφή έχουμε $x^{-1}gx \in H$, $\forall x \in G$, και επιλέγοντας $x = e$, θα έχουμε $g \in H$. Επομένως $\mathsf{Ker}(\Phi) \subseteq H$. Αν $N \trianglelefteq G$ είναι μια κανονική υποομάδα της G έτσι ώστε $N \subseteq H$, τότε λόγω κανονικότητας θα έχουμε $x^{-1}gx \in N$ και άρα $x^{-1}gx \in H$, διότι $N \subseteq H$. Αυτό σημαίνει ότι $g \in \mathsf{Ker}(\Phi)$ και άρα $N \subseteq \mathsf{Ker}(\Phi)$, δηλαδή η υποομάδα $\mathsf{Ker}(\Phi)$ είναι η μεγαλύτερη κανονική υποομάδα της G η οποία περιέχεται στην H.

Τέλος, θα έχουμε:

$$\mathsf{Ker}(\Phi) = \{g \in G \mid x^{-1}gx \in H,\ \forall x \in G\} = \{g \in G \mid g \in xHx^{-1},\ \forall x \in G\} = \{xHx^{-1} \subseteq G \mid \forall x \in G\} = \bigcap_{x\in G} xHx^{-1} \quad \blacksquare$$

Παρατηρούμε ότι, αν $H = \{e\}$ είναι η τετριμμένη υποομάδα της G, τότε $G/H = G$ και η παραπάνω Πρόταση συμπίπτει με το Θεώρημα του Cayley 6.5.1. Από την άλλη πλευρά, αν η υποομάδα H είναι κανονική, τότε θα έχουμε $xHx^{-1} = H$ και άρα: $\mathsf{Ker}(\Phi) = H$. Ιδιαίτερα αν η υποομάδα H είναι απλή, δηλαδή δεν έχει γνήσιες μη τετριμμένες κανονικές υποομάδες, τότε στην Πρόταση 6.5.7 αναγκαστικά θα έχουμε $\mathsf{Ker}(\Phi) = \{e\}$ ή $\mathsf{Ker}(\Phi) = H$. Στην πρώτη περίπτωση η απεικόνιση Φ είναι μονομορφισμός και άρα η G είναι μια υποομάδα της ομάδας μεταθέσεων $\mathsf{S}(G/H)$. Στην δεύτερη περίπτωση θα έχουμε $\mathsf{Ker}(\Phi) = H \trianglelefteq G$, δηλαδή η H είναι κανονική υποομάδα της G.

Πόρισμα 6.5.8. *Έστω G μια πεπερασμένη ομάδα και $H \lneqq G$ μια γνήσια υποομάδα της G έτσι ώστε*

$$\mathsf{o}(G) \nmid [G : H]!$$

Τότε η H περιέχει μια μη τετριμμένη γνήσια υποομάδα N της G η οποία είναι κανονική στην G. Ιδιαίτερα η G δεν είναι απλή ομάδα.

Απόδειξη. Θεωρούμε τον ομομορφισμό ομάδων:

$$\Phi \colon G \longrightarrow \mathsf{S}(G/H), \quad g \longmapsto \Phi(g) := \Phi_g \quad \text{όπου} \quad \Phi_g \colon G/H \longrightarrow G/H, \quad \Phi_g(Hx) = Hgx$$

Ο Φ δεν μπορεί να είναι μονομορφισμός, διότι διαφορετικά η ομάδα G θα ήταν ισόμορφη με μια υποομάδα της συμμετρικής ομάδας $\mathsf{S}(G/H)$ η οποία έχει τάξη $[G : H]!$ και τότε από το Θεώρημα του Lagrange θα έπρεπε $\mathsf{o}(G) \mid [G : H]!$ το οποίο είναι άτοπο. Επομένως η υποομάδα $\mathsf{Ker}(\Phi) \leq H$ της H η οποία είναι κανονική στην G δεν είναι η τετριμμένη, και προφανώς $\mathsf{Ker}(\Phi) \neq G$, διότι διαφορετικά θα είχαμε $\mathsf{Ker}(\Phi) = H = G$, το οποίο είναι άτοπο διότι $H \lneqq G$. Άρα η H περιέχει μια μη τετριμμένη υποομάδα N η οποία είναι κανονική στην G. $\blacksquare$

Παράδειγμα 6.5.9. Το Πόρισμα 6.5.8 χρησιμοιείται συνήθως για να δειχθεί ότι μια ομάδα δεν είναι απλή.

Για παράδειγμα μπορεί να αποδειχθεί ότι μια ομάδα G τάξης 36 έχει μια υποομάδα H τάξης 9, και άρα $36 = \mathsf{o}(G) \nmid [G:H]! = \frac{36}{9}! = 4!$. Τότε από το Πόρισμα 6.5.8 η G διαθέτει μια μη τετριμμένη κανονική υποομάδα N η οποία περιέχεται στην H και άρα $\mathsf{o}(N) = 3$ ή 9.

Παρόμοια μπορεί να αποδειχθεί ότι μια ομάδα G τάξης 99 έχει μια υποομάδα H τάξης 11, και άρα $99 = \mathsf{o}(G) \nmid [G:H]! = \frac{99}{11}! = 9!$. Τότε από το Πόρισμα 6.5.8 η G διαθέτει μια μη τετριμμένη κανονική υποομάδα N η οποία περιέχεται στην H και άρα $\mathsf{o}(N) = 11 = \mathsf{o}(H)$, και συνεπώς $H \trianglelefteq G$. $\surd$

Κλείνουμε με τρεις εφαρμογές της σχετικής εκδοχής του Θεωρήματος του Cayley.

Πόρισμα 6.5.10. *Έστω G μια ομάδα η οποία περιέχει μια υποομάδα H με δείκτη $[G:H] = n$. Τότε η G περιέχει μια κανονική υποομάδα K πεπερασμένου δείκτη $[G:K] < \infty$, η οποία περιέχεται στην H και $[G:K] \mid n!$.*

Απόδειξη. Θεωρούμε τον ομομορφισμό ομάδων:

$$\Phi\colon G \longrightarrow \mathsf{S}(G/H), \quad g \longmapsto \Phi(g) := \Phi_g \quad \text{όπου} \quad \Phi_g\colon G/H \longrightarrow G/H, \quad \Phi_g(Hx) = Hgx$$

Τότε η υποομάδα $K = \mathsf{Ker}(\Phi)$ είναι κανονική στην G, περιέχεται στην H, και η ομάδα πηλίκο G/K είναι, σύμφωνα με το Πρώτο Θεώρημα Ισομορφισμών, ισόμορφη με μια υποομάδα της ομάδας $\mathsf{S}(G/H)$ της οποίας η τάξη είναι $[G:H]! = n!$. Άρα από το Θεώρημα του Lagrange θα έχουμε $\infty > \mathsf{o}(G/K) = [G:K] \mid n!$. ■

Γνωρίζουμε ότι μια υποομάδα με δείκτη 2 είναι κανονική υποομάδα. Το επόμενο Πόρισμα γενικεύει αυτό το αποτέλεσμα.

Πόρισμα 6.5.11. *Έστω G μια πεπερασμένη ομάδα τάξης n και υποθέτουμε ότι p είναι ο μικρότερος πρώτος αριθμός ο οποίος διαιρεί την τάξη της ομάδας. Τότε κάθε υποομάδα H της G με δείκτη p είναι κανονική υποοομάδα της G.*

Απόδειξη. Έστω H μια υποομάδα της G με δείκτη $[G:H] = p$. Τότε, από το προηγούμενο Πόρισμα 6.5.10, έπεται ότι η G περιέχει μια κανονική υποομάδα K με δείκτη $[G:K] \mid p!$, η οποία περιέχεται στην H: $K \leq H$. Τότε προφανώς:

$$[G:K] \mid \mathsf{o}(G) \quad \text{και} \quad [G:K] \mid p! \quad \Longrightarrow \quad [G:K] \mid \big(\mathsf{o}(G), p!\big)$$

Τότε $[G:K] = p$. Πράγματι, έστω q ένας πρώτος ο οποίος διαιρεί τον δείκτη $[G:K]$ και άρα και τον μέγιστο κοινό διαιρέτη $\big(\mathsf{o}(G), p!\big)$. Επειδή $q \mid p!$, θα έχουμε ότι $q \mid k \leq p$ για κάποιο k με $1 \leq k \leq p$. Επειδή $q \mid \mathsf{o}(G)$ και ο p είναι ο μικρότερος πρώτος ο οποίος διαιρεί την τάξη $\mathsf{o}(G)$ της ομάδας θα έχουμε $q \leq p$. Άρα $q = p$ είναι ο μοναδικός πρώτος διαιρέτης του δείκτη $[G:K]$. Επειδή $[G:K] \mid p!$, προφανώς θα έχουμε $[G:K] = p$. Από τη σχέση $K \leq H \leq G$, θα έχουμε για τους δείκτες:

$$[G:H] \cdot [H:K] = [G:K]$$

Επειδή $[G:H] = p = [G:K]$, από την παραπάνω σχέση θα έχουμε $[H:K] = 1$ και επομένως $H = K$. Επειδή η K είναι κανονική, έπεται ότι η υποομάδα H είναι κανονική. ■

Πόρισμα 6.5.12. *Αν $n \geq 3$, τότε η μόνη γνήσια υποομάδα H της συμμετρικής ομάδας S_n με δείκτη $[\mathsf{S}_n : H] < n$ είναι η εναλλάσσουσα υποομάδα A_n.*

Απόδειξη. Έστω $H \lneqq \mathsf{S}_n$ μια γνήσια υποομάδα της S_n με δείκτη $[\mathsf{S}_n : H] \leq n-1$. Έστω $K = \mathsf{Ker}(\Phi)$, όπου

$$\Phi\colon \mathsf{S}_n \longrightarrow \mathsf{S}(\mathsf{S}_n/H), \quad g \longmapsto \Phi(g) := \Phi_g \quad \text{όπου} \quad \Phi_g\colon \mathsf{S}_n/H \longrightarrow \mathsf{S}_n/H, \quad \Phi_g(Hx) = Hgx$$

Από το Πρώτο Θεώρημα Ισομορφισμών η ομάδα πηλίκο S_n/K είναι ισόμορφη με μια υποομάδα της συμμετρικής ομάδας η οποία έχει τάξη $[\mathsf{S}_n : H]!$ και άρα $[\mathsf{S}_n : H]! \leq (n-1)!$ διότι από την υπόθεση $[\mathsf{S}_n : H] < n$. Τότε από το Θεώρημα τοτ Lagrange, θα έχουμε $\mathsf{o}(\mathsf{S}_n/K) \mid [\mathsf{S}_n : H]! \leq (n-1)!$ και άρα $\mathsf{o}(\mathsf{S}_n/K) \mid (n-1)!$. Ιδιαίτερα θα έχουμε $K \neq \{\iota\}$. Έτσι η K είναι μια γνήσια μη τετριμμένη κανονική υποομάδα της S_n. Γνωρίζουμε ότι η μοναδική τέτοια υποομάδα είναι η A_n. Άρα $K = \mathsf{A}_n$, και επειδή $K = \mathsf{A}_n \leq H \leq \mathsf{S}_n$, θα έχουμε:

$$[\mathsf{S}_n : H] \cdot [H : \mathsf{A}_n] = [\mathsf{S}_n : \mathsf{A}_n] = 2 \quad \Longrightarrow \quad [H : \mathsf{A}_n] = 1 \quad \Longrightarrow \quad H = \mathsf{A}_n$$

διότι $[\mathsf{S}_n : H] > 1$, καθώς η H είναι γνήσια υποομάδα της S_n. ■

6.5.3 Η εναλλάσσουσα εκδοχή του Θεωρήματος του Cayley

Θα αποδείξουμε ότι κάθε πεπερασμένη ομάδα είναι υποομάδα της εναλλάσσουσας υποομάδας μιας κατάλληλης συμμετρικής ομάδας.

Λήμμα 6.5.13. *Για κάθε $n \geq 1$ και για κάθε $m \geq n$, η συμμετρική ομάδα S_n είναι ισόμορφη με μια υποομάδα της συμμετρικής ομάδας S_m.*

Απόδειξη. Θεωρούμε το υποσύνολο

$$H = \{\sigma \in \mathsf{S}_m \mid \sigma(x) = x, \;\; 1 \leq x \leq n\}$$

Προφανώς το υποσύνολο $H \subseteq \mathsf{S}_m$ είναι μη κενό, διότι $\iota \in H$ και επίσης είναι κλειστό στην πράξη της συμμετρικής ομάδας S_m. Επομένως, επειδή η ομάδα S_m είναι πεπερασμένη, σύμφωνα με γνωστό κριτήριο, το υποσύνολο H είναι μια υποομάδα της S_m. Θεωρούμε την απεικόνιση

$$f : \mathsf{S}_n \longrightarrow \mathsf{S}_m, \quad f(\sigma) = \tilde{\sigma}, \quad \text{όπου} \quad \tilde{\sigma}(i) = \sigma(i), \;\; 1 \leq x \leq n \quad \text{και} \quad \tilde{\sigma}(x) = x, \;\; n+1 \leq x \leq m$$

Προφανώς η f είναι ομομορφισμός ομάδων, είναι «1-1» και η εικόνα $\mathsf{Im}(f)$ του f συμπίπτει με την υποομάδα H. Άρα η απεικόνιση f είναι ένας ισομορφισμός, και επομένως $\mathsf{S}_n \cong H \leq \mathsf{S}_m$. ■

Θεώρημα 6.5.14. *Κάθε πεπερασμένη ομάδα G τάξης n είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας ομάδας A_{n+2}.*

Απόδειξη. Θα δείξουμε πρώτα ότι η συμμετρική ομάδα S_n είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας υποομάδας A_{n+2} της συμμετρικής ομάδας S_{n+2}. Θεωρούμε τη συμμετρική ομάδα S_n ως υποομάδα της S_{n+2}, όπως στο παραπάνω Λήμμα 6.5.13, και τότε, αν μια μετάθεση $\sigma \in \mathsf{S}_n$ είναι άρτια ως μετάθεση της S_n, τότε προφανώς παραμένει και άρτια ως μετάθεση της S_{n+2}. Έτσι $\mathsf{S}_n \geq \mathsf{A}_n \leq \mathsf{A}_{n+2} \leq \mathsf{S}_{n+2}$. Με βάση αυτή την παρατήρηση, ορίζουμε απεικόνιση

$$\varphi : \mathsf{S}_n \longrightarrow \mathsf{A}_{n+2}, \quad \varphi(\sigma) = \begin{cases} \sigma, & \text{αν η } \sigma \text{ είναι άρτια} \\ \sigma \circ (n+1 \;\; n+2), & \text{αν η } \sigma \text{ είναι περιττή} \end{cases}$$

Θα δείξουμε ότι η απεικόνιση φ είναι ομομορφισμός ομάδων. Έστω σ, τ μεταθέσεις της $\mathsf{S}_n \leq \mathsf{S}_{n+2}$. Διακρίνουμε τις ακόλουθες περιπτωσεις:

1. Αν οι σ, τ είναι και οι δύο άρτιες, τότε επειδή και η $\sigma \circ \tau$ είναι άρτια, θα έχουμε: $\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ \tau = \varphi(\sigma \circ \tau)$.

2. Αν οι σ, τ είναι και οι δύο περιττές, θα έχουμε $\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ (n+1 \;\; n+2) \circ \tau \circ (n+1 \;\; n+2)$. Επειδή η ανάλυση της τ, ως μετάθεσης της S_n, σε ξένους κύκλους δεν περιέχει τα στοιχεία $\{n+1, n+2\}$, έπεται ότι οι μεταθέσεσι τ και $(n+1 \;\; n+2)$ μετατίθενται, και άρα:

   $$\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ (n+1 \;\; n+2) \circ \tau \circ (n+1 \;\; n+2) = \sigma \circ \tau \circ (n+1 \;\; n+2)^2 = \sigma \circ \tau \circ \iota = \sigma \circ \tau$$

   Επειδή η μετάθεση $\sigma \circ \tau$ είναι άρτια ώς σύνθεση περιττών μεταθέσεων, θα έχουμε $\varphi(\sigma \circ \tau) = \sigma \circ \tau$. Άρα $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

3. Έστω ότι η μετάθεση σ είναι άρτια και η μετάθεση τ είναι περιττή. Τότε θα έχουμε $\varphi(\sigma) = \sigma$ και $\varphi(\tau) = \tau \circ (n+1 \;\; n+2)$, έτσι $\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ \tau \circ (n+1 \;\; n+2)$. Η μετάθεση $\sigma \circ \tau$ είναι περιττή και γι' αυτό $\varphi(\sigma \circ \tau) = \sigma \circ \tau \circ (n+1 \;\; n+2)$. Άρα $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$.

4. Έστω ότι η μετάθεση σ είναι περιττή και η μετάθεση τ είναι άρτια. Τότε θα έχουμε $\varphi(\sigma) = \sigma \circ (n+1 \;\; n+2)$ και $\varphi(\tau) = \tau$, έτσι $\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ (n+1 \;\; n+2) \circ \tau$. Όπως και στην περίπτωση 2., οι μεταθέσεις $(n+1 \;\; n+2)$ και τ μετατίθενται και άρα,:

   $$\varphi(\sigma) \circ \varphi(\tau) = \sigma \circ (n+1 \;\; n+2) \circ \tau = \sigma \circ \tau \circ (n+1 \;\; n+2) = \varphi(\sigma \circ \tau)$$

   όπου η τελευταία ισότητα προέκυψε διότι η μετάθεση $\sigma \circ \tau$ είναι περιττή.

Επομένως καταλήγουμε ότι πράγματι η φ είναι ομομορφισμός ομάδων.

Η απεικόνιση φ είναι «1-1» διότι αν $\varphi(\sigma)=\iota$, τότε αν η σ είναι άρτια, θα έχουμε $\sigma=\iota$. Αν η σ είναι περιττή, θα έχουμε $\sigma\circ(n+1\ \ n+2)=\iota$ και τότε επειδή $(n+1\ \ n+2)^{-1}=(n+1\ \ n+2)$, θα έχουμε $\sigma=(n+1\ \ n+2)$ ως στοιχεία της S_{n+2}. Αυτό όμως είναι άτοπο διότι η σ ως στοιχείο της S_{n+2} αφήνει σταθερά τα στοιχεία $n+1$ και $n+2$. Άρα $\mathsf{Ker}(\varphi)=\{\iota\}$ και επομένως ο ομομορφισμός φ είναι «1-1», και άρα έχουμε έναν μονομορφισμό

$$\varphi\ :\ \mathsf{S}_n\ \rightarrowtail\ \mathsf{A}_{n+2}$$

Από το Θεώρημα του Cayley η ομάδα G είναι ισόμορφη με μια υποομάδα της S_n μέσω της αριστερής κανονικής αναπαράστασής της

$$\mathsf{L}_G\ :\ G\ \rightarrowtail\ \mathsf{S}_n$$

Η σύνθεση $\varphi\circ\mathsf{L}_G$ είναι τότε ο ζητούμενος μονομορφισμός ομάδων

$$\varphi\circ\mathsf{L}_G\ :\ G\ \rightarrowtail\ \mathsf{A}_{n+2}$$

μέσω του οποίου η ομάδα G είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας ομάδας A_{n+2}, διότι από το Πρώτο Θεώρημα Ισομορφισμών έχουμε:

$$G\ \xrightarrow{\cong}\ \mathsf{Im}(\varphi\circ\mathsf{L}_G)\ \leq\ \mathsf{A}_{n+2}$$ ■

Σε κάποιες περιπτώσεις το παραπάνω Θεώρημα μπορεί να βελτιωθεί, αν η ομάδα G είναι απλή.

Πόρισμα 6.5.15. *Έστω ότι G είναι μια απλή ομάδα με τάξη $\mathsf{o}(G)>2$ και έστω ότι η G περιέχει μια υποομάδα H με δείκτη $[G:H]=n>1$. Τότε η G είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας ομάδας A_n.*

Απόδειξη. Η απόδειξη αφήνεται σαν Άσκηση στον αναγνώστη, βλέπε την Άσκηση 6.6.47. ■

6.5.4 Η αβελιανή εκδοχή του Θεωρήματος του Cayley

Αν μια πεπερασμένη ομάδα G, ας πούμε τάξης n, είναι αβελιανή, τότε το Θεώρημα του Cayley υλοποιεί την G ως μια υποομάδα της συμμετρικής ομάδας S_n, η οποία δεν είναι αβελιανή, αν $n\geq 2$. Είναι εύλογο να αναρωτηθούμε αν υπάρχει μια «αβελιανή εκδοχή» του Θεωρήματος του Cayley, δηλαδή αν υπάρχει μια κλάση $\mathscr{A}$ πεπερασμένων αβελιανών ομάδων, έτσι ώστε κάθε πεπερασμένη αβελιανή ομάδα να υλοποιείται ως υποομάδα μιας ομάδας από την κλάση $\mathscr{A}$.

Όπως πιστοποιεί το ακόλουθο Θεώρημα το οποίο αναφέρουμε χωρίς απόδειξη, μια τέτοια κλάση πεπερασμένων αβελιανών ομάδων υπάρχει και είναι η πολλαπλασιαστική ομάδα των αντιστρέψιμων κλάσεων υπολοίπων $\mathsf{mod}\ n$, $n\geq 1$:

$$\mathscr{A}=\{\mathsf{U}(\mathbb{Z}_n)\mid n\in\mathbb{N}\}$$

Θεώρημα 6.5.16. *Έστω ότι G είναι μια πεπερασμένη αβελιανή ομάδα. Τότε υπάρχει ένας θετικός ακέραιος $n\geq 1$ και ένας μονομορφισμός ομάδων:*

$$f\ :\ G\ \rightarrowtail\ \mathsf{U}(\mathbb{Z}_n)$$

6.6 Ασκήσεις

Άσκηση 6.6.1. *Να αποδειχθεί το Λήμμα 6.4.13.*

Άσκηση 6.6.2. *Γνωρίζουμε ότι κάθε υποομάδα H μιας ομάδας G με δείκτη $[G:H]=2$ είναι κανονική. Να δοθεί παράδειγμα υποομάδας H μιας ομάδας G με δείκτη $[G:H]=3$ η οποία δεν είναι κανονική.*

Άσκηση 6.6.3. *Βρείτε την τάξη της δοθείσας ομάδας πηλίκου:*

1. $\mathbb{Z}_6/\langle [3]_6\rangle$
2. $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle [2]_4\rangle \times \langle [2]_{12}\rangle)$
3. $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle ([2]_4, [1]_2)\rangle$
4. $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{[0]_3\} \times \mathbb{Z}_5)$
5. $(\mathbb{Z}_2 \times S_3)/\langle ([1]_2, (123))\rangle$

Άσκηση 6.6.4. *Βρείτε την τάξη του στοιχείου:*

1. $[5]_{12} + \langle [4]_{12}\rangle$ *στην ομάδα πηλίκο* $\mathbb{Z}_{12}/\langle [4]_{12}\rangle$
2. $[26]_{60} + \langle [12]_{60}\rangle$ *στην ομάδα πηλίκο* $\mathbb{Z}_{60}/\langle [12]_{60}\rangle$
3. $([2]_3, [1]_6) + \langle ([1]_3, [1]_6)\rangle$ *στην ομάδα πηλίκο* $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle ([1]_3, [1]_6)\rangle$
4. $([2]_6, [0]_8) + \langle ([4]_6, [4]_8)\rangle$ *στην ομάδα πηλίκο* $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle ([4]_6, [4]_8)\rangle$

Άσκηση 6.6.5. *Να δειχθεί ότι υπάρχουν ισομορφισμοί ομάδων:*

1. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([0]_2, [1]_4)\rangle \cong \mathbb{Z}_2$
2. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([0]_2, [2]_4)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$
3. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([1]_2, [2]_4)\rangle \cong \mathbb{Z}_4$
4. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle (0, 4, [0]_8)\rangle \cong \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8$
5. $(\mathbb{Z} \times \mathbb{Z})/\langle (2, 2)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}$

Άσκηση 6.6.6. *Να δειχθεί ότι, αν G είναι μια πεπερασμένη αβελιανή ομάδα περιττής τάξης, τότε η απεικόνιση $f: G \longrightarrow G$, $f(x) = x^2$ είναι ένας αυτομορφισμός της G. Διατυπώστε και αποδείξτε μια γενικότερη εκδοχή του παραπάνω ισχυρισμού.*

Άσκηση 6.6.7.

1. *Έστω S ένα πεπερασμένο σύνολο στοιχείων της προσθετικής ομάδας $(\mathbb{Q}, +)$. Να δείξετε ότι η υποομάδα $\langle S\rangle$ η οποία παράγεται από το S είναι άπειρη κυκλική.*
2. *Έστω T ένα πεπερασμένο σύνολο στοιχείων της προσθετικής ομάδας πηλίκο $(\mathbb{Q}/\mathbb{Z}, +)$. Να δείξετε ότι η υποομάδα $\langle T\rangle$ η οποία παράγεται από το T είναι πεπερασμένη κυκλική.*

Άσκηση 6.6.8. *Να δειχθεί ότι η ομάδα πηλίκο $\mathbb{Q}/\mathbb{Z}$ είναι ισόμορφη με την ομάδα*

$$(G, \cdot), \quad \text{όπου} \quad G = \left\{e^{2\pi i\theta} \in \mathbb{C} \mid \theta \in \mathbb{Q}\right\}$$

και «$\cdot$» είναι ο συνήθης πολλαπλασιασμός μιγαδικών αριθμών.

Άσκηση 6.6.9. *Να δοθούν παραδείγματα:*

1. *Άπειρης ομάδας G, όλα τα στοιχεία της οποίας έχουν πεπερασμένη τάξη.*
2. *Ομάδας G η οποία δεν έχει στοιχεία πεπερασμένης τάξης > 1 αλλά περιέχει μια κανονική υποομάδα H έτσι ώστε όλα τα στοιχεία της ομάδας πηλίκου G/H έχουν πεπερασμένη τάξη.*

3. *Άπειρης ομάδας G η οποία περιέχει μια κανονική υποομάδα H όλα τα στοιχεία της οποίας έχουν πεπερασμένη τάξη, και η ομάδα πηλίκο G/H δεν έχει στοιχεία πεπερασμένης τάξης.*

Άσκηση 6.6.10. *Έστω η πολλαπλασιαστική ομάδα $\mathbb{C}^*$ των μη μηδενικών μιγαδικών αριθμών.*

1. *Αν $\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\} \leq \mathbb{C}^*$ είναι η ομάδα του κύκλου, να δειχθεί ότι η ομάδα-πηλίκο $\mathbb{C}^*/\mathsf{T}$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $\mathbb{R}^+$ των θετικών πραγματικών αριθμών.*

2. *Να δείξετε ότι το σύνολο*
$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid (a,b) \neq (0,0) \right\}$$
εφοδιασμένο με την πράξη πολλαπλασιασμού πινάκων είναι ομάδα και υπάρχει ισομορφισμός:
$$G \xrightarrow{\cong} \mathbb{C}^*$$

Άσκηση 6.6.11. *Θεωρούμε την ομάδα $\mathsf{S}(A)$ των μεταθέσεων επί ενός μη κενού συνόλου A. Έστω $G \leq \mathsf{S}(A)$ μια υποομάδα της $\mathsf{S}(A)$ και $X \subseteq A$ ένα υποσύνολο για το οποίο ισχύει ότι $f(X) \subseteq X$, $\forall f \in G$. Να δειχθεί ότι η απεικόνιση*
$$\phi \colon G \longrightarrow \mathsf{S}(X), \quad \phi(f) = f|_X$$
είναι ένας ομομορφισμός ομάδων, να προσδιοριστεί ο πυρήνας του, και να δειχθεί ότι, αν $f \in G$ και $f(x) = x$, $\forall x \in X$, τότε $f = \mathsf{Id}_A$, τότε η απεικόνιση ϕ είναι μονομορφισμός. Πόσα στοιχεία μπορεί να έχει το σύνολο X αν η απεικόνιση ϕ είναι μονομορφισμός;

Άσκηση 6.6.12. *Θεωρούμε την απεικόνιση*
$$f \colon \mathbb{Z}_{16} \longrightarrow \mathsf{U}(\mathbb{Z}_{17}), \quad f([k]_{16}) = [3^k]_{17}$$
Να δειχθεί ότι η απεικόνιση f είναι καλά ορισμένη και είναι ένας ισομορφισμός ομάδων.

Άσκηση 6.6.13. *Να δειχθεί ότι η απεικόνιση*
$$f : \mathbb{Z}_{22} \longrightarrow \mathsf{U}(\mathbb{Z}_{23}), \quad f([k]_{22}) = [5^k]_{23}$$
είναι ένας ισομορφισμός.

Άσκηση 6.6.14. *Να δειχθεί ότι η απεικόνιση*
$$f : \mathbb{Z}_{30} \longrightarrow \mathsf{U}(\mathbb{Z}_{31}), \quad f([k]_{30}) = [3^k]_{31}$$
είναι ένας ισομορφισμός.

Άσκηση 6.6.15. *Αν p είναι ένας πρώτος αριθμός, να εξετασθεί αν οι ομάδες $(\mathbb{Z}_{p-1}, +)$ και $(\mathsf{U}(\mathbb{Z}_p), \cdot)$ είναι ισόμορφες.*

Άσκηση 6.6.16. *Θεωρούμε την ομάδα $G = ([-1,1], \star)$, όπου, $\forall x, y \in [-1,1]$:*
$$x \star y = \frac{x+y}{1+xy}$$
Να δειχθεί ότι η ομάδα G είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{R}, +)$.

Άσκηση 6.6.17. *Αν $a, b \in \mathbb{R}$, όπου $a < b$, να οριστεί μια πράξη «$\star$» επί του κλειστού διαστήματος $[a, b] \subseteq \mathbb{R}$, έτσι ώστε το ζεύγος $([a, b], \star)$ να είναι ομάδα ισόμορφη με την προσθετική ομάδα $(\mathbb{R}, +)$.*

Άσκηση 6.6.18. *Υποθέτουμε ότι $f : G \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_6$ είναι ένας επιμορφισμός ομάδων, και έστω ότι η τάξη του πυρήνα $\mathsf{Ker}(f)$ είναι $\mathsf{o}(\mathsf{Ker}(f)) = 5$. Να δειχθεί ότι η ομάδα G διαθέτει υποομάδες τάξης $5, 19, 15, 20, 30$.*

Άσκηση 6.6.19. *Έστω ότι G είναι μια ομάδα και ότι $K \trianglelefteq G$ είναι μια κανονική υποομάδα της G. Έστω επίσης ότι H και N είναι δύο υποομάδες της G έτσι ώστε: $H \trianglelefteq N \leq G$.*

Να δειχθεί ότι υπάρχει ένας ισομορφισμός ομάδων:

$$NK/HK \xrightarrow{\cong} N/H(N \cap K)$$

Άσκηση 6.6.20. *Έστω G μια ομάδα και N μια κανονική υποομάδα της G. Να δείξετε ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα πηλίκο G/N είναι* **απλή**, *δηλαδή δεν περιέχει καμία γνήσια μη τετριμμένη κανονική υποομάδα.*
2. *Η N είναι μια μέγιστη κανονική υποομάδα της G.*

Άσκηση 6.6.21. *Έστω G μια ομάδα και H μια κανονική υποομάδα της G με δείκτη $[G : H] = p$, όπου p είναι ένας πρώτος αριθμός. Να δειχθεί ότι η ομάδα πηλίκο G/H είναι απλή.*

Άσκηση 6.6.22. *Να ολοκληρωθεί η απόδειξη του Λήμματος 6.4.12.*

Άσκηση 6.6.23. *Να εφαρμοστεί το Πρώτο Θεώρημα Ισομορφισμών για τους ομομορφισμούς ομάδων*

1. $f : \mathbb{R} \longrightarrow \mathbb{C}^*$, $f(x) = e^{2\pi i x}$.
2. $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, $f(x) = [nx]_m$.
3. $f : \mathsf{T} \longrightarrow \mathsf{T}$, $f(z) = z^n$, *όπου* T *είναι η ομάδα του κύκλου.*
4. $f : \mathbb{C}^* \longrightarrow \mathbb{R}^*$, $f(z) = |z|$.

Άσκηση 6.6.24. *Έστω $G = \langle a \rangle$ και $H = \langle b \rangle$ δύο κυκλικές ομάδες (όχι κατ' ανάγκη πεπερασμένες). Να εξεταστεί αν και πότε η αντιστοιχία $f : G \longrightarrow H$, $f(x^i) = y^i$ ορίζει έναν ομομορφισμό ομάδων.*

Άσκηση 6.6.25. *Έστω G μια ομάδα και N μια κανονική υποομάδα της G. Να δειχθεί ότι η ομάδα πηλίκο G/N είναι αβελιανή αν και μόνο αν $[G, G] \leq N$, όπου $[G, G]$ είναι η μεταθέτρια ομάδα της G.*

Άσκηση 6.6.26. *Έστω ότι $f, g : G \longrightarrow H$ είναι ομομορφισμοί ομάδων.*

1. *Να εξεταστεί αν το υποσύνολο $H = \{x \in G \mid f(x) = g(x)\}$ είναι υποομάδα της G.*
2. *Υπάρχει κάποια σχέση μεταξύ των τάξεων $\mathsf{o}(x)$ και $\mathsf{o}(f(x))$;*
3. *Να δειχθεί ότι αν ο ομομορφισμός f είναι επιμορφισμός και η ομάδα G είναι κυκλική (αβελιανή), τότε και η ομάδα H είναι κυκλική (αβελιανή).*
4. *Ισχύει το αντίστροφο του 3.;*

Άσκηση 6.6.27. *Θεωρούμε την πολλαπλασιαστική ομάδα* $\mathsf{GL}(2,\mathbb{R})$ *των αντιστρέψιμων πινάκων με στοιχεία πραγματικούς αριθμούς.*

1. *Να δείξετε ότι το υποσύνολο*
$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid ad \neq 0 \right\}$$
είναι υποομάδα της $\mathsf{GL}_2(\mathbb{R})$.

2. *Να δείξετε ότι το υποσύνολο*
$$H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid b \in \mathbb{R} \right\}$$
είναι κανονική υποομάδα της G.

3. *Να κατασκευάσετε έναν ισομορφισμό*
$$H \cong \mathbb{R}$$

4. *Να δειχθεί ότι η ομάδα πηλίκο* G/H *είναι αβελιανή.*

Άσκηση 6.6.28. *Θεωρούμε το σύνολο απεικονίσεων*
$$G = \left\{ \tau_{a,b} : \mathbb{R} \longrightarrow \mathbb{R} \mid \tau_{a,b}(x) = ax + b, \quad a, b \in \mathbb{R}, \quad a \neq 0 \right\}$$
το οποίο είναι ομάδα με πράξη την σύνθεση απεικονίσεων.

1. *Να δείξετε ότι το υποσύνολο*
$$H = \left\{ \tau_{1,b} \in G \mid b \in \mathbb{R} \right\}$$
είναι κανονική υποομάδα της G.

2. *Να προσδιορίσετε την ομάδα πηλίκο* G/H.

Άσκηση 6.6.29. *Θεωρούμε το σύνολο* $G = \mathbb{R}^* \times \mathbb{R}$ *στο οποίο ορίζουμε μια πράξη «*$\star$*» ως εξής:*
$$(a,b) \star (c,d) = (ac, ad + b)$$

1. *Να δειχθεί ότι το ζεύγος* $(G, \star)$ *είναι ομάδα.*

2. *Να δειχθεί ότι η ομάδα* G *είναι ισόμορφη με την ομάδα της Άσκησης 6.6.28.*

Άσκηση 6.6.30. *Θεωρούμε το ακόλουθο σύνολο* 2×2 *πινάκων με στοιχεία πραγματικούς αριθμούς:*
$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid x \neq 0 \right\}$$

1. *Να δειχθεί ότι το ζεύγος* $(G, \star)$ *είναι μια υποομάδα της* $\mathsf{GL}(2,\mathbb{R})$.

2. *Να δειχθεί ότι η ομάδα* G *είναι ισόμορφη με την ομάδα της Άσκησης 6.6.29.*

3. *Να εξεταστεί αν το υποσύνολο*
$$G = \left\{ \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid x > 0 \right\}$$
είναι κανονική υποομάδα της G. *Αν το υποσύνολο* H *είναι κανονική υποομάδα της* G, *να προσδιοριστεί η ομάδα πηλίκο* G/H.

Άσκηση 6.6.31. *Να δειχθεί ότι η απεικόνιση* $f : G \longrightarrow G$, $f(x) = x^{-1}$, *είναι αυτομορφισμός μιας ομάδας* G *αν και μόνο αν η* G *είναι αβελιανή. Αν η ομάδα* G *είναι αβελιανή, τότε η απεικόνιση* $G \longrightarrow G$, $x \longmapsto x^k$ *είναι ένας ενδομορφισμός της* G, $\forall k \in \mathbb{Z}$.

Άσκηση 6.6.32. *Θεωρούμε το ακόλουθο σύνολο* 3×3 *πινάκων υπεράνω του* $\mathbb{Q}$*:*

$$G=\left\{ A_q=\begin{pmatrix} q & q & 0\\ q & q & 0\\ q & q & 0\end{pmatrix}\in \mathsf{M}_2(\mathbb{Q}) \;\middle|\; q\neq 0\right\}$$

1. *Να δειχθεί ότι το σύνολο* G *εφοδιασμένο με την συνήθη πράξη πολλαπλασιασμού πινάκων αποτελεί μια αβελιανή ομάδα.*

2. *Να δειχθεί ότι η ομάδα* G *είναι ισόμορφη με την πολλαπλασιαστική ομάδα* $(\mathbb{Q}^*,\cdot)$ *των μη μηδενικών ρητών αριθμών.*

Άσκηση 6.6.33. *Θεωρούμε το ακόλουθο υποσύνολο του* $\mathbb{Q}$*:*

$$G=\left\{2^n3^m\in\mathbb{Q}\mid n,m\in\mathbb{Z}\right\}$$

1. *Δείξτε ότι το σύνολο* G *εφοδιασμένο με την συνήθη πράξη πολλαπλασιασμού ρητών αριθμών αποτελεί μια αβελιανή ομάδα.*
2. *Με ποια γνωστή σας ομάδα είναι ισόμορφη η ομάδα* G*;*
3. *Διατυπώστε και αποδείξτε μια γενικότερη εκδοχή των* 1. *και* 2..

Άσκηση 6.6.34. 1. *Να προσδιοριστεί η ομάδα πηλίκο* $\mathbb{R}^*/\mathbb{R}^{>0}$*, όπου* $\mathbb{R}^{>0}$ *είναι η υποομάδα της πολλαπλασιαστικής ομάδας* $\mathbb{R}^*$ *των μη μηδενικών πραγματικών αριθμών η οποία αποτελείται από όλους τους θετικούς πραγματικούς αριθμούς.*
2. *Έστω* $\langle i\rangle=\{1,-1,i,-i\}$ *η κυκλική υποομάδα της* $\mathbb{C}^*$ *η οποία παράγεται από τη φανταστική μονάδα. Να περιγραφεί η ομάδα πηλίκο* $\mathbb{C}^*/\langle i\rangle$ *και να δειχθεί ότι:* $\mathbb{C}^*/\langle i\rangle\cong\mathbb{C}^*$.

   Ποια είναι η γενίκευση αυτού του ισχυρισμού;
3. *Να περιγραφούν οι ομάδες πηλίκα* $\mathbb{C}^*/\mathbb{R}^{>0}$ *και* $\mathbb{C}^*/\mathsf{T}$*, όπου* $\mathsf{T}=\{z\in\mathbb{C}\mid |z|=1\}$ *είναι η ομάδα του κύκλου.*
4. *Να κατασκευάσετε έναν ισομορφισμό ομάδων*

$$\mathbb{R}/\mathbb{Z}\;\cong\;\mathbb{R}/2\pi\mathbb{Z}$$

Άσκηση 6.6.35. *Αν* G *είναι μια ομάδα, να δειχθεί ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Η ομάδα* G *είναι αβελιανή.*
2. *Η απεικόνιση* $f\colon G\longrightarrow G$*,* $f(g)=g^2$ *είναι ένας ομομορφισμός.*
3. *Η απεικόνιση* $f\colon G\times G\longrightarrow G$*,* $f(g,h)=g$ *είναι ένας ομομορφισμός.*

Άσκηση 6.6.36. *Να υπολογιστεί η αριστερή και η δεξιά κανονική αναπαράσταση της ομάδας του Klein* $\mathcal{V}_4$*.*

Άσκηση 6.6.37. *Να υπολογιστεί η αριστερή και η δεξιά κανονική αναπαράσταση της συμμετρικής ομάδας* S_3*.*

Άσκηση 6.6.38. *Να δειχθεί ότι υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{Aut}(\mathcal{V}_4)\xrightarrow{\cong}\mathsf{S}_3$$

όπου $\mathcal{V}_4$ *είναι η ομάδα του Klein.*

Άσκηση 6.6.39. *Να δειχθεί με αντιπαραδείγματα ότι υπάρχουν μη ισόμορφες ομάδες με ισόμορφες ομάδες αυτομορφισμών, και άρα γενικά θα έχουμε:*

$$\mathsf{Aut}(G) \cong \mathsf{Aut}(H) \quad \not\Longrightarrow \quad G \cong H$$

Άσκηση 6.6.40. *Έστω G μια ομάδα για την οποία ισχύει ότι δείκτης $[G : \mathsf{Z}(G)] = 4$. Να δειχθεί ότι η ομάδα $\mathsf{Inn}(G)$ είναι ισόμορφη με την ομάδα $\mathcal{V}_4$ του Klein.*

Άσκηση 6.6.41. *Να δειχθούν οι ακόλουθοι ισχυρισμοί σχετικά με ομάδες αυτομορφισμών συμμετρικών και εναλλασσουσών ομάδων:*[5]

1. $\mathsf{Aut}(\mathsf{S}_n) = \mathsf{Aut}(\mathsf{A}_n) = \{\iota\}$, *αν* $n = 1$ *ή* $n = 2$.
2. $\mathsf{Aut}(\mathsf{S}_3) \cong \mathsf{S}_3$ *και* $\mathsf{Aut}(\mathsf{A}_3) \cong \mathsf{S}_2$.

Άσκηση 6.6.42. *Έστω G μια ομάδα με τάξη $\mathsf{o}(G) = 2p$, όπου p είναι ένας περιττός πρώτος αριθμός. Να δειχθεί ότι η G περιέχει μια κανονική υποομάδα τάξης p.*

Άσκηση 6.6.43. *Έστω a ένας θετικός ακέραιος > 1. Να δειχθεί ότι για κάθε θετικό ακέραιο n ισχύει ότι*[6] *$n \mid \phi(a^n - 1)$.*

Υπόδειξη: Θεωρήστε μια κυκλική ομάδα $G = \langle x \rangle$ με τάξη $a^n - 1$ και δείξτε ότι η απεικόνιση $f : G \longrightarrow G$, $f(g) = g^a$ είναι ένας αυτομορφισμός της G του οποίου η τάξη στην ομάδα $\mathsf{Aut}(G)$ είναι ίση με n. Έτσι $n = \mathsf{o}(f) \mid |\mathsf{Aut}(G)| = \phi(|G|) = a^n - 1$.

Άσκηση 6.6.44. *Έστω G μια πεπερασμένη ομάδα η οποία διαθέτει έναν αυτομορφισμό $\phi \in \mathsf{Aut}(G)$ για τον οποίο ισχύει ότι:*

$$\forall x \in G : \quad \phi(x) = x \quad \Longrightarrow \quad x = e$$

1. *Να δειχθεί ότι*
$$G = \{x^{-1}\phi(x) \in G \mid x \in G\}$$
2. *Αν επιπλέον $\phi^2 = \iota$, να δειχθεί ότι η ομάδα G είναι αβελιανή περιττής τάξης.*

Υπόδειξη: Για το μέρος 2. να χρησιμοποιηθεί το μέρος 1., η Άσκηση 6.6.31, και η Άσκηση 3.9.11.

Άσκηση 6.6.45. *Θεωρούμε του μοναδιαίο πίνακα πραγματικών αριθμών I_n και συμβολίζουμε με E_k, $1 \le k \le n$ τις στήλες του. Ορίζουμε μιαν απεικόνιση*

$$\Phi : \mathsf{S}_n \longrightarrow \mathsf{GL}(n, \mathbb{R}), \quad f(\sigma) = \sigma(I_n)$$

όπου η k-στήλη του πίνακα $\sigma(I_n)$ είναι η $\sigma(k)$-στήλη $E_{\sigma(k)}$ του I_n.

1. *Να δειχθεί ότι η απεικόνιση Φ είναι ένας ομομορφισμός ομάδων. Ποιος είναι ο πυρήνας του ομομορφισμού Φ; Ποια είναι η εικόνα του Φ;*

[5] Αποδεικνύεται με περισσότερο προχωρημένες μεθόδους από όσες μπορούμε να αναλύσουμε εδώ ότι:

1. $\mathsf{Aut}(\mathsf{S}_6) \cong \mathsf{Aut}(\mathsf{A}_6)$ και $\mathsf{Inn}(\mathsf{S}_6) \cong \mathsf{S}_6$ και $[\mathsf{Aut}(\mathsf{S}_6) : \mathsf{Inn}(\mathsf{S}_6)] = 2$.
2. Για κάθε $6 \neq n > 3$: $\mathsf{Aut}(\mathsf{S}_n) \cong \mathsf{Aut}(\mathsf{A}_n) \cong \mathsf{S}_n$.

Για μια απόδειξη παραπέμπουμε στο βιβλίο [32].

[6] Ο ισχυρισμός της Άσκησης είναι ένα γνωστό αποτέλεσμα της στοιχειώδους Θεωρίας Αριθμών. Εδώ ζητείται να αποδειχθεί ο ισχυρισμός με χρήση Θεωρίας Ομάδων.

2. *Να δειχθεί ότι η εικόνα της σύνθεσης απεικονίσεων* $|\cdot|\circ\Phi\colon \mathsf{S}_n \longrightarrow \mathbb{R}^*$

$$\mathsf{S}_n \xrightarrow{\Phi} \mathsf{GL}(n,\mathbb{R}) \xrightarrow{|\cdot|} \mathbb{R}^*, \quad \sigma \longmapsto |\sigma(I_n)|$$

είναι η πολλαπλασιαστική ομάδα $\{1,-1\}$, *και η σύνθεση* $|\cdot|\circ\Phi$ *συμπίπτει με τον ομομορφισμό προσήμου* $\epsilon\colon \mathsf{S}_n \longrightarrow \{1,-1\}$, $\sigma \longmapsto \epsilon(\sigma)$.

Άσκηση 6.6.46. *Να εφαρμοστεί το Θεώρημα αντιστοιχίας 6.3.8 για τον ομομορφισμό ομάδων*

$$f\colon \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_6, \quad f([k]_{12}) = [k]_6$$

Άσκηση 6.6.47. *Να αποδειχθεί το Πόρισμα 6.5.15: Έστω ότι* G *είναι μια απλή ομάδα με τάξη* $\mathsf{o}(G) > 2$ *και υποθέτουμε ότι η* G *περιέχει μια υποομάδα* H *με δείκτη* $[G:H] = n > 1$. *Να δειχθεί η* G *είναι ισόμορφη με μια υποομάδα της εναλλάσσουσας ομάδας* A_n.

Άσκηση 6.6.48. *Έστω* G *μια αβελιανή ομάδα τάξης* 9 *η οποία παράγεται από δύο στοιχεία* a *και* b *τάξης* 3, *για παράδειγμα* $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. *Να δειχθεί ότι το πλήθος των αυτομορφισμών της* G *είναι ίσο με* 48.

Άσκηση 6.6.49. *Έστω* G *μια ομάδα. Μια υποομάδα* $H \leq G$ *καλείται* **χαρακτηριστική υποομάδα** *της* G *αν* $\phi(H) \subseteq H$, $\forall \phi \in \mathsf{Aut}(G)$.

1. *Να δειχθεί ότι κάθε χαρακτηριστική υποομάδα της* G *είναι κανονική υποομάδα της* G.
2. *Να δειχθεί ότι μια υποομάδα* H *της* G *είναι κανονική υποομάδα αν και μονον αν* $\phi(H) \subseteq H$, $\forall \phi \in \mathsf{Inn}(G)$.
3. *Είναι κάθε κανονική υποομάδα της* G *χαρακτηριστική υποομάδα της* G;
   Υπόδειξη: Θεωρήστε την ομάδα $G = \{e, a, b, ab\}$ *των τεσσάρων στοιχείων του Klein και την (κανονική) υποομάδα* $H = \{e, a\}$.

Άσκηση 6.6.50. *Έστω* G *μια ομάδα.*

1. *Να δειχθεί ότι το κέντρο* $\mathsf{Z}(G)$ *της* G *είναι χαρακτηριστική υποομάδα της* G.
2. *Να δειχθεί ότι η μεταθέτρια υποομάδα* $[G,G]$ *της* G *είναι είναι χαρακτηριστική υποομάδα της* G.
3. *Να δειχθεί ότι μια χαρακτηριστική υποομαδα, άρα και κανονική υποομάδα, μιας κανονικής υποομάδας* N *της* G *είναι κανονική υποομάδα της* G.

Άσκηση 6.6.51. *Έστω ότι* $\{G_i\}_{i=1}^n$ *και* $\{H_j\}_{j=1}^m$ *είναι αβελιανές ομάδες, και έστω*

$$G = G_1 \times G_2 \times \cdots \times G_n \qquad \text{και} \qquad H = H_1 \times H_2 \times \cdots \times H_m$$

οι αντίστοιχες ομάδες ευθύ γινόμενο. Να δειχθεί ότι υπάρχει ένας ισομορφισμός ομάδων:

$$\mathsf{Hom}(G,H) \xrightarrow{\cong} \prod_{i=1}^{n}\prod_{j=1}^{m} \mathsf{Hom}(G_i,H_j)$$

Άσκηση 6.6.52. *Να σχεδιαστεί ο πίνακας Cayley της ομάδας των αυτομορφισμών τών κυκλικών ομάδων* $\mathbb{Z}_8$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ *και* $\mathbb{Z}_{15}$.
Τι παρατηρείτε για τις ομάδες αυτομορφισμών $\mathsf{Aut}(\mathbb{Z}_8)$ *και* $\mathsf{Aut}(\mathbb{Z}_{10})$;

Άσκηση 6.6.53. *Να ολοκληρώσετε την απόδειξη του Λήμματος 6.4.12.*

Άσκηση 6.6.54. *Έστω $f: G \longrightarrow G$ ένας αυτομορφισμός μιας ομάδας G. Αν $N \trianglelefteq G$ είναι μια κανονική υποομάδα της G έτσι ώστε $f(N) \subseteq N$, να περιγράψετε πώς μπορεί η f να ορίσει έναν αυτομορφισμό $f: G/N \longrightarrow G/N$ της ομάδας πηλίκο G/N.*

Αν $G = \mathsf{S}_3$ και $N = \langle (1\ 2\ 3) \rangle \trianglelefteq \mathsf{S}_3$, να δοθεί παράδειγμα αυτομορφισμού της S_3 έτσι ώστε $f(N) \subseteq N$ και να περιγραφεί ο επαγόμενος αυτομορφισμός $f^*: \mathsf{S}_3/N \longrightarrow \mathsf{S}_3/N$.

Άσκηση 6.6.55. *Αν G είναι μια ομάδα, θεωρούμε, για κάθε $g \in G$, τις «1-1» και «επί» απεικονίσεις*

$$\mathsf{L}_g: G \longrightarrow G, \quad \mathsf{L}_g(x) = gx \qquad \text{και} \qquad \mathsf{R}_g: G \longrightarrow G, \quad \mathsf{R}_g(x) = xg$$

1. *Να δειχθεί ότι $\forall g, h \in G$: $\mathsf{L}_g \circ \mathsf{R}_h = \mathsf{R}_h \circ \mathsf{L}_g$.*
2. *Αν $f: G \longrightarrow G$ είναι μια «1-1» και «επί» απεικονίση έτσι ώστε $\forall h \in G$: $\mathsf{R}_h \circ f = f \circ \mathsf{R}_h$, τότε υπάρχει $g \in G$ έτσι ώστε: $f = \mathsf{L}_g$.*
3. *Να δειχθεί ότι*
$$\bigcap_{g \in G} \mathsf{C}_{\mathsf{S}(G)}(\mathsf{R}_g) = \mathsf{Im}(\mathsf{L}) \cong G$$
όπου $\mathsf{L}: G \longrightarrow G$, $g \longmapsto \mathsf{L}_g$ είναι η αριστερή κανονική αναπαράσταση της G.

Άσκηση 6.6.56. *Έστω $f: G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων.*

1. *Αν H είναι μια κανονική υποομάδα της G_1 η οποία περιέχει του πυρήνα του f, δηλαδή $\mathsf{Ker}(f) \leq H \trianglelefteq G_1$, τότε η υποομάδα $f(H)$ είναι μια κανονική υποομάδα της $\mathsf{Im}(f)$ και υπάρχει ένας ισομορφισμός ομάδων*
$$f^*: G_1/H \xrightarrow{\cong} \mathsf{Im}(f)/f(H)$$
Ιδιαίτερα αν ο f είναι επιμορφισμός, τότε υπάρχει ένας ισομορφισμός ομάδων
$$f^*: G_1/H \xrightarrow{\cong} G_2/f(H)$$
2. *Αν K είναι μια κανονική υποομάδα της $\mathsf{Im}(f)$, δηλαδή $K \trianglelefteq \mathsf{Im}(f) \leq G_2$, τότε η υποομάδα $f^{-1}(K)$ είναι μια κανονική υποομάδα της G_1 και υπάρχει ένας ισομορφισμός ομάδων*
$$f^*: G_1/f^{-1}(K) \xrightarrow{\cong} \mathsf{Im}(f)/K$$
Ιδιαίτερα αν ο f είναι επιμορφισμός, τότε υπάρχει ένας ισομορφισμός ομάδων
$$f^*: G_1/f^{-1}(K) \xrightarrow{\cong} G_2/K$$

Άσκηση 6.6.57. *Έστω G μια ομάδα και $f: G \longrightarrow G$ ένας ενδομορφισμός της G. Υποθέτουμε ότι*

$$\forall \iota_g \in \mathsf{Inn}(G): \quad f \circ \iota_g = \iota_g \circ f$$

Να δειχθεί ότι το υποσύνολο $H = \{x \in G \mid f^2(x) = f(x)\}$ είναι μια κανονική υποομάδα της G.

Άσκηση 6.6.58. *Έστω G μια πεπερασμένη αβελιανή ομάδα και υποθέτουμε ότι κάθε μη ταυτοτικό στοιχείο της G έχει τάξη ίση με 2. Να δειχθεί ότι υπάρχει ένας θετικός ακέραιος m έτσι ώστε:*

$$G \xrightarrow{\cong} \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2 \quad (m - \text{παράγοντες})$$

Σκοπός της επόμενης Άσκησης είναι η απόδειξη του ισχυρισμού ότι κάθε πεπερασμένη ομάδα G με $|G| > 2$ περιέχει έναν μη ταυτοτικό αυτομορφισμό.

Άσκηση 6.6.59. *Έστω ότι G είναι μια ομάδα με τάξη $|G|>2$.*

1. *Αν η ομάδα G δεν είναι αβελιανή, τότε $\mathsf{Z}(G)\neq G$ και άρα η ομάδα πηλίκο $G/\mathsf{Z}(G)$, η οποία είναι ισόμορφη με την ομάδα $\mathsf{Inn}(G)$ των εσωτερικών αυτομορφισμών της G, δεν είναι η τετριμμένη.*

   Άρα η G περιέχει έναν μη ταυτοτικό (εσωτερικό) αυτομορφισμό.

2. *Έστω ότι η ομάδα G είναι αβελιανή.*

   (α') Υποθέτουμε ότι η G περιέχει τουλάχιστον ένα στοιχείο $a\neq e$ με τάξη $\neq 2$. Να δειχθεί ότι η απεικόνιση $f: G\longrightarrow G$, $f(x)=x^{-1}$ είναι ένας μη ταυτοτικός αυτομορφισμός της G.

   (β') Υποθέτουμε ότι όλα τα μη ταυτοτικά στοιχεία της G έχουν τάξη ίση με 2. Τότε από την Άσκηση 6.6.58, έχουμε έναν ισομορφισμό

   $$G \xrightarrow{\cong} \mathbb{Z}_2\times\mathbb{Z}_2\times\cdots\times\mathbb{Z}_2 \quad (m-\text{παράγοντες})$$

   για κάποιον θετικό ακέραιο n, όπου $\mathbb{Z}_2=\langle a_k\rangle$, $1\leq k\leq m$. Να δειχθεί ότι ορίζοντας $f: G\longrightarrow G$, $f(a_1)=a_2$ και $f(a_k)=a_k$, $3\leq k\leq m$, αποκτούμε έναν μη ταυτοτικό αυτομορφισμό της G.

Να συμπεράνετε ότι κάθε πεπερασμένη ομάδα G με $|G|>2$ περιέχει έναν μη ταυτοτικό αυτομορφισμό:

$$2<|G|<\infty \implies |\mathsf{Aut}(G)|\neq 1$$

Άσκηση 6.6.60. *Έστω $f: G\longrightarrow G$ ένας αυτομορφισμός μιας πεπερασμένης ομάδας G ο οποίος στέλνει περισσότερα από τα $\frac{3}{4}$ των στοιχείων της G στο αντίστροφο τους. Να δειχθεί ότι η ομάδα G είναι αβελιανή και $f(x)=x^{-1}$, $\forall x\in G$.*

Υπόδειξη - Σκιαγράφηση Απόδειξης: *Έστω $|G|=n$. Θέτουμε $H=\{a\in G\mid f(a)=a^{-1}\}$ και τότε $|H|>\frac{3}{4}n$.*

1. *Να δειχθεί ότι $\forall h\in H$: $|H\cap Hh|>\frac{n}{2}$.*
2. *Να δειχθεί ότι για κάθε $h\in H$: $H\cap Hh\subseteq \mathsf{N}_G(h)$, από όπου έπεται ότι $\frac{3}{4}n<|\mathsf{N}_G(h)|\,|G|=n$ και επομένως $\mathsf{N}_G(h)=G$, δηλαδή $h\in\mathsf{Z}(G)$. Έτσι $H\subseteq\mathsf{Z}(G)$.*
3. *Επειδή $H\subseteq\mathsf{Z}(G)$, έπεται ότι $\frac{3}{4}n<|\mathsf{Z}(G)|\,|G|=n$ και επομένως $\mathsf{Z}(G)=G$, δηλαδή η ομάδα G είναι αβελιανή.*
4. *Να δειχθεί ότι το υποσύνολο H είναι μια υποομάδα της G.*
5. *Από τις σχέσεις $\frac{3}{4}n<|H|\,|G|=n$ έπεται ότι $|H|=|G|$ και επομένως $H=G$.*

Άσκηση 6.6.61. *Θεωρώντας τη μη αβελιανή ομάδα $Q=\{\pm 1,\pm i,\pm j,\pm k\mid i^2=j^2=k^2=ijk=-1\}$ των τετρανίων του Hamilton, να κατασκευαστεί ένας αυτομορφισμός της ομάδας Q ο οποίος στέλνει ακριβώς τα $\frac{3}{4}$, δηλαδή 6, των 8 στοιχείων της Q στο αντίστροφό τους.*[7]

Άσκηση 6.6.62. *Έστω G μια πεπερασμένη ομάδα άρτιας τάξης $2n$. Υποθέτουμε ότι τα μισά στοιχεία της G έχουν τάξη 2 και τα υπόλοιπα μισά σχηματίζουν μια υποομάδα τάξης n. Να δειχθεί ότι η H είναι μια αβελιανή υποομάδα της G με τάξη έναν περιττό αριθμό.*

Υπόδειξη-Σκιαγράφηση Απόδειξης: *Έστω K το σύνολο των στοιχείων της G με τάξη 2.*

1. *Τότε $G=K\cup H$ και η H είναι μια κανονική υποομάδα της G διότι είναι δείκτη $[G:H]=\frac{2n}{n}=2$ στην G.*

[7] Αποδεικνύεται ότι υπάρχει ένας ισομορφισμός ομάδων:

$$\mathsf{Aut}(Q)\ \cong\ \mathsf{S}_4$$

2. *Για κάθε στοιχείο* $k = k^{-1} \in K$, *και για κάθε στοιχείο* $h \in H$, *να δειχθεί ότι* $hk = (hk)^{-1}$ *και* $h = kh^{-1}k$. *Επομένως*
$$\forall x \in H: \quad x = kx^{-1}k$$
3. *Αν* $x, y \in H$, *τότε γράφοντας* $x = kx^{-1}k$ *και* $y = ky^{-1}k$, *να δειχθεί ότι* $xy = yx$. *Επομένως η* H *είναι αβελιανή.*
4. *Η τάξη της* H *είναι περιττός αριθμός διότι διαφορετικά η* H *θα περιείχε ένα στοιχείο τάξης* 2, *το οποίο είναι άτοπο.*

Μέρος ΙΙ

Θεωρία Δακτυλίων

Κεφάλαιο 7

Δακτύλιοι: Βασικές Ιδιότητες και Παραδείγματα

Στο παρόν Κεφάλαιο θα μελετήσουμε την θεμελιώδη έννοια του δακτυλίου, θα αναπτύξουμε τις βασικές ιδιότητες δακτυλίων και θα αναλύσουμε μια σειρά κατασκευών και παραδειγμάτων δακτυλίων επί των οποίων θα υλοποιηθεί η θεωρία.

7.1 Η Έννοια του Δακτυλίου και Βασικές Ιδιότητες

Ξεκινάμε με την έννοια του δακτυλίου η οποία υποδεικνύει μια ενδιαφέρουσα αλληλεπίδραση μεταξύ προσθετικής αβελιανής ομάδας και πολλαπλασιαστικού μονοειδούς.

Ορισμός 7.1.1. *Ένας* **δακτύλιος** *είναι μια τριάδα* $(R,+,\cdot)$*, όπου:*

1. *Το ζεύγος* $(R,+)$ *είναι μια αβελιανή ομάδα.*
2. *Το ζεύγος* $(R,\cdot)$ *είναι ένα μονοειδές.*
3. *Ικανοποιείται η* **επιμεριστική ιδιότητα** *της πράξης της πρόσθεσης «+» ως προς την πράξη του πολλαπλασιασμού «·»:*

$$\forall r,s,t\in R: \qquad r\cdot(s+t)=r\cdot s+r\cdot t \quad \text{και} \quad (r+s)\cdot t=r\cdot t+s\cdot t \tag{Επιμεριστική Ιδιότητα}$$

Το ουδέτερο ή μηδενικό στοιχείο της ομάδας το συμβολίζουμε με 0 *ή* 0_R*, και θα το καλούμε το* **μηδενικό στοιχείο** *του δακτυλίου* R*, και το ουδέτερο ή μοναδιαίο στοιχείο του μονοειδούς* $(R,\cdot)$ *θα το συμβολίζουμε με* 1 *ή με* 1_R*, και θα το καλούμε* **μονάδα** *του δακτυλίου* R*.*

Αναλυτικότερα, ένας δακτύλιος είναι μια τριάδα $(R,+,\cdot)$, αποτελούμενη από ένα συνολο R το οποίο είναι εφοδιασμένο με δύο εσωτερικές διμελείς πράξεις

$$+ : R\times R \longrightarrow R, \quad (r_1,r_2)\longmapsto r_1+r_2 \tag{πρόσθεση}$$

$$\cdot : R\times R \longrightarrow R, \quad (r_1,r_2)\longmapsto r_1\cdot r_2 \tag{πολλαπλασιασμός}$$

έτσι ώστε να ικανοποιούνται τα ακόλουθα αξιώματα:

1. Η πράξη «+» είναι **προσεταιριστική**, δηλαδή ισχύει ότι:

$$\forall r_1,r_2,r_3\in R: \quad r_1+(r_2+r_3)=(r_1+r_2)+r_3 \tag{7.1}$$

2. Υπάρχει ένα στοιχείο 0_R ή απλά $0\in R$, το οποίο καλείται **μηδενικό στοιχείο** του R, έτσι ώστε:

$$\forall r\in R: \quad r+0_R=r=0_R+r \tag{7.2}$$

3. Για κάθε στοιχείο $r \in R$, υπάρχει ένα στοιχείο $-r \in R$, το οποίο καλείται **αντίθετο στοιχείο** του r, έτσι ώστε να ισχύει:
$$\forall r \in R, \ \exists -r \in R: \quad r + (-r) = 0_R = (-r) + r \tag{7.3}$$

4. Η πράξη «+» είναι **μεταθετική**
$$\forall r, s \in R: \qquad r + s = s + r \tag{7.4}$$

5. Η πράξη «·» είναι **προσεταιριστική**
$$\forall r_1, r_2, r_3 \in R: \quad r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3 \tag{7.5}$$

6. Για τις πράξεις «+» και «·» ισχύει η **επιμεριστική ιδιότητα**
$$\forall r, s, t \in R: \qquad r \cdot (s + t) = r \cdot s + r \cdot t \qquad \text{και} \qquad (r + s) \cdot t = r \cdot t + s \cdot t \tag{7.6}$$

7. Υπάρχει ένα στοιχείο $1 \in R$, το οποίο καλείται **μονάδα** του R, έτσι ώστε:
$$\forall r \in R: \quad r \cdot 1_R = r = 1_R \cdot r \tag{7.7}$$

Παρατήρηση 7.1.2. Όπως γνωρίζουμε από τη θεωρία ομάδων και μονοειδών, τα στοιχεία 0_R και 1_R στον ορισμό δακτυλίου είναι μοναδικά, και από τώρα και στο εξής, αν δεν δημιουργείται κίνδυνος σύγχυσης, θα τα συμβολίζουμε απλά με 0 και 1 αντίστοιχα. Παρόμοια, το αντίθετο $-r$ του στοιχείου r είναι μοναδικό.

Από τώρα και στο εξής, θα χρησιμοποιούμε τις συμβάσεις και τους συμβολισμούς για πράξεις, μονοειδή, και ομάδες, που εισαγάγαμε και ακολουθήσαμε στο Πρώτο μέρος των σημειώσεων. Έτσι, για παράδειγμα, θα γράφουμε $r + (-s) = r - s$. Τέλος, χάριν απλότητας, και αν δεν υπάρχει κίνδυνος σύγχυσης, θα γράφουμε απλώς R για έναν δακτύλιο $(R, +, \cdot)$. ▲

Παρατήρηση 7.1.3. Ο Ορισμός 7.1.1 αφορά την έννοια του δακτυλίου, και είναι ο επικρατέστερος. Ακριβέστερα, ο Ορισμός 7.1.1 περιγράφει την έννοια του **προσεταιριστικού δακτυλίου με μονάδα**. Υπάρχουν και κάποιες διαφοροποιήσεις στον ορισμό δακτυλίου στη βιβλιογραφία:

1. Αν στον Ορισμό 7.1.1 απαλείψουμε το αξίωμα (7.7) περί ύπαρξης μονάδας, τότε αποκτούμε την έννοια του **δακτυλίου χωρίς μονάδα**, και με αυτή την ορολογία εννοούμε ότι ο δακτύλιος δεν έχει απαραίτητα μονάδα. Υπάρχουν αρκετά ενδιαφέροντα παραδείγματα δακτυλίων χωρίς μονάδα τα οποία θα μελετήσουμε, αλλά το κύριο αντικείμενο μελέτης μας στις παρούσες σημειώσεις θα αφορά δακτυλίους με μονάδα.

2. Αν στον Ορισμό 7.1.1 απαλείψουμε το αξίωμα (7.5) περί προσεταιριστικότητας του πολλαπλασιασμού, τότε αποκτούμε την έννοια του **μη προσεταιριστικού δακτυλίου** και με αυτή την ορολογία εννοούμε ότι η πράξη του πολλαπλασιασμού του δακτύλιου δεν είναι απαραίτητα προσεταιριστική. Υπάρχουν αρκετά ενδιαφέροντα παραδείγματα μη προσεταιριστικών δακτυλίων χωρίς μονάδα τα οποία θα αναφέρουμε, αλλά το κύριο αντικείμενο μελέτης μας θα αφορά σχεδόν αποκλειστικά προσεταιριστικούς δακτυλίους με μονάδα. ▲

Η επόμενη Πρόταση περιέχει βασικές ιδιότητες οι οποίες απορρέουν από τα αξιώματα δακτυλίου. Αυτές οι ιδιότητες, καθώς και η απόδειξή τους, μας είναι ήδη γνωστές από την Ενότητα 1.3 του Κεφαλαίου 1, η οποία περιγράφει γενικές ιδιότητες πράξεων. Εδώ ενδιαφερόμαστε για τις πράξεις «+» και «·» ενός δακτυλίου $(R, +, \cdot)$, και υπενθυμίζουμε ότι, επειδή για την πράξη «+» της πρόσθεσης υπάρχει ουδέτερο στοιχείο, το 0_R, μπορούμε να ορίσουμε τα ακέραια πολλαπλάσια nx, κάθε στοιχείου $x \in R$ του δακτυλίου R, όπου $n \in \mathbb{Z}$:

$$nx := \begin{cases} \underbrace{x + x + \cdots + x}_{n-\text{παράγοντες}}, & \text{αν } n \geq 1 \\ 0_R, & \text{αν } n = 0 \\ \underbrace{(-x) + (-x) + \cdots + (-x)}_{(-n)-\text{παράγοντες}}, & \text{αν } n < 0 \end{cases}$$

Παρόμοια, επειδή για την πράξη «·» του πολλαπλασιασμού υπάρχει ουδέτερο στοιχείο, το 1_R, ορίζονται οι φυσικές δυνάμεις x^n κάθε στοιχείου $x \in R$ του δακτυλίου R, όπου $n \in \mathbb{N}_0$:

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \cdots \cdot x}_{n-\text{παράγοντες}}, & \text{αν } n \geq 1 \\ 1_R, & \text{αν } n = 0 \end{cases}$$

Πρόταση 7.1.4. *Έστω $R = (R, +, \cdot)$ ένας δακτύλιος. Αν $x, x_1, x_2, \cdots, x_n$, $n \geq 1$, είναι στοιχεία του R, τότε:*

1. *Τα στοιχεία $x_1 + x_2 + \cdots + x_n$ και $x_1 \cdot x_2 \cdot \cdots \cdot x_n$ του R είναι μονοσήμαντα ορισμένα.*
2. *Για κάθε μετάθεση $\sigma \in \mathsf{S}_n$, ισχύει ότι:*

$$x_1 + x_2 + \cdots + x_n = x_{\sigma(1)} + x_{\sigma(2)} + \cdots + x_{\sigma(n)}$$

Αν επιπλέον $x_i \cdot x_j = x_j \cdot x_i$, $1 \leq i, j \leq n$, τότε:

$$x_{\sigma(1)} \cdot x_{\sigma(2)} \cdot \cdots \cdot x_{\sigma(n)} = x_1 \cdot x_2 \cdot \cdots \cdot x_n$$

3. *Για κάθε $n, m \in \mathbb{Z}$:*
   - *(α΄)* $(n+m)x = nx + mx$.
   - *(β΄)* $n(mx) = (nm)x$.
   - *(γ΄)* $-(nx) = (-n)x = n(-x)$.
   - *(δ΄)* $n(x_1 + x_2) = nx_1 + nx_2$.
4. *Για κάθε $n, m \in \mathbb{N}_0$:*
   - *(α΄)* $x^{n+m} = x^n \cdot x^m$.
   - *(β΄)* $(x^n)^m = x^{nm}$.
   - *(γ΄)* *Αν* $x_1 \cdot x_2 = x_2 \cdot x_1$, *τότε:* $(x_1 \cdot x_2)^n = x_1^n \cdot x_2^n$.

Η επόμενη Πρόταση περιέχει βασικές ιδιότητες οι οποίες απορρέουν από τα αξιώματα δακτυλίου και οι οποίες αφορούν αλληλεπίδρασεις μεταξύ των πράξεων «+» και «·» σε έναν δακτύλιο $R = (R, +, \cdot)$.

Πρόταση 7.1.5. *Έστω $R = (R, +, \cdot)$ ένας δακτύλιος. Τότε ισχύουν οι εξής ιδιότητες:*

1. $\forall r \in R$: $r \cdot 0_R = 0_R = 0_R \cdot r$ *και* $(-1_R) \cdot r = -r = r \cdot (-1_R)$.
2. $\forall r, s \in R$: $(-r) \cdot s = r \cdot (-s) = -(r \cdot s)$ *και* $(-r) \cdot (-s) = r \cdot s$.
3. $\forall x, y, z \in R$: $x \cdot (y - z) = x \cdot y - x \cdot z$ *και* $(x - y) \cdot z = x \cdot z - y \cdot z$.
4. *Έστω ότι* $\{r_i\}_{i=1}^n$ *και* $\{s_j\}_{j=1}^m$ *είναι στοιχεία του δακτυλίου R. Τότε:*

$$\begin{aligned} (r_1 + r_2 + \cdots + r_n) \cdot (s_1 + s_2 + \cdots + s_m) &= (\sum_{i=1}^{n} r_i) \cdot (\sum_{j=1}^{m} s_j) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{m} r_i s_j \\ &= r_1 \cdot s_1 + \cdots + r_n \cdot s_1 + r_1 \cdot s_2 + \cdots + r_n \cdot s_2 + \cdots + r_1 \cdot s_m + \cdots + r_n \cdot s_m \end{aligned}$$

5. $\forall n \in \mathbb{Z}$, $\forall x, y \in R$:
   - *(α΄)* $n(x \cdot y) = (nx) \cdot y = x \cdot (ny)$

(β') $(nx)\cdot(my)=(nm)(x\cdot y)$.

(γ') $(n1_R)\cdot x=nx$.

Απόδειξη. 1. Χρησιμοποιώντας την επιμεριστική ιδιότητα (7.6) και τον νόμο διαγραφής στην ομάδα $(R,+)$, θα έχουμε

$$r\cdot 0_R=r\cdot(0_R+0_R)=r\cdot 0_R+r\cdot 0_R \implies r\cdot 0_R=0_R \quad \text{και} \quad 0_R\cdot r=(0_R+0_R)\cdot r=0_R\cdot r+0_R\cdot r \implies 0_R\cdot r=0_R$$

Παρόμοια:

$$(-1_R)\cdot r+r=(-1_R)\cdot r+1_R\cdot r=((-1_R)+1_R)\cdot r=0_R\cdot r=0_R=0_R\cdot r=(1_R+(-1_R))\cdot r=1_R\cdot r+(-1_R)\cdot r$$

Επομένως $(-1_R)\cdot r=-r$, και ανάλογα εργαζόμενοι θα έχουμε $r\cdot(-1_R)=-r$.

2. Χρησιμοποιώντας την επιμεριστική ιδιότητα (7.6), και το μέρος 1., θα έχουμε:

$$r\cdot s+r\cdot(-s)=r\cdot(s+(-s))=r\cdot 0_R=0_R=0_R\cdot s=((-r)+r)\cdot s=(-r)\cdot s+r\cdot s \implies (-r)\cdot s=-(r\cdot s)$$

$$r\cdot s+r\cdot(-s)=r\cdot(s+(-s))=r\cdot 0_R=0_R=r\cdot 0_R=r\cdot((-s)+s)=r\cdot(-s)+r\cdot s \implies r\cdot(-s)=-(r\cdot s)$$

Παρόμοια, χρησιμοποιώντας τις παραπάνω σχέσεις, θα έχουμε:

$$(-r)\cdot(-s)=-(r\cdot(-s))=-(-(r\cdot s))=r\cdot s$$

3. Χρησιμοποιώντας την επιμεριστική ιδιότητα, και το μέρος 2., θα έχουμε:

$$x\cdot(y-z)=x\cdot(y+(-z))=x\cdot y+x\cdot(-z)=x\cdot y+(-(x\cdot z))=x\cdot y-x\cdot z$$

Παρόμοια αποδεικνύεται η σχέση $(x-y)\cdot z=x\cdot z-y\cdot z$.

4. Υποθέτουμε πρώτα ότι $r=1$, και εφαρμόζουμε την Αρχή Μαθηματικής Επαγωγής στο πλήθος m των στοιχείων $\{s_j\}_{j=1}^m$. Αν $m=1$, τότε δεν έχουμε να αποδείξουμε τίποτα. Αν $s=2$, τότε το ζητούμενο προκύπτει από την επιμεριστική ιδιότητα (7.6). Υποθέτουμε ότι $r_1\cdot(\sum_{j=1}^k s_j)=\sum_{j=1}^k r_1\cdot s_j$, για κάθε k με $2\le k<m$. Τότε $r_1\cdot(\sum_{j=1}^m s_j)=r_1\cdot(s_1+\sum_{j=2}^m s_j)=r_1\cdot s_1+r_1\cdot\sum_{j=1}^m s_j=r_1\cdot s_1+\sum_{j=2}^m r_1\cdot s_j=\sum_{j=1}^m r_1\cdot s_j$. Άρα η ζητούμενη σχέση ισχύει αν $r=1$, και για κάθε $m\ge 1$. Υποθέτουμε ισχύει για κάθε k με $2\le k<n$ και για κάθε $m\ge 1$, δηλαδή $(\sum_{i=1}^k r_i)\cdot(\sum_{j=1}^m s_j)=\sum_{i=1}^k\sum_{j=1}^m r_i\cdot s_j$. Τότε $(\sum_{i=1}^n r_i)\cdot(\sum_{j=1}^m s_j)=(r_1+\sum_{i=2}^n r_i)\cdot(\sum_{j=1}^m s_j)=r_1\cdot\sum_{j=1}^m s_j+(\sum_{i=2}^n r_i)\cdot(\sum_{j=1}^m s_j)=\sum_{j=1}^m r_1\cdot s_j+\sum_{i=2}^n\sum_{j=1}^m r_i\cdot s_j=\sum_{i=1}^n\sum_{j=1}^m r_i\cdot s_j$.

5. Θέτοντας $r_1=r_2=\cdots=r_n=x$, $m=1$, και $s_1=y$ στο μέρος 3., θα έχουμε:

$$(nx)\cdot y=(x+x+\cdots+x)\cdot y=x\cdot y+x\cdot y+\cdots+x\cdot y=n(x\cdot y) \quad \text{και}$$

Παρόμοια, θέτοντας $n=1$, $r_1=x$, και $s_1=s_2=\cdots=s_n=y$, $m=1$, στο μέρος 3., θα έχουμε:

$$x\cdot(ny)=x\cdot(y+y+\cdots+y)=x\cdot y+x\cdot y+\cdots+x\cdot y=n(x\cdot y)$$

Θέτοντας $r_i=x$, $1\le i\le n$ και $s_j=y$, $1\le j\le m$, θα έχουμε:

$$(nx)\cdot(ny)=(\sum_{i=1}^n r_i)\cdot(\sum_{j=1}^m s_j)=\sum_{i=1}^n\sum_{j=1}^m r_i\cdot s_j=(nm)(x\cdot y)$$

Τέλος, θέτοντας στην παραπάνω σχέση $x=1_R$, $m=1$, και $y=x$, θα έχουμε:

$$(n1_R)\cdot x=n(1_R\cdot x)=nx$$

■

Από τώρα και στο εξης σταθεροποιούμε έναν δακτύλιο $R = (R, +, \cdot)$.

Αν x, y είναι στοιχεία του R, τότε για το στοιχείο $(x+y)^2 = (x+y)\cdot(x+y)$, από την Πρόταση 7.1.5, θα έχουμε $(x+y)^2 = x\cdot x + x\cdot y + y\cdot x + y\cdot y = x^2 + x\cdot y + y\cdot x + y^2$. Αυτό το ανάπτυγμα δεν είναι απαραίτητα ίσο με το ανάπτυγμα $x^2 + 2x\cdot y + y^2$, και ο λόγος είναι ότι γενικά, όπως θα δούμε και σε παραδείγματα αργότερα, $x\cdot y + y\cdot x \neq x\cdot y + x\cdot y = 2x\cdot y$, με άλλα λόγια αυτό συμβαίνει διότι γενικά $x\cdot y \neq y\cdot x$.

Θα λέμε ότι δυο στοιχεία $x, y \in R$ **μετατίθενται**, αν: $x\cdot y = y\cdot x$. Για στοιχεία τα οποία μετατίθενται σε έναν δακτύλιο ισχύει ο ακόλουθος οικείος τύπος, όπου $r^0 = 1_R$. Υπενθυμίζουμε ότι, αν $0 \leq k \leq n$, τότε ορίζεται ο *Διωνυμικός συντελεστής*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

και ισχύουν τα εξής: $\binom{n}{0} = \binom{n}{n} = \binom{n}{k} = 1$, και $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$.

Πρόταση 7.1.6 (Τύπος Διωνύμου)**.** *Έστω ότι x, y είναι δύο στοιχεία σε έναν δακτύλιο R για τα οποία ισχύει ότι $x\cdot y = y\cdot x$. Τότε για κάθε θετικό ακέραιο n ισχύει ότι:*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}\cdot y^k \tag{7.8}$$

Απόδειξη. Η απόδειξη θα γίνει με χρήση της Αρχής Μαθηματικής Επαγωγής. Για $n = 1$, δεν χρειάζεται να δείξουμε τίποτα, διότι $(x+y)^1 = x+y = \binom{1}{0}x + \binom{1}{1}y$. Υποθέτουμε ότι η σχέση (7.8) ισχύει για τον θετικό ακέραιο n. Τότε, χρησιμοποιώντας επανειλημμένα την επιμεριστική ιδιότητα και την μεταθετικότητα των στοιχείων x, y, θα έχουμε:

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)^n\cdot(x+y)\\
&= \Big(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\cdot y^k\Big)\cdot(x+y)\\
&= \Big(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\cdot y^k\Big)\cdot x + \Big(\sum_{k=0}^{n}\binom{n}{k}x^{n-k}\cdot y^k\Big)\cdot y\\
&= \sum_{k=0}^{n}\binom{n}{k}x^{n-k+1}\cdot y^k + \sum_{k=0}^{n}\binom{n}{k}x^{n-k}\cdot y^{k+1}\\
&= \binom{n}{0}x^{n+1} + \Big(\binom{n}{0}+\binom{n}{1}\Big)x^n\cdot y^1 + \cdots + \Big(\binom{n}{k-1}+\binom{n}{k}\Big)x^{n+1-k}\cdot y^k + \cdots + \binom{n}{n}y^{n+1}\\
&= \binom{n+1}{0}x^{n+1} + \binom{n+1}{1}x^n\cdot y^1 + \cdots + \binom{n+1}{k}x^{n+1-k}\cdot y^k + \cdots + \binom{n+1}{n+1}y^{n+1}
\end{aligned}$$

Άρα η σχέση (7.8) ισχύει και για τον θετικό ακέραιο $n+1$ και επομένως, σύμφωνα με την Αρχή Μαθηματικής Επαγωγής, είναι αληθής για κάθε φυσικό αριθμό n. ■

Παρατηρούμε ότι, όταν δύο στοιχεία σε έναν δακτύλιο μετατίθενται, τότε πολλές ιδιότητες οι οποίες μας είναι οικείες από ιδιότητες γνωστών μας αριθμητικών συστημάτων ισχύουν και σε έναν δακτύλιο. Αυτή η παρατήρηση, καθώς και το γεγονός ότι, όπως θα δούμε στην επόμενη υποενότητα, σε πολλά σημαντικά παραδείγματα δακτυλίων όλα τα στοιχεία μετατίθενται, μας οδηγεί στον ακόλουθο ορισμό.

Ορισμός 7.1.7. *Ένας δακτύλιος R καλείται* **μεταθετικός δακτύλιος** *αν, $\forall x, y \in R$ ισχύει ότι: $x\cdot y = y\cdot x$.*

Η κλάση των μεταθετικών δακτυλίων είναι η πλέον μελετημένη κλάση δακτυλίων, και σε αυτές τις σημειώσεις θα μελετήσουμε κυρίως αυτή την κλάση δακτυλίων καθώς αυτή έχει πλούσια θεωρία και υποστηρίζεται όπως θα δούμε και απο πολλά οικεία και σημαντικά παραδείγματα.

Σε ένα σύνολο R με ακριβώς ένα στοιχείο, έστω $R = \{\omega\}$, μπορούν να οριστούν πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» κατά προφανή τρόπο έτσι ώστε η τριάδα $(R, +, \cdot)$ να είναι δακτύλιος: $\omega + \omega = \omega$ και $\omega \cdot \omega = \omega$. Το μηδενικό στοιχείο του R συμπίπτει με την μονάδα του R: $1_R = 0_R = \omega$. Αντίστροφα, αν $(R, +, \cdot)$ είναι ένας δακτύλιος με την ιδιότητα $1_R = 0_R$, τότε για κάθε στοιχείο $r \in R$ θα έχουμε: $r = 1_R \cdot r = 0_R \cdot r = 0_R$, και επομένως $R = \{0_R\}$, δηλαδή το σύνολο R είναι μονοσύνολο. Άρα ένας δακτύλιος αποτελείται από ένα μόνο στοιχείο αν και μονον αν $0_R = 1_R$. Ένας δακτύλιος για τον οποίο συμβαίνει ότι $0_R = 1_R$ καλείται ο **μηδενικός** ή ο **τετριμμένος δακτύλιος** και δεν θα μας απασχολήσει στη συνέχεια.

Από τώρα και στο εξής, θα χρησιμοποιούμε τις παραπάνω βασικές ιδιότητες δακτυλίων χωρίς ιδιαίτερη αναφορά. Επίσης, όταν δεν δημιουργείται σύγχυση, θα γράφουμε απλά xy για το γινόμενο $x \cdot y$ δύο στοιχείων $x, y \in R$, σε έναν δακτύλιο R.

7.2 Παραδείγματα Δακτυλίων

Στην παρούσα υποενότητα θα περιγράψουμε αναλυτικά παραδείγματα και κλάσεις παραδειγμάτων δακτυλίων, και τα οποία θα μας απασχολήσουν και στη συνέχεια. Επίσης θα μελετήσουμε ειδικού τύπου δακτυλίους οι οποίοι ταξινομούν σημαντικές ιδιότητες τις οποίες μπορεί να έχει ή να μην έχει ένας δακτύλιος.

Ξεκινάμε με κάποια οικεία παραδείγματα δακτυλίων. Κάποια από αυτά θα αποτελέσουν πηγή γενικεύσεων και αιτία εισαγωγής νέων κλάσεων και τύπων δακτυλίων.

Παράδειγμα 7.2.1.

1. (Ο Δακτύλιος $\mathbb{Z}$ των Ακεραίων). Το πρωταρχικό παράδειγμα δακτυλίου είναι ο δακτύλιος $\mathbb{Z}$ των ακεραίων, δηλαδή η τριάδα $(\mathbb{Z}, +, \cdot)$, όπου «+» και «·» είναι οι συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού ακεραίων. Είναι οικείο και άμεσα διαπιστώσιμο ότι η τριάδα $(\mathbb{Z}, +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. Το μηδενικό στοιχείο είναι το 0 και η μονάδα το 1.

2. (Ο Δακτύλιος $\mathbb{Q}$ των Ρητών). Το σύνολο $\mathbb{Q}$ των ρητών αριθμών, δηλαδή η τριάδα $(\mathbb{Q}, +, \cdot)$, όπου «+» και «·» είναι οι συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού ρητών αριθμών. Είναι οικείο και άμεσα διαπιστώσιμο ότι η τριάδα $(\mathbb{Q}, +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. Το μηδενικό στοιχείο είναι το 0 και η μονάδα το 1.

3. (Ο Δακτύλιος $\mathbb{R}$ των Πραγματικών). Το σύνολο $\mathbb{R}$ των πραγματικών αριθμών, δηλαδή η τριάδα $(\mathbb{R}, +, \cdot)$, όπου «+» και «·» είναι οι συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών. Είναι οικείο και άμεσα διαπιστώσιμο ότι η τριάδα $(\mathbb{R}, +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. Το μηδενικό στοιχείο είναι το 0 και η μονάδα το 1.

4. (Ο Δακτύλιος $\mathbb{C}$ των Μιγαδικών). Το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών, δηλαδή η τριάδα $(\mathbb{C}, +, \cdot)$, όπου «+» και «·» είναι οι συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών. Είναι οικείο και άμεσα διαπιστώσιμο ότι η τριάδα $(\mathbb{C}, +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. Το μηδενικό στοιχείο είναι το 0 και η μονάδα το 1. $\surd$

Παράδειγμα 7.2.2. Έστω X ένα τυχόν μη κενό σύνολο και θεωρούμε το σύνολο $\mathscr{F}(X, \mathbb{R})$ όλων των πραγματικών συναρτήσεων ορισμένων επί του X:

$$\mathscr{F}(X, \mathbb{R}) = \{f : X \longrightarrow \mathbb{R} \mid f : \text{ συνάρτηση}\}$$

Όπως στο Μέρος I, επί του συνόλου X ορίζονται πράξεις πρόσθεσης και πολλαπλασιασμού

$$+, \cdot \ : \ \mathscr{F}(X, \mathbb{R}) \times \mathscr{F}(X, \mathbb{R}) \longrightarrow \mathscr{F}(X, \mathbb{R}), \quad (f, g) \longmapsto f + g, \ f \cdot g$$

όπου $(f + g)(x) = f(x) + g(x)$, και $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in X$.

Τότε είναι εύκολο να διαπιστωθεί ότι το σύνολο $(\mathscr{F}(X, \mathbb{R}), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα. Το μηδενικό στοιχείο του δακτυλίου $\mathscr{F}(X, \mathbb{R})$ είναι η σταθερή μηδενική συνάρτηση $0 : X \longrightarrow \mathbb{R}$, $0(x) = 0$, $\forall x \in X$, και η μονάδα του δακτυλίου $\mathscr{F}(X, \mathbb{R})$ είναι η σταθερή συνάρτηση με τιμή 1, δηλαδή $1 : X \longrightarrow \mathbb{R}$, $1(x) = 1$, $\forall x \in X$. Η διαπίστωση των αξιωμάτων είναι άμεση, καθώς συνίσταται στη διαπίστωση των αντίστοιχων αξιωμάτων για τον δακτύλιο $(\mathbb{R}, +, \cdot)$, για τον οποίο γνωρίζουμε ότι ισχύουν. $\surd$

Παράδειγμα 7.2.3. Έστω $(M,+)$ μια προσθετική αβελιανή ομάδα. Θεωρούμε το σύνολο

$$\mathsf{End}_{\mathbb{Z}}(M) = \{f\colon M \longrightarrow M \mid f:\ \text{ενδομορφισμός της } M\} = \{f\colon M \longrightarrow M \mid f(x+y) = f(x)+f(y),\ \forall x,y \in M\}$$

Γνωρίζουμε ότι το σύνολο $\mathsf{End}_{\mathbb{Z}}(M)$ είναι αβελιανή ομάδα με πράξη «+» την πρόσθεση ενδομορφισμών:

$$\forall f,g \in \mathsf{End}_{\mathbb{Z}}(M):\quad f+g:\ M \longrightarrow M,\quad (f+g)(x) = f(x)+g(x)$$

Πράγματι η απεικόνιση $f+g$ ειναι ενδομορφισμός της M διότι $(f+g)(x+y) = f(x+y)+g(x+y) = f(x)+f(y)+g(x)+g(y) = f(x)+g(x)+f(y)+g(y) = (f+g)(x)+(f+g)(y)$. Η αβελιανή ομάδα $(\mathsf{End}_{\mathbb{Z}}(M),+)$ είναι επίσης εφοδιασμένη και με την πράξη «$\circ$» της σύνθεσης απεικονίσεων. Πράγματι η σύνθεση

$$f\circ g:\ M \longrightarrow M,\quad (f\circ g)(x) = f(g(x))$$

ενδομορφισμών $f,g \in \mathsf{End}_{\mathbb{Z}}(M)$ είναι ενδομορφισμός διότι $(f\circ g)(x+y) = f(g(x+y)) = f(g(x)+g(y)) = f(g(x))+f(g(y)) = (f\circ g)(x)+(f\circ g)(y)$. Επειδή η σύνθεση απεικονίσεων είναι προσεταιριστική, και προφανώς η ταυτοτική απεικόνιση Id_M του M είναι ενδομορφισμός, έπεται ότι το ζεύγος $(\mathsf{End}_{\mathbb{Z}}(M),\circ)$ είναι ένα μονοειδές. Τέλος, αν $f,g,h \in \mathsf{End}_{\mathbb{Z}}(M)$, τότε, $\forall x \in M$:

$$[f\circ(g+h)](x) = f((g+h)(x)) = f(g(x)+h(x)) = f(g(x))+f(h(x)) = (f\circ g)(x)+(f\circ h)(x)$$

$$[(f+g)\circ h](x) = ((f+g)(h(x)) = f(h(x))+g(h(x)) = (f\circ h)(x)+(g\circ h)(x)$$

Άρα $f\circ(g+h) = f\circ g+f\circ h$ και $(f+g)\circ h = f\circ h+g\circ h$, δηλαδή ισχύει η επιμεριστική ιδιότητα και επομένως η τριάδα $(\mathsf{End}_{\mathbb{Z}}(M),+,\cdot)$ είναι ένας δακτύλιος με μονάδα, τον ταυτοτικό ενδομορφισμό Id_M, ο οποίος καλείται ο **δακτύλιος ενδομορφισμών** της αβελιανής ομάδας M.

Ο δακτύλιος ενδομορφισμών $\mathsf{End}_{\mathbb{Z}}(M)$ γενικά δεν είναι μεταθετικός. Για παράδειγμα, έστω η αβελιανή ομάδα ευθύ γινόμενο $M = \mathbb{Z}\times\mathbb{Z}$ της προσθετικής ομάδας $(\mathbb{Z},+)$ με τον εαυτό της, και έστω οι απεικονίσεις

$$f,g\colon \mathbb{Z}\times\mathbb{Z} \longrightarrow \mathbb{Z}\times\mathbb{Z},\quad f(n,m) = (m,n),\quad g(n,m) = (n,n+m)$$

Είναι εύκολο να διαπιστωθεί ότι οι απεικονίσεις f,g είναι ενδομορφισμοί της $\mathbb{Z}\times\mathbb{Z}$, και ισχύει $f\circ g \neq g\circ f$ διότι, για παράδειγμα,

$$(f\circ g)(1,1) = f(g(1,1)) = f(1,2) = (2,1) \neq (1,2) = g(1,1) = g(f(1,1)) = (g\circ f)(1,1)$$

Άρα ο δακτύλιος ενδομορφισμών $\mathsf{End}_{\mathbb{Z}}(\mathbb{Z}\times\mathbb{Z})$ δεν είναι μεταθετικός. $\surd$

Τα παραπάνω είναι παραδείγματα δακτυλίων με άπειρο πλήθος στοιχείων. Υπάρχουν όμως και ενδιαφέροντα παραδείγματα δακτυλίων με πεπερασμένο πλήθος στοιχείων.

Παράδειγμα 7.2.4. Για κάθε θετικό ακέραιο $n \geq 1$, θεωρούμε την προσθετική αβελιανή ομάδα $(\mathbb{Z}_n,+)$ των κλάσεων υπολοίπων mod n. Γνωρίζουμε ότι το σύνολο $\mathbb{Z}_n$ είναι εφοδιασμένο και με την πράξη πολλαπλασιασμού «$\cdot$» κλάσεων υπολοίπων mod n, έτσι ώστε το ζεύγος $(\mathbb{Z}_n,\cdot)$ να είναι ένα μεταθετικό μονοειδές. Επειδή προφανώς ισχύει ότι:

$$[x]_n\cdot([y]_n+[z]_n) = [x]_n\cdot[y+z]_n = [x\cdot(y+z)]_n = [x\cdot y+x\cdot z]_n = [x]_n\cdot[y]_n+[x]_n\cdot[z]_n$$

έπεται ότι ισχύει και η επιμεριστική ιδιότητα, και η τριάδα $(\mathbb{Z}_n,+,\cdot)$ είναι ένας μεταθετικός δακτύλιος με μηδενικό στοιχείο την κλάση $[0]_n$ και μονάδα την κλάση $[1]_n$. $\surd$

Στο παραπάνω Παράδειγμα 7.2.1 έχουμε εγκλείσεις δακτυλίων $\mathbb{Z}\subseteq\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$ και καθένα από τα εμπλεκόμενα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι δακτύλιος με τις ίδιες πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών περιορισμένες στο υποσύνολο. Αυτή η παρατήρηση μας οδηγεί φυσιολογικά στην έννοια του υποδακτυλίου.

Ορισμός 7.2.5. *Ένα υποσύνολο $S \subseteq R$ καλείται* **υποδακτύλιος** *του δακτυλίου $R = (R, +, \cdot)$, αν το ζεύγος $(S, +)$ είναι υποομάδα της προσθετικής ομάδας $(R, +)$ του δακτυλίου R, και το ζεύγος $(S, \cdot)$ είναι υπομονοειδές του πολλαπλασιαστικού μονοειδούς $(R, \cdot)$.*

Αναλυτικότερα, το υποσύνολο S είναι υποδακτύλιος του R, αν:

1. $\forall x, y \in S$: $x - y \in S$.
2. $\forall x, y \in S$: $x \cdot y \in S$.
3. $1_R \in S$.

Έτσι στις εγκλείσεις $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, κάθε δακτύλιος είναι υποδακτύλιος του επομένου.

Όπως βλέπουμε, η έννοια του υποδακτυλίου είναι ανάλογη της έννοιας της υποομάδας (και του υπομονοειδούς). Παρ' όλα αυτά η σπουδαιότητα των υποδακτυλίων στη θεωρία δακτυλίων δεν είναι ανάλογη με τη σπουδαιότητα των υποομάδων στη θεωρία ομάδων, και χρησιμεύει κυρίως στην αναγνώριση νέων δακτυλίων από παλαιούς, όπως δείχνει η ακόλουθη Πρόταση.

Πρόταση 7.2.6. *Έστω $R = (R, +, \cdot)$ ένας δακτύλιος και $S \subseteq R$ ένα υποσύνολο του R. Τότε το S είναι υποδακτύλιος του R αν και μόνο αν το σύνολο S είναι κλειστό στις πράξεις «$+$» και «$\cdot$» του δακτυλίου R, και η τριάδα $(S, +, \cdot)$ είναι δακτύλιος.*

Απόδειξη. Προφανώς, αν το σύνολο S είναι κλειστό στις πράξεις «$+$» και «$\cdot$» του δακτυλίου R και η τριάδα $(S, +, \cdot)$ με τις επαγόμενες πράξεις είναι δακτύλιος, τότε το ζεύγος $(S, +)$ είναι ομάδα και το ζεύγος $(S, \cdot)$ είναι μονοειδές. Επομένως, από την Πρόταση 2.4.5 και το Πόρισμα 1.4.8, έπεται ότι το S είναι υποδακτύλιος του R. Αντίστροφα, αν το υποσύνολο S είναι υποδακτύλιος του R, τότε το ζεύγος $(S, +)$ είναι υποομάδα της ομάδας $(R, +)$, και το ζεύγος $(S, \cdot)$ είναι υπομονοειδές του $(R, \cdot)$, και τότε ικανοποιούνται όλα τα αξιώματα του Ορισμού 7.1.1, με πιθανή εξαίρεση το αξίωμα (7.6) που αφορά την επιμεριστική ιδιότητα. Είναι όμως προφανές ότι ισχύει η επιμεριστική ιδιότητα στο S διότι ισχύει στον δακτύλιο R και οι πράξεις «$+$» και «$\cdot$» είναι οι περιορισμοί στο S των πράξεων του δακτυλίου R. ■

Προφανώς, αν ο S είναι υποδακτύλιος του R, τότε οι δακτύλιοι R και S έχουν την ίδια μονάδα, και ο δακτύλιος S είναι μεταθετικός αν ο R είναι μεταθετικός. Γενικότερα, όπως θα δούμε και στη συνέχεια, ένας υποδακτύλιος κληρονομεί κάποιες από τις ιδιότητες, αλλά όχι όλες, του δακτυλίου.

Παράδειγμα 7.2.7. 1. Θεωρούμε τα υποσύνολα του συνόλου $\mathbb{C}$ των μιγαδικών αριθμών

$$\mathbb{Z}[i] = \{m + ni \in \mathbb{C} \mid m, n \in \mathbb{Z}\} \quad \text{και} \quad \mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

τα οποία περιέχουν την μονάδα 1 του δακτυλίου $\mathbb{C}$ και για τα οποία διαπιστώνουμε εύκολα ότι είναι κλειστά στην αφαίρεση και στον πολλαπλασιασμό μιγαδικών αριθμών. Επομένως τα υποσύνολα $\mathbb{Z}[i]$ και $\mathbb{Q}[i]$ είναι υποδακτύλιοι του $\mathbb{C}$, και άρα, σύμφωνα με την Πρόταση 7.2.6, είναι δακτύλιοι. Ο δακτύλιος $\mathbb{Z}[i]$ καλείται ο **δακτύλιος των ακέραιων του Gauss** και ο δακτύλιος $\mathbb{Q}[i]$ καλείται ο **δακτύλιος των ρητών του Gauss**.

2. Για κάθε θετικό ακέραιο m, ο οποίος είναι ελεύθερος τετραγώνου,[1] θεωρούμε το υποσύνολο

$$\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$$

Τότε $a + b\sqrt{m} = c + d\sqrt{m}$, όπου $a, b, c, d \in \mathbb{Z}$, αν και μόνο αν $a = c$ και $b = d$. Πράγματι, αν $a + b\sqrt{m} = c + d\sqrt{m}$, και $b \neq d$ ή $a \neq c$, τότε θα έχουμε $a \neq c$, διότι διαφορετικά θα έχουμε $\sqrt{m} = 0$ και αυτό είναι άτοπο ή $b - d \neq 0$ αντίστοιχα. Επομένως, σε κάθε περίπτωση $\frac{a-c}{b-d} = \sqrt{m}$, όπου οι $a - c$ και $b - d$ είναι μη μηδενικοί ακέραιοι και τότε $m = (\frac{a-c}{b-d})^2$. Αυτό είναι άτοπο διότι ο m είναι ελεύθερος τετραγώνου. Επομένως αναγκαστικά θα έχουμε $a = c$ και $b = d$.

[1] Ένας ακέραιος καλείται ελεύθερος τετραγώνου, αν δεν διαιρείται από τετράγωνο ακεραίου $\neq 1$.

Προφανώς, $1 = 1 + 0\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$. Αν $a + b\sqrt{m},\ c + d \in \sqrt{m} \in \mathbb{Z}[\sqrt{m}]$, τότε

$$(a + b\sqrt{m}) - (c + d\sqrt{m}) = (a - c) + (b - d)\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$$

$$(a + b\sqrt{m}) \cdot (c + d\sqrt{m}) = (ac + dbd) + (ad + bc)\sqrt{m} \in \mathbb{Z}[\sqrt{m}]$$

Επομένως το υποσύνολο $\mathbb{Z}[\sqrt{m}]$ είναι ένας υποδακτύλιος του $\mathbb{R}$, ο οποίος είναι μεταθετικός διότι ο δακτύλιος $\mathbb{R}$ είναι μεταθετικός.

3. Για ένα κλειστό διάστημα της πραγματικής ευθείας $[a, b] \subseteq \mathbb{R}$, θεωρούμε το σύνολο

$$\mathscr{C}([a, b], \mathbb{R}) = \{f : [a, b] \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$$

όλων των συνεχών πραγματικών συναρτήσεων ορισμένων επί του $[a, b]$. Το σύνολο $\mathscr{C}([a, b], \mathbb{R})$ είναι υποσύνολο του δακτυλίου $\mathscr{F}([a, b], \mathbb{R})$ όλων των πραγματικών συναρτήσεων επί του $[a, b]$ και ως τέτοιο είναι υπδακτύλιος διότι περιέχει την ταυτοτική συνάρτηση $1 : [a, b] \longrightarrow \mathbb{R}$, η οποία είναι συνεχής, και περιέχει την διαφορά $f - g$ και το γινόμενο $f \cdot g$ συναρτήσεων $f, g \in \mathscr{C}([a, b], \mathbb{R})$, καθώς η διαφορά και το γινόμενο συνεχών συναρτήσεων είναι συνεχής συνάρτηση. Επειδή ο δακτύλιος $\mathscr{F}([a, b], \mathbb{R})$ είναι μεταθετικός, έπεται ότι ο δακτύλιος $\mathscr{C}([a, b], \mathbb{R})$ είναι ένας μεταθετικός δακτύλιος με μονάδα.

4. Έστω $\mathcal{V} = (\mathcal{V}, +, \cdot)$ ένας $\mathbb{K}$-διανυσματικός χώρος, όπου $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ ή $\mathbb{C}$. Υπενθυμίζουμε από τη Γραμμική Άλγεβρα, ότι η τριάδα $(\mathcal{V}, +, \cdot)$ ένας $\mathbb{K}$-*διανυσματικός χώρος*, αν το ζεύγος $(\mathcal{V}, +)$ είναι αβελιανή ομάδα και $\cdot : \mathbb{K} \times \mathcal{V} \longrightarrow \mathcal{V},\ (k, \vec{x}) \longmapsto k \cdot \vec{x}$ είναι μια εξωτερική πράξη, ο *βαθμωτός πολλαπλασιασμός* του $\mathbb{K}$ επί του $\mathcal{V}$, για την οποία ισχύουν τα εξής: $(\alpha)\ k \cdot (\vec{x} + \vec{y}) = k \cdot \vec{x} + k \cdot \vec{y}$, $(\beta)\ (k + l) \cdot \vec{x} = k \cdot \vec{x} + l \cdot \vec{x}$, $(\gamma)\ (kl) \cdot \vec{x} = k \cdot (l \cdot \vec{x})$, $(\delta)\ 1 \cdot \vec{x} = \vec{x}$, όπου $\vec{x}, \vec{y} \in \mathcal{V}$ και $k, l \in \mathbb{K}$. Υπενθυμίζουμε ότι μια απεικόνιση $f : \mathcal{V} \longrightarrow \mathcal{V}$ καλείται $\mathbb{K}$-*γραμμική* αν $(\alpha)\ f(\vec{x} + \vec{y}) = f(\vec{x}) + f(\vec{y})$, και $(\beta)\ f(k \cdot \vec{x}) = kf(\vec{x})$, όπου $\vec{x}, \vec{y} \in \mathcal{V}$ και $k \in \mathbb{K}$.

   Θεωρούμε το σύνολο

$$\mathsf{End}_{\mathbb{K}}(\mathcal{V}) = \{f : \mathcal{V} \longrightarrow \mathcal{V} \mid f : \mathbb{K}\text{-γραμμική απεικόνιση}\}$$

   Προφανώς $\mathsf{End}_{\mathbb{K}}(\mathcal{V}) \subseteq \mathsf{End}_{\mathbb{Z}}(\mathcal{V})$, και ο ταυτοτικός ενδομορφισμός $\mathrm{Id}_{\mathcal{V}}$ της αβελιανής ομάδας $(\mathcal{V}, +)$ είναι $\mathbb{K}$-γραμμική απεικόνιση. Επιπλέον είναι γνωστό από τη Γραμμική Άλγεβρα, και είναι εύκολο να διαπιστωθεί, ότι η διαφορά και η σύνθεση $\mathbb{K}$-γραμμικών απεικονίσεων είναι $\mathbb{K}$-γραμμική απεικόνιση. Επομένως το σύνολο $\mathsf{End}_{\mathbb{K}}(\mathcal{V})$ είναι ένας υποδακτύλιος του δακτυλίου $(\mathsf{End}_{\mathbb{Z}}(\mathcal{V}), +, \circ)$, βλέπε το Παράδειγμα 7.2.3 και άρα είναι ένας δακτύλιος με μονάδα, ο δακτύλιος των $\mathbb{K}$-**γραμμικών απεικονίσεων** ή ο **δακτύλιος ενδομορφισμών** του $\mathbb{K}$-διανυσματικού χώρου $\mathcal{V}$.

   Ο δακτύλιος $\mathsf{End}_{\mathbb{K}}(\mathcal{V})$ γενικά δεν είναι μεταθετικός. Για παράδειγμα, αν $\mathbb{K} = \mathbb{R}$ και $\mathcal{V} = \mathbb{R}^2$, τότε οι απεικονίσεις

$$f, g : \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \quad f(x, y) = (y, x), \quad g(x, y) = (x, x + y)$$

   είναι γραμμικές, άρα είναι στοιχεία του δακτυλίου $\mathsf{End}_{\mathbb{K}}(\mathcal{V})$, και όπως και στο Παράδειγμα 7.2.3, έχουμε $f \circ g \neq g \circ f$. Άρα ο δακτύλιος ενδομορφισμών $\mathsf{End}_{\mathbb{K}}(\mathbb{R}^2)$ δεν είναι μεταθετικός. $\surd$

Παρατήρηση 7.2.8. Θεωρούμε το υποσύνολο $2\mathbb{Z} \subseteq \mathbb{Z}$ των άρτιων ακεραίων. Το υποσύνολο $2\mathbb{Z}$ είναι προφανώς κλειστό στη διαφορά και στον πολλαπλασιασμό ακεραίων. Όμως το υποσύνολο δεν είναι υποδακτύλιος διότι δεν περιέχει τη μονάδα 1 του δακτυλίου $\mathbb{Z}$. Στην πραγματικότητα το υποσύνολο δεν έχει ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό και επομένως δεν είναι δακτύλιος με την έννοια του ορισμού 7.1.1, παρόλο που ικανοποιεί όλα τα αξιώματα του Ορισμού, εκτός από την ύπαρξη μονάδας. Πράγματι, αν υπήρχε ουδέτερο στοιχείο $e = 2m$, τότε θα είχαμε $2m \cdot 2k = 2k$, για κάθε $k \in \mathbb{Z}$ και τότε για $k = 1$ θα έπρεπε $2m = 1$, το οποίο είναι άτοπο. Έτσι το σύνολο $2\mathbb{Z}$ είναι ένας δακτύλιος χωρίς μονάδα.

Από την άλλη πλευρά, κάθε προσθετική αβελιανή ομάδα $R = (R, +)$ μπορεί να θεωρηθεί ως δακτύλιος χωρίς μοναδα ορίζοντας τετριμμένο πολλαπλασιασμό $x \cdot y = 0,\ \forall x, y \in R$. ▲

Παρατήρηση 7.2.9. Στη βιβλιογραφία δεν συναντάται πάντα η συνθήκη 3. στον ορισμό υποδακτυλίου 7.2.5. Συνήθως αυτό συμβαίνει όταν ο ορισμός δακτυλίου δεν απαιτεί την ύπαρξη μονάδας. Σκοπός αυτών των περισσότερο γενικών ορισμών είναι η κάλυψη περισσοτέρων κλάσεων (υπο)δακτυλιών. Θα καλούμε **υποδακτύλιο χωρίς μονάδα** του δακτυλίου R, ένα μη κενό υποσύνολο S του R το οποίο ικανοποιεί τις δύο πρώτες συνθήκες του Ορισμού 7.2.5, αλλά όχι απαραίτητα τη συνθήκη 3.

Ας δούμε κάποια φαινόμενα τα οποία εμφανίζονται όταν δεν απαιτήσουμε την ύπαρξη μονάδας σε έναν υποδακτύλιο.

1. Υπάρχουν δακτύλιοι (με μονάδα) οι οποίοι περιέχουν υποδακτυλίους χωρίς μονάδα. Για παράδειγμα, ο δακτύλιος $\mathbb{Z}$ έχει μονάδα, αλλά περιέχει ως υποδακτύλιο χωρίς μονάδα, το υποσύνολο $2\mathbb{Z}$ των άρτιων ακεραίων, βλέπε την Παρατήρηση 7.2.8.

2. Υπάρχουν υποδακτύλιοι (με μονάδα) σε δακτυλίους χωρίς μονάδα. Για παράδειγμα, το σύνολο $R = \left\{ \left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) \mid x, y \in \mathbb{R} \right\}$ με τις συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων είναι, όπως μπορεί να διαπιστωθεί εύκολα, ένας δακτύλιος χωρίς μονάδα και περιέχει ως υποδακτύλιο το υποσύνολο $S = \left\{ \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right) \mid x \in \mathbb{R} \right\}$ ο οποίος έχει μονάδα $1_S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

3. Υπάρχουν δακτύλιοι με μονάδα οι οποίοι περιέχουν υποδακτυλίους με διαφορετική μονάδα. Για παράδειγμα, το σύνολο $R = \left\{ \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \mid x, y, z, w \in \mathbb{R} \right\}$ των 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς είναι, με τις συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων, δακτύλιος με μονάδα τον μοναδιαίο πίνακα $I_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Το σύνολο S του μέρους 2. είναι υποδακτύλιος του R με διαφορετική μονάδα. Επίσης, όπως θα δούμε αργότερα, το ευθύ γινόμενο ομάδων $R = \mathbb{Z} \times \mathbb{Z}$ μπορεί να γίνει δακτύλιος με μονάδα το ζεύγος $1_R = (1,1)$. Ο δακτύλιος R περιέχει ως υποδακτύλιο το υποσύνολο $S = \{(x,0) \in \mathbb{Z} \times \mathbb{Z} \mid x \in \mathbb{Z}\}$ ο οποίος έχει μονάδα το ζεύγος $1_S = (1,0) \neq (1,1) = 1_R$. ▲

Σε καθένα από τα επόμενα παραδείγματα τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, θεωρούνται ως (μεταθετικοί) δακτύλιοι με μονάδα εφοδιασμένα με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού, όπως στο Παράδειγμα 7.2.1.

Παράδειγμα 7.2.10. (Δακτύλιοι Πινάκων) Έστω $\mathbb{K} = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ή $\mathbb{C}$, και έστω $\mathsf{M}_n(\mathbb{K})$ το σύνολο όλων των τετραγωνικών $n \times n$ πινάκων A με στοιχεία από το $\mathbb{K}$:

$$\mathsf{M}_n(\mathbb{K}) = \left\{ A = (a_{ij}) \mid a_{ij} \in \mathbb{R},\ 1 \leq i, j \leq n \right\}, \quad \text{όπου} \quad A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{m2} & \cdots & a_{nn} \end{pmatrix}$$

Όπως στο μέρος 4 του Παραδείγματος 2.2.2 το σύνολο $\mathsf{M}_n(\mathbb{K})$ είναι εφοδιασμένο με τις πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» τετραγωνικών πινάκων. Υπενθυμίζουμε ότι, αν $A = (a_{ij})$ και $B = (b_{ij})$ είναι δύο τετραγωνικοί πίνακες, τότε:

$$A + B = (c_{ij}), \quad \text{όπου} \quad c_{ij} = a_{ij} + b_{ij}, \quad 1 \leq i, j \leq n$$

$$A \cdot B = ((A \cdot B)_{ij}) = (c_{ij}), \quad \text{όπου} \quad c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad 1 \leq i, j \leq n$$

και το ζεύγος $(\mathsf{M}_n(\mathbb{K}), +)$ είναι μια αβελιανή ομάδα με μηδενικό στοιχείο τον μηδενικό πίνακα $\mathsf{O} = (x_{ij})$, όπου $x_{ij} = 0$, $1 \leq i, j \leq n$, και το ζεύγος $(\mathsf{M}_n(\mathbb{K}), \cdot)$ είναι ένα μονοειδές με μονάδα τον μοναδιαίο $n \times n$ πίνακα $I_n = (\delta_{ij})$, όπου δ_{ij} είναι το δ του Kronecker, δηλαδή $\delta_{ij} = \begin{cases} 1, & \text{αν, } i = j \\ 0, & \text{αν, } i \neq j \end{cases}$, $1 \leq i, j \leq n$. Αν A και B είναι δυο τετραγωνικοί πίνακες όπως παραπάνω και $C = (c_{ij})$ είναι ένας τρίτος πίνακας, τότε θα έχουμε:

$$(A+B)\cdot C = (a_{ij}+b_{ij})\cdot(c_{ij}) = (d_{ij}), \quad \text{όπου} \quad d_{ij} = \sum_{k=1}^{n} (a_{ik}+b_{ik})c_{kj} = \sum_{k=1}^{n} (a_{ik}c_{kj}+b_{ik})c_{kj}) = \sum_{k=1}^{n} a_{ik}c_{kj} + \sum_{k=1}^{n} b_{ik}c_{kj}$$

$$A\cdot C+B\cdot C=(a_{ij}\cdot(c_{ij})+(b_{ij})\cdot(c_{ij})=(d'_{ij})\quad \text{όπου}\quad d'_{ij}=\sum_{k=1}^{n}a_{ik}c_{kj}+\sum_{k=1}^{n}b_{ik}c_{kj}$$

Άρα $d_{ij}=d'_{ij}$, $1\le i,j\le n$, και επομένως $(A+B)\cdot C=A\cdot C+B\cdot C$. Εργαζόμενοι παρόμοια, βλέπουμε ότι $A\cdot(B+C)=A\cdot B+A\cdot C$, δηλαδή ισχύει η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση. Συνοψίζοντας, δείξαμε ότι η τριάδα $(\mathsf{M}_n(\mathbb{K}),+,\cdot)$ ικανοποιεί τα αξιώματα του Ορισμού 7.1.1 και άρα είναι ένας δακτύλιος, ο **δακτύλιος των** $n\times n$**-πινάκων** με στοιχεία από το $\mathbb{K}$.

Επειδή, όταν $n\ge 2$, ο πολλαπλασιασμός $n\times n$ πινάκων γενικά δεν είναι μεταθετική πράξη, ο δακτύλιος $\mathsf{M}_n(\mathbb{K})$ γενικά δεν είναι μεταθετικός, για παράδειγμα:

$$\begin{pmatrix}1&1&\cdots&1\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0\end{pmatrix}\cdot\begin{pmatrix}1&0&\cdots&0\\1&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\1&0&\cdots&0\end{pmatrix}=\begin{pmatrix}n&0&\cdots&0\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0\end{pmatrix}\neq\begin{pmatrix}1&1&\cdots&1\\1&1&\cdots&1\\\vdots&\vdots&\ddots&\vdots\\1&1&\cdots&1\end{pmatrix}=\begin{pmatrix}1&0&\cdots&0\\1&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\1&0&\cdots&0\end{pmatrix}\cdot\begin{pmatrix}1&1&\cdots&1\\0&0&\cdots&0\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0\end{pmatrix}\quad\surd$$

Παράδειγμα 7.2.11. Έστω $\mathbb{K}=\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, ή $\mathbb{C}$, και έστω $\mathsf{AT}_n(\mathbb{K})$ το σύνολο όλων των άνω τριγωνικών $n\times n$ πινάκων A με στοιχεία από το $\mathbb{K}$:

$\mathsf{AT}_n(\mathbb{K})=\{A=(a_{ij})\in\mathsf{M}_n(\mathbb{K})\mid a_{ij}=0,\ 1\le j<i\le n\}$, δηλαδή ένα τυπικό στοιχείο του $\mathsf{AT}_n(\mathbb{K})$ είναι της μορφής

$$A=(a_{ij})=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\0&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&a_{nn}\end{pmatrix}$$

Όπως μπορεί να διαπιστωθεί εύκολα, βλέπε την Άσκηση 7.6.3, το υποσύνολο $\mathsf{AT}_n(\mathbb{K})$ είναι ένας υποδακτύλιος του $\mathsf{M}_n(\mathbb{K})$, και άρα είναι ένας δακτύλιος, ο δακτύλιος των **άνω τριγωνικών** $n\times n$**-πινάκων** με στοιχεία από το $\mathbb{K}$, και ο οποίος δεν είναι μεταθετικός.

Σημειώνουμε ότι το υποσύνολο

$$I=\{A=(a_{ij})\in\mathsf{AT}_n(\mathbb{K})\mid a_{ii}=0,\ 1\le i\le n\},\quad \text{δηλαδή ένα τυπικό στοιχείο του } I \text{ είναι της μορφής}$$

$$A=(a_{ij})=\begin{pmatrix}0&a_{12}&\cdots&a_{1n}\\0&0&\cdots&a_{2n}\\\vdots&\vdots&\ddots&\vdots\\0&0&\cdots&0\end{pmatrix}$$

είναι μη κενό, και κλειστό στις πράξεις της πρόσθεσης και του πολλαπλασιασμού πινάκων. Επομένως το υποσύνολο I είναι ένας υποδακτύλιος, χωρίς μονάδα διότι $I_n\notin I$, του $\mathsf{AT}_n(\mathbb{K})$. Παρατηρούμε ότι ο υποδακτύλιος χωρίς μονάδα I του $\mathsf{AT}_n(\mathbb{K})$ ικανοποιεί την ισχυρότερη ιδιότητα ότι $A\cdot X\in I$ και $X\cdot A\in I$, για κάθε πίνακα $A\in\mathsf{AT}_n(\mathbb{K})$ και για κάθε πίνακα $X\in I$. $\surd$

Παράδειγμα 7.2.12. (Δακτύλιοι Τυπικών Δυναμοσειρών) Έστω ότι $\mathbb{K}$ είναι ένα εκ των συνόλων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Θεωρούμε το σύνολο

$$\mathsf{A}(\mathbb{K})=\{\mathsf{a}=(a_n)_{n\ge0}\mid a_n\in\mathbb{K},\ \forall n\ge0\}$$

των ακολουθιών με στοιχεία από το σύνολο $\mathbb{K}$. Υπενθυμίζουμε ότι, όπως στο μέρος 10 του Παραδείγματος 1.3.8, επί του $\mathsf{A}(\mathbb{K})$ ορίζονται πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» ως εξής: Αν $\mathsf{a}=(a_n)_{n\ge0}$ και $\mathsf{b}=(b_n)_{n\ge0}$ είναι στοιχεία του $\mathsf{A}(\mathbb{K})$, τότε:

$$+:\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad \mathsf{a}+\mathsf{b}=\mathsf{c}=(c_n)_{n\ge0},\quad \text{όπου}\quad c_n=a_n+b_n,\ \ \forall n\ge0$$

$$\cdot:\mathsf{A}(\mathbb{K})\times\mathsf{A}(\mathbb{K})\longrightarrow\mathsf{A}(\mathbb{K}),\quad \mathsf{a}\cdot\mathsf{b}=\mathsf{d}=(d_n)_{n\ge0},\quad \text{όπου}\quad d_n=\sum_{k=0}^{n}a_kb_{n-k},\ \ \forall n\ge0$$

Από το μέρος 5 του Παραδείγματος 2.2.10 γνωρίζουμε ότι το ζεύγος $(\mathsf{A}(\mathbb{K}),+)$ είναι μια αβελιανή ομάδα με μηδενικό στοιχείο την μηδενική ακολουθία $0=(a_n)_{n\geq 0}$, όπου $a_n=0$, $\forall n\geq 0$, και το ζεύγος $(\mathsf{A}(\mathbb{K}),\cdot)$ είναι ένα μεταθετικό μονοειδές, με μονάδα την ακολουθία $1=(a_n)_{n\geq 0}$, όπου $a_0=1$, και $a_n=0$, $\forall n\geq 1$.

Αν $\mathsf{a}=(a_n)_{n\geq 0}$, $\mathsf{b}=(b_n)_{n\geq 0}$, και $\mathsf{c}=(c_n)_{n\geq 0}$, είναι στοιχεία του $\mathsf{A}(\mathbb{K})$, τότε:

$$\mathsf{a}\cdot(\mathsf{b}+\mathsf{c})=\mathsf{x},\quad \text{όπου}\quad x_n=\sum_{k=0}^{n}a_k(b_{n-k}+c_{n-k})=\sum_{k=0}^{n}(a_kb_{n-k}+a_kc_{n-k})=\sum_{k=0}^{n}a_kb_{n-k}+\sum_{k=0}^{n}a_nc_{n-k}$$

$$\mathsf{a}\cdot\mathsf{b}+\mathsf{a}\cdot\mathsf{c}=\mathsf{y},\quad \text{όπου}\quad y_n=\sum_{k=0}^{n}a_kb_{n-k}+\sum_{k=0}^{n}a_nc_{n-k}$$

Άρα θα έχουμε $\mathsf{a}\cdot(\mathsf{b}+\mathsf{c})=\mathsf{a}\cdot\mathsf{b}+\mathsf{a}\cdot\mathsf{c}$, και παρόμοια βλέπουμε ότι $(\mathsf{a}+\mathsf{b})\cdot\mathsf{c}=\mathsf{a}\cdot\mathsf{b}+\mathsf{a}\cdot\mathsf{c}$. Έτσι ισχύει η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση ακολουθιών, και επομένως η τριάδα $(\mathsf{A}(\mathbb{K}),+,\cdot)$ είναι ένας δακτύλιος με μονάδα, την ακολουθία $1=(1,0,0,\cdots,0,\cdots)$, ο οποίος καλείται ο **δακτύλιος των τυπικών δυναμοσειρών** με στοιχεία από το $\mathbb{K}$, και από τώρα και στο εξής θα συμβολίζεται με $\mathbb{K}[\![t]\!]$. Ένα στοιχείο $\mathsf{a}=(a_n)_{n\geq 0}$ του $\mathbb{K}[\![t]\!]$ θα καλείται **τυπική δυναμοσειρά** με συντελεστές από το $\mathbb{K}$.

Ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι μεταθετικός. Πραγματικά, θα έχουμε

$$\mathsf{a}\cdot\mathsf{b}=\mathsf{x},\quad \text{όπου}\quad x_n=\sum_{k=0}^{n}a_kb_{n-k}=a_0b_n+a_1b_{n-1}+\cdots+a_nb_0$$

$$\mathsf{b}\cdot\mathsf{a}=\mathsf{y},\quad \text{όπου}\quad y_n=\sum_{k=0}^{n}b_ka_{n-k}=b_0a_n+b_1a_{n-1}+\cdots+b_na_0$$

Επειδή ο πολλαπλασιασμός στο $\mathbb{K}$ είναι μεταθετική πράξη, έπεται άμεσα ότι $x_n=y_n$, $\forall n\geq 0$, και επομένως $\mathsf{a}\cdot\mathsf{b}=\mathsf{b}\cdot\mathsf{a}$. Συνεπώς ο δακτύλιος $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του $\mathbb{K}$ είναι μεταθετικός. $\surd$

Παράδειγμα 7.2.13. (Δακτύλιοι Πολυωνύμων) Θεωρούμε τον δακτύλιο $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών με στοιχεία από το $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένας εκ των δακτυλίων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Έστω το ακόλουθο υποσύνολο του $\mathbb{K}[\![t]\!]$:

$$\mathbb{K}[t]=\left\{\mathsf{a}=(a_n)_{n\geq 0}\in\mathsf{A}(\mathbb{K})\mid \exists n\geq 0:\ a_k=0,\ \forall k>n\right\}$$

Προφανώς η ακολουθία $1=(1,0,0,\cdots,0,\cdots)$ ανήκει στο υποσύνολο $\mathbb{K}[t]$. Αν $\mathsf{a}=(a_n)_{n\geq 0}$ και $\mathsf{b}=(b_n)_{n\geq 0}$ είναι δύο στοιχεία του $\mathbb{K}[t]$, τότε υπάρχουν ακέραιοι $n,m\geq 0$ έτσι ώστε: $a_k=0$, $\forall k>n$ και $b_k=0$, $\forall k>m$. Τότε προφανώς θα έχουμε $a_k+b_k=0$, $\forall k>\max\{n,m\}$, και αυτό σημαίνει ότι η ακολουθία $\mathsf{a}+\mathsf{b}\in\mathbb{K}[t]$. Τέλος, για κάθε $k>n+m$ θα έχουμε $\sum_{i=0}^{k}a_ib_{k-i}=a_0b_k+a_1b_{k-1}+\cdots+a_kb_0=0$, το οποίο σημαίνει ότι η ακολουθία $\mathsf{a}\cdot\mathsf{b}\in\mathbb{K}[t]$. Συνοψίζοντας, δείξαμε ότι το υποσύνολο $\mathbb{K}[t]$ είναι υποδακτύλιος του $\mathbb{K}[\![t]\!]$. Άρα η τριάδα $(\mathbb{K}[t],+,\cdot)$ είναι ένας δακτύλιος με μονάδα, την ακολουθία $1=(1,0,0,\cdots,0,\cdots)$, ο οποίος καλείται ο **δακτύλιος των πολυωνύμων** με στοιχεία από το $\mathbb{K}$, και ο οποίος είναι μεταθετικός διότι ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι μεταθετικός. Ένα στοιχείο $\mathsf{a}=(a_n)_{n\geq 0}$ του $\mathbb{K}[t]$ θα καλείται **πολυώνυμο** με συντελεστές από το $\mathbb{K}$. $\surd$

Παρατήρηση 7.2.14. (Ο Συνήθης Συμβολισμός Τυπικών Δυναμοσειρών και Πολυωνύμων). Θεωρούμε τον δακτύλιο $\mathbb{K}[\![t]\!]$ με στοιχεία από το $\mathbb{K}\in\{\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C}\}$.

Θεωρούμε μια τυπική δυναμοσειρά $\mathsf{a}=(a_n)_{n\geq 0}$ του $\mathbb{K}[\![t]\!]$. Εισάγουμε συμβολισμό:

$$t^0:=(1,0,0,\cdots,0,\cdots),\quad t:=(0,1,0,\cdots,0,\cdots),\quad \text{και γενικότερα:}\quad t^n:=\underbrace{(0,0,\cdots,\ 0,1,0,\cdots,0,\cdots)}_{\text{το 1 στην }(n+1)-\text{Θέση}},\quad \forall n\geq 0$$

Προφανώς, οι παραπάνω ακολουθίες είναι πολυώνυμα, και παρατηρούμε ότι το πολυώνυμο t^n είναι η n-οστή δύναμη του πολυωνύμου t ως προς την πράξη του πολλαπλασιασμού πολυωνύμων: $t^n=t\cdot t\cdots t$ (n-παράγοντες).

Επίσης, αν $k\in\mathbb{K}$, θα γράφουμε:

$$k\mathsf{a}=(ka_n)_{n\geq 0}:=(k,0,0,\cdots,0,\cdots)\cdot(a_0,a_1,\cdots,a_n,\cdots)=(ka_0,ka_1,\cdots,ka_n,\cdots)$$

για το γινόμενο της ακολουθίας $\mathsf{k} = (k, 0, 0, \cdots, 0, \cdots)$ με την ακολουθία $\mathsf{a} = (a_n)_{n\geq 0}$,

Με βάση τους παραπάνω συμβολισμούς, και λαμβάνοντας υπόψη τις πράξεις πρόσθεσης και πολλαπλασιασμού τυπικών δυναμοσειρών, για την τυπική δυναμοσειρά $\mathsf{a} = (a_n)_{n\geq 0}$, θα έχουμε:

$$\begin{aligned}
\mathsf{a} = (a_n)_{n\geq 0} &= (a_0, a_1, \cdots, a_n, \cdots) \\
&= (a_0, 0, \cdots, 0, 0, 0, \cdots) + (0, a_1, \cdots, 0, 0, 0, \cdots) + \cdots + (0, 0, \cdots, 0, a_n, 0, \cdots) \\
&= a_0(1, 0, \cdots, 0, 0, 0, \cdots) + a_1(0, 1, \cdots, 0, 0, 0, \cdots) + \cdots + a_n(0, 0, \cdots, 0, 1, 0 \cdots) \\
&= a_0 1 + a_1 t + \cdots + a_n t^n + \cdots \\
&:= \sum_{n=0}^{\infty} a_n t^n
\end{aligned}$$

Μια τυπική δυναμοσειρά, όπως η παραπάνω, θα συμβολίζεται συνήθως με τον οικείο συμβολισμό $P(t) = \sum_{n=0}^{\infty} a_n t^n$. Αν η δυναμοσειρά $P(t) = \sum_{n=0}^{\infty} a_n t^n$ είναι πολυώνυμο, δηλαδή ανήκει στον υποδακτύλιο $\mathbb{K}[t]$, τότε υπάρχει $n \geq 0$, έτσι ώστε $a_k = 0$, $\forall k > n$. Έτσι θα έχουμε ότι οι ακολουθίες $a_k t^k$, $\forall k > n$ είναι οι μηδενικές ακολουθίες και έτσι δεν συνεισφέρουν στο τυπικό άθροισμα $\sum_{n=0}^{\infty} a_n t^n$, και γι' αυτό σ' αυτή την περίπτωση θα γράφουμε

$$P(t) = \sum_{k=0}^{n} a_k t^k = a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

δηλαδή θα έχουμε τον οικείο συμβολισμό πολυωνύμων. Τέλος, από τώρα και στο εξής, χάριν απλότητας, θα παραλείπουμε την μονάδα 1 των δακτυλίων $\mathbb{K}[t]$ και $\mathbb{K}[\![t]\!]$ και θα γράφουμε $a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ αντί $a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$. ▲

Κλείνουμε την παρούσα ενότητα με ένα σημαντικό παράδειγμα μη μεταθετικού δακτυλίου

Παράδειγμα 7.2.15. (Ο Δακτύλιος των Τετρανίων του Hamilton) Θεωρούμε τον δακτύλιο $\mathsf{M}_2(\mathbb{C})$ των 2×2-πινάκων με στοιχεία μιγαδικούς αριθμούς. Έστω το υποσύνολο

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \mid a, b \in \mathbb{C} \right\} = \left\{ \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \mid a_k \in \mathbb{R},\ 0 \leq k \leq 3 \right\} \tag{7.9}$$

όπου $\overline{a} = x - yi$ συμβολίζει τον συζυγή του μιγαδικού αριθμού $a = x + yi \in \mathbb{C}$, $x, y \in \mathbb{R}$. Υπενθυμίζουμε ότι η συζυγία μιγαδικών αριθμών είναι η απεικόνιση $\mathbb{C} \longrightarrow \mathbb{C}$, $z = a + bi \longrightarrow \overline{z} = a - bi$, και ικανοποιεί τις σχέσεις $\overline{z \pm w} = \overline{z} \pm \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$, $\overline{\overline{z}} = z$, και $\overline{z} = z$ αν και μόνο αν $z \in \mathbb{R}$.

Ισχυρισμός: Το υποσύνολο $\mathbb{H}$ είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{C})$.

Η μονάδα του δακτυλίου $\mathsf{M}_2(\mathbb{C})$, δηλαδή ο μοναδιαίος 2×2 πίνακας μιγαδικών αριθμών I_2 ανήκει στο υποσύνολο $\mathbb{H}$, όπως προκύπτει αν θέσουμε $a = 1$ και $b = 0$ στην (7.9).

Έστω $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ και $B = \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix}$ στοιχεία του $\mathbb{H}$. Τότε χρησιμοποιώντας τις ιδιότητες της συζυγίας θα έχουμε:

$$A - B = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} - \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -\overline{b}+\overline{d} & \overline{a}-\overline{c} \end{pmatrix} = \begin{pmatrix} a-c & b-d \\ -\overline{b-d} & \overline{a-c} \end{pmatrix} \in \mathbb{H}$$

$$A \cdot B = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -c\overline{b} - \overline{a}\overline{d} & -d\overline{b} + \overline{a}\overline{c} \end{pmatrix} = \begin{pmatrix} ac - b\overline{d} & ad + b\overline{c} \\ -\overline{ad + b\overline{c}} & \overline{ac - b\overline{d}} \end{pmatrix} \in \mathbb{H}$$

Επομένως, συμπεραίνουμε ότι το υποσύνολο $\mathbb{H}$ είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{C})$, και άρα είναι ένας δακτύλιος, γνωστός ως ο **δακτύλιος των τετρανίων του Hamilton**. Σημειώνουμε ότι ο δακτύλιος $\mathbb{H}$ δεν είναι μεταθετικός, διότι, για παράδειγμα, οι πίνακες $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ και $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ είναι στοιχεία του $\mathbb{H}$, και

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \cdot \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

Γράφοντας ένα στοιχείο του δακτυλίου $\mathbb{H}$ χρησιμοποιώντας την παράσταση $z = a + bi$ για κάθε μιγαδικό αριθμό z, όπου $a, b \in \mathbb{R}$, θα έχουμε ότι τα στοιχεία του $\mathbb{H}$ είναι της μορφής:

$$q = \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix}$$

Χρησιμοποιώντας τους πίνακες, στοιχεία του $\mathbb{H}$,

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

μπορούμε να γράψουμε το τυχόν στοιχείο q του H μοναδικά ως $\mathbb{R}$-γραμμικό συνδυασμό των στοιχείων $\{I_2, I, J, K\} \subseteq \mathbb{H}$, εξής:

$$q = a_0 \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + a_1 \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + a_2 \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + a_3 \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = a_0 I_2 + a_1 I + a_2 J + a_3 K \quad \surd$$

7.3 Κατασκευές Δακτυλίων

Στην παρούσα ενότητα θα μελετήσουμε διάφορες κατασκευές δακτυλίων, ιδιαίτερα θα δούμε μεθόδους μέσω των οποίων μπορούμε να αποκτήσουμε με φυσικό τρόπο νέους δακτυλίους από παλαιούς.

Για λόγους αναφοράς, σημειώνουμε ότι για κάθε δακτύλιο $R = (R, +, \cdot)$ ορίζεται ένας νέος δακτύλιος $R^{\mathsf{op}} = (R, +, \cdot^{\mathsf{op}})$, όπου $\forall x, y \in R$:

$$x \cdot^{\mathsf{op}} y = y \cdot x$$

ο οποίος καλείται ο **αντίθετος δακτύλιος** του R. Σημειώνουμε ότι ως σύνολα και ως αβελιανές ομάδες οι δακτύλιοι R και R^{op} είναι ταυτόσημοι, έχουν όμως αντίθετη πολλαπλασιαστική δομή. Προφανώς ο δακτύλιος R είναι μεταθετικός αν και μόνο αν ως δακτύλιοι $R = R^{\mathsf{op}}$.

7.3.1 Τομή Υποδακτυλίων και Υποδακτύλιοι Παραγόμενοι από Υποσύνολα

Έστω $R = (R, +, \cdot)$ ένας δακτύλιος με μονάδα $1 = 1_R$.

Λήμμα 7.3.1. *Αν $\{S_i\}_{i \in I}$ είναι μια οικογένεια υποδακτυλίων του R, τότε η τομή $\cap_{i \in I} S_i$ είναι ένας υποδακτύλιος του R.*

Απόδειξη. Επειδή $1 \in S_i$, $\forall i \in I$, έπεται ότι $1 \in \cap_{i \in I} S_i$. Έστω $x, y \in \cap_{i \in I} S_i$. Τότε $x, y \in S_i$, $\forall i \in I$, και επομένως επειδή κάθε υποσύνολο S_i είναι υποδακτύλιος του R, έπεται ότι $x - y$, $x \cdot y \in S_i$, $\forall i \in I$. Αυτό σημαίνει ότι $x - y$, $x \cdot y \in \cap_{i \in I} S_i$, και άρα η τομή $\cap_{i \in I} S_i$ είναι ένας υποδακτύλιος του R. ■

Πόρισμα 7.3.2. *Έστω $X \subseteq R$ ένα υποσύνολο του R. Τότε το υποσύνολο*

$$\langle X \rangle = \bigcap \{S \subseteq R \mid S : \text{ υποδακτύλιος του } R \text{ και } X \subseteq S\}$$

είναι υποδακτύλιος του R, και είναι ο μικρότερος υποδακτύλιος του R ο οποίος περιέχει το σύνολο X.

Απόδειξη. Προφανώς ο δακτύλιος R είναι υποδακτύλιος του εαυτού του και περιέχει το υποσύνολο X. Έτσι η οικογένεια $\mathscr{S} := \{S \subseteq R \mid S : \text{ υποδακτύλιος του } R \text{ και } X \subseteq S\}$ είναι μη κενή, και τότε από το Λήμμα 7.3.1, έπεται ότι το υποσύνολο $\langle X \rangle$ είναι ένας υποδακτύλιος του R ο οποίος εκ κατασκευής περιέχει το X. Αν T είναι ένας υποδακτύλιος του S ο οποίος περιέχει το X, τότε $T \in \mathscr{S}$ και επομένως $\langle X \rangle \subseteq T$, δηλαδή $\langle X \rangle$ είναι ο μικρότερος υποδακτύλιος του R ο οποίος περιέχει το σύνολο X. ■

Αν $X \subseteq R$ είναι ένα υποσύνολο του R, τότε ο υποδακτύλιος $\langle X \rangle$ καλείται ο **υποδακτύλιος του R ο οποίος παράγεται από το X**.

Ορισμός 7.3.3. *Ο υποδακτύλιος του R ο οποίος παράγεται από την μονάδα 1_R του R καλείται ο* **πρωτοδακτύλιος** *του R.*

Έτσι ο πρωτοδακτύλιος του R είναι ο υποδακτύλιος $\langle 1_R\rangle$. Προφανώς, για κάθε $n\in\mathbb{Z}$, θα έχουμε $n\in\langle 1_R\rangle$ και άρα $\mathbb{Z}1_R=\{n1_R\in R \mid n\in\mathbb{Z}\}\subseteq\langle 1_R\rangle$. Το υποσύνολο $\mathbb{Z}1_R$ είναι υποδακτύλιος του R, διότι προφανώς περιέχει τη μονάδα 1_R, αφού $1_R=11_R$, και επίσης είναι κλειστό στο άθροισμα και στον πολλαπλασιασμό του R, διότι από τις Προτάσεις 7.1.4 και 7.1.5, έχουμε $(n1_R)+(m1_R)=(n+m)1_R$ και $(n1_R)\cdot(m1_R)=(nm)1_R$. Αν S είναι υποδακτύλιος του R ο οποίος περιέχει την μονάδα 1_R, τότε προφανώς θα περιέχει και κάθε ακέραιο πολλαπλάσιο της μονάδας, και άρα $\mathbb{Z}1_R\subseteq S$. Επομένως θα έχουμε:

$$\langle 1_R\rangle=\mathbb{Z}1_R$$

Θα δούμε αργότερα ότι ο πρωτοδακτύλιος του δακτυλιου R είναι ισόμορφος, με μια κατάλληλη έννοια, είτε με τον δακτύλιο των ακεραίων $\mathbb{Z}$ είτε με τον δακτύλιο $\mathbb{Z}_n$ των ακεραίων mod n.

Παράδειγμα 7.3.4. Θεωρούμε τον δακτύλιο $\mathbb{C}$ των μιγαδικών αριθμών. Έστω $X\subseteq\mathbb{C}$.

1. Αν $X=\emptyset$, τότε ο δακτύλιος $\langle\emptyset\rangle$ περιέχει το 1, επειδή είναι υποδακτύλιος θα περιέχει και όλους τους θετικούς ακέραιους $n=1+1+\cdots+1$ (n-παράγοντες), θα περιέχει το $0=1-1$, το $-1=0-1$, και θα περιέχει και τους αρνητικούς ακεραίους $-n=(-1)\cdot n,\ n\in\mathbb{N}$. Άρα $\mathbb{Z}\subseteq\langle\emptyset\rangle$ και επειδή το $\mathbb{Z}$ είναι υποδακτύλιος του $\mathbb{C}$, θα έχουμε $\langle\emptyset\rangle=\mathbb{Z}$.

2. Αν $X=\{\frac{1}{n}\}$, όπου n είναι ένας σταθερός θετικός ακέραιος, τότε ο υποδακτύλιος $\langle\frac{1}{n}\rangle$ θα περιέχει όπως και πριν τον υποδακτύλιο των ακεραίων $\mathbb{Z}$, και επίσης μαζί με το στοιχείο $\frac{1}{n}$ θα περιέχει και όλες τις δυνάμεις $\frac{1}{n^k},\ k\geq 0$. Έτσι θα περιέχει και το υποσύνολο $S=\{\frac{x}{n^k}\in\mathbb{C}\mid x\in\mathbb{Z},\ k\in\mathbb{N}_0\}$. Επειδή, όπως μπορεί να διαπιστωθεί εύκολα, το υποσύνολο S είναι υποδακτύλιος του $\mathbb{C}$, έπεται ότι $\langle\frac{1}{n}\rangle=S$.

3. Αν $X=\{i\}$, τότε ο υποδακτύλιος $\langle i\rangle$ του $\mathbb{C}$ περιέχει όπως και πριν το $\mathbb{Z}$, και προφανώς θα περιέχει και τα ακέραια πολλαπλάσια $\mathbb{Z}i=\{bi\in\mathbb{C}\mid b\in\mathbb{Z}\}$ του i. Τότε θα περιέχει και τον υποδακτύλιο $\mathbb{Z}[i]=\{a+bi\in\mathbb{C}\mid a,b\in\mathbb{Z}\}$ των ακεραίων του Gauss, και άρα $\langle i\rangle=\mathbb{Z}[i]$.

4. Στον δακτύλιο $\mathbb{C}[t]$ των πολυωνύμων με συντελεστές από τους μιγαδικούς αριθμούς, έστω $X=\{t^n\}$, όπου n είναι ένας σταθερός μη αρνητικός ακέραιος. Τότε ο υποδακτύλιος $\langle t^n\rangle$ θα περιέχει όπως παραπάνω το σύνολο $\mathbb{Z}$ των ακεραίων, όπου κάθε ακέραιος m θεωρείται ως το σταθερό πολυώνυμο $P(t)=m$, και επίσης και όλα τα πολυώνυμα της μορφής $a_0+a_1t^n+a_2(t^n)^2+\cdots+a_k(t^n)^k,\ \forall k\geq 0$. Επειδή το σύνολο όλων αυτών των πολυωνύμων είναι υποδακτύλιος του $\mathbb{C}[t]$, έπεται ότι $\langle t^n\rangle=\{a_0+a_1t^n+a_2t^{2n}+\cdots+a_kt^{kn}\in\mathbb{C}[t]\mid a_k\in\mathbb{Z},\ k\geq 0\}$.

5. Στον δακτύλιο $\mathsf{M}_n(\mathbb{C})$ των $n\times n$ πινάκων με συντελεστές από τους μιγαδικούς αριθμούς, έστω $X=\{A\}$, όπου A είναι ένας σταθερός $n\times n$ πίνακας. Τότε ο υποδακτύλιος $\langle A\rangle$ θα περιέχει όπως παραπάνω το σύνολο mI_n όλων των $n\times n$ διαγώνιων πινάκων με τον ακέραιο m στην διαγώνιο, και επίσης θα περιέχει και όλες τις μη αρνητικές δυνάμεις $A^k,\ k\geq 0$, του πίνακα A, και επομένως και τα γινόμενα $mI_n\cdot A^k$, $\forall m\in\mathbb{Z},\ \forall k\geq 0$. Επομένως θα περιέχει και το σύνολο $S=\{a_oI_n+a_1A+a_2A^2+\cdots+a_kA^k\in\mathsf{M}_n\mathbb{C})\mid a_k\in\mathbb{Z},\ k\geq 0\}$. Επειδή, όπως μπορεί να διαπιστωθεί εύκολα, το υποσύνολο S είναι υποδακτύλιος του $\mathsf{M}_n(\mathbb{C})$, έπεται ότι $\langle A\rangle=\{a_oI_n+a_1A+a_2A^2+\cdots+a_kA^k\in\mathsf{M}_n\mathbb{C})\mid a_k\in\mathbb{Z},\ k\geq 0\}$. $\surd$

Στη συνέχεια θα μας απασχολήσει μια σημαντική ειδική περίπτωση υποδακτυλίου παραγόμενου από ένα πεπερασμένο υποσύνολο. Από τώρα και στο εξής, έστω $R\subseteq S$ ένας υποδακτύλιος ενός δακτυλίου S, και έστω $u\in R$. Συμβολίζουμε με

$$R[u]=\langle R\cup\{u\}\rangle$$

τον υποδακτύλιο του S ο οποίος παράγεται από το σύνολο $R\cup\{u\}$, ή, όπως θα λέμε από τώρα και στο εξής, τον **υποδακτύλιο του S ο οποίος παράγεται από το στοιχείο $u\in S$ υπεράνω του R**. Μερικές φορές θα λέμε και ότι ο υποδακτύλιος $R[u]$ προήλθε με την *προσάρτηση του στοιχείου u στον υποδακτύλιο R*.

Πρόταση 7.3.5. *Υποθέτουμε ότι το στοιχείο u μετατίθεται με κάθε στοιχείο του R: $r\cdot u = u\cdot r$, $\forall r\in R$. Τότε:*

$$R[u] = \{r_0 + r_1 u + r_2 u^2 + \cdots + r_n u^n \in S \mid r_i \in R,\ \ n \geq 0\}$$

Απόδειξη. Το υποσύνολο στα δεξιά της παραπάνω σχέσης, έστω T, περιέχει την μονάδα του δακτυλίου, όπως προκύπτει αν θέσουμε $r_0 = 1$ και $r_i = 0$, $\forall i \geq 0$. Αν $x = \sum_{k=0}^{n} r_k u^k$ και $y = \sum_{k=0}^{m} r'_k u^k$, είναι στοιχεία του T, τότε χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $n \leq m$, και να θέσουμε $r_{n+1} = \cdots = r_m = 0$. Τότε, χρησιμοποιώντας ότι το στοιχείο u μετατίθεται με κάθε στοιχείο του υποδακτυλίου R, θα έχουμε: $r_i u^i \cdot r_j u^j = r_i r_j u^{i+j}$ και άρα με χρήση της επιμεριστικής ιδιότητας έπεται ότι:

$$x - y = \sum_{k=0}^{m} (r_k - r'_k) u^k \ \in\ T \quad \text{και} \quad x\cdot y = \sum_{k=0}^{n+m} \Big(\sum_{i=0}^{k} r_i r'_{k-i}\Big) u^k \ \in\ T$$

Επομένως το σύνολο T είναι ένας υποδακτύλιος του S και περιέχει το u, διότι $u = 1\cdot u$, και περιέχει και τον υποδακτύλιο R, διότι $r = r\cdot 1 = r\cdot u^0$. Από την άλλη πλευρά, αν V είναι ένας υποδακτύλιος του S ο οποίος περιέχει τον R και το u, τότε προφανώς θα περιέχει όλες τις μη αρνητικές δυνάμεις u^k, $k \geq 0$, του u, θα περιέχει όλα τα γινόμενα $r\cdot u^k$, όπου $r \in R$ και $k \geq 0$, τέλος θα περιέχει και όλα τα στοιχεία του S της μορφής $\sum_{k=0}^{n} r_k u^k$, $\forall n \geq 0$. Επομένως θα περιέχει και τον υποδακτύλιο T. Αυτό δείχνει ότι ο υποδακτύλιος T είναι ο μικρότερος υποδακτύλιος του S ο οποίος περιέχει τον R και το u, και άρα $R[u] = T$. ■

Παρατήρηση 7.3.6.

1. Η έκφραση ενός στοιχείου x του δακτυλίου $R[u]$ ως $x = r_0 + r_1 u + r_2 u^2 + \cdots + r_n u^n$, όπου $r_i \in R$, $0 \leq i \leq n$, για προφανείς λόγους καλείται *πολυωνυμική έκφραση ή πολυώνυμο ως προς u*.

2. Η έκφραση ενός στοιχείου x του δακτυλίου $R[u]$ ως $x = r_0 + r_1 u + r_2 u^2 + \cdots + r_n u^n$ γενικά **δεν** είναι μοναδική. Δηλαδή, αν επίσης $x = r'_0 + r'_1 u + r'_2 u^2 + \cdots + r'_m u^m$, όπου $r_i, r'_j \in R$, $0 \leq i \leq n$, $0 \leq j \leq m$, δεν είναι απαραίτητο να ισχύει $n = m$ και $r_i = r'_i$, $\forall i \geq 0$. Για παράδειγμα, στον δακτύλιο $\mathbb{C} = \mathbb{R}[i]$, έχουμε $i^2 = (-1)\cdot 1 + 0\cdot i$ και $i^2 = 0\cdot 1 + 1\cdot i^2$, δηλαδή δύο διαφορετικές γραφές του i^2 στην μορφή $r_0 + r_1 u + r_2 u^2 + \cdots + r_n u^n$, $r_i \in \mathbb{R}$ και $u = i$. Αργότερα θα δούμε την εξήγηση για το πού οφείλεται αυτή η έλλειψη μοναδικότητας στην παραπάνω γραφή. ▲

Παράδειγμα 7.3.7.

1. Προφανώς ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι ο υποδακτύλιος του $\mathbb{C}$, ο οποίος παράγεται υπεράνω του $\mathbb{Z}$ από τη φανταστική μονάδα i. Παρόμοια, ο δακτύλιος $\mathbb{Q}[i]$ των ακεραίων του Gauss είναι ο υποδακτύλιος του $\mathbb{C}$, ο οποίος παράγεται υπεράνω του $\mathbb{Q}$ από την φανταστική μονάδα i. Ο δακτύλιος $\mathbb{C}$ συμπίπτει με τον υποδακτύλιο του εαυτού του ο οποίος παράγεται υπεράνω του $\mathbb{R}$ από τη φανταστική μονάδα i: $\mathbb{R}[i] = \mathbb{C}$.

2. Ο υποδακτύλιος $\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$, όπου d δεν είναι τετράγωνο ακεραίου, π.χ. $d = 2$ ή $d = -3$, είναι ο υποδακτύλιος του $\mathbb{C}$, ο οποίος παράγεται υπεράνω του $\mathbb{Z}$ από τον, εν γένει μιγαδικό, αριθμό $\sqrt{d}$.

3. Ο υποδακτύλιος $\mathbb{Z}[\sqrt[n]{m}]$, όπου $n, m \geq 2$, είναι ο υποδακτύλιος του $\mathbb{C}$, ο οποίος παράγεται υπεράνω του $\mathbb{Z}$ από τον, πραγματικό αριθμό $\sqrt[n]{m}$, και έχει την ακόλουθη περιγραφή:

$$\mathbb{Z}[\sqrt[n]{m}] = \{a_0 + a_1 \sqrt[n]{m} + a_2 (\sqrt[n]{m})^2 + \cdots + a_{n-1} (\sqrt[n]{m})^{n-1} \in \mathbb{C} \mid a_k \in \mathbb{Z},\ 0 \leq k \leq n-1\}$$

4. Έστω $1 \neq \zeta_n \in \mathbb{C}$ μια n-οστή ρίζα της μονάδας. Τότε ο υποδακτύλιος του $\mathbb{C}$ ο οποίος παράγεται από την ζ_n υπεράνω του $\mathbb{Z}$ είναι

$$\mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta^{n-1} \ \in\ \mathbb{C} \mid a_k \in \mathbb{Z},\ 0 \leq k \leq n-1\}$$

Δακτύλιοι της μορφής $\mathbb{Z}[\zeta_n]$, όπου ζ_n είναι μια n-οστή ρίζα της μονάδας, είναι γνωστοί ως δακτύλιοι Kummer[2] και παίζουν σημαντικό ρόλο στη Θεωρία Αριθμών. √

[2]Ernst Eduard Kummer (1810-1893) [https://en.wikipedia.org/wiki/Ernst_Kummer]: Γερμανός μαθηματικός με σημαντική συμβολή στη Θεωρία Αριθμών, στην Άλγεβρα και στην Αλγεβρική Γεωμετρία.

Γενικεύοντας, αν $\mathscr{U} = \{u_1, u_2, \cdots, u_n\} \subseteq S$ είναι ένα υποσύνολο του δακτυλίου S και αν τα στοιχεία του $\mathscr{U}$ μετατίθενται μεταξύ τους και με τα στοιχεία του υποδακτυλίου R του S, τότε ο **υποδακτύλιος του S ο οποίος παράγεται από τα στοιχεία $u_1, u_2, \cdots, u_n \in S$ υπεράνω του R** προκύπτει επαγωγικά ως εξής:

$$R[u_1, u_2] = (R[u_1])[u_2], \quad R[u_1, u_2, u_3] = (R[u_1, u_2])[u_3], \quad \cdots \quad R[u_1, u_2, \cdots, u_n] = (R[u_1, u_2, \cdots, u_{n-1}])[u_n]$$

και τα στοιχεία του είναι πεπερασμένα αθροίσματα γινομένων στοιχείων του δακτυλίου R με γινόμενα μη αρνητικών δυνάμεων των στοιχείων $u_1, u_2, \cdots, u_n$:

$$R[u_1, u_2, \cdots, u_n] = \left\{ \sum_{(i)} r_{i_1 i_2 \cdots i_n} u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n} \ \in \ S \ \middle| \ r_{i_1 i_2 \cdots i_n} \in R, \ \ k_{i_j} \geq 0, \ \ 1 \leq j \leq n \right\}$$

όπου $(i) = (i_1, i_2, \cdots, i_n) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \cdots \mathbb{N}_0$. Έτσι ένα τυπικό στοιχείο του δακτυλίου $R[u_1, u_2, \cdots, u_n]$ είναι ένα πεπερασμένο άθροισμα στον δακτύλιο S της μορφής:

$$r_{0\cdots 0} + r_{10\cdots 0} u_1 + \cdots + r_{0\cdots 01} u_n + \cdots + r_{20\cdots 0} u_1^2 + \cdots r_{11\cdots 0} u_1 u_2 + \cdots + r_{0\cdots 11} u_{n-1} u_n + \cdots + r_{00\cdots 0k} u_n^k + \cdots$$

Παράδειγμα 7.3.8. Έστω $\mathscr{U} = \left\{ i, \sqrt{2} \right\} \subseteq \mathbb{C}$. Ο υποδακτύλιος του $\mathbb{C}$ ο οποίος παράγεται από τα $i, \sqrt{2}$ υπεράνω του $\mathbb{Z}$, επειδή $i^2 = -1$ και $\sqrt{2}^2 = 2$, είναι

$$\mathbb{Z}[i, \sqrt{2}] = \left\{ a + bi + c\sqrt{2} + d\sqrt{2}i \ \in \ \mathbb{C} \ \middle| \ a, b, c, d \in \mathbb{Z} \right\} \quad \surd$$

Γενικότερα, έστω $X \subseteq S \supseteq Y$ δύο σύνολα στοιχείων του δακτυλίου S και έστω R ένας υποδακτύλιος του S. Υποθέτουμε για ευκολία ότι ο δακτύλιος S είναι μεταθετικός. Τότε

$$R[X][Y] = R[X \cup Y]$$

Πραγματικά, ο δακτύλιος $R[X \cup Y]$ περιέχει τον υποδακτύλιο R, το υποσύνολο X, και επομένως περιέχει και τον υποδακτύλιο $R[X]$. Έτσι, επειδή ο $R[X \cup Y]$ περιέχει τον υποδακτύλιο $R[X]$ και το υποσύνολο Y, θα περιέχει και τον υποδακτύλιο $R[X][Y]$. Άρα θα έχουμε $R[X][Y] \subseteq R[X \cup Y]$. Από την άλλη πλευρά, ο δακτύλιος $R[X][Y]$ περιέχει τον υποδακτύλιο R και τα υποσύνολα X και Y, άρα και το υποσύνολο $X \cup Y$. Τότε όμως θα περιέχει και τον υποδακτύλιο $R[X \cup Y]$ ο οποίος παράγεται υπεράνω του R από το υποσύνολο $X \cup Y$, και άρα $R[X \cup Y] \subseteq R[X][Y]$. Επομένως θα έχουμε $R[X][Y] = R[X \cup Y]$.

7.3.2 Δακτύλιοι Πινάκων

Στην παρούσα υποενότητα θα γενικεύσουμε το Παράδειγμα 7.2.10 του δακτυλίου $\mathsf{M}_n(\mathbb{K})$, όπου $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Έστω $R = (R, +, \cdot)$ ένας δακτύλιος, και $n \geq 1$ ένας θετικός ακέραιος. Όπως ακριβώς και με τον δακτύλιο πινάκων με στοιχεία από το $\mathbb{K}$, ορίζουμε τον **δακτύλιο $\mathsf{M}_n(R)$ των $n \times n$ πινάκων με στοιχεία από τον δακτύλιο** R να είναι το σύνολο όλων των διατάξεων $n \times n$ στοιχείων από τον δακτύλιο R, δηλαδή $n \times n$ *πινάκων*, της μορφής

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Συνήθως ένας $n \times n$ πίνακας A όπως παραπάνω θα παριστάται σε συντομευμένη μορφή ως $A = (A_{ij})$ ή $A = (a_{ij})$, υπονοώντας ότι το στοιχείο στην (i, j)-θέση του πίνακα A, δηλαδή στην τομή της i-γραμμής με την j-στήλη, είναι ο αριθμό A_{ij} ή a_{ij} αντίστοιχα. Ορίζουμε δύο πίνακες $A = (a_{ij})$ και $B = (b_{ij})$ να είναι *ίσοι πίνακες*, αν: $a_{ij} = b_{ij}$, $1 \leq i, j \leq n$.

Στο σύνολο $\mathsf{M}_n(R)$ ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων όπως ακριβώς και έχουμε ορίσει την πρόσθεση και τον πολλαπλασιασμό πινάκων με στοιχεία αριθμούς, αυτή τη φορά χρησιμοποιώντας τις πράξεις πρόσθεσης και πολλαπλασιασμού του δακτυλίου R. Έτσι, αν $A = (a_{ij})$ και $B = (b_{ij})$ είναι δύο $n \times n$ πίνακες με στοιχεία από το R, τότε:

$$A + B = (c_{ij}), \quad \text{όπου} \quad c_{ij} = a_{ij} + b_{ij}, \quad 1 \leq i, j \leq n$$

$$A\cdot B=(c_{ij}),\quad \text{όπου}\quad c_{ij}=\sum_{k=1}^{n}a_{ik}b_{kj},\quad 1\le i,j\le n$$

Τότε το ζεύγος $(\mathsf{M}_n(R),+)$ είναι μια αβελιανή ομάδα με ουδέτερο στοιχείο τον μηδενικό πίνακα $0=(x_{ij})$, όπου $x_{ij}=0$, $1\le i,j\le n$, είναι το μηδενικό στοιχείο του R, και ο αντίθετος του πίνακα $A=(a_{ij})$ είναι ο πίνακας $-A=(-a_{ij})$, όπου $-a_{ij}$ είναι το αντίθετο στοιχείο του a_{ij} στον δακτύλιο R. Παρόμοια το ζεύγος $(\mathsf{M}_n(R),\cdot)$ είναι ένα μονοειδές με μοναδιαίο στοιχείο τον πίνακα $I_n=(\delta_{ij})$, όπου $\delta_{ij}=0$ (το μηδενικό στοιχείο του R), αν $i\neq j$, και $\delta_{ij}=1$ (η μονάδα του R), αν $i=j$. Όπως ακριβώς και στο Παράδειγμα 7.2.10, βλέπουμε ότι ικανοποιείται η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση, και επομένως η τριάδα $(\mathsf{M}_n(R),+,\cdot)$, είναι ένας δακτύλιος, ο **δακτύλιος των $n\times n$ πινάκων υπεράνω του δακτυλίου** R, με μονάδα τον μοναδιαίο πίνακα I_n. Όπως στο Παράδειγμα 7.2.10, ο δακτύλιος $\mathsf{M}_n(R)$ γενικά δεν είναι μεταθετικός.

Προφανώς ο δακτύλιος $\mathsf{M}_n(R)$ ειναι μεταθετικός αν και μόνο ο R είναι μεταθετικός και $n=1$, βλέπε την Άσκηση 7.6.4.

Θα δούμε πως μπορούμε να παραστήσουμε με πιο συμπαγή τρόπο έναν πίνακα $A=(a_{ij})\in\mathsf{M}_n(R)$. Γι' αυτόν τον σκοπό ορίζουμε n^2 πίνακες $E_{ij}\in\mathsf{M}_n(R)$, $1\le i,j\le n$, ως εξής

$$E_{ij}=\begin{pmatrix}0&\cdots&0&0&0&\cdots&0\\ \vdots&\ddots&\vdots&\vdots&\vdots&\vdots&\vdots\\ 0&\cdots&0&0&0&\cdots&0\\ 0&\cdots&0&1&0&\cdots&0\\ 0&\cdots&0&0&0&\cdots&0\\ \vdots&\vdots&\vdots&\vdots&\vdots&\ddots&\vdots\\ 0&\cdots&0&0&0&\cdots&0\end{pmatrix}\qquad(\text{η μονάδα 1 του } R \text{ βρίσκεται στην } (i,j)\text{-θέση})$$

Τότε, χρησιμοποιώντας το πώς ορίστηκαν οι πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων και θέτοντας

$$\forall r\in R:\quad rA=r(a_{ij})=(ra_{ij})$$

θα έχουμε:

$$A=(a_{ij})=\sum_{i,j=1}^{n}a_{ij}E_{ij}$$

Σημειώνουμε ότι το σύνολο πινάκων $\{E_{ij}\}_{i,j=1}^{n}$ ικανοποιεί τις ακόλουθες σχέσεις:

$$E_{ij}\cdot E_{kl}=\delta_{jk}E_{il}=\begin{cases}E_{il}, & \text{αν: } j=k\\ 0, & \text{αν: } j\neq k\end{cases}\qquad(1\le i,j\le n)$$

$$1_{\mathsf{M}_n(R)}=I_n=\sum_{k=1}^{n}E_{kk}\qquad\text{και}\qquad E_{kk}^2=E_{kk}\qquad(1\le k\le n)$$

Ο δακτύλιος $\mathsf{M}_n(R)$ περιέχει ως υποδακτυλίους, τον δακτύλιο $\mathsf{B}_n(R)$ των βαθμωτών πινάκων, όπου ένας πίνακας $A=(a_{ij})$ καλειται *βαθμωτός*, αν $A=rI_n$, για κάποιο στοιχείο $r\in R$. Επίσης το σύνολο $\mathsf{D}_n(R)$ των διαγώνιων πινάκων, όπου ένας πίνακας $A=(a_{ij})$ καλείται *διαγώνιος*, αν $a_{ij}=0$ για κάθε $1\le i\neq j\le n$, είναι ένας υποδακτύλιος του $\mathsf{M}_n(R)$. Τέλος, το σύνολο $\mathsf{AT}_n(R)$ των άνω τριγωνικών πινάκων, όπου υπενθυμίζουμε ότι ένας πίνακας $A=(a_{ij})$ καλείται *άνω τριγωνικός*, αν $a_{ij}=0$ για κάθε $1\le j<i\le n$, είναι ένας υποδακτύλιος του $\mathsf{M}_n(R)$. Παρατηρούμε ότι έχουμε εγκλείσεις υποδακτυλίων:

$$\mathsf{B}_n(R)\ \subseteq\ \mathsf{D}_n(R)\ \subseteq\ \mathsf{AT}_n(R)\ \subseteq\ \mathsf{M}_n(R)$$

Οι αποδείξεις των παραπάνω σχέσεων και ισχυρισμών είναι άμεσες και αφήνονται ως άσκηση στον αναγνώστη.

Η παραπάνω γενική κατασκευή μάς επιτρέπει τη θεώρηση δακτυλίων πινάκων $\mathsf{M}_n(R)$ με στοιχεία σε δακτυλίους R της μορφές $R=\mathbb{Z}_n$, $R=\mathbb{K}[t]$, $R=\mathbb{H}$, $R=\mathbb{Z}[\zeta_n]$ κλπ.

7.3.3 Δακτύλιοι Πολυωνύμων

Στην παρούσα υποενότητα θα γενικεύσουμε το Παράδειγμα 7.2.13 του δακτυλίου πολυωνύμων $\mathbb{K}[t]$, όπου $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$.

Έστω $R = (R, +, \cdot)$ ένας μεταθετικός δακτύλιος. Μια ακολουθία με τιμές στον δακτύλιο R είναι μια απεικόνιση $\mathsf{a} \colon \mathbb{N}_0 \longrightarrow R$, $\mathsf{a}(n) = a_n$. Ως συνήθως μια ακολουθία a συμβολίζεται με αναγραφή των τιμών της: $\mathsf{a} = (a_n)_{n\geq 0}$. Συμβολίζουμε με $R[\![t]\!]$ το σύνολο όλων των ακολουθιών στοιχείων του R:

$$R[\![t]\!] = \left\{\mathsf{a} = (a_n)_{n\geq 0} \mid a_n \in R, \quad n \geq 0\right\}$$

στο οποίο ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» ως εξής:

$$+ \,:\, R[\![t]\!] \times R[\![t]\!] \longrightarrow R[\![t]\!], \quad \mathsf{a} + \mathsf{b} = \mathsf{c} = (c_n)_{n\geq 0}, \quad \text{όπου} \quad c_n = a_n + b_n, \ \ \forall n \geq 0$$

$$\cdot \,:\, R[\![t]\!] \times R[\![t]\!] \longrightarrow R[\![t]\!], \quad \mathsf{a} \cdot \mathsf{b} = \mathsf{d} = (d_n)_{n\geq 0}, \quad \text{όπου} \quad d_n = \sum_{k=0}^{n} a_k b_{n-k}, \ \ \forall n \geq 0$$

Όπως ακριβώς και στο Παράδειγμα 7.2.12, και χρησιμοποιώντας την δομή δακτυλίου του R, βλέπουμε εύκολα ότι η τριάδα $(R[\![t]\!], +, \cdot)$ είναι ένας δακτύλιος με μονάδα, την ακολουθία $1 = (1, 0, 0, \cdots, 0, \cdots)$. Το μηδενικό στοιχείο είναι η μηδενική ακολουθία $0 = (0, 0, \cdots, 0, \cdots)$, και το αντίθετο στοιχείο της ακολουθίας $\mathsf{a} = (a_n)_{n\geq 0}$ είναι η ακολουθία $-\mathsf{a} = (-a_n)_{n\geq 0}$. Επειδή ο δακτύλιος R είναι μεταθετικός, ο πολλαπλασιασμός του $R[\![t]\!]$ δείχνει ότι ο δακτύλιος $R[\![t]\!] = (R[\![t]\!], +, \cdot)$ είναι επίσης μεταθετικός, και καλείται ο **δακτύλιος των τυπικών δυναμοσειρών υπεράνω του** R.

Έστω το ακόλουθο υποσύνολο του $R[\![t]\!]$:

$$R[t] = \left\{\mathsf{a} = (a_n)_{n\geq 0} \in R[\![t]\!] \mid \exists n \geq 0 \colon \ a_k = 0, \ \forall k > n\right\}$$

Όπως και στο Παράδειγμα 7.2.13, εύκολα βλέπουμε ότι το υποσύνολο $R[t]$ είναι ένας υποδακτύλιος του $R[\![t]\!]$, ο οποίος είναι μεταθετικός, διότι ο δακτύλιος $R[\![t]\!]$ είναι μεταθετικός, ο οποίος καλείται ο **δακτύλιος των πολυωνύμων υπεράνω του** R.

Συμβολίζοντας:

$$t^0 := \left(1, 0, 0, \cdots, 0, \cdots\right), \quad t := \left(0, 1, 0, \cdots, 0, \cdots\right), \quad \text{και γενικότερα:} \quad t^n := \underbrace{\left(0, 0, \cdots, \ 0, 1, 0, \cdots, 0, \cdots\right)}_{\text{το } 1 \text{ στην } (n+1)-\text{θέση}}, \quad \forall n \geq 0$$

θα έχουμε ότι οι παραπάνω ακολουθίες είναι πολυώνυμα υπεράνω του R και παρατηρούμε ότι το πολυώνυμο t^n είναι η n-οστή δύναμη του πολυωνύμου t ως προς την πράξη του πολλαπλασιασμού πολυωνύμων: $t^n = t \cdot t \cdots t$ (n-παράγοντες).

Επίσης, για κάθε στοιχείο $r \in R$, γράφοντας:

$$r\mathsf{a} = (ra_n)_{n\geq 0} = \left(ra_0, ra_1, \cdots, ra_n, \cdots\right)$$

για το γινόμενο της ακολουθίας $\mathsf{r} = (r, 0, \cdots, 0, \cdots)$ με την ακολουθία $\mathsf{a} = (a_0, a_1, \cdots, a_n, \cdots)$, όπως στο παράδειγμα 7.2.14, κάθε στοιχείο $\mathsf{a} = (a_n)_{n\geq 0}$, καλείται **τυπική δυναμοσειρά** υπεράνω του R, και μπορεί να εκφραστεί και να γραφεί ως εξής:

$$P(t) = \sum_{n=0}^{\infty} a_n t^n = a_0 1 + a_1 t + a_2 t^2 + \cdots a_n t^n + \cdots$$

Αν η τυπική δυναμοσειρά $P(t) = \sum_{n=0}^{\infty} a_n t^n$ ανήκει στον υποδακτύλιο $R[t]$, τότε υπάρχει $n \geq 0$ έτσι ώστε $a_n = 0$, $\forall k > n$. Τότε η τυπική δυναμοσειρά καλείται **πολυώνυμο** υπεράνω του R, και μπορεί να εκφραστεί και να γραφεί ως εξής:

$$P(t) = \sum_{k=0}^{n} a_n t^n = a_0 1 + a_1 t + a_2 t^2 + \cdots a_n t^n$$

Χάριν απλότητας, η ακολουθία (πολυώνυμο) 1 παραλείπεται από τις παραπάνω εκφράσεις.

Παρατηρούμε ότι ο δακτύλιος πολυωνύμων $R[t]$ είναι ο υποδακτύλιος του $R[\![t]\!]$ ο οποίος παράγεται υπεράνω του R από το στοιχείου του t, και συνήθως καλείται ο **δακτύλιος πολυωνύμων στη μια μεταβλητή** t. Οι παραπάνω κατασκευές μάς επιτρέπουν να θεωρήσουμε τυπικές δυναμοσειρές και πολυώνυμα υπεράνω οποιουδήποτε μεταθετικού δακτυλίου και θα μας φανούν χρήσιμες στη συνέχεια.

Για παράδειγμα, έστω όπως και παραπάνω R ένας μεταθετικός δακτύλιος, και έστω $R_1 = R[t_1]$ ο δακτύλιος πολυωνύμων υπεράνω του R. Επειδή ο δακτύλιος R_1 είναι μεταθετικός, έπεται ότι μπορούμε να επαναλάβουμε τη διαδικασία και να θεωρήσουμε τον δακτύλιο πολυωνύμων $R_2 = R_1[t_2] = R[t_1][t_2]$, (εισάγουμε νέο σύμβολο t_2 για να μην υπάρχει σύγχυση με το σύμβολο t_1), ο οποίος είναι μεταθετικός, συμβολίζεται με $R[t_1, t_2]$ και καλείται ο **δακτύλιος των πολυωνύμων στις δύο μεταβλητές** t_1 και t_2. Τα στοιχεία του θα είναι της μορφής

$$P(t_1, t_2) = \sum_{k_2=0}^{n_2} P_{k_2}(t_1)\, t_2^{k_2}, \qquad P_{k_2}(t_1) = \sum_{r_{k_1}=0}^{n_{k_2}} a_{r_{k_1}}\, t_1^{r_{k_1}}$$

ή με αναγωγή όμοιων όρων, επειδή ο δακτύλιος $R[t_1, t_2]$ είναι μεταθετικός, θα έχουμε ότι ένα τυπικό στοιχείο του δακτυλίου $R[t_1, t_2]$ είναι ένα πεπερασμένο άθροισμα της μορφής

$$P(t_1, t_2) = \sum_{(i)} a_{i_1 i_2}\, t_1^{i_1}\, t_2^{i_2} = a_{00} + a_{10}\, t_1 + a_{01}\, t_2 + a_{20}\, t_1^2 + a_{11}\, t_1\, t_2 + a_{02}\, t_2^2 + \cdots, \qquad (i) = (i_1, i_2) \in \mathbb{N}_0 \times \mathbb{N}_0$$

Επειδή ο δακτύλιος $R[t_1, t_2]$ είναι μεταθετικός μπορούμε να επαναλάβουμε την διαδικασία για ένα πεπερασμένο πλήθος, ας πούμε n, βημάτων, και να αποκτήσουμε τον **δακτύλιο πολυωνύμων** $R[t_1, t_2, \cdots, t_n]$ **στις** n **μεταβλητές** $t_1,\ t_2,\ \cdots,\ t_n$:

$$R[t_1, t_2] = (R[t_1])[t_2], \quad R[t_1, t_2, t_3] = (R[t_1, t_2])[t_3], \ \cdots, \quad R[t_1, t_2, \cdots, t_n] = (R[t_1, t_2, \cdots, t_{n-1}])[t_n]$$

και τα στοιχεία του οποίου είναι πεπερασμένα αθροίσματα γινομένων στοιχείων του δακτυλίου R με γινόμενα μη αρνητικών δυνάμεων των στοιχείων $t_1, t_2, \cdots, t_n$:

$$R[t_1, t_2, \cdots, t_n] = \left\{ \sum_{(i)} r_{i_1 i_2 \cdots i_n}\, t_1^{k_1}\, t_2^{k_2} \cdots t_n^{k_n} \ \in\ S \ \middle|\ r_{i_1 i_2 \cdots i_n} \in R,\ \ k_{i_j} \geq 0,\ \ 1 \leq j \leq n \right\}$$

όπου $(i) = (i_1, i_2, \cdots, i_n) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \cdots \times \mathbb{N}_0$.

7.3.4 Ευθέα Γινόμενα Δακτυλίων

Στην παρούσα ενότητα θα μελετήσουμε την σημαντική κατασκευή του ευθέος γινομένου δακτυλίων. Χάριν απλότητας αναλύουμε πρώτα την κατασκευή του ευθέος γινομένου $R \times S$ δύο δακτυλίων $R = (R, +, \cdot)$ και $S = (S, +, \cdot)$, όπου χρησιμοποιούμε για ευκολία τα ίδια σύμβολα «+» και «·» για τις πράξεις πρόσθεσης και πολλαπλασιασμού των R και S αντίστοιχα.

Τότε έχουμε τις αβελιανές ομάδες $(R, +)$ και $(S.+)$ και τα μονοειδή $(R, \cdot)$ και $(S, \cdot)$. Επομένως, όπως στις Προτάσεις 1.4.35 και 2.7.1, ορίζεται η αβελιανή ομάδα $(R \times S, +)$ και το μονοειδές $(R \times S, \cdot)$, όπου υπενθυμίζουμε ότι οι πράξεις «+» και «·» επί του $R \times S$ ορίζονται, «κατά συνιστώσα» ως εξής:

$$+ \ : \ (R \times S) \times (R \times S) \ \longrightarrow \ (R \times S), \qquad (r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

$$\cdot \ : \ (R \times S) \times (R \times S) \ \longrightarrow \ (R \times S), \qquad (r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

Το μηδενικό στοιχείο της αβελιανής ομάδας $(R \times S, +)$ είναι το ζεύγος $(0_R, 0_S)$, όπου 0_R και 0_S είναι τα μηδενικά στοιχεία των ομάδων $(R, +)$ και $(S, +)$, τα οποία από τώρα και στο εξής θα τα συμβολίζουμε απλά με 0. Το αντίθετο του ζεύγους (r, s) είναι το ζεύγος $(-r, -s)$, όπου $-r$ και $-s$ είναι τα αντίθετα των στοιχείων r και s στις ομάδες $(R, +)$ και $(S, +)$. Το μοναδιαίο στοιχείο του μονοειδούς $(R \times S, \cdot)$ είναι το ζεύγος $(1_R, 1_S)$, όπου 1_R και 1_S είναι τα μοναδιαία στοιχεία των μονοειδών $(R, \cdot)$ και $(S, \cdot)$, τα οποία από τώρα και στο εξής θα τα συμβολίζουμε απλά με 1. Σημειώνουμε ότι, χάριν απλότητας, χρησιμοποιούμε τα ίδια σύμβολα για τις πράξεις πρόσθεσης και πολλαπλασιασμού, στα σύνολα R, S και $R \times S$. Αυτή η σύμβαση δεν δημιουργεί σύγχυση, αλλά είναι καλό να την έχουμε πάντα υπόψη μας.

Αν $(r_i, s_i) \in R \times S$, $1 \leq i \leq 3$, τότε:

$$(r_1,s_1)\cdot\big((r_2,s_2)+(r_3,s_3)\big) = (r_1,s_1)\cdot(r_2+r_3,s_2+s_3) = \big(r_1\cdot(r_2+r_3), s_1\cdot(s_2+s_3)\big) = (r_1\cdot r_2 + r_1\cdot r_3, s_1\cdot s_2 + s_1\cdot s_3) =$$
$$= (r_1\cdot r_2, s_1\cdot s_2) + (r_1\cdot r_3, s_1\cdot s_3) = (r_1,s_1)\cdot(r_2,s_2) + (r_1,s_1)\cdot(r_3,s_3)$$

Παρόμοια βλέπουμε ότι $\big((r_1,s_1)+(r_2,s_2)\big)\cdot(r_3,s_3) = (r_1,s_1)\cdot(r_3,s_3) + (r_2,s_2)\cdot(r_3,s_3)$. Άρα ικανοποιείται η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση, και επομένως η τριάδα $(R\times S, +, \cdot)$ είναι ένας δακτύλιος, ο **δακτύλιος ευθύ γινόμενο** των δακτυλίων R και S. Το μηδενικό στοιχείο του $R\times S$ είναι το ζεύγος $(0,0)$ και η μονάδα του δακτυλίου $R\times S$ είναι το ζεύγος $(1,1)$.

Παρατηρούμε ότι ο δακτύλιος $R\times S$ είναι μεταθετικός αν και μόνο αν οι δακτύλιοι R και S είναι μεταθετικοί. Πράγματι, αν οι δακτύλιοι R και S είναι μεταθετικοί, τότε, για κάθε $(r_i, s_i) \in R\times S$, $1 \leq i \leq 2$, θα έχουμε:

$$(r_1,s_1)\cdot(r_2,s_2) = (r_1\cdot r_2, s_1\cdot s_2) = (r_2\cdot r_1, s_2\cdot s_1) = (r_2,s_2)\cdot(r_1,s_1)$$

και άρα ο δακτύλιος $R\times S$ είναι μεταθετικός. Αντίστροφα, αν ο δακτύλιος $R\times S$ είναι μεταθετικός, τότε:

$$(r_1,1)\cdot(r_2,1) = (r_2,1)\cdot(r_1,1) \implies (r_1\cdot r_2, 1) = (r_2\cdot r_1, 1) \implies r_1\cdot r_2 = r_2\cdot r_1$$
$$(1,s_1)\cdot(1,s_2) = (1,s_2)\cdot(1,s_1) \implies (1, s_1\cdot s_1) = (1, s_2\cdot s_1) \implies s_1\cdot s_2 = s_2\cdot s_1$$

και άρα οι δακτύλιοι R και S είναι μεταθετικοί.

Αν $R_i = (R_i, +, \cdot)$, $1 \leq i \leq n$, είναι μια πεπερασμένη ακολουθία δακτυλίων (χρησιμοποιούμε πάντα τα ίδια σύμβολα για τις πράξεις πρόσθεσης και πολλαπλασιασμού, για τα μηδενικά στοιχεία, και τις μονάδες των δακτυλίων R_i, $1 \leq i \leq n$), τότε στο καρτεσιανό γινόμενο

$$\prod_{i=1}^{n} R_i = \big\{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \leq i \leq n\big\}$$

ορίζεται μια αβελιανή ομάδα $(\prod_{i=1}^n R_i, +)$ και ένα μονοειδές $(\prod_{i=1}^n R_i, \cdot)$, όπου οι πράξεις πρόσθεσης και πολλαπλασιασμού επί του $\prod_{i=1}^n R_i$ ορίζονται, «κατά συνιστώσα», ως εξής:

$$+ : \prod_{i=1}^n R_i \times \prod_{i=1}^n R_i \longrightarrow \prod_{i=1}^n R_i, \qquad (r_1, r_2, \cdots, r_n) + (r_1', r_2', \cdots, r_n') = (r_1 + r_1', r_2 + r_2', \cdots, r_n + r_n')$$
$$\cdot : \prod_{i=1}^n R_i \times \prod_{i=1}^n R_i \longrightarrow \prod_{i=1}^n R_i, \qquad (r_1, r_2, \cdots, r_n) \cdot (r_1', r_2', \cdots, r_n') = (r_1 \cdot r_1', r_2 \cdot r_2', \cdots, r_n \cdot r_n')$$

Τότε, όπως και παραπάνω, εύκολα βλέπουμε ότι ικανοποιείται η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση του $\prod_{i=1}^n R_i$, και επομένως η τριάδα $(\prod_{i=1}^n R_i, +, \cdot)$ είναι ένας δακτύλιος, ο **δακτύλιος ευθύ γινόμενο** των δακτυλίων $R_1, R_2, \cdots, R_n$. Το μηδενικό στοιχείο του δακτυλίου $\prod_{i=1}^n R_i$ είναι η n-άδα $0 = (0, 0, \cdots, 0)$ και η μονάδα του είναι η n-άδα $1 = (1, 1, \cdots, 1)$.

Παρόμοια με την περίπτωση $n = 2$, ο δακτύλιος $\prod_{i=1}^n R_i$ είναι μεταθετικός αν και μονον αν οι δακτύλιοι R_i, $1 \leq i \leq n$, είναι μεταθετικοί.

Η παραπάνω κατασκευή μορεί να γενικευθεί για τυχούσα οικογένεια δακτυλίων. Θεωρούμε μια οικογένεια δακτυλίων $\mathscr{R} = \{R_i\}_{i\in I}$, όπου $R_i = (R_i, +_i, \cdot_i)$, $i \in I$, και I είναι ένα τυχόν σύνολο δεικτών. Όπως και πριν, χάριν απλότητας, θα συμβολίζουμε τις πράξεις πρόσθεσης και πολλαπλασιασμού των δακτυλίων R_i μετ τα ίδια σύμβολα «+» και «·» αντίστοιχα. Στο καρτεσιανό γινόμενο

$$\prod_{i\in I} R_i = \big\{(r_i)_{i\in I} \mid r_i \in R_i,\ i \in I\big\}$$

ορίζουμε πράξεις πρόσθεσης «+» καο πολλαπλασιασμού «·», «κατά συνιστώσα», ως εξής:

$$+ : \prod_{i\in I} R_i \times \prod_{i\in I} R_i \longrightarrow \prod_{i\in I} R_i, \qquad (r_i)_{i\in I} + (r_i')_{i\in I} = (r_i + r_i')_{i\in I}$$
$$\cdot : \prod_{i\in I} R_i \times \prod_{i\in I} R_i \longrightarrow \prod_{i\in I} R_i, \qquad (r_i)_{i\in I} \cdot (r_i')_{i\in I} = (r_i \cdot r_i')_{i\in I}$$

Τότε η τριάδα $\prod_{i\in I} R_i = (\prod_{i\in I} R_i, +, \cdot)$ αποτελεί δακτύλιο, τον **δακτύλιο ευθύ γινόμενο της οικογένειας δακτυλίων** $\{R_i\}_{i\in I}$, και ο οποίος είναι μεταθετικός αν και μόνο αν ο δακτύλιος R_i είναι μεταθετικός $\forall\, i \in I$. Το μηδενικό στοιχείο του δακτυλίου $\prod_{i\in I} R_i$ είναι η ακολουθία $(r_i)_{i\in I}$, όπου $r_i = 0$, $(= 0_{R_i})$, $\forall\, i \in I$, και η μονάδα του είναι η ακολουθία $(r_i)_{i\in I}$, όπου $r_i = 1$ $(= 1_{R_i})$, $\forall\, i \in I$.

7.3.5 Δακτύλιοι Συναρτήσεων

Έστω $R=(R,+,\cdot)$ ένας δακτύλιος, και X ένα τυχόν μη κενό σύνολο. Θεωρούμε το σύνολο

$$\mathscr{F}(X,R)=\{f\colon X\longrightarrow R \mid f\colon \text{απεικόνιση}\}$$

Στο σύνολο $\mathscr{F}(X,R)$ ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού

$$+\ :\ \mathscr{F}(X,R)\times\mathscr{F}(X,R)\ \longrightarrow\ \mathscr{F}(X,R),\quad (f,g)\longmapsto f+g\colon X\longrightarrow R,\quad (f+g)(x)=f(x)+g(x)$$

$$\cdot\ :\ \mathscr{F}(X,R)\times\mathscr{F}(X,R)\ \longrightarrow\ \mathscr{F}(X,R),\quad (f,g)\longmapsto f\cdot g\colon X\longrightarrow R,\quad (f\cdot g)(x)=f(x)\cdot g(x)$$

όπου, $\forall x\in X$, $f(x)+g(x)$ και $f(x)\cdot g(x)$ συμβολίζει το αποτέλεσμα των πράξεων «+» και «·» στον δακτύλιο R. Τότε από το μέρος 4 του Παραδείγματος 2.2.10, καθώς και από την Πρόταση 1.4.13, έπεται ότι η αβελιανή ομάδα $(R,+)$ και το μονοειδές $(R,\cdot)$, επάγουν δομή αβελιανής ομάδας στο ζεύγος $(\mathscr{F}(X,R),+)$ και δομή μονοειδούς στο ζεύγος $(\mathscr{F}(X,R),\cdot)$. Αν $f,g,h\in\mathscr{F}(X,R)$, τότε, $\forall x\in X$, χρησιμοποιώντας την επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στον δακτύλιο R, θα έχουμε:

$$[f\cdot(g+h)](x)=f(x)\cdot(g+h)(x)=f(x)\cdot(g(x)+h(x))=f(x)\cdot g(x)+f(x)+h(x)\quad\Longrightarrow\quad f\cdot(g+h)=f\cdot g+f\cdot h$$

Παρόμοια θα έχουμε: $(f+g)\cdot h=f\cdot h+g\cdot h$. Επομένως ικανοποιείται η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση στο $\mathscr{F}(X,R)$, και επομένως η τριάδα $\mathscr{F}(X,R)=(\mathscr{F}(X,R),+,\cdot)$ είναι ένας δακτύλιος. Η μονάδα του δακτυλίου $\mathscr{F}(X,R)$ είναι η σταθερή απεικόνιση $1\colon X\longrightarrow R$, $1(x)=1\ (=1_R)$, και το μηδενικό στοιχείο του είναι η σταθερή απεικόνιση $0\colon X\longrightarrow R$, $0(x)=0\ (=0_R)$.

Αν ο δακτύλιος R είναι μεταθετικός, τότε επειδή, $\forall x\in X$:

$$(f\cdot g)(x)=f(x)\cdot g(x)=g(x)\cdot f(x)=(g\circ f)(x)$$

θα έχουμε $f\cdot g=g\cdot f$ και ο δακτύλιος $\mathscr{F}(X,R)$ είναι μεταθετικός. Αντίστροφα, αν ο δακτύλιος $\mathscr{F}(X,R)$ είναι μεταθετικός, και $r,s\in R$, τότε θεωρούμε τις σταθερές απεικονίσεις $\mathsf{r}\colon X\longrightarrow R$, $\mathsf{r}(x)=r$, και $\mathsf{s}\colon X\longrightarrow R$, $\mathsf{s}(x)=s$. Επειδή $\mathsf{r}\cdot\mathsf{s}=\mathsf{s}\cdot\mathsf{r}$, για κάθε $x\in X$, θα έχουμε: $(\mathsf{r}\cdot\mathsf{s})(x)=(\mathsf{s}\cdot\mathsf{r})(x)$, δηλαδή $\mathsf{r}(x)\cdot\mathsf{s}(x)=\mathsf{s}(x)\cdot\mathsf{r}(x)$, και άρα $r\cdot s=s\cdot r$. Επομένως ο δακτύλιος R είναι μεταθετικός.

Οι δακτύλιοι $\mathscr{F}(X,\mathbb{R}$ ή $\mathscr{F}(X,\mathbb{C})$, για κατάλληλα σύνολα X, περιέχουν σημαντικούς υποδακτυλίους, όπως για παράδειγμα δακτυλίους συνεχών, διαφορίσιμων, πραγματικών ή μιγαδικών συναρτήσεων.

7.3.6 Κεντροποιητές και το Κέντρο ενός Δακτυλίου

Κάθε δακτύλιος $R=(R,+,\cdot)$ περιέχει ενδιαφέροντες υποδακτυλίους.

Το **κέντρο** του R ορίζεται να είναι το ακόλουθο υποσύνολο του R:

$$\mathsf{Z}(R)=\{r\in R \mid x\cdot r=r\cdot x,\ \forall x\in R\}$$

Ισχυρισμός: Το κέντρο του R είναι ένας μεταθετικός υποδακτύλιος του R.

Πράγματι, η μονάδα 1_R ανήκει προφανώς στο κέντρο διότι $1_R\cdot x=x=x\cdot 1_R$, $\forall x\in R$. Έστω $r,s\in\mathsf{Z}(R)$ και $x\in R$. Τότε θα έχουμε:

$$(r-s)\cdot x=r\cdot x-s\cdot x=x\cdot r-x\cdot s=x\cdot(r-s)$$

$$(r\cdot s)\cdot x=r\cdot(s\cdot x)=r\cdot(x\cdot s)=(r\cdot x)\cdot s=(x\cdot r)\cdot s=x\cdot(r\cdot s)$$

Οι παραπάνω σχέσεις δείχνουν ότι το κέντρο $\mathsf{Z}(R)$ είναι ένας υποδακτύλιος του R, ο οποίος είναι προφανώς μεταθετικός. Παρατηρουμε ότι ο δακτύλιος R είναι μεταθετικός αν και μονον αν $R=\mathsf{Z}(R)$.

Γενικότερα, αν $X\subseteq R$ είναι ένα υποσύνολο του δακτυλίου R, τότε ο **κεντροποιητής** του υποσυνόλου X είναι το ακόλουθο υποσύνολο του R:

$$\mathsf{C}_R(X)=\{r\in R \mid x\cdot r=r\cdot x,\ \forall x\in X\}$$

Τότε, όπως παραπάνω, ο κεντροποιητής του X είναι ένας υποδακτύλιος του R, και προφανώς: $\mathsf{C}_R(R)=\mathsf{Z}(R)$.

Παρατηρούμε ότι

$$X\subseteq Y\subseteq R\quad\Longrightarrow\quad \mathsf{Z}(R)=\mathsf{C}_R(R)\ \subseteq\ \mathsf{C}_R(Y)\ \subseteq\ \mathsf{C}_R(X)$$

όπου στις εγκλείσεις στα δεξιά κάθε δακτύλιος είναι υποδακτύλιος του επόμενου.

Παράδειγμα 7.3.9. Θα προσδιορίσουμε τους κεντροποιητές των στοιχείων E_{ij}, $1 \le i, j \le 2$:

$$E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

καθώς και το κέντρο του δακτυλίου $\mathsf{M}_2(\mathbb{K})$, όπου $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$. Έστω $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{M}_2(\mathbb{K})$ ένας τυχών πίνακας.

1. $A \cdot E_{11} = E_{11} \cdot A \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \iff A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$

   Άρα: $\mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(E_{11}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid a, d \in \mathbb{K} \right\}$ είναι ο υποδακτύλιος των διαγώνιων πινάκων.

2. $A \cdot E_{12} = E_{12} \cdot A \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} 0 & a \\ 0 & c \end{pmatrix} = \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} \iff A = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$

   Άρα: $\mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(E_{12}) = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid a, b \in \mathbb{K} \right\}$.

3. $A \cdot E_{21} = E_{21} \cdot A \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} b & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \iff A = \begin{pmatrix} a & 0 \\ c & a \end{pmatrix}$

   Άρα: $\mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(E_{12}) = \left\{ \begin{pmatrix} a & 0 \\ c & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid a, c \in \mathbb{K} \right\}$.

4. $A \cdot E_{22} = E_{22} \cdot A \iff \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c & d \end{pmatrix} \iff A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$

   Άρα: $\mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(E_{11}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid a, d \in \mathbb{K} \right\}$ είναι ο υποδακτύλιος των διαγώνιων πινάκων.

5. Αν ο πίνακας $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ανήκει στο κέντρο $\mathsf{Z}(\mathsf{M}_2(\mathbb{K}))$ του δακτυλίου $\mathsf{M}_2(\mathbb{K})$, τότε προφανώς ο A μετατίθεται με τον πίνακα E_{11}, οπότε $b = c = 0$ και μετατίθεται και με τον E_{12}, οπότε $a = d$. Έτσι $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2$. Αντίστροφα κάθε βαθμωτός πίνακας aI_2 ανήκει στο κέντρο του $\mathsf{M}_2(\mathbb{K})$ διότι για κάθε πίνακα R, χρησιμοποιώντας ότι ο δακτύλιος $\mathbb{K}$ είναι μεταθετικός, θα έχουμε: $aI_2 \cdot R = a(I_2 \cdot R) = aR = Ra = RI_2 a = R(aI_2)$. Επομένως:

$$\mathsf{Z}(\mathsf{M}_2(\mathbb{K})) = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid r \in \mathbb{K} \right\} \quad \surd$$

Παράδειγμα 7.3.10. Θεωρούμε τον δακτύλιο των τετρανίων του Hamilton:

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \;\middle|\; a, b \in \mathbb{C} \right\}$$

Αν ο πίνακας $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}$ ανήκει στο κέντρο $\mathsf{Z}(\mathbb{H})$, τότε ο πίνακας A ιδιαίτερα μετατίθεται με τους πίνακες $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ και $C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ οι οποίοι ανήκουν στον δακτύλιο $\mathbb{H}$. Έτσι:

$$A \cdot B = B \cdot A \implies \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \implies \begin{pmatrix} -b & a \\ -\overline{a} & -\overline{b} \end{pmatrix} = \begin{pmatrix} -\overline{b} & \overline{a} \\ -a & -b \end{pmatrix} \implies a = \overline{a} \text{ και } b = \overline{b}$$

Άρα οι αριθμοί a, b είναι πραγματικοί: $a, b \in \mathbb{R}$. Επιπρόσθετα θα έχουμε:

$$A\cdot C = C\cdot A \implies \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\cdot\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\cdot\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \implies \begin{pmatrix} bi & ai \\ ai & -bi \end{pmatrix} = \begin{pmatrix} -bi & ai \\ ai & bi \end{pmatrix} \implies bi = -bi \implies b = 0$$

Άρα $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2$, $a \in \mathbb{R}$. Αντίστροφα, κάθε τέτοιος πίνακας A προφανώς ανήκει στο κέντρο του δακτυλίου $\mathbb{H}$. Επομένως:

$$\mathsf{Z}(\mathbb{H}) = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathbb{H} \mid a \in \mathbb{R} \right\} \quad \surd$$

Παράδειγμα 7.3.11. Στον δακτύλιο $\mathsf{M}_2(\mathbb{K})$, όπου $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, θα δείξουμε ότι:

$$\mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(L) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & 0 & a \end{pmatrix} \in \mathsf{M}_3(\mathbb{K}) \;\middle|\; a, b, c \in \mathbb{K} \right\}, \quad \text{όπου} \quad L = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Αν $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in \mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(L) := R$, τότε θα έχουμε:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}\cdot\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \implies \begin{pmatrix} 0 & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \end{pmatrix} = \begin{pmatrix} a_{13} & a_{12} & 0 \\ a_{23} & a_{22} & 0 \\ a_{33} & a_{32} & 0 \end{pmatrix}$$

και επομένως: $a_{13} = a_{12} = a_{23} = a_{21} = a_{32} = 0$ και $a_{11} = a_{33}$. Έτσι ο πίνακας A είναι της μορφής $\begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ c & 0 & a \end{pmatrix}$.
Αντίστροφα είναι άμεσα διαπιστώσιμο ότι κάθε πίνακας αυτής της μορφής ανήκει στον υποδακτύλιο $R = \mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(L)$. Αν $K = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, και $\mathscr{U} = \{L, K\}$, τότε παρόμοια βλέπουμε ότι

$$S := \mathsf{C}_{\mathsf{M}_2(\mathbb{K})}(\mathscr{U}) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & a \end{pmatrix} \in \mathsf{M}_3(\mathbb{K}) \;\middle|\; a, b \in \mathbb{K} \right\}$$

Αν και οι δακτύλιοι R και S προέκυψαν με παρόμοιο τρόπο, έχουν θεμελιώδες διαφορές στην δομή τους. Για παράδειγμα, ο δακτύλιος S δεν περιέχει μη μηδενικούς μηδενοδύναμους πίνακες, δηλαδή πίνακες A έτσι ώστε $A^n = 0$ για κάποιο $n \geq 1$, αντίθετα ο δακτύλιος R περιέχει τέτοιους πίνακες, π.χ. περιέχει τον μη-μηδενικό πίνακα $A = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ c & 0 & 0 \end{pmatrix}$ για τον οποίο ισχύει ότι $A^2 = 0$, και αυτό έχει δραστικές συνέπειες στη δομή τους.[3] $\surd$

7.4 Είδη Στοιχείων και Τύποι Δακτυλίων

Στην παρούσα ενότητα θα απομονώσουμε διάφορες ενδιαφέρουσες, ιδιότητες που μπορεί να ικανοποιούν τα στοιχεία ενός δακτυλίου, και μέσω αυτών των ιδιοτήτων θα ορίσουμε σημαντικές κλάσεις δακτυλίων.

Έστω $R = (R, +, \cdot)$ ένας δακτύλιος.

[3] Ο δακτύλιος S αποτελεί παράδειγμα «ημιαπλού» δακτυλίου. Ο δακτύλιος R δεν είναι ημιαπλός.

Ένα στοιχείο $r \in R$ καλείται **αριστερός διαιρέτης του μηδενός**, αν $r \neq 0$ και υπάρχει στοιχείο $0 \neq s \in R$ έτσι ώστε $r \cdot s = 0$. Παρόμοια το στοιχείο s καλείται **δεξιός διαιρέτης του μηδενός**, αν $s \neq 0$ και υπάρχει στοιχείο $0 \neq r \in R$ έτσι ώστε $r \cdot s = 0$. Αν $0 \neq r \in R$ και $r \cdot s = 0$ για κάποιο $0 \neq s \in R$, τότε πρόφανώς το r είναι αριστερός διαιρέτης του 0 και το s είναι δεξιός διαιρέτης του 0. Ένα στοιχείο του R καλείται **διαιρέτης του μηδενός** αν είναι αριστερός και δεξιός διαιρέτης του μηδενός. Προφανώς, αν ο δακτύλιος R είναι μεταθετικός, τότε δεν χρειάζεται να κάνουμε διάκριση μεταξύ αριστερών και δεξιών διαιρετών του μηδενός.

Για παράδειγμα, στον δακτύλιο $\mathsf{M}_2(\mathbb{K})$, όπου $\mathbb{K} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, και όπου $A = \begin{pmatrix} 1 & 2 \\ -2 & -4 \end{pmatrix}$ και $B = \begin{pmatrix} 6 & -2 \\ -3 & 1 \end{pmatrix}$, έχουμε $A \cdot B = 0$ και άρα ο A είναι αριστερός διαιρέτης του μηδενός και ο B είναι δεξιός διαιρέτης του μηδενός. Παρατηρούμε ότι $B \cdot A \neq 0$. Από την άλλη πλευρά μπορεί ένα στοιχείο σε έναν δακτύλιο να είναι αριστερός διαιρέτης του μηδενός, αλλά όχι δεξιός διαιρέτης του μηδενός, βλέπε την Άσκηση 7.6.12.

Ορισμός 7.4.1. *Ένας μη μηδενικός δακτύλιος R καλείται* **περιοχή** *ή* **δακτύλιος χωρίς διαιρέτες του μηδενός**, *αν:*

$$\forall r, s \in R: \quad r \cdot s = 0 \implies r = 0 \ \text{ ή } \ s = 0$$

Ένας μεταθετικός δακτύλιος ο οποίος είναι περιοχή καλείται **ακέραια περιοχή**.

Ισοδύναμα, ο δακτύλιος $R \neq \{0\}$ είναι περιοχή, αν $0 \neq r \in R$ και $0 \neq s \in R$, συνεπάγεται ότι $r \cdot s \neq 0$. Προφανώς ο μη μηδενικός δακτύλιος R είναι περιοχή, αν και μόνο αν δεν έχει δεξιούς ή αριστερούς διαιρέτες του μηδενός.

Παράδειγμα 7.4.2. Θα δούμε κάποια παραδείγματα και αντιπαραδείγματα (ακέραιων) περιοχών.

1. Θεωρούμε τον μεταθετικό δακτύλιο $\mathbb{Z}_4$. Τότε το στοιχείο $[2]_4$ είναι αριστερός και δεξιός διαιρέτης του μηδέν, διότι $[2]_4 \neq [0]_4$ και $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4$.

   Γενικότερα αν n είναι ένας σύνθετος θετικός ακέραιος, και $n = m \cdot k$, όπου $1 < m, k < n$, τότε ο δακτύλιος $\mathbb{Z}_n$ περιέχει διαιρέτες του μηδενός. Πράγματι, προφανώς θα έχουμε $[m]_n \neq [0]_n \neq [k]_n$, διότι διαφορετικά αν, για παράδειγμα $[m]_n = [0]_n$, τότε θα έχουμε $n \mid m$ και άρα $n \leq m$, το οποίο είναι άτοπο. Επιπλέον

   $$[m]_n \cdot [k]_n = [m \cdot k]_n = [n]_n = [0]_n$$

   Επομένως τα στοιχεία $[m]_n$ και $[k]_n$ είναι διαιρέτες του μηδενός.

   Συμεραίνουμε ότι:

   $$\text{ο θετικός ακέραιος } n \text{ είναι σύνθετος} \implies \text{ο δακτύλιος } \mathbb{Z}_n \text{ δεν είναι ακέραια περιοχή}$$

2. Θεωρούμε τον δακτύλιο $\mathsf{M}_2(R)$ των 2×2 πινάκων υπεράνω του R, όπου $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$, ή ο R μπορεί να είναι οποιοσδήποτε μη-μηδενικός δακτύλιος. Τότε ο δακτύλιος $\mathsf{M}_2(R)$ δεν είναι περιοχή, διότι περιέχει πάντα διαιρέτες του μηδενός. Για παράδειγμα οι πίνακες E_{11} και E_{22} είναι (δεξιοί και αριστεροί) διαιρέτες του μηδενός

   $$E_{11} \cdot E_{22} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{και} \quad E_{22} \cdot E_{11} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

   Γενικότερα ο δακτύλιος $\mathsf{M}_n(R)$, $n > 1$, περιέχει πάντα διαιρέτες του μηδενός, διότι: $E_{ij} \cdot E_{kl} = 0$, για κάθε $j \neq k$, και επομένως δεν είναι περιοχή.

3. Στον μεταθετικό δακτύλιο $\mathscr{C}([0,1], \mathbb{R}) = \{f : [0,1] \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$, οι συνεχείς συναρτήσεις

   $$f : [0,1] \longrightarrow \mathbb{R}, \quad f(x) = \begin{cases} 0, & \text{αν: } x \in [0, \frac{1}{2}] \\ x - \frac{1}{2}, & \text{αν: } x \in (\frac{1}{2}, 1] \end{cases}$$

   $$g : [0,1] \longrightarrow \mathbb{R}, \quad g(x) = \begin{cases} -x + \frac{1}{2}, & \text{αν: } x \in [0, \frac{1}{2}] \\ 0, & \text{αν: } x \in (\frac{1}{2}, 1] \end{cases}$$

   είναι μη μηδενικές και $f \cdot g = 0$, δηλαδή είναι (δεξιοί και αριστεροί) διαιρέτες του μηδενός. Επομένως ο δακτύλιος $\mathscr{C}([0,1], \mathbb{R})$ δεν είναι ακέραια περιοχή.

4. Σε αντίθεση με τα παραπάνω παραδείγματα δακτυλίων οι οποίοι δεν είναι (ακέραιες) περιοχές, οι μεταθετικοί δακτύλιοι $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$, προφανώς δεν περιέχουν διαιρέτες του μηδενός και άρα είναι ακέραιες περιοχές. $\surd$

Παρατήρηση 7.4.3. 1. Κάθε υποδακτύλιος μιας (ακέραιας) περιοχής είναι (ακέραια) περιοχή.

2. Το ευθύ γινόμενο μη μηδενικών (μεταθετικών) δακτυλίων δεν είναι ποτέ (ακέραια) περιοχή. Πράγματικα, αν R και S είναι δύο δακτύλιοι, τότε επειδή

$$(1,0)\cdot(0,1)=(0,0)$$

τα στοιχεία $(1,0)$ και $(0,1)$ είναι πάντα διαιρέτες του μηδενός. Παρόμοια για κάθε οικογένεια μη μηδενικών (μεταθετικών) δακτυλίων $\{R_i\}_{i\in I}$, όπου για το σύνολο δεικτών I είναι $|I|>1$, ο δακτύλιος ευθύ γινόμενο $\prod_{i\in I} R_i$ δεν είναι ποτέ (ακέραια) περιοχή. ▲

Το επόμενο Λήμμα πιστοποιεί ότι σε μια περιοχή ισχύουν οι Νόμοι Διαγραφής, όπως στις ομάδες, βλέπε την Πρόταση 2.1.8.

Λήμμα 7.4.4 (Νόμοι Διαγραφής)**.** *Έστω R μια περιοχή. Τότε ισχύουν τα εξής, $\forall\, a,b,c\in R$:*

$$a\neq 0,\quad a\cdot b=a\cdot c \implies b=c \quad \textit{και} \quad c\neq 0,\quad a\cdot c=b\cdot c \implies a=b$$

Αντίστροφα κάθε δακτύλιος $R\neq\{0\}$ για τον οποίου ισχύουν οι παραπάνω Νόμοι Διαγραφής, είναι περιοχή.

Απόδειξη. Έστω $a\neq 0$ και $a\cdot b=a\cdot c$. Τότε $a\cdot(b-c)=0$, και επειδή ο δακτύλιος R είναι περιοχή και $a\neq 0$, θα έχουμε $b-c=0$, δηλαδή $b=c$. Ανάλογα, αν $c\neq 0$ και $a\cdot c=b\cdot c$, τότε θα έχουμε $a=b$.

Αντίστροφα, έστω ότι $R\neq 0$ και ισχύουν οι παραπάνω Νόμοι Διαγραφής. Τότε, αν $a\cdot b=0$ και $a\neq 0$, τότε θα έχουμε $a\cdot b=a\cdot 0$, και από τον Νόμο Διαγραφής, έπεται ότι $b=0$. Παρόμοια, αν $b\neq 0$ και $a\cdot b=0$, τότε $a\cdot b=0\cdot b$ και από τον Νόμο Διαγραφής, έπεται ότι $a=0$. Επομένως ο δακτύλιος R είναι περιοχή. ■

Όπως θα δούμε αργότερα ο δακτύλιος πολυωνύμων $R[t]$ υπεράνω μιας ακέραιας περιοχής R είναι επίσης ακέραια περιοχή.

Ένα στοιχείο r του δακτυλίου R είναι **αντιστρέψιμο**, αν είναι αντιστρέψιμο στοιχείο του μονοειδούς $(R,\cdot)$, δηλαδή, αν υπάρχει στοιχείο $s\in R$ έτσι ώστε: $r\cdot s=1=s\cdot r$. Το στοιχείο s είναι τότε μοναδικό, συμβολίζεται με r^{-1} και καλείται το **αντίστροφο στοιχείο** του r. Το σύνολο όλων των αντιστρέψιμων στοιχείων του R συμβολίζεται με

$$\mathsf{U}(R)=\{r\in R \mid r:\ \text{αντιστρέψιμο στοιχείο}\}$$

και σύμφωνα με την Πρόταση 2.2.4, το ζεύγος $(\mathsf{U}(R),\cdot)$ είναι ομάδα, η οποία καλείται η **ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου** R. Επομένως, $1\in\mathsf{U}(R)$, και αν $r,s\in\mathsf{U}(R)$, τότε $r\cdot s\in\mathsf{U}(R)$, και $r^{-1}\in\mathsf{U}(R)$. Σημειώνουμε ότι $(r^{-1})^{-1}=r$ και $(r\cdot s)^{-1}=s^{-1}\cdot r^{-1}$.

Παράδειγμα 7.4.5. 1. $\mathsf{U}(\mathbb{Z})=\{1,-1\}$.

2. $\mathsf{U}(\mathbb{Q})=\mathbb{Q}^*$, $\mathsf{U}(\mathbb{R})=\mathbb{R}^*$, $\mathsf{U}(\mathbb{C})=\mathbb{C}^*$.

3. $\mathsf{U}(\mathsf{M}_n(\mathbb{K}))=\mathsf{GL}(n,\mathbb{K})$.

4. Γενικότερα για κάθε μεταθετικό δακτύλιο R ορίζεται η ομάδα $\mathsf{U}(\mathsf{M}_n(R))=\mathsf{GL}(n,R)$ των αντιστρέψιμων $n\times n$ πινάκων με στοιχεία από τον δακτύλιο R. $\surd$

Παράδειγμα 7.4.6 (Η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρέψιμων στοιχείων του $\mathbb{Z}_n$)**.** Για την ομάδα $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρεψίμων στοιχείων του δακτυλίου $\mathbb{Z}_n$, το παράδειγμα 2.2.5 δείχνει ότι:

$$\mathsf{U}(\mathbb{Z}_n)=\{[k]_n\in\mathbb{Z}_n \mid (k,n)=1\}$$

και άρα η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ είναι μια αβελιανή ομάδα τάξης $\phi(n)$, όπου ϕ είναι η συνάρτηση του Euler. $\surd$

Παράδειγμα 7.4.7 (Η ομάδα $\mathsf{U}(\mathbb{Z}[i])$ των αντιστρέψιμων στοιχείων των ακεραίων του Gauss)**.** Θεωρούμε τον δακτύλιο των ακεραίων του Gauss

$$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

Αν το στοιχείο $z = a + bi \in \mathbb{Z}[i]$ είναι αντιστρέψιμο, τότε υπάρχει στοιχείο $c + di \in \mathbb{Z}[i]$ έτσι ώστε: $(a + bi) \cdot (c + di) = 1$. Λαμβάνοντας συζυγείς μιγαδικούς αριθμούς σ' αυτή τη σχέση, θα έχουμε: $(a - bi) \cdot (c - di) = 1$, και τότε θα έχουμε:

$$a^2 + b^2 = 1 \quad \text{και} \quad c^2 + d^2 = 1$$

Επειδή οι αριθμοι a, b, c, d είναι ακέραιοι, οι μόνες λύσεις των παραπάνω εξισώσεων είναι $a = \pm 1$ και $b = 0$ ή $a = 0$ και $b = \pm 1$. Επομένως

$$\mathbb{Z}[i] = \{1, -1, i, -i\}$$

και άρα η ομάδα $\mathbb{Z}[i]$ είναι η κυκλική ομάδα $\langle i \rangle$ τάξης 4 η οποία παράγεται από το i. $\surd$

Παράδειγμα 7.4.8 (Η ομάδα $\mathsf{U}(\mathbb{H})$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{H}$ των τετρανίων του Hamilton)**.** Θεωρούμε τον δακτύλιο $\mathbb{H}$ των τετρανίων του Hamilton

$$\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \mid a, b \in \mathbb{C} \right\} = \left\{ \begin{pmatrix} a_0 + a_1 i & a_2 + a_3 i \\ -a_2 + a_3 i & a_0 - a_1 i \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \mid a_k \in \mathbb{R},\ 0 \le k \le 3 \right\}$$

Αν $A = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H}$, τότε η ορίζουσα του πίνακα A, θεωρούμενου ως πίνακα μιγαδικών αριθμών, είναι

$$\mathsf{Det}(A) = \mathsf{Det}\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = a\overline{a} + b\overline{b} = |a|^2 + |b|^2$$

Επομένως ο πίνακας $A \in \mathbb{H}$ είναι αντιστρέψιμος ως 2×2 πίνακας μιγαδικών αριθμών αν και μόνο αν $\mathsf{Det}(A) = |a|^2 + |b|^2 \neq 0$ δηλαδή αν και μόνο αν $(a, b) \neq (0, 0)$, δηλαδή αν και μόνο αν $A \neq 0$. Σ' αυτήν την περίπτωση, από την Γραμμική Άλγεβρα, γνωρίζουμε ότι ο αντίστροφός A^{-1} του A είναι:

$$A^{-1} = \begin{pmatrix} \frac{a}{\mathsf{Det}(A)} & \frac{-b}{\mathsf{Det}(A)} \\ \frac{\overline{b}}{\mathsf{Det}(A)} & \frac{a}{\mathsf{Det}(A)} \end{pmatrix}$$

Επειδή ο πίνακας A^{-1} είναι προφανώς στοιχείο του $\mathbb{H}$, έπεται ότι: *ένας πίνακας $A \in \mathbb{H}$ είναι αντιστρέψιμο στοιχείο του $\mathbb{H}$ αν και μόνο αν $A \neq 0$*, δηλαδή

$$\mathsf{U}(\mathbb{H}) = \mathbb{H}^*$$

Έτσι, αν και ο δακτύλιος $\mathbb{H}$ δεν είναι μεταθετικός, έχει κοινή με τους δακτυλίους $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, την ιδιότητα ότι κάθε μη μηδενικό στοιχείο του είναι αντιστρέψιμο.

Σημειώνουμε ότι η ομάδα $\mathsf{U}(\mathbb{H}) = \mathbb{H}^*$ περιέχει ως υποομάδα την ομάδα των τετρανίων Q του Hamilton, βλέπε το Παράδειγμα 2.4.20. $\surd$

Κάποια από τα παραπάνω παραδείγματα μας οδηγούν φυσιολογικά στον ακόλουθο ορισμό μιας θεμελιώδους κλάσης δακτυλίων.

Ορισμός 7.4.9. *Ένας δακτύλιος R καλείται* **δακτύλιος διαίρεσης**, *αν κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο. Ένας μεταθετικός δακτύλιος διαίρεσης καλείται* **σώμα**.

Παράδειγμα 7.4.10.

1. Οι δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$, και $\mathbb{C}$ είναι σώματα.
2. Ο δακτύλιος των τετρανίων του Hamilton είναι ένας δακτύλιος διαίρεσης ο οποίος δεν είναι σώμα. Ιστορικά ο δακτύλιος $\mathbb{H}$ αποτέλεσε το πρώτο παράδειγμα μη μεταθετικού δακτυλίου διαίρεσης.

3. Θεωρούμε τον υποδακτύλιο του σώματος $\mathbb{R}$ των πραγματικών αριθμών

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$$

Προφανώς ο δακτύλιος $\mathbb{Q}[\sqrt{2}]$ είναι μεταθετικός. Έστω $a + b\sqrt{2}$ ένα μη μηδενικό στοιχείο του $\mathbb{Q}[\sqrt{2}]$. Τότε $(a, b) \neq (0, 0)$ και ο ρητός αριθμός $a^2 - 2b^2 \neq 0$, διότι διαφορετικά, αν $a^2 = 2b^2$ και $b = 0$, τότε $a = 0$, το οποίο είναι άτοπο, και αν $a^2 = 2b^2$ και $b \neq 0$, τότε $a \neq 0$ και θα είχαμε $(\frac{a}{b})^2 = 2$, δηλαδή ο αριθμός $\sqrt{2}$ θα ήταν ρητός, το οποίο είναι άτοπο. Άρα ορίζεται ο ρητός αριθμός

$$\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

και όπως μπορούμε εύκολα να υπολογίσουμε: $(a + b\sqrt{2})^{-1} = \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Έτσι κάθε μη μηδενικό στοιχείο του $\mathbb{Q}[\sqrt{2}]$ είναι αντιστρέψιμο, και επομένως ο δακτύλιος $\mathbb{Q}[\sqrt{2}]$ είναι σώμα.

4. Ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι ακέραια περιοχή (ως υποδακτύλιος του σώματος $\mathbb{C}$), αλλά δεν είναι σώμα, διότι τα μόνα αντιστρέψιμα στοιχεία του είναι τα ± 1, και $\pm i$.

Αντίθετα ο δακτύλιος $\mathbb{Q}[i]$ των ρητών του Gauss

$$\mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

είναι σώμα διότι είναι μεταθετικός, ως υποδακτύλιος του $\mathbb{C}$, και αν $0 \neq a + bi \in \mathbb{Q}[i]$, οπότε $a^2 + b^2 \neq 0$, το στοιχείο $a + bi$ είναι αντιστρέψιμο με αντίστροφο το στοιχείο

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \in \mathbb{Q}[i] \quad \surd$$

Παρατήρηση 7.4.11. Ο Joseph Wedderburn[4] απέδειξε ότι μη μεταθετικοί δακτύλιοι διαίρεσης μπορεί να βρεθούν μόνο μεταξύ δακτυλίων διαίρεσης με άπειρο πλήθος στοιχείων:

Θεώρημα 7.4.12 (Wedderburn (1905)). *Κάθε δακτύλιος διαίρεσης με πεπερασμένο πλήθος στοιχείων είναι μεταθετικός και άρα είναι σώμα.*

Η απόδειξη του Θεωρήματος του Wedderburn δεν θα μας απασχολήσει διότι ξεφεύγει από τα πλαίσια των σημειώσεων.[5] ▲

Μέχρι τώρα έχουμε δει τρεις σημαντικές κλάσεις δακτυλίων: τις (ακέραιες) περιοχές, τους δακτυλίους διαίρεσης, και τα σώματα. Η ακόλουθη Πρόταση δείχνει ότι πεπερασμένες περιοχές είναι δακτύλιοι διαίρεσης.

Θεώρημα 7.4.13. *Κάθε περιοχή με πεπερασμένο πλήθος στοιχείων είναι δακτύλιος διαίρεσης.*
Ιδιαίτερα κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη. Έστω R μια πεπερασμένη περιοχή, και υποθέτουμε χωρίς βλάβη της γενικότητας ότι

$$R = \{x_1, x_2, \cdots, x_n\}$$

Έστω $x \in R$ ένα μη μηδενικό στοιχείο του R, και ορίζουμε απεικόνιση

$$f_x \colon R \longrightarrow R, \quad f_x(x_i) = x \cdot x_i$$

[4] Joseph Henry Maclagan Wedderburn (1882-1948) [https://en.wikipedia.org/wiki/Joseph_Wedderburn]: Σκώτος μαθηματικός ο οποίος εργάστηκε στην Αμερική (Princeton) με θεμελιώδη συμβολή στην Άλγεβρα, ειδικότερα στη Θεωρία Δακτυλίων, στη Θεωρία Ομάδων και στη Γραμμική Άλγεβρα. Είναι γνωστός κυρίως για το θεώρημα του ότι κάθε πεπερασμένος δακτύλιος διαίρεσης είναι σώμα, βλέπε το Θεώρημα 7.4.12, και για την απόδειξη ενός σημαντικού θεωρήματος, γνωστού σήμερα ως θεώρημα των Wedderburn-Artin περί της δομής των ημιαπλών αλγεβρών.

[5] Για μια απόδειξη του Θεωρήματος του Wedderburn παραπέμπουμε στο βιβλίο [18].

Η απεικόνιση f_x είναι «1-1» διότι αν $f_x(x_i) = f_x(x_j)$, τότε $x \cdot x_i = x \cdot x_j$ και τότε, επειδή $x \neq 0$, από τον Νόμο Διαγραφής σε περιοχές, βλέπε το Λήμμα 7.4.4, έπεται ότι $x_i = x_j$ και η f_x είναι «1-1». Επειδή το σύνολο R είναι πεπερασμένο, έπεται ότι η απεικόνιση f_x είναι «1-1» και «επί». Έτσι, για την μονάδα $1 \in R$, υπάρχει $x_i \in T = R$ έτσι ώστε $f_x(x_i) = 1$, δηλαδή $x \cdot x_i = 1$. Εργαζόμενοι ακριβώς ανάλογα με την απεικόνιση

$$g_x : R \longrightarrow R, \quad g_x(x_i) = x_i \cdot x$$

βλέπουμε ότι η g είναι «1-1» και «επί» και άρα υπάρχει $x_j \in R$ έτσι ώστε $g_x(x_j) = 1$, δηλαδή $x_j \cdot x = 1$. Τότε $x_j \cdot x \cdot x_i = 1 \cdot x_i = x_i$ και επομένως $x_j \cdot 1 = x_i$, δηλαδή $x_j = x_i := y$. Τότε $x \cdot y = 1 = y \cdot x$ και άρα το x είναι αντιστρέψιμο. Έτσι κάθε μη μηδενικό στοιχείο του R είναι αντιστρέψιμο και επομένως ο R ειναι δακτύλιος διαίρεσης. ■

Παρατήρηση 7.4.14. 1. Έστω R μια πεπερασμένη περιοχή. Τότε από το Θεώρημα 7.4.13 έπεται ότι ο δακτύλιος R είναι δακτύλιος διαίρεσης και από το Θεώρημα του Wedderburn έπεται ότι 7.4.12, έπεται ότι ο δακτύλιος R είναι σώμα. Άρα :

$$R : \text{πεπερασμένη περιοχή} \quad \Longrightarrow \quad R : \text{σώμα}$$

2. Έστω R μια πεπερασμένη ακεραία περιοχή χωρίς απαραίτητα μονάδα, δηλαδή R είναι ένα πεπερασμένο σύνολο το οποίο ικανοποιεί όλα τα αξιώματα μεταθετικού δακτυλίου, εκτός από την ύπαρξη μονάδας, και έτσι ώστε $a \cdot b = 0 \Longrightarrow a = 0$ ή $b = 0$. Τότε ο R έχει μονάδα και άρα είναι μια ακέραια περιοχή, και γι' αυτό είναι σώμα, σύμφωνα με το Θεώρημα 7.4.13.

   Πράγματι, για κάθε στοιχείο $x \in R$, $x \neq 0$, οι απεικονίσεις f_x και g_x του Θεωρήματος 7.4.13 είναι «1-1» και «επί», και άρα υπάρχουν μοναδικά στοιχεία x_i και x_j, έτσι ώστε $f_x(x_i) = x = f_y(x_j)$, δηλαδή $x \cdot x_i = x = x_j \cdot x$. Λόγω μεταθετικότητας θα έχουμε και $x = x \cdot x_j$, και άρα λόγω μοναδικότητας θα έχουμε $x_i = x_j$. Επομένως, υπάρχει ένα στοιχείο $e := x_i = x_j$ έτσι ώστε $x \cdot e = x = e \cdot x$, $\forall x \neq 0$. Αν $x = 0$, τότε $0 \cdot e = 0 = e \cdot 0$, όπως προκύπτει από το μέρος 1. της Πρότασης 7.1.5, στο οποίο δεν χρησιμοποιήθηκε η ύπαρξη μονάδας. Άρα $x \cdot e = x = e \cdot x$, και άρα $e = 1$ είναι η μονάδα του δακτυλίου. ▲

Θεώρημα 7.4.15. *Ισχύουν οι εξής συνεπαγωγές μεταξύ των παρακάτω κλάσεων δακτυλίων :*

$$R : \textit{Σώμα} \quad \Longrightarrow \quad R : \textit{Δακτύλιος Διαίρεσης} \quad \Longrightarrow \quad R : \textit{Περιοχή}$$

οι οποίες γενικά είναι μη-αναστρέψιμες.

Αν περιοριστούμε σε πεπερασμένους δακτυλίους, οι παραπάνω κλάσεις συμπίπτουν :

$$|R| < \infty \quad \Longrightarrow \quad R : \textit{Σώμα} \quad \Longleftrightarrow \quad R : \textit{Δακτύλιος Διαίρεσης} \quad \Longleftrightarrow \quad R : \textit{Ακέραια Περιοχή}$$

Απόδειξη. 1. Έστω R ένα σώμα. Τότε εξ ορισμού ο δακτύλιος R είναι δακτύλιος διαίρεσης.

2. Έστω R ένας δακτύλιος διαίρεσης. Έστω $a, b \in R$ και υποθέτουμε ότι $a \cdot b = 0$. Αν $a \neq 0$, τότε επειδή ο R είναι δακτύλιος διαίρεσης, έπεται ότι υπάρχει το αντίστροφο a^{-1} στοιχείο του a και ισχύει $a \cdot a^{-1} = 1 = a^{-1} \cdot a$. Τότε θα έχουμε :

$$a \cdot b = 0 \quad \Longrightarrow \quad a^{-1} \cdot a \cdot b = a^{-1} \cdot 0 = 0 \quad \Longrightarrow \quad 1 \cdot b = 0 \quad \Longrightarrow \quad b = 0$$

   Αν $b \neq 0$, τότε ανάλογα δείχνουμε ότι αναγκαστικά $a = 0$. Άρα ο δακτύλιος R είναι περιοχή.

3. Ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ακέραια περιοχή, αλλά δεν είναι δακτύλιος διαίρεσης διότι $\mathsf{U}(\mathbb{Z}) = \{\pm 1\} \neq \mathbb{Z}^*$.

   Ο δακτύλιος των τετρανίων του Hamilton είναι ένας δακτύλιος διαίρεσης ο οποίος δεν είναι σώμα.

4. Αν ο δακτύλιος R είναι πεπερασμένος, τότε από το Θεώρημα 7.4.13, έπεται ότι κάθε πεπερασμένη περιοχή είναι δακτύλιος διαίρεσης, και άρα : $R : \Delta\text{ακτύλιος Διαίρεσης} \Longleftrightarrow R : \Pi\text{εριοχή}$. Τέλος από το Θεώρημα του Wedderburn 7.4.12, έπεται ότι κάθε πεπερασμένος δακτύλιος διαίρεσης είναι μεταθετικός και άρα $R : \Sigma\text{ώμα} \Longleftrightarrow R : \Delta\text{ακτύλιος Διαίρεσης}$. ■

Η επόμενη Πρόταση χαρακτηρίζει πότε ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα.

Πρόταση 7.4.16. *Για τον δακτύλιο $\mathbb{Z}_n$, όπου $n>1$, τα ακόλουθα είναι ισοδύναμα:*

1. *Ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα.*
2. *Ο δακτύλιος $\mathbb{Z}_n$ είναι ακέραια περιοχή.*
3. *Ο n είναι πρώτος.*

Απόδειξη. Η ισοδυναμία 1. $\iff$ 2. προκύπτει άμεσα από το Θεώρημα 7.4.15. Αν ο δακτύλιος $\mathbb{Z}_n$ είναι ακέραια περιοχή, τότε σύμφωνα με το μέρος 1 του Παραδείγματος 7.4.2 ο αριθμός n δεν μπορεί να είναι σύνθετος, και άρα είναι πρώτος, δηλαδή 2. $\implies$ 3. Τέλος, αν ο αριθμός n είναι πρώτος, έστω $[k]_n \in \mathbb{Z}_n$ ένα μη μηδενικό στοιχείο. Επειδή $[k]_n \neq [0]_n$, θα έχουμε $n \nmid k$, και, επειδή ο n είναι πρώτος, θα έχουμε $(k,n)=1$. Τότε υπάρχουν ακέραιοι a,b έτσι ώστε $ak+bn=1$ και τότε $[a]_n[k]_n+[b]_n[n]_n=[1]_n$, δηλαδή $[a]_n[k]_n=[1]_n$. Επειδή ο δακτύλιος $\mathbb{Z}_n$ είναι μεταθετικός, έπεται ότι το στοιχείο $[k]_n$ είναι αντιστρέψιμο. Άρα κάθε μη μηδενικό στοιχείο του $\mathbb{Z}_n$ είναι αντιστρέψιμο και επομένως ο δακτύλιος είναι σώμα, δηλαδή 3. $\implies$ 1., και επομένως όλες οι συνθήκες είναι ισοδύναμες. ■

7.5 Χαρακτηριστική Δακτυλίου

Στον δακτύλιο $\mathbb{Z}_n$, υπάρχει ένας θετικός ακέραιος, ο n, έτσι ώστε $nx=0,\ \forall x\in\mathbb{Z}_n$. Αντίθετα στον δακτύλιο των ακεραίων $\mathbb{Z}$, δεν υπάρχει θετικός ακέραιος n έτσι ώστε $nx=0,\ \forall x\in\mathbb{Z}$. Αυτή η διαφοροποίηση μας οδηγεί στον ακόλουθο ορισμό.

Ορισμός 7.5.1. *Έστω R ένας δακτύλιος. Αν υπάρχει θετικός ακέραιος k έτσι ώστε $kx=0,\ \forall x\in R$, τότε ο αριθμός*

$$\mathrm{char}(R)=\min\{k\in\mathbb{N}\mid kx=0,\ \forall x\in R\}$$

καλείται η **χαρακτηριστική** *του δακτυλίου R.*

Αν δεν υπάρχει τέτοιος θετικός ακέραιος k, τότε θέτουμε: $\mathrm{char}(R)=0$.

Λήμμα 7.5.2. *Για έναν δακτύλιο R έχουμε,* $\mathrm{char}(R)=0$ *αν δεν υπάρχει $k\in\mathbb{N}$ έτσι ώστε $k1_R=0$, διαφορετικά:*

$$\mathrm{char}(R)=\min\{k\in\mathbb{N}\mid k1_R=0\}>0$$

Απόδειξη. Αν $\mathrm{char}(R)=n>0$, τότε προφανώς $n1_R=0$. Αν $k1_R=0$, για κάποιον θετικό ακέραιο k, τότε $k1_R\cdot x=0\cdot x=0$, και άρα, επειδή $1_R\cdot x=x$, θα έχουμε $k\cdot x=0,\ \forall x\in R$. Τότε όμως εξ' ορισμού θα έχουμε $n\le k$ και αυτό σημαίνει $n=\min\{k\in\mathbb{N}\mid k1_R=0\}$. Αντίστροφα, αν $n=\min\{k\in\mathbb{N}\mid k1_R=0\}$, τότε όπως και πριν θα έχουμε $n1_R=0$, από όπου $nx=0,\ \forall x\in R$. Αν $kx=0,\ \forall x\in R$, τότε $k1_R=0$, και άρα $n\le k$. Αυτό δείχνει ότι $\mathrm{char}(R)=n$. Αν $\mathrm{char}(R)=0$, τότε δεν υπάρχει $k\in\mathbb{N}$, έτσι ώστε $n1_R=0$, διότι διαφορετικά θα είχαμε όπως παραπάνω $\mathrm{char}(R)=n>0$. Αντιστροφα, αν δεν υπάρχει $k\in\mathbb{N}$ έτσι ώστε $k1_R=0$, τότε δεν υπάρχει $k\in\mathbb{N}$ έτσι ώστε $kx=0,\ \forall x\in R$, και επομένως $\mathrm{char}(R)=0$. ■

Πρόταση 7.5.3. *Για μια ακέραια περιοχή R, έχουμε:* $\mathrm{char}(R)=0$ *ή* $\mathrm{char}(R)$*: πρώτος.*

Απόδειξη. Έστω $\mathrm{char}(R)=n>0$, και έστω ότι ο n δεν είναι πρώτος. Τότε μπορούμε να γράψουμε $n=m\cdot k$, όπου $1<m,k<n$. Όμως από το Λήμμα 7.5.2, και το μέρος 5.*b*) της Πρότασης 7.1.5 θα έχουμε

$$0=n1_R=(m\cdot k)1_R=(m1_R)\cdot(k1_R)\quad\Longrightarrow\quad(m1_R)=0\quad\text{ή}\quad(k1_R)=0$$

Και οι δύο εκδοχές μάς οδηγουν σε αντίφαση διότι από το Λήμμα 7.5.2 έχουμε $n=\mathrm{char}(R)=\min\{k\in\mathbb{N}\mid k1_R=0\}>m,k$. Άρα ο n είναι πρώτος. ■

Παράδειγμα 7.5.4. 1. $\mathsf{char}(\mathbb{Z}) = \mathsf{char}(\mathbb{Q}) = \mathsf{char}(\mathbb{R}) = \mathsf{char}(\mathbb{C}) = 0$.

2. $\mathsf{char}(\mathbb{Z}_n) = n$.

   Πράγματι έχουμε $n[1]_n = [n]_n = [0]_n$. Αν $k[1]_n = [0]_n$, τότε $[k]_n = [0]_n$ από όπου $n \mid k$ και άρα $n \leq k$. Επομένως $n = \min\{k \in \mathbb{N} \mid k[1]_n = 0\}$ και έτσι: $\mathsf{char}(\mathbb{Z}_n) = n$.

3. Αν R είναι ένας πεπερασμένος δακτύλιος, έστω $|R| = n < \infty$, τότε η αβελιανή ομάδα $(R, +)$ είναι πεπερασμένη και επομένως από γνωστή συνέπεια του Θεωρήματος του Lagrange, θα έχουμε $nx = 0$, $\forall x \in R$. Άρα $\mathsf{char}(R) > 0$.

4. Δεν έχουν μόνο οι πεπερασμένοι δακτύλιοι πεπερασμένη μη μηδενική χαρακτηριστική. Πράγματι, έστω ο δακτύλιος πολυωνύμων $\mathbb{Z}_2[t]$ υπεράνω του σώματος $\mathbb{Z}_2$ το οποίο έχει χαρακτηριστική $\mathsf{char}(\mathbb{Z}_2) = 2$. Τότε, χρησιμοποιώντας ότι $2x = 0$, $\forall x \in \mathbb{Z}_2$, για κάθε στοιχείο $P(t) = a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ του $\mathbb{Z}_2[t]$, θα έχουμε:

$$2P(t) = 2(a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n) = (2a_0)1 + (2a_1)t + (2a_2)t^2 + \cdots + (2a_n)t^n = 0$$

   Άρα $\mathsf{char}(\mathbb{Z}_2[t]) = 2$ και προφανώς ο δακτύλιος $\mathbb{Z}_2[t]$ έχει άπειρο πλήθος στοιχείων. $\surd$

7.6 Ασκήσεις

Άσκηση 7.6.1. *Να δειχθεί ότι ένας δακτύλιος R είναι μεταθετικός αν και μόνο αν για κάθε $x, y \in R$ ισχύει ότι: $(x+y)^2 = x^2 + 2xy + y^2$.*

Άσκηση 7.6.2. *Έστω $R = (R, +, \cdot)$ ένας δακτύλιος. Στο σύνολο R ορίζουμε μια νέα πράξη $\circ$ ως εξής, $\forall x, y \in R$:*

$$x \circ y = x + y - xy$$

1. *Να δειχθεί ότι το ζεύγος $(R, \circ)$ είναι μονοειδές*
2. *Ποια είναι η ομάδα των αντιστρέψιμων στοιχείων του μονοειδούς $(R, \circ)$;*

Άσκηση 7.6.3. *Να επαληθευθεί ότι το σύνολο $\mathsf{AT}_n(\mathbb{K})$ των άνω τριγωνικών $n \times n$ πινάκων με στοιχεία από το $\mathbb{K}$ είναι ένας μη μεταθετικός υποδακτύλιος του δακτυλίου πινάκων $\mathsf{M}_n(\mathbb{K})$.*

Άσκηση 7.6.4. *Αν R είναι ένας δακτύλιος, τότε να δειχθεί ότι ο δακτύλιος $\mathsf{M}_n(R)$ των $n \times n$ πινάκων υπεράνω του R είναι μεταθετικός αν και μόνο αν ο R είναι μεταθετικός και $n = 1$.*

Άσκηση 7.6.5. *Να δειχθεί ότι, αν ο δακτύλιος $\mathbb{K}$ είναι σώμα, τότε ένας πίνακας $A \in \mathsf{M}_n(\mathbb{K})$ είναι διαιρέτης του μηδενός αν και μόνο αν $\mathsf{Det}(A) = 0$. Ισχύει το συμπέρασμα αν ο δακτύλιος $\mathbb{K}$ δεν είναι σώμα;*

Άσκηση 7.6.6. *Να δειχθεί ότι στον δακτύλιο $\mathbb{Z}_n$, ένα στοιχείο είναι διαιρέτης του μηδενός αν και μονον αν δεν είναι αντιστρέψιμο.*

Άσκηση 7.6.7. *Έστω η προσθετική ομάδα $(\mathbb{Z}, +)$. Να περιγραφούν όλες οι δυνατές πράξεις πολλαπλασιασμού «$\star$» επί του συνόλου $\mathbb{Z}$, έτσι ώστε η τριάδα $(\mathbb{Z}, +, \star)$ να αποτελεί δακτύλιο με μονάδα.*

Άσκηση 7.6.8. *Έστω η προσθετική ομάδα $(\mathbb{Z}_n, +)$, $n \geq 2$. Να περιγραφούν όλες οι δυνατές πράξεις πολλαπλασιασμού «$\star$» επί του συνόλου $\mathbb{Z}_n$, έτσι ώστε η τριάδα $(\mathbb{Z}_n, +, \star)$ να αποτελεί δακτύλιο με μονάδα.*

Άσκηση 7.6.9. *Θεωρούμε τις προσθετικές αβελιανές ομάδες $(\mathbb{Q}/\mathbb{Z},+)$ και $(\mathbb{R}/\mathbb{Z},+)$. Να εξεταστεί αν υπάρχουν πράξεις πολλαπλασιασμού «$\star$» και «$*$» επί των συνόλων $\mathbb{Q}/\mathbb{Z}$ και $\mathbb{R}/\mathbb{Z}$ αντίστοιχα, έτσι ώστε οι τριάδες $(\mathbb{Q}/\mathbb{Z},+,\star)$ και $(\mathbb{R}/\mathbb{Z},+,*)$ να αποτελούν δακτύλιο (με μονάδα).*

Άσκηση 7.6.10. *Έστω $(R,+,\cdot)$ μια τριάδα η οποία ικανοποιεί όλα τα αξιώματα του ορισμού δακτυλίου με μονάδα, εκτός από την μεταθετικότητα της πρόσθεσης. Να δείξετε οτι ισχύει η μεταθετικότητα της πρόσθεσης και η τριάδα $(R,+,\cdot)$ είναι ένας δακτύλιος.*

Σχόλιο 7.6.11. *Αν στην Άσκηση 7.6.10 για την τριάδα $(R,+,\cdot)$ δεν απαιτήσουμε την ύπαρξη μονάδας, τότε το συμπέρασμα της Άσκησης δεν ισχύει. Πράγματι, έστω $(R,+)$ μια (προσθετική) μη αβελιανή ομάδα με παραπάνω από ένα στοιχεία, για παράδειγμα η συμμετρική ομάδα S_3 τάξης 6. Ορίζουμε πράξη πολλαπλασιασμού ως εξής: $r\cdot s = 0_R,\ \ \forall r,s\in R$. Τότε η τριάδα $(R,+,\cdot)$ ικανοποιεί όλα τα αξιώματα του ορισμού δακτυλίου χωρίς μονάδα (αν υπάρχει μονάδα 1_R, τότε $1_R = 1_R 1_R = 0_R$ και επομένως $R=\{0_R\}$ το οποίο είναι άτοπο διότι $|R|>1$), εκτός από τη μεταθετικότητα της πρόσθεσης. Η τελευταία ιδιότητα δεν είναι δυνατόν να ισχύει, διότι η ομάδα R δεν είναι αβελιανή.*

Η παραπάνω ανάλυση δείχνει ότι κάθε αβελιανή ομάδα R μπορεί να θεωρηθεί ως δακτύλιος (χωρίς μονάδα αν $|R|>1$) με τετριμμένο πολλαπλασιασμό. $\surd$

Άσκηση 7.6.12. *Για κάθε θετικό ακέραιο n, θεωρούμε το σύνολο πινάκων*

$$R=\begin{pmatrix}\mathbb{Z} & \mathbb{Z}_n\\ 0 & \mathbb{Z}\end{pmatrix}=\left\{\begin{pmatrix}x & [y]_n\\ 0 & z\end{pmatrix}\mid x,y,z\in\mathbb{Z}\right\}$$

στο οποίο ορίζουμε πράξεις πρόσθεσης «$+$» και πολλαπλασιασμού «$\cdot$», ως εξής:

$$\begin{pmatrix}x & [y]_n\\ 0 & z\end{pmatrix}+\begin{pmatrix}x' & [y']_n\\ 0 & z'\end{pmatrix}=\begin{pmatrix}x+x' & [y+y']_n\\ 0 & z+z'\end{pmatrix}\quad \text{και}\quad \begin{pmatrix}x & [y]_n\\ 0 & z\end{pmatrix}\cdot\begin{pmatrix}x' & [y']_n\\ 0 & z'\end{pmatrix}=\begin{pmatrix}xx' & [xy'+yz']_n\\ 0 & zz'\end{pmatrix}$$

1. *Να δειχθεί ότι η τριάδα $(R,+,\cdot)$ είναι ένας δακτύλιος, όπου*
$$0_R=\begin{pmatrix}0 & [0]_n\\ 0 & 0\end{pmatrix}\quad \text{και}\quad 1_R=\begin{pmatrix}1 & [1]_n\\ 0 & 1\end{pmatrix}$$
2. *Να δειχθεί ότι ο πίνακας $\begin{pmatrix}n & [1]_n\\ 0 & 0\end{pmatrix}$ είναι αριστερός διαιρέτης του μηδενός, αλλά όχι δεξιός διαιρέτης του μηδενός, στον δακτύλιο R.*
3. *Να προσδιοριστεί το κέντρο $\mathsf{Z}(R)$ του δακτυλίου R.*
4. *Να προσδιοριστεί η ομάδα $\mathsf{U}(R)$ των αντιστρέψιμων στοιχείων του R.*

Άσκηση 7.6.13. *Έστω ότι x,y είναι στοιχεία ενός δακτυλίου R και υποθέτουμε ότι $x^n=y^n$ και $x^m=y^m$, όπου n,m είναι σχετικά πρώτοι θετικοί ακέραιοι, δηλαδή $(x,y)=1$. Να δειχθεί ότι $x=y$.*

Άσκηση 7.6.14. *Έστω ότι R είναι ένας δακτύλιος για τον οποίο ισχύει ότι:*

$$\forall a,b\in R:\quad (ab)^2=a^2b^2$$

Να δειχθεί ότι ο δακτύλιος R είναι μεταθετικός.

Άσκηση 7.6.15. *Θεωρούμε τον δακτύλιο $\mathscr{F}(\mathbb{R},\mathbb{R})$ όλων των απεικονίσεων $f:\mathbb{R}\longrightarrow\mathbb{R}$. Να εξεταστεί αν το ακόλουθο υποσύνολο*

$$S=\left\{A\in\mathscr{F}(\mathbb{R},\mathbb{R})\mid \exists f,g,h\in\mathscr{F}(\mathbb{R},\mathbb{R}): A(x)=f(x)+g(x)\sin(nx)+h(x)\cos(nx),\ \forall x\in\mathbb{R}\right\}$$

είναι ένας υποδακτύλιος του $\mathscr{F}(\mathbb{R},\mathbb{R})$.

Άσκηση 7.6.16. *Ποια από τα επόμενα σύνολα μαζί με τις αναφερόμενες πράξεις αποτελούν δακτύλιους;*

1. $$R = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών.

2. $$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων.

3. $$R = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων.

4. $$R = \{A \in \mathsf{M}_2(\mathbb{R}) \mid \mathsf{Det}(A) = 0\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων.

5. $$R = \left\{ \frac{m}{n} \in \mathbb{Q} \mid n \text{ περιττός} \right\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού ρητών αριθμών.

6. $$R = \{r\, i \mid r \in \mathbb{R}\}$$
   όπου $i^2 = -1$, μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών.

7. $$\mathbb{Q}(\sqrt[3]{5}) = \{a + b\sqrt[3]{5} \in \mathbb{R} \mid a, b \in \mathbb{R}\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών.

8. $$R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid 3 \nmid b \right\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού ρητών αριθμών.

Άσκηση 7.6.17. *Να δείξετε ότι για το κέντρο $\mathsf{Z}(\mathbb{H})$ του δακτυλίου των τετρανίων του Hamilton ισχύει ότι:*

$$\mathsf{Z}(\mathbb{H}) = \mathsf{Z}(\mathsf{M}_2(\mathbb{R}))$$

Άσκηση 7.6.18. *Να δειχθεί ότι το σύνολο*

$$R = \{m + n\sqrt{-3} \in \mathbb{C} \mid \text{είτε } m, n \in \mathbb{Z} \text{ είτε } m = \frac{a}{2} \text{ και } n = \frac{b}{2} \text{ όπου οι } a, b \text{ είναι περιττοί ακέραιοι}\}$$

είναι ένας υποδακτύλιος του $\mathbb{C}$.

Άσκηση 7.6.19. *Για κάθε μη μηδενικό ακέραιο d ο οποίος είναι ελεύθερος τετραγώνου, δηλαδή δεν υπάρχει πρώτος το τετράγωνο του οποίου διαιρεί τον d, να δειχθεί ότι το σύνολο*

$$\mathbb{Z}[\sqrt{d}] = \{m + n\sqrt{d} \in \mathbb{C} \mid m, n \in \mathbb{Z}\}$$

είναι ένας υποδακτύλιος του $\mathbb{C}$.

Άσκηση 7.6.20. *Έστω $q \in \mathbb{Q}$ ένας ρητός αριθμός. Θεωρούμε το ακόλουθο σύνολο*

$$R_q = \left\{ \begin{pmatrix} a & b \\ qb & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{Q}) \mid a, b \in \mathbb{Q} \right\}$$

1. *Να δειχθεί ότι το σύνολο R_q είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{Q})$.*
2. *Να δειχθεί ότι ο δακτύλιος R_q είναι δακτύλιος διαίρεσης αν και μόνο αν δεν υπάρχει ρητός $r \in \mathbb{Q}$ έτσι ώστε $r^2 = q$.*
3. *Είναι ο δακτύλιος R_q σώμα;*
4. *Με ποιον γνωστό σας δακτύλιο συμπίπτει ο δακτύλιος R_{-1};*

Άσκηση 7.6.21. *Να προσδιοριστούν όλοι οι διαιρέτες του μηδενός των επόμενων δακτυλίων:*
(1) $\mathbb{Z}_4$, (2) $\mathbb{Z}_8$, (3) $\mathbb{Z}_{11}$, (4) $\mathbb{Z}_4 \times \mathbb{Z}_4$

Ένα στοιχείο $a \in R$ σε έναν δακτύλιο R καλείται **ταυτοδύναμο**, αν $a^2 = a$. Για παράδειγμα τα στοιχεία $0, 1$ κάθε δακτυλίου είναι ταυτοδύναμα.

Άσκηση 7.6.22. *Ένας δακτύλιος με μονάδα R καλείται* **δακτύλιος του Boole**, *αν κάθε στοιχείο του είναι ταυτοδύναμο, δηλαδή:*

$$\forall r \in R: \quad r^2 = r$$

Να δειχθεί ότι κάθε δακτύλιος του Boole R είναι μεταθετικός και $\mathsf{char}(R) = 2$, αν $R \neq \{0\}$.

Άσκηση 7.6.23. *Έστω R ένας δακτύλιος για τον οποίο ισχύει ότι:*

$$\forall r \in R: \quad r^3 = r$$

Να δειχθεί ότι ο R είναι μεταθετικός.[6]

Άσκηση 7.6.24. *Έστω R ένας δακτύλιος για τον οποίο ισχύει ότι:*

$$\forall r \in R: \quad r^6 = r$$

Να δειχθεί ότι $r^2 = r$, $\forall r \in R$, δηλαδή ο R είναι δακτύλιος του Boole και άρα ο R είναι μεταθετικός.

Άσκηση 7.6.25. *Να δειχθεί ότι ένας δακτύλιος R είναι δακτύλιος του Boole αν και μόνο αν ο R είναι μεταθετικός και ισχύει ότι, $\forall a, b \in R$: $(a+b)ab = 0$.*

Άσκηση 7.6.26. *Έστω A ένα τυχόν σύνολο και θεωρούμε το δυναμοσύνολο $\mathscr{P}(A)$ του A το οποίο θεωρούμε εφοδιασμένο με τις ακόλουθες πράξεις «+» «πρόσθεσης» και «·» «πολλαπλασιασμού»:*

$$+ : \mathscr{P}(A) \times \mathscr{P}(A) \longrightarrow \mathscr{P}(A), \quad X + Y = (X \setminus Y) \bigcup (Y \setminus X) \qquad \textit{(Συμμετρική Διαφορά)}$$

$$\cdot : \mathscr{P}(A) \times \mathscr{P}(A) \longrightarrow \mathscr{P}(A), \quad X \cdot Y = X \bigcap Y \qquad \textit{(Τομή)}$$

1. *Να δειχθεί ότι η τριάδα $\mathscr{P}(A) = (\mathscr{P}(A), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα.*

[6] Ένα σημαντικό Θεώρημα του Jacobson πιστοποιεί ότι: *αν R είναι ένας δακτύλιος για τον οποίο ισχύει ότι:*

$$\forall x \in R, \ \exists n_x \in \mathbb{N}: \quad x^{n_x} = x$$

τότε ο δακτύλιος R είναι μεταθετικός.

- Nathan Jacobson (5 Οκτωβρίου 1910 - 5 Δεκεμβρίου 1999) [https://en.wikipedia.org/wiki/Nathan_Jacobson]: Σημαντικός Αμερικανός μαθηματικός, πολωνικής καταγωγής, με θεμελιώδη συμβολή στην Άλγεβρα και ιδιαίτερα στη Θεωρία Δακτυλίων.

2. *Να δειχθεί ότι ο δακτύλιος $\mathscr{P}(A)$ είναι δακτύλιος του Boole.*

3. *Να περιγραφούν οι δακτύλιοι $\mathscr{P}(A)$, όταν $A = \{1,2\}$ και $A = \{1,2,3\}$.*

Ένα στοιχείο $r \in R$ σε έναν δακτύλιο R καλείται **μηδενοδύναμο**, αν υπάρχει θετικός ακέραιος n έτσι ώστε: $r^n = 0$.

Άσκηση 7.6.27. *Ποια είναι τα μηδενοδύναμα και ταυτοδύναμα στοιχεία σε μια (ακέραια) περιοχή; Βρείτε πέντε ταυτοδύναμα και πέντε μηδενοσύναμα στοιχεία στον δακτύλιο $\mathsf{M}_2(\mathbb{R})$.*

Άσκηση 7.6.28. *Να δειχθεί ότι, αν u είναι ένα μηδενοδύναμο στοιχείο σε έναν δακτύλιο R, τότε το στοιχείο $1+u$ είναι αντιστρέψιμο.*

Άσκηση 7.6.29. *Έστω ότι $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ είναι η πρωτογενής ανάλυσης του θετικού ακέραιου $n > 1$.*

1. *Να δειχθεί ότι ο δακτύλιος $\mathbb{Z}_n$ περιέχει μη μηδενικά μηδενοδύναμα στοιχεία αν και μόνο αν ο θετικός ακέραιος n δεν είναι ελεύθερος τετραγώνου, δηλαδή υπάρχει πρώτος p έτσι ώστε το τετράγωνό του να διαιρεί τον n.*

2. *Να δειχθεί ότι το στοιχείο $[k]_n \in \mathbb{Z}_n$ είναι μηδενοδύναμο αν και μόνο αν $p_1 p_2 \cdots p_m \mid k$.*

Άσκηση 7.6.30. *Να δειχθεί ότι οι επόμενοι δακτύλιοι αποτελούν ακέραιες περιοχές:*

1. $$\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$
   όπου $i^2 = -1$, μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών.

2. $$\mathbb{Q}(i) = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$
   όπου $i^2 = -1$, μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού μιγαδικών αριθμών.

3. $$\mathbb{Z}(\sqrt{5}) = \{a + b\sqrt{5} \in \mathbb{R} \mid a, b \in \mathbb{Z}\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών.

4. $$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \in \mathbb{R} \mid a, b, c, d \in \mathbb{Q}\}$$
   μαζί με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πραγματικών αριθμών.

Άσκηση 7.6.31. *Έστω $(R, +, \cdot)$ ένας δακτύλιος και $u \in R$ ένα στοιχείο του το οποίο ικανοποιεί την ιδιότητα ότι υπάρχει στοιχείο $v \in R$ έτσι ώστε $uvu = u$ και $vu^2v = 1$. Να δειχθεί ότι το στοιχείο u είναι αντιστρέψιμο και $v = u^{-1}$.*

Άσκηση 7.6.32. *Έστω $(R, +, \cdot)$ ένας δακτύλιος και $u \in R$ ένα στοιχείο του το οποίο ικανοποιεί την ιδιότητα ότι υπάρχει μοναδικό στοιχείο $v \in R$ έτσι ώστε $uvu = u$. Να δειχθεί ότι το στοιχείο u είναι αντιστρέψιμο και $v = u^{-1}$.*

Άσκηση 7.6.33. *Έστω $(R, +, \cdot)$ ένας δακτύλιος και $a, b \in R$ είναι δύο αντιστρέψιμα στοιχεία του, και υποθέτουμε ότι το στοιχείο $ab - 1$ είναι αντιστρέψιμο. Να δειχθεί ότι τα στοιχεία $a - b^{-1}$ και $(a - b^{-1})^{-1} - a^{-1}$ είναι αντιστρέψιμα και*

$$((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$$

Άσκηση 7.6.34. *Έστω $(R,+,\cdot)$ ένας δακτύλιος χωρίς μονάδα με τουλάχιστον δύο στοιχεία και ο οποίος ικανοποιεί την επιπλέον ιδιότητα ότι, για κάθε $a \in R$, $a \neq 0$, υπάρχει μοναδικό στοιχείο $b \in R$ έτσι ώστε $aba = a$. Να δειχθεί ότι:*

1. *ο R δεν διαθέτει διαιρέτες του μηδενός.*
2. *$bab = b$.*
3. *ο R διαθέτει μοναδιαίο στοιχείο.*
4. *ο R είναι δακτύλιος διαίρεσης.*

Άσκηση 7.6.35. *Ποιοι από τους επόμενους δακτύλιους είναι σώματα;*
(1) $\mathbb{Z}[i]$, (2) $\mathbb{Q} \times \mathbb{Q}$, (3) $\mathbb{Z}_{13}$.

Άσκηση 7.6.36. *Να προσδιοριστούν τα αντιστρέψιμα στοιχεία των επόμενων δακτυλίων:*
(1) $\mathbb{Z}_{10}$, (2) $\mathbb{Z}_2 \times \mathbb{Z}_4$, (3) $\mathbb{Z}[i]$, *όπου* $i^2 = -1$, (4) $\mathbb{Z} \times \mathbb{Z}$, (5) $\mathbb{H}$.

Άσκηση 7.6.37. *Αν $n_1, n_2, \cdots, n_k$, είναι θετικοί ακέραιοι, ποια είναι η χαρακτηριστική του δακτυλίου ευθέος γινόμενου $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$;*

Άσκηση 7.6.38. *Ποια είναι η χαρακτηριστική των επόμενων δακτυλίων;*
(1) $\mathbb{Z}_{10} \times \mathbb{Z}_8$, (2) $\mathbb{C}$, (3) $\mathbb{Z} \times \mathbb{Z}$, (4) $\mathbb{H}$, (5) $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}_3$.

Άσκηση 7.6.39. *Να βρεθεί η χαρακτηριστική των δακτυλίων ενδομορφισμών*

$$\mathsf{End}_{\mathbb{Z}}(\mathbb{Z}), \quad \mathsf{End}_{\mathbb{Z}}(\mathbb{Z}_3), \quad \mathsf{End}_{\mathbb{Z}}(\mathbb{Z}_p) \quad (p : \textit{πρώτος}), \quad \mathsf{End}_{\mathbb{Z}}(\mathbb{Z}_n)$$

Άσκηση 7.6.40. *Να δοθεί παράδειγμα μεταθετικού δακτυλίου ο οποίος δεν είναι σώμα του οποίου η χαρακτηριστική είναι πρώτος αριθμός.*

Άσκηση 7.6.41. *Να δειχθεί ότι όλα τα μη μηδενικά στοιχεία της προσθετικής ομάδας $(\mathbb{K},+)$ ενός σώματος $\mathbb{K}$ έχουν την ίδια τάξη.*

Άσκηση 7.6.42. *Να δειχθεί ότι σε ένα σώμα $\mathbb{F}$ χαρακτηριστικής $\mathsf{char}(\mathbb{F}) = p > 0$ ισχύει:*

$$\forall\, a, b \in \mathbb{F}: \quad (a+b)^p = a^p + b^p$$

Άσκηση 7.6.43. *Έστω ότι $(M,+)$ είναι μια προσθετική αβελιανή ομάδα και έστω*

$$\mathsf{End}_{\mathbb{Z}}(M) = \{f : M \longrightarrow M \mid f : \textit{είναι ομομορφισμός ομάδων}\}$$

Στο σύνολο $\mathsf{End}_{\mathbb{Z}}(M)$ ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «∘», ως εξής, $\forall\, f, g \in \mathsf{End}_{\mathbb{Z}}(M)$:

$$f+g:\ M \longrightarrow M, \quad (f+g)(m) = f(m) + g(m)$$

$$f \circ g:\ M \longrightarrow M, \quad (f \circ g)(m) = f(g(m))$$

Να δειχθεί ότι η τριάδα $(\mathsf{End}_{\mathbb{Z}}(M), +, \circ)$ είναι ένας δακτύλιος. Να δοθούν παραδείγματα αβελιανών ομάδων M έτσι ώστε ο δακτύλιος $\mathsf{End}_{\mathbb{Z}}(M)$ να είναι (α) μεταθετικός, και (β) μη μεταθετικός.

Άσκηση 7.6.44. *Έστω R ένας δακτύλιος, όχι απαραίτητα με μονάδα. Να δείξετε ότι το σύνολο*

$$\mathbb{Z} \times R = \{(n, r) \mid n \in \mathbb{Z} \text{ και } r \in R\}$$

εφοδιασμένο με τις πράξεις:

$$(n, r) + (m, s) = (n + m, r + s) \qquad \text{και} \qquad (n, r) \cdot (m, s) = (nm, ns + rm + rs)$$

είναι ένας δακτύλιος με μονάδα.

Άσκηση 7.6.45. *Να δειχθεί ότι το σύνολο $\mathbb{Z}_3 \times \mathbb{Z}_3$ εφοδιασμένο με τις ακόλουθες πράξεις πρόσθεσης και πολλαπλασιασμού, $\forall x, y, z, w \in \mathbb{Z}_3$:*

$$(x, y) + (z, w) = (x + y, z + w) \qquad \text{και} \qquad (x, y) \cdot (z, w) = (xz - yw, xw + yz)$$

είναι ένα σώμα και να βρεθεί η χαρακτηριστική του.

Άσκηση 7.6.46. *Θεωρούμε τον δακτύλιο πινάκων $\mathsf{M}_2(\mathbb{Z}_2)$.*

1. *Να βρεθεί το πλήθος των στοιχείων του δακτυλίου $\mathsf{M}_2(\mathbb{Z}_2)$.*
2. *Να βρεθούν όλα τα αντιστρέψιμα στοιχεία του δακτυλίου $\mathsf{M}_2(\mathbb{Z}_2)$.*
3. *Να βρεθεί η χαρακτηριστική του δακτυλίου $\mathsf{M}_2(\mathbb{Z}_2)$.*

Άσκηση 7.6.47. *Έστω ότι R είναι ένας δακτύλιος για τον οποίο ισχύει ότι $\forall a \in R$: $a^2 = 0 \implies a = 0$. Να δειχθεί ότι τα ταυτοδύναμα στοιχεία του R ανήκουν στο κέντρο του R.*

Άσκηση 7.6.48. *Να προσδιοριστούν τα ταυτοδύναμα στοιχεία του δακτυλίου $\mathbb{Z}_n$, $n \geq 2$.*

Άσκηση 7.6.49. *Έστω ότι x, y είναι στοιχεία σε έναν δακτύλιο R. Να δειχθεί ότι:*

$$1 - xy \in \mathsf{U}(R) \qquad \Longleftrightarrow \qquad 1 - yx \in \mathsf{U}(R)$$

όπου $\mathsf{U}(R)$ είναι η ομάδα των αντιστρέψιμων στοιχείων του R.

Άσκηση 7.6.50. *Έστω ότι R είναι ένας δακτύλιος και θεωρούμε τον δακτύλιο $\mathsf{M}_n(R)$. Να δειχθεί ότι το σύνολο S όλων των διαγώνιων πινάκων με στοιχεία από τον δακτύλιο R είναι ένας υποδακτύλιος του $\mathsf{M}_n(R)$ και να προσδιοριστεί η ομάδα $\mathsf{U}(S)$ των αντιστρέψιμων στοιχείων του.*

Άσκηση 7.6.51. *Έστω R ένας πεπερασμένος δακτύλιος με μονάδα. Να δείξετε ότι ο R είναι δακτύλιος διαίρεσης αν και μόνο αν ο R δεν έχει διαιρέτες του μηδενός.*

Άσκηση 7.6.52. *Έστω R ένας δακτύλιος.*

1. *Αν $a, b \in R$, όπου $b \neq 0$, και ισχύει $aba = 0$, να δειχθεί ότι το στοιχείο a είναι αριστερός ή δεξιός διαιρέτης του μηδενός.*
2. *Υποθέτουμε ότι για κάθε στοιχείο $a \in R$, υπάρχει στοιχείο $b \in R$ έτσι ώστε: $aba = a$. Να δειχθεί ότι κάθε μη αντιστρέψιμο στοιχείο του R είναι διαιρέτης του μηδενός.*
3. *Να εξεταστεί αν το σύνολο των διαιρετών του μηδενός ενός δακτυλίου είναι κλειστό στην πρόσθεση, και στον πολλαπλασιασμό από αριστερά ή δεξιά με στοιχεία του δακτυλίου.*

Άσκηση 7.6.53. *Έστω R ένας δακτύλιος με μονάδα. Αν ένα στοιχείο $a \in R$ έχει περισσότερα από ένα δεξιά αντίστροφα στοιχεία (δηλαδή στοιχεία $a' \in R$ έτσι ώστε $aa' = 1_R$) τότε να δείξετε ότι το a έχει άπειρα δεξιά αντίστροφα στοιχεία.*[7]

Άσκηση 7.6.54. *Να εξεταστεί αν υπάρχει ακέραια περιοχή με ακριβώς 10 στοιχεία.*

Άσκηση 7.6.55. *Αν σε έναν δακτύλιο R ισχύει ότι:*

$$\forall r \in R: \quad r^2 = r \in \mathsf{Z}(R)$$

να δειχθεί ότι ο δακτύλιος R είναι μεταθετικός.

Άσκηση 7.6.56. *Έστω*

$$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \mid a,b,c,d \in \mathbb{Q}\right\}$$

και $\alpha = \sqrt{2} + \sqrt{3}$. Να δειχθεί ότι $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\alpha)$, όπου $\mathbb{Q}[\alpha]$ είναι ο μικρότερος υποδακτύλιος του $\mathbb{R}$ ο οποίος περιέχει τα στοιχεία $\sqrt{2}$ και $\sqrt{3}$.

Άσκηση 7.6.57. *Έστω R μια ακέραια περιοχή και υποθέτουμε ότι υπάρχει ένα στοιχείο $r \in R$, $r \neq 0$, και θετικός ακέραιος $n \in \mathbb{N}$ έτσι ώστε: $nr = 0_R$. Να δειχθεί ότι: $\mathsf{char}(R) = p$ για κάποιον πρώτο διαιρέτη p του n.*

Άσκηση 7.6.58. *Έστω R ένας δακτύλιος με περισσότερα από ένα στοιχεία. Υποθέτουμε ότι η εξίσωση $ax = b$ έχει λύση για κάθε $0 \neq a \in R$ και για κάθε $b \in R$. Να δείξετε ότι ο δακτύλιος R είναι δακτύλιος διαίρεσης.*

Άσκηση 7.6.59. *Να δοθεί παράδειγμα ακέραιας περιοχής με άπειρο πλήθος στοιχείων και πεπερασμένη χαρακτηριστική.*

Άσκηση 7.6.60. *Στον δακτύλιο $\mathbb{H}$ των τετρανίων του Hamilton, βλέπε το Παράδειγμα 7.2.15, θεωρούμε στοιχεία:*

$$X = a_0 I_2 + a_1 I + a_2 J + a_3 K \quad \text{και} \quad Y = b_0 I_2 + b_1 I + b_2 J + b_3 K, \quad a_i, b_i \in \mathbb{R},\ 0 \leq i \leq 3$$

και ορίζουμε απεικόνιση

$$\mathsf{N}: \mathbb{H} \longrightarrow \mathbb{H}, \quad \mathsf{N}(X) = X \cdot \overline{X}$$

όπου $\overline{X} = a_0 I_2 - a_1 I - a_2 J - a_3 K$.

1. *Να δειχθεί ότι:*

$$\overline{X+Y} = \overline{X} + \overline{Y}, \quad \overline{\overline{X}} = X, \quad \overline{X \cdot Y} = \overline{Y} \cdot \overline{X}, \quad \text{και} \quad \overline{X} = Q \iff a_i = 0,\ 1 \leq i \leq 3$$

2. *Να δειχθεί ότι: $\mathsf{N}(X) = (a_0^2 + a_1^2 + a_2^2 + a_3^2) I_2$, και:*

$$\mathsf{N}(X \cdot Y) = \mathsf{N}(X) \cdot \mathsf{N}(Y)$$

3. *Να δειχθεί ότι ο πίνακας X ικανοποιεί την εξίσωση:*

$$X^2 - \mathsf{T}(X)X + \mathsf{N}(X) = 0$$

όπου $\mathsf{T}(X) = 2a_0$.

[7] Το αποτέλεσμα αυτό οφείλεται στον:
Irving Kaplansky (22 Μαρτίου 1917 - 25 Ιουνίου 2006) [https://en.wikipedia.org/wiki/Irving_Kaplansky]: Σημαντικός Καναδός μαθηματικός ο οποίος έζησε και εργάστηκε στις ΗΠΑ, με σημαντική συμβολή σε πολλούς ερευνητικούς κλάδους και ιδιαίτερα στην Άλγεβρα.

Άσκηση 7.6.61. *Στον δακτύλιο $\mathbb{H}$ των τετρανίων του Hamilton, βλέπε το Παράδειγμα 7.2.15, θεωρούμε το υποσύνολο $\mathbb{H}_0$ όλων των πινάκων της μορφής $X = a_0 I_2 + a_1 I + a_2 J + a_3 K$, όπου $a_i \in \mathbb{Q}$, $0 \leq i \leq 3$. Να δειχθεί ότι το υποσύνολο $\mathbb{H}_0$ είναι ένας υποδακτύλιος του $\mathbb{H}$ ο οποίος είναι δακτύλιος διαίρεσης.*

Άσκηση 7.6.62. *Στον δακτύλιο $\mathbb{H}$ των τετρανίων του Hamilton, βλέπε το Παράδειγμα 7.2.15, θεωρούμε το υποσύνολο*

$$R = \left\{ X = a_0 I_2 + a_1 I + a_2 J + a_3 K \in \mathbb{H} \mid \text{είτε } a_i \in \mathbb{Z} \text{ είτε } a_i = \frac{m_i}{2} \text{ όπου οι } m_i \text{ είναι περιττοί ακέραιοι} \right\}$$

1. *Να δειχθεί ότι ο R είναι ένας υποδακτύλιος του $\mathbb{H}$.*
2. *Να δειχθεί ότι οι πίνακες $\mathsf{T}(X), \mathsf{N}(X)$ είναι ακέραια βαθμωτά πολλαπλάσια του μοναδιαίου πίνακα I_2.*
3. *Είναι ο R δακτύλιος διαίρεσης;*

Κεφάλαιο 8

Ιδεώδη, Δακτύλιοι Πηλίκα και τα Θεωρήματα Ισομορφισμών

Στο παρόν Κεφάλαιο θα μελετήσουμε την σημαντική έννοια του (αριστερού, δεξιού, ή αμφίπλευρου) ιδεώδους ενός δακτυλίου, έννοια η οποία θα μας επιτρέψει να κατασκευάσουμε δακτυλίους πηλίκα κατ' αναλογία με την κατασκευή των ομάδων πηλίκων μιας ομάδας ως προς τις κανονικές υποομάδες της. Η δομή των ιδεωδών ενός δακτυλίου, (αριστερών, δεξιών, αμφίπλευρων) διαδραματίζει σημαντικό ρόλο στην δομή του δακτυλίου. Θα μελετήσουμε επίσης την έννοια του ομομορφισμού δακτυλίων, έννοια η οποία θα μας επιτρέψει την σύγκριση και σε μερικές περιπτώσεις την ταύτιση δακτυλίων, όταν αυτοί έχουν παρόμοιες ή ταυτόσημες αλγεβρικές ιδιότητες. Σ' αυτό το πλαίσιο θα αποδείξουμε, όπως στη Θεωρία Ομάδων, τα ανάλογα Θεωρήματα Ισομορφισμών, και θα αναλύσουμε κάποιες από τις συνέπειές τους.

8.1 Ιδεώδη

Είδαμε στο προηγούμενο Κεφάλαιο την έννοια του υποδακτυλίου, έννοια η οποία χρησίμευσε κυρίως για την αναγνώριση και κατασκευή νέων δακτυλίων ως υποσυνόλων ήδη γνωστών μας δακτυλίων. Υπάρχει αναλογία στην έννοια του υποδακτυλίου με την έννοια της υποομάδας μιας ομάδας, αν και η έννοια της υποομάδας είναι πολύ πιο χρήσιμη στη Θεωρία Ομάδων, από ότι είναι η έννοια του υποδακτυλίου στη Θεωρία Δακτυλίων. Από την άλλη πλευρά, είδαμε ότι η έννοια της κανονικής υποομάδας αποδείχθηκε πολύ σημαντική, καθώς μας επέτρεψε την κατασκευή των ομάδων πηλίκων και γενικότερα η θεωρία τους είναι περισσότερο πλούσια. Η αντίστοιχη έννοια στη Θεωρία Δακτυλίων είναι η έννοια του ιδεώδους, και γενικότερα οι δεξιές ή αριστερές εκδοχές της.

Από τώρα και στο εξής, σταθεροποιούμε έναν μη μηδενικό δακτύλιο $R = (R, +, \cdot)$.

Ορισμός 8.1.1. *Μια υποομάδα $I \subseteq R$ της προσθετικής ομάδας $(R, +)$ καλείται:*

1. **αριστερό ιδεώδες** *του R, αν, $\forall r \in R$, $\forall x \in I$: $r \cdot x \in I$.*
2. **δεξιό ιδεώδες** *του R, αν, $\forall r \in R$, $\forall x \in I$: $x \cdot r \in I$.*
3. **(αμφίπλευρο) ιδεώδες** *ή (διπλό ιδεώδες) του R, αν, $\forall r \in R$, $\forall x \in I$: $r \cdot x \in I$ και $x \cdot r \in I$.*

Έτσι ένα μη κενό υποσύνολο $I \subseteq R$ είναι (α) αριστερό, (β) δεξιό, (γ) αμφίπλευρο ιδεώδες, αν $\forall r \in R$ και $\forall x, y \in I$:

1. $x - y \in I$.
2. (α) $r \cdot x \in I$, (β) $x \cdot r \in I$, (γ) $r \cdot x \in I$ και $x \cdot r \in I$.

Προφανώς, αν ο δακτύλιος R είναι μεταθετικός, τότε κάθε δεξιό ή αριστερό ιδεώδες είναι αμφίπλευρο ιδεώδες και έτσι δεν χρειάζεται να κάνουμε διάκριση μεταξύ αριστερών και δεξιών ιδεωδών. Χάριν απλότητας, από τώρα και στο εξής, ιδεώδες θα σημαίνει αμφίπλευρο ή διπλό ιδεώδες.

Παρατήρηση 8.1.2. Όπως προκύπτει από τον ορισμό, ένα υποσύνολο είναι (αμφίπλευρο) ιδεώδες αν και μόνο αν είναι αριστερό και δεξιό ιδεώδες. Επίσης, αν και υποδακτύλιοι και ιδεώδη είναι υποομάδες της προσθετικής ομάδας του δακτυλίου και επίσης είναι κλειστοί στον πολλαπλασιασμό του δακτυλίου, και κάθε ιδεώδες είναι υποδακτύλιος χωρίς μονάδα, υπάρχουν δύο σημαντικές διαφορές οι οποίες διαφοροποιούν κατά πολύ τη θεωρία τους. Πρώτον, ένα ιδεώδες δεν περιέχει απαραίτητα τη μονάδα του δακτυλίου. Όπως θα δούμε, αν αυτό συμβαίνει τότε το ιδεώδες συμπίπτει με τον δακτύλιο. Δεύτερον, ένα ιδεώδες είναι κλειστό στον πολλαπλασιασμό των στοιχείων του από τα δεξιά και τα αριστερά με στοιχεία του δακτυλίου, και όχι μόνο με στοιχεία του ιδεώδους. ▲

Κάθε δακτύλιος έχει πάντα δύο ιδεώδη: ο ίδιος ο δακτύλιος R είναι ιδεώδες, και το μονοσύνολο $\{0\}$ είναι ιδεώδες. Ένα ιδεώδες I του R καλείται **γνήσιο ιδεώδες** αν $I \neq R$. Το ιδεώδες $\{0\}$ καλείται το **μηδενικό ιδεώδες**. Υπάρχουν δακτύλιοι οι οποίοι έχουν μόνο δύο ιδέωδη: ο δακτύλιος R καλείται **απλός δακτύλιος**, αν τα μόνα ιδεώδη του είναι ο ίδιος ο δακτύλιος R και το μηδενικό ιδεώδες $\{0\}$. Από την άλλη πλευρά, ένας μη μεταθετικός δακτύλιος R έχει σχεδόν πάντα, ακόμα και αν είναι απλός, πολύ περισσότερα αριστερά ή δεξιά ιδεώδη. Τα ιδεώδη R και $\{0\}$ καλούνται τα **τετριμμένα ιδεώδη** του R. Κάθε άλλο ιδεώδες του R καλείται *μη τετριμμένο*.

Πριν περάσουμε να δούμε παραδείγματα (αριστερών ή δεξιών) ιδεωδών, θα δούμε πρώτα κάποιες στοιχειώδεις ιδιότητες.

Πρόταση 8.1.3. *Έστω I ένα (αριστερό ή δεξιό) ιδεώδες του δακτυλίου R.*

1. *$I = R \iff 1_R \in I \iff$ το I περιέχει ένα αντιστρέψιμο στοιχείο του R.*
2. *Αν ο δακτύλιος R είναι δακτύλιος διαίρεσης, τότε $I = R$ ή $I = \{0\}$.*
3. *Κάθε δακτύλιος διαίρεσης, ιδιαίτερα κάθε σώμα, είναι απλός δακτύλιος.*

Απόδειξη. 1. Αν $I = R$, τότε προφανώς $1_R \in I$ και αν $1_R \in I$, τότε το I περιέχει ένα αντιστρέψιμο στοιχείο του R. Έστω ότι το I περιέχει ένα αντιστρέψιμο στοιχείο a του R, και ας υποθέσουμε ότι το I είναι αριστερό ιδεώδες του R. Επειδή το a είναι αντιστρέψιμο, υπάρχει το αντίστροφό του $a^{-1} \in R$. Τότε επειδή το I είναι αριστερό ιδεώδες του R και $a \in I$, θα έχουμε $a^{-1} \cdot a = 1_R \in I$. Τότε για κάθε στοιχείο $r \in R$, θα έχουμε $r = r \cdot 1_R \in I$. Άρα το I περιέχει κάθε στοιχείο του R και επομένως $I = R$.

Αν το I είναι δεξιό ή αμφίπλευρο ιδεώδες, εργαζόμαστε ακριβώς ανάλογα.

2. Επειδή κάθε μη μηδενικό στοιχείο σε έναν δακτύλιο διαίρεσης είναι αντιστρέψιμο, θα έχουμε είτε $I = \{0\}$ ή το I περιέχει ένα αντιστρέψιμο στοιχείο. Στην δεύτερη περίπτωση από το 1. θα έχουμε $I = R$.
3. Προκύπτει άμεσα από το 2.. ■

Έτσι από την πλευρά της θεωρίας ιδεωδών οι περισσότερο απλοί στη δομή τους δακτύλιοι είναι οι δακτύλιοι διαίρεσης στην όχι απαραίτητα μεταθετική περίπτωση, και τα σωματα στην μεταθετική περίπτωση. Όπως θα δούμε αργότερα, αντίστροφα, κάθε μεταθετικός απλός δακτύλιος είναι σώμα, αλλά υπάρχουν απλοί δακτύλιοι οι οποίοι δεν είναι δακτύλιοι διαίρεσης.

Από τις παραπάνω παρατηρήσεις έπεται ότι τα ιδέωδη των δακτυλίων $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ είναι τα τετριμμένα. Αυτό δεν συμβαίνει για την περίπτωση του δακτυλίου των ακεραίων όπως δείχνει η ακόλουθη Πρόταση η οποία περιγράφει τα ιδεώδη του $\mathbb{Z}$.

Πρόταση 8.1.4. *Τα ιδεώδη του δακτυλίου $\mathbb{Z}$ των ακεραίων, συμπίπτουν με τις υποομάδες της προσθετικής ομάδας $(\mathbb{Z}, +)$ και άρα είναι τα εξης:*

$$n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}, \quad n = 0, 1, 2, 3, \cdots$$

Απόδειξη. Γνωρίζουμε ότι η προσθετική ομάδα $(\mathbb{Z},+)$ είναι κυκλική, και τα υποσύνολα $\langle n\rangle = n\mathbb{Z}$, $n \geq 0$, είναι υποομάδες της προσθετικής ομάδας $(\mathbb{Z},+)$, και κάθε υποομάδα της $(\mathbb{Z},+)$ είναι αυτής της μορφής, βλέπε το Παράδειγμα 4.1.6. Αν $x = nk \in n\mathbb{Z}$, τότε λόγω μεταθετικότητας, για κάθε ακέραιο $z \in \mathbb{Z}$ θα έχουμε $znk = nzk \in n\mathbb{Z}$. Άρα οι υποομάδες $n\mathbb{Z}$ είναι ιδεώδη του $\mathbb{Z}$. Αντίστροφα, αν I είναι ένα ιδεώδες του $\mathbb{Z}$, τότε το υποσύνολο I είναι εξ ορισμού υποομάδα της προσθετικής ομάδας $(\mathbb{Z},+)$, και άρα θα είναι της μορφής $n\mathbb{Z}$, για κάποιο $n \geq 0$. ■

Παρόμοια μπορούν να περιγραφούν τα ιδεώδη του δακτυλίου των κλάσεων υπολοίπων mod n:

Πρόταση 8.1.5. *Τα ιδεώδη του δακτυλίου $\mathbb{Z}_n$ των ακεραίων* mod n, $n \geq 1$, *συμπίπτουν με τις υποομάδες της προσθετικής ομάδας $(\mathbb{Z}_n,+)$ και άρα είναι τα εξης:*

$$d\mathbb{Z}_n = \{d[x]_n \in \mathbb{Z}_n \mid d \mid n\}$$

Απόδειξη. Γνωρίζουμε ότι η προσθετική ομάδα $(\mathbb{Z}_n,+)$ είναι κυκλική, και τα υποσύνολα $\langle d[1]_n\rangle = \langle [d]_n\rangle = d\mathbb{Z}_n$, $d \mid n$, είναι υποομάδες της προσθετικής ομάδας $(\mathbb{Z}_n,+)$, και κάθε υποομάδα της $(\mathbb{Z}_n,+)$ είναι αυτής της μορφής, βλέπε το Θεώρημα 4.1.10. Αν $d[x]_n = [dx]_n \in d\mathbb{Z}_n$, τότε λόγω μεταθετικότητας, για κάθε κλάση ισοτιμίας $[z]_n \in \mathbb{Z}_n$ θα έχουμε $[z]_n[dx]_n = [zxd]_n = d[zx]_n \in d\mathbb{Z}_n$. Άρα οι υποομάδες $d\mathbb{Z}_n$ είναι ιδεώδη του $\mathbb{Z}_n$. Αντίστροφα, αν I είναι ένα ιδεώδες του $\mathbb{Z}_n$, τότε το υποσύνολο I είναι εξ ορισμού υποομάδα της προσθετικής ομάδας $(\mathbb{Z}_n,+)$, και άρα θα είναι της μορφής $d\mathbb{Z}_n$, για κάποιο $d \mid n$. ■

Παράδειγμα 8.1.6. Θεωρούμε τον δακτύλιο $R = \mathsf{M}_2(\mathbb{K})$ των 2×2 πινάκων, υπεράνω του $\mathbb{K} \in \{\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}\}$, και έστω $S = \mathsf{AT}_2(\mathbb{K}) \subseteq \mathsf{M}_2(\mathbb{K})$ ο υποδακτύλιος των 2×2 άνω τριγωνικών πινάκων. Επίσης θεωρούμε το υποσύνολο

$$I = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \in \mathsf{M}_2(\mathbb{K}) \mid x \in \mathbb{K} \right\}$$

το οποίο είναι υποδακτύλιος χωρίς μονάδα των S και R. Τότε προφανως $I \subseteq \mathsf{AT}_2(\mathbb{K}) \subseteq \mathsf{M}_2(\mathbb{K})$.

1. Το I δεν είναι αριστερό ή δεξιό ιδεώδες του $\mathsf{M}_2(\mathbb{K})$.
   Πράγματι: $\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right) \in \mathsf{M}_2(\mathbb{K})$ και $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) \in I$, αλλά: $\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&0\\1&0\end{smallmatrix}\right) \notin I$ και $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}1&1\\1&1\end{smallmatrix}\right) = \left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right) \notin I$.
2. Το I είναι αριστερό ιδεώδες του $\mathsf{AT}_2(\mathbb{K})$.
   Πράγματι: για κάθε $\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right) \in \mathsf{AT}_2(\mathbb{K})$ και κάθε $\left(\begin{smallmatrix}x&0\\0&0\end{smallmatrix}\right) \in I$, έχουμε: $\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}x&0\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}ax&0\\0&0\end{smallmatrix}\right) \in I$.
3. Το I είναι δεν είναι δεξιό ιδεώδες του $\mathsf{AT}_2(\mathbb{K})$.
   Πράγματι: για κάθε $\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right) \in \mathsf{AT}_2(\mathbb{K})$ και κάθε $\left(\begin{smallmatrix}x&0\\0&0\end{smallmatrix}\right) \in I$, έχουμε: $\left(\begin{smallmatrix}x&0\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}a&b\\0&d\end{smallmatrix}\right) = \left(\begin{smallmatrix}xa&xb\\0&0\end{smallmatrix}\right) \notin I$. √

8.1.1 Ιδεώδη Παραγόμενα από Υποσύνολα

Οι προηγούμενες δύο προτάσεις δείχνουν ότι στους δακτυλίους $\mathbb{Z}$ και $\mathbb{Z}_n$, $n \geq 0$, κάθε ιδεώδες αποτελείται από τα πολλαπλάσια ενός στοιχείου του δακτυλίου με όλα τα στοιχεία του δακτυλίου. Αργότερα θα δούμε και άλλους δακτυλίους με αυτή την ιδιότητα. Οι Προτάσεις 8.1.4 και 8.1.5 μας οδηγούν φυσιολογικά στην θεώρηση ιδεωδών που «παράγονται» από ένα στοιχείο του δακτυλίου.

Έστω $r \in R$ ένα στοιχείο του δακτυλίου R, και θεωρούμε τα εξής υποσύνολα του R:

$$Rr = \{x\cdot r \in R \mid x \in R\} \qquad \text{και} \qquad rR = \{r\cdot y \in R \mid y \in R\}$$

• Ισχυρισμός: *Το υποσύνολο Rr είναι το μικρότερο αριστερό ιδεώδες του R το οποίο περιέχει το r, και το υποσύνολο rR είναι το μικρότερο δεξιό ιδεώδες του R το οποίο περιέχει το r.*

Πράγματι, προφανώς το υποσύνολο Rr δεν είναι κενό διότι $r = 1_R\cdot r \in Rr$. Έστω $x\cdot r, y\cdot r \in Rr$, όπου $x, y \in R$, και $z \in R$. Τότε θα έχουμε $x\cdot r - y\cdot r = (x-y)\cdot r \in Rr$, και $z\cdot(x\cdot r) = (z\cdot x)\cdot r \in Rr$. Έτσι το υποσύνολο Rr είναι ένα αριστερό ιδεώδες του R το οποίο περιέχει το r. Αν I είναι ένα αριστερό ιδεώδες του R το οποίο

περιέχει το r, τότε για κάθε στοιχείο $x\cdot r\in Rr$ θα έχουμε και $x\cdot r\in I$ διότι $r\in I$ και το I είναι αριστερό ιδεώδες. Επομένως $Rr\subseteq I$ και το Rr είναι το μικρότερο αριστερό ιδεώδες του R το οποίο περιέχει το r. Παρόμοια το rR είναι το μικρότερο δεξιό ιδεώδες του R το οποίο περιέχει το r.

Με βάση τις παραπάνω παρατηρήσεις είναι εύλογο να αναρωτηθούμε, ποιο είναι το μικρότερο ιδεώδες το οποίο περιέχει το στοιχείο $r\in R$. Η προφανής επιλογή να θεωρήσουμε κατ' αναλογία το σύνολο $\{x\cdot r\cdot y\in R\mid x,y\in R\}$ δεν είναι σωστή αν ο δακτύλιος δεν είναι μεταθετικός, διότι το παραπάνω σύνολο δεν είναι απαραίτητα κλειστό στην πρόσθεση του R: γενικά δεν μπορούμε να γνωρίζουμε αν το στοιχείο $x_1\cdot r\cdot y_1+x_2\cdot r\cdot y_2$ ανήκει στο υποσύνολο. Έτσι οδηγούμαστε φυσιολογικά στην θεώρηση του ακόλουθου υποσυνόλου:

$$RrR=\left\{x_1\cdot r\cdot y_1+x_2\cdot r\cdot y_2+\cdots+x_n\cdot r\cdot y_n\ \in\ R\ \middle|\ x_i,y_i\in R,\ n\in\mathbb{N}\right\}$$

• Ισχυρισμός: *Το υποσύνολο RrR είναι το μικρότερο (αμφίπλευρο) ιδεώδες του R το οποίο περιέχει το r.*

Πράγματι, προφανώς το υποσύνολο RrR δεν είναι κενό διότι $r=1_R\cdot r\cdot 1_R\in RrR$. Έστω $\sum_{k=1}^{n}x_k\cdot r\cdot y_k$, $\sum_{k=1}^{m}z_k\cdot r\cdot w_k\in R$, όπου $x_k,y_k,z_l,w_l\in R$, $1\le k\le n$, $1\le l\le m$, και $z\in R$. Τότε από την κατασκευή του υποσυνόλου RrR, θα έχουμε $\sum_{k=1}^{n}x_k\cdot r\cdot y_k-\sum_{k=1}^{m}z_k\cdot r\cdot w_k\in RrR$, και $z\cdot(\sum_{k=1}^{n}x_k\cdot r\cdot y_k)=\sum_{k=1}^{n}(z\cdot x_k)\cdot r\cdot y_k\in RrR$ και $(\sum_{k=1}^{n}x_k\cdot r\cdot y_k)\cdot z=\sum_{k=1}^{n}x_k\cdot r\cdot(y_k\cdot z)\in RrR$. Έτσι το υποσύνολο RrR είναι ένα αμφίπλευρο ιδεώδες του R το οποίο περιέχει το r. Έστω τώρα I ένα αμφίπλευρο ιδεώδες του R το οποίο περιέχει το r, και $\sum_{k=1}^{n}x_k\cdot r\cdot y_k\in RrR$ ένα στοιχείο του RrR. Επειδή το I περιέχει το r και είναι κλειστό στον πολλαπλασιασμό από αριστερά και δεξιά με στοιχεία του R, θα έχουμε ότι $x_k\cdot r\cdot y_k\in I$, $1\le k\le n$. Επειδή το I είναι και κλειστό στο άθροισμα στοιχείων του, θα έχουμε $\sum_{k=1}^{n}x_k\cdot r\cdot y_k\in I$. Έτσι $RrR\subseteq I$ και το RrR είναι το μικρότερο αμφίπλευρο ιδεώδες του R το οποίο περιέχει το r.

Παρατήρηση 8.1.7. Αν ο δακτύλιος R είναι μεταθετικός, τότε για κάθε $r\in R$: $Rr=RrR=rR$.

Επίσης συχνά θα χρησιμοποιούμε και τους συμβολισμούς:

$$(r)_{\mathfrak{r}}=rR,\qquad {}_{\mathfrak{l}}(r)=Rr,\qquad (r)=RrR\quad\blacktriangle$$

Ορισμός 8.1.8. *Αν r είναι ένα στοιχείο του δακτυλίου R, τότε:*

1. *το Rr καλείται το* **αριστερό ιδεώδες του R το οποίο παράγεται από το r.**
2. *το rR καλείται το* **δεξιό ιδεώδες του R το οποίο παράγεται από το r.**
3. *το RrR καλείται το (αμφίπλευρο)* **ιδεώδες του R το οποίο παράγεται από το r.**

Οι παραπάνω έννοιες περιγράφουν τα αριστερά, δεξιά ή αμφίπλευρα ιδεώδη τα οποία παράγονται από ένα στοιχείο του δακτυλίου. Για να περιγράψουμε τα αριστερά, δεξιά ή αμφίπλευρα ιδεώδη τα οποία παράγονται από ένα υποσύνολο στοιχείων του δακτυλίου χρειαζόμαστε κάποια προεργασία.

Λήμμα 8.1.9. *Η τομή μιας οικογένειας (αριστερών, αντίστοιχα δεξιών) ιδεωδών του δακτυλίου R είναι (αριστερό, αντίστοιχα δεξιό) ιδεώδες του R. Ιδιαίτερα, αν $X\subseteq R$ είναι ένα τυχόν υποσύνολο, τότε η τομή όλων των (αριστερών, αντίστοιχα δεξιών) ιδεωδών του δακτυλίου R τα οποία περιέχουν το X είναι ένα (αριστερό, αντίστοιχα δεξιό) ιδεώδες του R, και μάλιστα είναι το μικρότερο (αριστερό, αντίστοιχα δεξιό) ιδεώδες του R το οποίο περιέχει το X.*

Απόδειξη. Θα δώσουμε την απόδειξη για αμφίπλευρα ιδεώδη. Η απόδειξη για αριστερά ή δεξιά ιδεώδη είναι ακριβώς ανάλογη. Έστω $\mathscr{I}=\{I_k\}_{k\in K}$ μια οικογένεια ιδεωδών του R. Επειδή η τομή υποομάδων μιας ομάδας είναι υποομάδα της ομάδας, έπεται ότι η τομή $I=\cap_{k\in K}I_k$ της οικογένειας $\mathscr{I}$ είναι μια υποομάδα της προσθετικής ομάδας $(R,+)$. Έστω $x\in I$ και $r\in R$. Τότε $x\in I_k$, $\forall k\in K$, και επομένως επειδή το I_k είναι ιδεώδες, έχουμε $x\cdot r,r\cdot x\in I_k$, $\forall k\in K$. Άρα $x\cdot r,r\cdot x\in\cap_{k\in K}I_k=I$ και γι' αυτό το I είναι ένα ιδεώδες του R.

Επιλέγοντας ως $\mathscr{I}$ την οικογένεια όλων των ιδεωδών του R τα οποία περιέχουν ένα υποσύνολο $X\subseteq R$, η οποία δεν είναι κενή διότι περιέχει το ιδεώδες R, προφανώς θα έχουμε ότι η τομή $\cap_{I\in\mathscr{I}}I$ είναι ένα ιδεώδες του R το οποίο προφανώς περιέχει το X. Αν J είναι ένα ιδεώδες του R το οποίο περιέχει το X, τότε $J\in\mathscr{I}$ και γι' αυτό $\cap_{I\in\mathscr{I}}I\subseteq J$. Επομένως η τομή $\cap_{I\in\mathscr{I}}I$ είναι το μικρότερο ιδεώδες του R το οποίο περιέχει το X. ■

Παράδειγμα 8.1.10. Στον δακτύλιο $\mathbb{Z}$ των ακεραίων, θεωρούμε τα ιδεώδη $n\mathbb{Z}$ και $m\mathbb{Z}$, όπου $n, m \geq 1$. Τότε

$$n\mathbb{Z} \bigcap m\mathbb{Z} = [n,m]\mathbb{Z}$$

Πράγματι, έστω $x \in n\mathbb{Z} \cap m\mathbb{Z}$, και τότε $x = nk = ml$, για κάποιους ακέραιους k, l. Έτσι $n \mid x$ και $m \mid x$, και τότε από τη Στοιχειώδη Θεωρία Αριθμών, γνωρίζουμε ότι $[n,m] \mid x$, δηλαδή $x = [n,m]r$, για κάποιον ακέραιο r. Έτσι $x \in [n,m]\mathbb{Z}$ και άρα $n\mathbb{Z} \cap m\mathbb{Z} \subseteq [n,m]\mathbb{Z}$. Αντίστροφα, έστω $x \in [n,m]\mathbb{Z}$, και άρα $x = [n,m]k$ για κάποιον ακέραιο k. Προφανως θα έχουμε $[n,m] = rn$ και $[n,m] = sm$, και τότε $x = nrk = msk$, δηλαδή $x \in n\mathbb{Z} \cap m\mathbb{Z}$. Έτσι $[n,m]\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z}$, και επομένως έχουμε τη ζητούμενη ισότητα: $n\mathbb{Z} \bigcap m\mathbb{Z} = [n,m]\mathbb{Z}$.

Αν οι αριθμοί n, m είναι πρώτοι μεταξύ τους, δηλαδή $(n,m) = 1$, τότε είναι $[n,m] = nm$, και επομένως ιδιαίτερα θα έχουμε:

$$(n,m) = 1 \quad \Longrightarrow \quad n\mathbb{Z} \bigcap m\mathbb{Z} = nm\mathbb{Z}$$

Η τελευταία συνεπαγωγή δεν είναι τυχαία. Θα δούμε μια γενίκευσή της αργότερα όταν θα αναλύσουμε την έννοια του γινομένου ιδεωδών. $\surd$

Η τομή όλων των αριστερών, αντίστοιχα δεξιών, αντίστοιχα (αμφίπλευρων) ιδεωδών του δακτυλίου R τα οποία περιέχουν το X καλείται το (**αριστερό**, αντίστοιχα **δεξιό**, αντίστοιχα (αμφίπλευρο) **ιδεώδες του** R **το οποίο παράγεται από το** X, και συμβολίζεται με ${}_{\mathfrak{l}}(X)$, αντίστοιχα $(X)_{\mathfrak{r}}$, αντίστοιχα (X). Έτσι, αν $X = \{x_1, x_2, \cdots, x_n\}$, θα γράφουμε αντίστοιχα:

$${}_{\mathfrak{l}}(x_1, x_2, \cdots, x_n), \qquad (x_1, x_2, \cdots, x_n)_{\mathfrak{r}}, \qquad (x_1, x_2, \cdots, x_n)$$

Ορισμός 8.1.11. *Ένα αριστερό, αντίστοιχα δεξιό, αντίστοιχα (αμφίπλευρο) ιδεώδες I του R καλείται* **πεπερασμένα παραγόμενο** *αν υπάρχει πεπερασμένο υποσύνολο $\{x_1, x_2, \cdots, x_n\} \subseteq I$, έτσι ώστε να ισχύει αντίστοιχα:*

$$I = {}_{\mathfrak{l}}(x_1, x_2, \cdots, x_n), \qquad I = (x_1, x_2, \cdots, x_n)_{\mathfrak{r}}, \qquad I = (x_1, x_2, \cdots, x_n)$$

Το αριστερό, αντίστοιχα δεξιό, αντίστοιχα (αμφίπλευρο) ιδεώδες I του R καλείται **κύριο** *αν υπάρχει $x \in I$, έτσι ώστε να ισχύει αντίστοιχα:*

$$I = {}_{\mathfrak{l}}(x), \qquad I = (x)_{\mathfrak{r}}, \qquad I = (x)$$

Με βάση την ανάλυση που προηγήθηκε, γνωρίζουμε τη μορφή των κύριων, αριστερών, δεξιών ή αμφίπλευρων, ιδεωδών R. Ποιά είναι όμως η μορφή των ιδεωδών ${}_{\mathfrak{l}}(x_1, x_2, \cdots, x_n)$, $(x_1, x_2, \cdots, x_n)_{\mathfrak{r}}$, $(x_1, x_2, \cdots, x_n)$;

Πρόταση 8.1.12. *Άν $X = \{x_1, x_2, \cdots, x_n\} \subseteq R$, τότε:*

1. *Το αριστερό ιδεώδες ${}_{\mathfrak{l}}(x_1, x_2, \cdots, x_n)$ το οποίο παράγεται από το X είναι:*

$${}_{\mathfrak{l}}(x_1, x_2, \cdots, x_n) = \Big\{ \sum_{k=1}^{n} r_k \cdot x_k \ \in \ R \mid r_k \in R,\ 1 \leq k \leq n,\ n \in \mathbb{N} \Big\} \tag{8.1}$$

2. *Το δεξιό ιδεώδες $(x_1, x_2, \cdots, x_n)_{\mathfrak{r}}$ το οποίο παράγεται από το από το X είναι:*

$$(x_1, x_2, \cdots, x_n)_{\mathfrak{r}} = \Big\{ \sum_{k=1}^{n} x_k \cdot r_k \ \in \ R \mid r_k \in R,\ 1 \leq k \leq n,\ n \in \mathbb{N} \Big\} \tag{8.2}$$

3. *Το ιδεώδες $(x_1, x_2, \cdots, x_n)$ το οποίο παράγεται από το X είναι ίσο με:*

$$\Big\{ \sum_{i_1=1}^{m_1} r_{1i_1} \cdot x_1 \cdot s_{1i_1} + \sum_{i_2=1}^{m_2} r_{2i_2} \cdot x_2 \cdot s_{2i_2} + \cdots + \sum_{i_n=1}^{m_n} r_{ni_n} \cdot x_n \cdot s_{ni_n} \ \in \ R \ \Big| \ r_{ki_k}, s_{k_{ik}} \in R,\ 1 \leq k \leq n,\ 1 \leq i_k \leq m_k \Big\} \tag{8.3}$$

Απόδειξη. 1. Έστω I το σύνολο στα δεξιά της (8.1), και έστω $x=\sum_{k=1}^{n} r_k\cdot x_k \in I$ και $y=\sum_{k=1}^{n} r'_k\cdot x_k \in I$, όπου $r_k, r'_k \in R$, $1\leq k\leq n$, και $r\in R$. Τότε εκ κατασκευής, $I\neq\emptyset$ διότι το I περιέχει τα στοιχεία x_k καθώς: $x_k = 1_R\cdot x_k$, $1\leq k\leq n$. Επίσης το στοιχείο $x-y=\sum_{k=1}^{n}(r_k-r'_k)\cdot x_k$ ανήκει στο I. Τέλος, το στοιχείο $r\cdot x = r\cdot\sum_{k=1}^{n} r_k\cdot x_k = \sum_{k=1}^{n}(r\cdot r_k)\cdot x_k \in I$, και άρα το I είναι ένα αριστερό ιδεώδες του R το οποίο περιέχει το Q. Άρα $\iota\big(x_1,x_2,\cdots,x_n\big)\subseteq I$. Αντίστροφα, κάθε αριστερό ιδέωδες J που περιέχει το X θα περιέχει προφανώς και αριστερά πολλαπλάσια των x_k με στοιχεία του R, καθώς και πεπερασμένα αθροίσματα τέτοιων στοιχείων. Άρα θα περιέχει και το I. Αυτό όμως σημαίνει ότι το ιδεώδες $\iota\big(x_1,x_2,\cdots,x_n\big)$ το οποίο ορίστηκε να είναι η τομή τέτοιων ιδεωδών J θα περιέχει το I. Επομένως $I=\iota\big(x_1,x_2,\cdots,x_n\big)$.

2. Η απόδειξη είναι παρόμοια με την απόδειξη του 1.

3. Έστω I το σύνολο στα δεξιά της (8.3). Ένα τυπικό στοιχείο του I είναι της μορφής $a_1+a_2+\cdots+a_n$, όπου $a_k=\sum_{i_k=1}^{m_k} r_{ki_k}\cdot x_k\cdot s_{ki_k}$, $1\leq k\leq n$. Επειδή τα στοιχεία r_{ki_k} και s_{lj_l} είναι τυχαία στοιχεία του δακτυλίου R, έπεται άμεσα ότι το σύνολο I περιέχει τα στοιχεία x_k, $1\leq k\leq n$, του X. Επιπλέον πεπερασμένα αθροίσματα ή διαφορές στοιχείων της μορφής a_k παραμένουν στοιχεία της ίδιας μορφής, και παρόμοια, εκ κατασκευής, πεπερασμένα αθροίσματα ή διαφορές στοιχείων της μορφής $a_1+a_2+\cdots+a_n$ παραμένουν στοιχεία της ίδιας μορφής. Τέλος, στοιχεία της μορφής a_k είναι κλειστά στον πολλαπλασιασμό με στοιχεία του δακτυλίου από τα δεξιά και αριστερά, και το ίδιο συμβαίνει προφανώς και με πεπερασμένα αθροίσματα στοιχείων αυτής της μορφής. Έτσι το I είναι ένα ιδεώδες του R το οποίο περιέχει το X και γι' αυτό $(X)\subseteq I$. Αντίστροφα, αν J είναι ένα ιδεώδες του R το οποίο περιέχει το X, τότε επειδή είναι ιδεώδες και περιέχει τα στοιχεία x_k, $1\leq k\leq n$, θα περιέχει και τα στοιχεία της μορφής a_k και επομένως θα περιέχει και όλα τα στοιχεία της μορφής $a_1+a_2+\cdots+a_n$. Άρα το J θα περιέχει και το I. Άρα το I περιέχεται σε κάθε ιδεώδες του R το οποίο περιέχει το X και επομένως $I\subseteq(X)$. Επομένως, τελικά θα έχουμε $(X)=I$. ■

Από την παραπάνω περιγραφή, παρατηρούμε ότι, αν ο δακτύλιος είναι μεταθετικός, ή γενικότερα αν τα στοιχεία $x_1,x_2,\cdots,x_n$ ανήκουν στο κέντρο του R, τότε το αριστερό, το δεξιό, και το αμφίπλευρο ιδεώδες που παράγονται απο αυτά τα στοιχεία συμπίπτουν.

Παράδειγμα 8.1.13. Έστω R ένας δακτύλιος και $\mathsf{M}_n(R)$ ο δακτύλιος των $n\times n$-πινάκων υπεράνω του R. Θεωρούμε τους πίνακες E_{ij}, $1\leq i,j\leq n$.

1. Θα προσδιορίσουμε το αριστερό ιδεώδες $\iota\big(E_{ij}\big)$ το οποίο παράγεται από τον πίνακα E_{ij}. Για κάθε πίνακα $A=(a_{ij})$ θα έχουμε:

$$A\cdot E_{ij}=\begin{pmatrix} & & j-\text{στήλη} & & \\ 0 & \cdots & a_{1i} & \cdots & 0\\ 0 & \cdots & a_{2i} & \cdots & 0\\ \vdots & \cdots & \cdots & \cdots & 0\\ 0 & \cdots & a_{n-1i} & \cdots & 0\\ 0 & \cdots & a_{ni} & \cdots & 0 \end{pmatrix}$$

   δηλαδή ο πίνακας $A\cdot E_{ij}$ είναι ο πίνακας του οποίου η j-στήλη είναι η i-στήλη του A και όλες οι άλλες στήλες είναι οι μηδενικές. Επομένως θα έχουμε

$$\iota\big(E_{ij}\big)=\big\{A\cdot E_{ij}\in\mathsf{M}_n(R)\mid A=(a_{ij})\in\mathsf{M}_n(R)\big\}=\big\{A=(a_{kl})\in\mathsf{M}_n(R)\mid a_{kl}=0,\forall\, l\neq j\big\}$$

   είναι το υποσύνολο όλων των $n\times n$ πινάκων με μηδενικές όλες τις στήλες, εκτός ενδεχομένως της j-στήλης.

2. Θα προσδιορίσουμε το δεξιό ιδεώδες $\big(E_{ij}\big)_{\mathrm{r}}$ το οποίο παράγεται από τον πίνακα E_{ij}. Για κάθε πίνακα

$A=(a_{ij})$ θα έχουμε:

$$E_{ij}\cdot A=\begin{pmatrix} 0 & \cdots & \cdots & \cdots & 0\\ 0 & \cdots & \cdots & \cdots & 0\\ a_{j1} & a_{j2} & \cdots & a_{jn-1} & a_{jn}\\ 0 & \cdots & \cdots & \cdots & 0\\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \quad i-\text{γραμμή}$$

δηλαδή ο πίνακας $E_{ij}\cdot A$ είναι ο πίνακας του οποίου η i-γραμμή είναι η j-γραμμή του A και όλες οι άλλες γραμμές είναι οι μηδενικές. Επομένως θα έχουμε

$$\left(E_{ij}\right)_{\mathfrak{r}}=\left\{E_{ij}\cdot A\in \mathsf{M}_n(R)\mid A=(a_{ij})\in \mathsf{M}_n(R)\right\}=\left\{A=(a_{kl})\in \mathsf{M}_n(R)\mid a_{kl}=0,\forall k\neq i\right\}$$

είναι το υποσύνολο όλων των $n\times n$ πινάκων με μηδενικές όλες τις γραμμές, εκτός ενδεχομένως της i-γραμμής.

3. Θα προσδιορίσουμε το ιδεώδες $\left(E_{ij}\right)$ το οποίο παράγεται από τον πίνακα E_{ij}. Χρησιμοποιώντας ότι το (E_{ij}) είναι αριστερό και δεξιό ιδεώδες και περιέχει τον πίνακα E_{ij}, για κάθε k,l με $1\leq k,l\leq n$, θα έχουμε ότι

$$E_{ki}\cdot E_{ij}=E_{kj}\ \in\ (E_{ij})\qquad \text{και}\qquad E_{kj}\cdot E_{jl}=E_{kl}\ \in\ (E_{ij})$$

Άρα το ιδεώδες (E_{ij}) περιέχει όλους τους πίνακες $E_{k,l}$, $1\leq k,l\leq n$. Επειδή για κάθε πίνακα $A=(a_{ij})$ έχουμε:

$$A=(a_{ij})=\sum_{k,l=1}^{n,m}a_{kl}E_{kl}$$

έπεται ότι το ιδεώδες (E_{ij}) περιέχει κάθε πίνακα A και επομένως $(E_{ij})=\mathsf{M}_n(R)$. $\surd$

Παράδειγμα 8.1.14. Στον δακτύλιο $\mathscr{C}([0,1],\mathbb{R})=\left\{f\colon [0,1]\longrightarrow\mathbb{R}\mid f:\ \text{συνεχής}\right\}$, το υποσύνολο

$$I_r=\left\{f\in\mathscr{C}([0,1],\mathbb{R})\mid f(r)=0\right\}\quad (r\in[0,1])$$

είναι ένα ιδεώδες του $\mathscr{C}([0,1],\mathbb{R})$ το οποίο αποδεικνύεται ότι δεν είναι πεπερασμένα παραγόμενο, βλέπε την Άσκηση 8.5.32. $\surd$

Παράδειγμα 8.1.15. Έστω R ένας μεταθετικός δακτύλιος, και έστω $R[t]$ ο δακτύλιος των πολυωνύμων υπεράνω του R. Το σύνολο

$$I=\left\{\sum_{i=0}^{n}a_it^i\in R[t]\mid a_0=0\right\}$$

όλων των πολυωνύμων, με μηδενικό σταθερό όρο, είναι ένα ιδεώδες του $R[t]$ και μάλιστα $I=(t)$. Πράγματι κάθε στοιχείο του ιδεώδους (t) είναι της μορφής $tP(t)$ και άρα έχει μηδενικό σταθερό όρο, δηλαδή ανήκει στο I. Αντίστροφα, κάθε στοιχείο του I είναι της μορφης $P(t)=a_1t+a_2t^2+\cdot a_nt^n=t(a_1+a_2t^2+\cdots a_nt^{n-1})$ και άρα ανήκει στο (t).

Το σύνολο

$$J=\left\{\sum_{i=0}^{n}a_it^i\in\mathbb{Z}[t]\mid a_0\in 2\mathbb{Z}\right\}$$

των πολυωνύμων με ακέραιους συντελεστές και άρτιο σταθερό όρο είναι ένα ιδεώδες του $\mathbb{Z}[t]$ και μάλιστα $J=(2,t)$, όπου 2 συμβολίζει το σταθερό πολυώνυμο με σταθερό όρο ίσο με 2. Πράγματι, θα έχουμε ότι ένα τυπικό στοιχείο του J είναι της μορφής $P(t)=2b_0+a_1t+a_2t^2+\cdots+a_nt^n=2Q(t)+tR(t)$, όπου $Q(t)=2b_0$ και $R(t)=a_1+a_2t+\cdots+a_nt^{n-1}$. Τότε $P(t)\in(2,t)$ και άρα $J\subseteq(2,t)$. Αντίστροφα, κάθε στοιχείο του $(2,t)$ είναι της μορφής $P(t)=2Q(t)+tR(t)$, όπου $Q(t),R(t)\in\mathbb{Z}[t]$. Προφανώς ο σταθερός όρος του $P(t)$ είναι άρτιος και άρα $P(t)\in J$. Επομένως $J=(2,t)$.

Το ιδεώδες $(2,t)$ δεν είναι κύριο διότι, αν $(2,t)=(P(t))$, τότε $2=Q(t)P(t)$ και $t=R(t)P(t)$. Θεωρώντας βαθμούς πολυωνύμων σ' αυτές τις σχέσεις, βλέπε το Κεφάλαιο 9, θα έχουμε ότι $\deg(P(t)Q(t))=\deg P(t)+\deg Q(t)$, από όπου έπεται ότι $\deg P(t)=0$, και άρα το πολυώνυμο $P(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο, έστω $P(t)=a$, όπου $a\in\mathbb{Z}\setminus\{0\}$. Τότε όμως θα έχουμε $ab=2$, απ' όπου $a=\pm1$ ή $a=\pm2$. Από την άλλη πλευρά, θα έχουμε $1=\deg(P(t)R(t))=\deg P(t)+\deg R(t)=\deg R(t)$, και άρα $R(t)=c+dt$, για κάποια στοιχεία $c,d\in\mathbb{Z}$. Τότε θα έχουμε $t=a(c+dt)=ac+adt$, από όπου $ac=0$ και $ad=1$. Επειδή $a\neq0$, θα έχουμε $c=0$ και $a=\pm1$. Τότε όμως $(P(t))=(\pm1)=\mathbb{Z}[t]$. Αυτό είναι άτοπο διότι, για παράδειγμα, το σταθερό πολυώνυμο $\pm1\in(2,t)$ δεν έχει άρτιο σταθερό όρο. $\surd$

Παράδειγμα 8.1.16. Έστω ότι R_1, R_2, $\cdots$, R_n είναι δακτύλιοι και θεωρούμε το ευθύ γινόμενό τους

$$R_1\times R_2\times\cdots\times R_n=\{(r_1,r_2,\cdots,r_n)\mid r_i\in R_i,\ 1\leq i\leq n\}$$

και έστω $e_i=(0,\cdots0,1_{R_i},0,\cdots,0)$ (το στοιχείο 1_{R_i} είναι στην i-οστή θέση), $1\leq i\leq n$. Προφανώς τα στοιχεία e_i ανήκουν στο κέντρο του δακτυλίου $\prod_{i=1}^n R_i$. Έτσι θα έχουμε ότι

$$\iota(e_i)=(e_i)_\tau=(e_i)=\Big\{\underbrace{(0,\cdots,0,r_i,0,\cdots,0)}_{i-\text{θέση}}\mid r_i\in R_i\Big\},\qquad 1\leq i\leq n$$

είναι ιδέωδη του $\prod_{i=1}^n R_i$. $\surd$

Κλείνουμε την παρούσα υποενότητα με το ακόλουθο αποτέλεσμα το οποίο χαρακτηρίζει τους δακτυλίους διαίρεσης και τα σώματα με χρήση ιδεωδών, και συμπληρώνει την Πρόταση 8.1.3.

Πρόταση 8.1.17. *Έστω R ένας δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα.*

1. *Ο R είναι δακτύλιος διαίρεσης.*
2. *Τα μόνα αριστερά (ή δεξιά) ιδεώδη του R είναι τα τετριμμένα: R και $\{0\}$.*

Ιδιαίτερα ένας μεταθετικός δακτύλιος είναι σώμα αν και μονον αν είναι απλός.

Απόδειξη. Η κατεύθυνση 1. $\Longrightarrow$ 2. αποδείχθηκε στο μέρος 2. της Πρότασης 8.1.3.

2. $\Longrightarrow$ 1. Υποθέτουμε ότι ο R διαθέτει μόνο τα τετριμμένα αριστερά ιδεώδη. Έστω $0\neq r\in R$. Θεωρούμε το κύριο αριστερό ιδεώδες $Rr=\{xr\in R\mid x\in R\}$ του R το οποίο παράγεται από το r. Τότε θα έχουμε $Rr=R$ ή $Rr=\{0\}$. Αν $Rr=\{0\}$, τότε $0=1_Rr=r$ και αυτό είναι άτοπο. Άρα $Rr=R$ και επομένως, υπάρχει $s\in R$ έτσι ώστε $s\cdot r=1_R$. Προφανώς $s\neq0$, διότι διαφορετικά θα είχαμε $1_R=0$ το οποίο δεν ισχύει. Θεωρούμε το κύριο αριστερό ιδεώδες $Rs=\{xs\in R\mid x\in R\}$ του R το οποίο παράγεται από το s. Επειδή $s\neq0$, όπως και πριν, θα έχουμε $Rs=R$, και επομένως υπάρχει στοιχείο $t\in R$ έτσι ώστε $t\cdot s=1_R$. Τότε

$$s\cdot r=1_R\quad\text{και}\quad t\cdot s=1_R\quad\Longrightarrow\quad t\cdot(s\cdot r)=t\quad\Longrightarrow\quad(t\cdot s)\cdot r=t\quad\Longrightarrow\quad1_R\cdot r=r=t\quad\Longrightarrow\quad r\cdot s=1_R$$

Άρα $r\cdot s=1_R=s\cdot r$ και το στοιχείο είναι αντιστρέψιμο. Έτσι δείξαμε ότι κάθε μη-μηδενικό στοιχείο του R είναι αντιστρέψιμο και επομένως ο δακτύλιος R είναι δακτύλιος διαίρεσης. ■

Σχόλιο 8.1.18. Το παραπάνω αποτέλεσμα στην Πρόταση 8.1.17, δεν ισχύει αν στη θέση αριστερό ή δεξιό ιδεώδες έχουμε αμφίπλευρο ιδεώδες. Για παράδειγμα, όπως θα δούμε ο δακτύλιος $\mathsf{M}_n(R)$, όπου R είναι ένα σώμα, είναι απλός και δεν είναι δακτύλιος διαίρεσης αν $n>1$, βλέπε την Πρόταση 8.1.19. Έτσι έχει μόνο δύο (αμφίπλευρα) ιδεώδη, τα τετριμμένα, αλλά πολλά αριστερά ή δεξιά ιδεώδη. $\surd$

Πρόταση 8.1.19. *Έστω R ένας δακτύλιος διαίρεσης. Τότε ο δακτύλιος $\mathsf{M}_n(R)$ είναι απλός, δηλαδή τα μόνα του ιδεώδη είναι τα τετριμμένα: $\{0\}$ και $\mathsf{M}_n(R)$.*

Απόδειξη. Έστω I ένα μη μηδενικό ιδεώδες του $\mathsf{M}_n(R)$. Επομένως το ιδεώδες I περιέχει έναν μη-μηδενικό πίνακα $A=(a_{ij})$, και επομένως υπάρχουν k,l με $1\leq k,l\leq n$, έτσι ώστε $a_{kl}\neq 0$. Από το Παράδειγμα 8.1.13 για κάθε $1\leq i,j\leq n$ θα έχουμε:

$$E_{ik}\cdot A\cdot E_{lj}=a_{kl}E_{ij}$$

και άρα ο πίνακας $a_{kl}E_{ij}$ ανήκει στο ιδεώδες I. Επειδή ο δακτύλιος R είναι δακτύλιος διαίρεσης το στοιχείο a_{kl} είναι αντιστρέψιμο και άρα υπάρχει το αντίστροφό του a_{kl}^{-1}. Πολλαπλασιάζοντας την παραπάνω σχέση με τον βαθμωτό πίνακα $a_{kl}^{-1}I_n$, θα έχουμε:

$$a_{kl}^{-1}I_n\cdot a_{kl}E_{ij}=E_{ij}\in I$$

Έτσι το ιδεώδες I περιέχει όλους τους πίνακες E_{ij}, $1\leq i,j\leq n$. Όπως στο μέρος 3. του Παραδείγματος 8.1.13, έπεται ότι το ιδεώδες $I=\mathsf{M}_n(R)$. Άρα ο δακτύλιος $\mathsf{M}_n(R)$ είναι απλός. ■

Σχόλιο 8.1.20. Το παραπάνω αποτέλεσμα στην Πρόταση 8.1.19, δεν ισχύει αν ο δακτύλιος R δεν είναι δακτύλιος διαίρεσης. Αυτό το οποίο ισχύει είναι ότι: *«υπάρχει μια «1-1» και «επί» αντιστοιχία ανάμεσα στα ιδεώδη του R και στα ιδεώδη του $\mathsf{M}_n(R)$»*. Η αντιστοιχία αυτή δίνεται από την απεικόνιση $I\longmapsto \mathsf{M}_n(I)$, όπου $\mathsf{M}_n(I)$ αποτελείται από όλους τους πίνακες $A=(a_{ij})$ του δακτυλίου $\mathsf{M}_n(R)$ των οποίων τα στοιχεία a_{ij} ανήκουν στο ιδεώδες I του R, βλέπε την Άσκηση 8.5.18. Έτσι ο δακτύλιος $\mathsf{M}_n(R)$ είναι απλός αν και μόνο αν ο δακτύλιος R είναι απλός. Επειδή κάθε δακτύλιος διαίρεσης είναι απλός, έπεται ότι η Πρόταση 8.1.19 είναι ειδική περίπτωση αυτού του αποτελέσματος. √

8.1.2 Άθροισμα και Γινόμενο Ιδεωδών

Στην παρούσα υποενότητα θα δούμε δυο σημαντικές κατασκευές ιδεωδών σε ένα δακτύλιο R, το άθροισμα και το γινόμενο ιδεωδών.

Άθροισμα Ιδεωδών

Όπως και στη Θεωρία Ομάδων, όπου ένωση υποομάδων δεν είναι απαραίτητα υποομάδα, έτσι και στη θεωρία Δακτυλίων, ένωση (αριστερών ή δεξιών) ιδεωδών δεν είναι απαραίτητα (αριστερό ή δεξιό) ιδεώδες. Για παράδειγμα, η ένωση $3\mathbb{Z}\cup 4\mathbb{Z}$ των ιδεωδών του $\mathbb{Z}$ δεν είναι ιδεώδες, διότι διαφορετικά θα περιέχει το στοιχείο $3+4=7$, και αυτό είναι άτοπο. Παρόμοια θεωρούμε τα αριστερά ιδεώδη

$$I=\left\{\begin{pmatrix}x&0\\0&0\end{pmatrix}\in \mathsf{AT}_2(\mathbb{R})\mid x\in\mathbb{R}\right\}\qquad\text{και}\qquad J=\left\{\begin{pmatrix}0&y\\0&0\end{pmatrix}\in \mathsf{AT}_2(\mathbb{R})\mid y\in\mathbb{R}\right\}$$

του δακτυλίου $\mathsf{AT}_2(\mathbb{R})$ των 2×2 άνω τριγωνικών πινάκων υπεράνω του $\mathbb{R}$. Τότε το υποσύνολο $I\cup J$ δεν είναι αριστερό ιδεώδες του $\mathsf{AT}_2(\mathbb{R})$ διότι, αν και περιέχει τους πίνακες $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)$ και $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$, δεν περιέχει το άθροισμά τους $\left(\begin{smallmatrix}1&1\\0&0\end{smallmatrix}\right)$. Το μικρότερο αριστερό ιδεώδες του $\mathsf{AT}_2(\mathbb{R})$ το οποίο περιέχει αυτούς τους πίνακες είναι το

$$\left\{\begin{pmatrix}x&y\\0&0\end{pmatrix}\in \mathsf{AT}_2(\mathbb{R})\mid x,y\in\mathbb{R}\right\}$$

Γενικεύοντας, έστω $\{I_k\}_{k=1}^n$ μια πεπερασμένη συλλογή αριστερών, δεξιών ή αμφίπλευρων ιδεωδών. Θεωρούμε το ακόλουθο υποσύνολο του R:

$$\sum_{k=1}^n I_k=I_1+I_2+\cdots+I_n=\{x_1+x_2+\cdots+x_n\in R\mid x_k\in I_k\ 1\leq k\leq n\}$$

Πρόταση 8.1.21. *Το σύνολο $I_1+I_2+\cdots+I_n$ είναι ένα αριστερό, δεξιό ή αμφίπλευρο ιδεώδες αντίστοιχα, και μάλιστα είναι το μικρότερο αριστερό, δεξιό ή αμφίπλευρο ιδεώδες αντίστοιχα το οποίο περιέχει το σύνολο $\cup_{k=1}^n I_k$. Με άλλα λόγια, έχουμε ότι το σύνολο $\sum_{k=1}^n I_k$ συμπίπτει με τα ιδεώδη $\iota\left(\cup_{k=1}^n I_k\right)$, $\left(\cup_{k=1}^n I_k\right)_\iota$, $\left(\cup_{k=1}^n I_k\right)$ αντίστοιχα.*

Απόδειξη. Προφανώς το σύνολο $\sum_{k=1}^{n} I_k$ περιέχει κάθε I_k, διότι κάθε στοιχείο $x \in I_k$ μπορεί να γραφεί ως $x = 0 + \cdots + 0 + x + 0 \cdots + 0$, όπου το x βρίσκεται στην k-θέση, $1 \leq k \leq n$. Έστω $a = \sum_{k=1}^{n} x_k$ και $b = \sum_{k=1}^{n} y_k$ δύο στοιχεία του υποσυνόλου $\sum_{k=1}^{n} I_k$, όπου $x_k, y_k \in I_k$, και $r \in R$. Τότε, χρησιμοποιώντας την επιμεριστική ιδιότητα, και ότι κάθε I_k είναι υποομάδα της προσθετικής ομάδας $(R, +)$, θα έχουμε: $a - b = \sum_{k=1}^{n} x_k - \sum_{k=1}^{n} y_k = \sum_{k=1}^{n} (x_k - y_k) \in \sum_{k=1}^{n} I_k$. Αν τα I_k είναι αριστερά ιδεώδη, τότε $r \cdot x_k \in I_k$ και επομένως $r \cdot \sum_{k=1}^{n} x_k = \sum_{k=1}^{n} (r \cdot x_k) \in \sum_{k=1}^{n} I_k$. Άρα το σύνολο $\sum_{k=1}^{n} I_k$ είναι ένα αριστερό ιδεώδες το οποίο περιέχει τα αριστερά ιδεώδη I_k, $1 \leq k \leq n$, και άρα περιέχει την ένωση $\cup_{k=1}^{n} I_k$. Αυτό σημαίνει ότι $\iota\big(\cup_{k=1}^{n} I_k\big) \subseteq \sum_{k=1}^{n} I_k$. Αντίστροφα, αν J είναι ένα αριστερό ιδεώδες του R το οποίο περιέχει την ένωση $\cup_{k=1} I_k$, τότε θα περιέχει καθένα από τα I_k, $1 \leq k \leq n$, και επειδή είναι αριστερό ιδεώδες, θα περιέχει και κάθε άθροισμα στοιχείων $\sum_{k=1}^{n} x_k$, όπου $x_k \in I_k$, $1 \leq k \leq n$. Άρα θα περιέχει και το αριστερό ιδεώδες $\sum_{k=1}^{n} I_k$, και γι' αυτό θα έχουμε $\sum_{k=1}^{n} I_k \subseteq J$. Αυτό σημαίνει ότι $\sum_{k=1}^{n} I_k \subseteq \iota\big(\cup_{k=1}^{n} I_k\big)$, και επομένως θα έχουμε $\sum_{k=1}^{n} I_k = \iota\big(\cup_{k=1}^{n} I_k\big)$. Αν τα I_k είναι δεξιά ιδεώδη ή αμφίπλευρα ιδεώδη, τότε εργαζόμαστε ακριβώς ανάλογα. ■

Αν $\{I_k\}_{k=1}^{n}$ είναι μια συλλογή αριστερών, δεξιών, ή αμφίπλευρων ιδεωδών του δακτυλίου R, τότε το αριστερό, δεξιό ή αμφίπλευρο ιδεώδες αντίστοιχα, $\sum_{k=1}^{n} I_k$ καλείται το **άθροισμα** των αριστερών, δεξιών, ή αμφίπλευρων ιδεωδών $I_1, I_2, \cdots, I_n$.

Παρατήρηση 8.1.22. Αν $X = \{x_1, x_2, \cdots, x_n\} \subseteq R$, θέτουμε, για $1 \leq i \leq n$:

$$I_i = \iota(x_i) = Rx_i, \qquad J_i = (x_i)_\tau = x_i R, \qquad K_i = (x_i) = Rx_i R$$

Τότε, όπως προκύπτει από τις Πρότασεις 8.1.12 και 8.1.21, θα έχουμε:

$$\sum_{i=1}^{n} I_i = \iota(x_1, x_2, \cdots, x_n), \qquad \sum_{i=1}^{n} J_i = (x_1, x_2, \cdots, x_n)_\tau, \qquad \sum_{i=1}^{n} K_i = (x_1, x_2, \cdots, x_n) \quad \blacktriangle$$

Παράδειγμα 8.1.23. Έστω ότι R_1, R_2, $\cdots$, R_n είναι δακτύλιοι και θεωρούμε το ευθύ γινόμενό τους

$$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \leq i \leq n\}$$

Θεωρούμε τα ιδεώδη

$$\iota(e_i) = (e_i)_\tau = (e_i) = \Big\{\underbrace{(0, \cdots, 0, r_i, 0, \cdots, 0)}_{i-\text{θέση}} \mid r_i \in R_i\Big\}, \qquad 1 \leq i \leq n$$

τα οποία παράγονται από τα στοιχεία e_i, όπου $e_i = (0, \cdots 0, 1_{R_i}, 0, \cdots, 0)$ (το στοιχείο 1_{R_i} είναι στην i-οστή θέση), $1 \leq i \leq n$, όπως στο Παράδειγμα 8.1.16. Τότε προφανώς θα έχουμε

$$R_1 \times R_2 \times \cdots \times R_n = \sum_{i=1}^{n} (e_i) \quad \surd$$

Κλείνουμε την παρούσα υποενότητα με το ακόλουθο παράδειγμα.

Παράδειγμα 8.1.24. Στον δακτύλιο $\mathbb{Z}$ των ακεραίων θεωρούμε τα ιδεώδη $n\mathbb{Z}$ και $m\mathbb{Z}$, $n, m \geq 1$. Τότε

$$n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$$

Έστω $d = (n, m)$ ο μέγιστος κοινός διαιρέτης των n, m. Τότε $d \mid n$ και άρα $n = dk$ και $d \mid m$ και άρα $m = dl$, για κάποιους θετικούς ακεραίους k, l. Αν $x \in n\mathbb{Z} + m\mathbb{Z}$, τότε υπάρχουν ακέραιοι $z, w \in \mathbb{Z}$, έτσι ώστε $z = nz + mw$. Έτσι θα έχουμε:

$$x = nz + mw = dkz + dlw = d \cdot (kz + lw) \implies x \in d\mathbb{Z} \implies n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$$

Αντίστροφα, αν $x \in d\mathbb{Z}$, θά έχουμε $x = dz$ για έναν θετικό ακέραιο z. Επειδή $d = (n, , m)$, γνωρίζουμε από την στοιχειώδη Θεωρία Αριθμών ότι υπάρχουν ακέραιοι $k, l \in \mathbb{Z}$ έτσι ώστε $d = nk + ml$, και τότε θα έχουμε:

$$x = dz = (nk + ml) \cdot z = n(kz) + m(lz) \implies x \in n\mathbb{Z} + m\mathbb{Z} \implies d\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$$

Από τις παραπάνω σχέσεις προκύπτει ο ισχυρισμός: $d\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}$. $\surd$

Ευθύ Άθροισμα Ιδεωδών

Μια σημαντική ειδική περίπτωση ευθέος αθροίσματος ιδεωδών αποτελεί το ευθύ άθροισμα ιδεώδων το οποίο χαρακτηρίζεται από την μοναδικότητα της γραφής των στοιχείων του ως άθροισμα στοιχείων των ιδεωδών.

Πρόταση 8.1.25. *Έστω $\{I_k\}_{k=1}^n$ μια πεπερασμένη οικογένεια αριστερών, δεξιών ή αμφίπλευρων ιδεωδών, του δακτυλίου R. Τότε, θέτοντας $I = I_1 + I_2 + \cdots + I_n$, τα ακόλουθα είναι ισοδύναμα:*

1. *Κάθε στοιχείο $x \in I$ γράφεται κατά μοναδικό τρόπο ως άθροισμα στοιχείων των I_k, $1 \le k \le n$:*
$$x = x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_n, \quad x_k, y_k \in I_k, \quad 1 \le k \le n \quad \Longrightarrow \quad x_k = y_k, \quad 1 \le k \le n$$
2. $x_1 + x_2 + \cdots + x_n = 0, \quad x_k \in I_k, \quad 1 \le k \le n \quad \Longrightarrow \quad x_k = 0, \quad 1 \le k \le n.$
3. *Για κάθε $k = 1, 2, \cdots, n$:*
$$\left(I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n\right) \bigcap I_k = \{0\}$$

Απόδειξη. 1. «$\Longrightarrow$» 2. Υποθέτουμε ότι ισχύει η συνθήκη του μέρους 1., και έστω $x_1 + x_2 + \cdots + x_n = 0$, όπου $x_k \in I_k$, $1 \le k \le n$. Επειδή $0 \in I_k$, $1 \le k \le n$, θα έχουμε $x_1 + x_2 + \cdots + x_n = 0 = 0 + 0 + \cdots + 0$, απ' όπου η υπόθεση δίνει ότι $x_k = 0$, $1 \le k \le n$.

2. «$\Longrightarrow$» 3. Υποθέτουμε ότι ισχύει η συνθήκη του μέρους 2., και έστω $x \in \left(I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n\right) \bigcap I_k$, όπου k είναι ένα τυχαίο στοιχείο εκ των $1, 2, \cdots, n$. Τότε θα έχουμε $x \in I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n$, απ' όπου $x = x_1 + x_2 + \cdots + x_{k-1} + x_{k+1} + \cdots x_n$, για κάποια στοιχεία $x_l \in I_l$, $1 \le l \ne k \le n$. Η τελευταία σχέση γράφεται

$$x_1 + x_2 + \cdots + x_{k-1} + (-x) + x_{k+1} + \cdots x_n = 0, \quad \text{όπου} \quad x_l \in I_l, \quad 1 \le l \ne k \le n \quad \text{και} \quad -x \in I_k$$

Από την υπόθεση τότε θα έχουμε $x_l = 0$, $1 \le l \ne k \le n$, και $x = 0$. Επομένως $\left(I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n\right) \bigcap I_k = \{0\}$.

3. «$\Longrightarrow$» 1. Υποθέτουμε ότι ισχύει η συνθήκη του μέρους 3., και έστω $x = x_1 + x_2 + \cdots + x_n = y_1 + y_2 + \cdots + y_n$, όπου $x_k, y_k \in I_k$, $1 \le k \le n$. Τότε, για κάθε $k = 1, 2, \cdots, n$, θα έχουμε

$$-x_k + y_k = (x_1 - y_1) + (x_2 - t_2) + \cdots + (x_{k-1} - y_{k-1}) + (x_{k+1} - y_{k+1}) + \cdots (x_n - y_n)$$

όπου, επειδή το I_i είναι αριστερό, δεξιό ή αμφίπλευρο ιδεώδες, θα έχουμε $x_i - y_i \in I_i$, $1 \le i \ne k \le n$ και $-x_k + y_k \in I_k$. Τότε όμως $I_k \ni -x_k + y_k = (x_1 - y_1) + (x_2 - t_2) + \cdots + (x_{k-1} - y_{k-1}) + (x_{k+1} - y_{k+1}) + \cdots (x_n - y_n) \in I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n$. Έτσι $-x_k + y_k \in \left(I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots + I_n\right) \bigcap I_k = \{0\}$ και άρα $x_k = y_k$. Επειδή το $k \in \{1, 2, \cdots, n\}$ επιλέχθηκε τυχαία, θα έχουμε $x_k = y_k$, $1 \le k \le n$. ■

Ορισμός 8.1.26. *Αν για το άθροισμα $I_1 + I_2 + \cdots + I_n$ δεξιών, αριστερών, ή αμφίπλευρων ιδεωδών I_k, $1 \le k \le n$, του δακτυλίου R ικανοποιείται μια από τις ισοδύναμες συνθήκες της Πρότασης 8.1.25, τότε το άθροισμα δεξιών, αριστερών ή αμφίπλευρων ιδεωδών $I_1 + I_2 + \cdots + I_n$ καλείται* **ευθύ άθροισμα** *και θα συμβολίζεται ως εξής:*

$$I_1 + I_2 + \cdots + I_n = I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

Προφανώς, αν το άθροισμα $I_1 + I_2 + \cdots + I_n = I_1 \oplus I_2 \oplus \cdots \oplus I_n$ δεξιών, αριστερών, ή αμφίπλευρων ιδεωδών I_k, $1 \le k \le n$, του δακτυλίου R είναι ευθύ, τότε

$$k \ne j \quad \Longrightarrow \quad I_k \cap I_j = \{0\}$$

διότι $I_j \subseteq I_1 + \cdots + I_{k-1} + I_{k+1} + \cdots I_n$. Σημειώνουμε ότι η αντίστροφη συνεπαγωγή δεν ισχύει, βλέπε την Άσκηση 8.5.20.

Παράδειγμα 8.1.27. Έστω ότι R_1, R_2, $\cdots$, R_n είναι δακτύλιοι και θεωρούμε το ευθύ γινόμενό τους

$$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \leq i \leq n\}$$

Τότε, όπως προκύπτει από το Παράδειγμα 8.1.23, ο δακτύλιος R είναι το ευθύ άθροισμα των ιδεωδών του (e_k), τα οποία παράγονται από τα στοιχεία e_i, όπου $e_i = (0, \cdots 0, 1_{R_i}, 0, \cdots, 0)$ (το στοιχείο 1_{R_i} είναι στην i-οστή θέση), $1 \leq i \leq n$:

$$\iota(e_i) = (e_i)_\tau = (e_i) = \Big\{(\underbrace{0, \cdots, 0, r_i, 0, \cdots, 0}_{i-\text{θέση}}) \mid r_i \in R_i\Big\}, \qquad 1 \leq i \leq n$$

Έτσι θα έχουμε:

$$R = (e_1) \oplus (e_2) \oplus \cdots \oplus (e_n) \quad \surd$$

Γινόμενα Ιδεωδών

Μια οικογένεια (αμφίπλευρων) ιδεώδων $\{I_k\}_{k=1}^n$ του R ορίζει και ένα επιπρόσθετο αμφίπλευρο ιδέωδες του R. Αν I και J είναι δύο ιδεώδη του R, τότε είναι εύλογο να θεωρήσουμε το σύνολο των στοιχείων $\{x \cdot y \in R \mid x \in I,\ y \in J\}$, αν και είναι κλειστό στον πολλαπλασιασμό από τα αριστερά και τα δεξιά με στοιχεία του δακτυλίου, δεν είναι είναι κλειστό στο άθροισμα στοιχείων του, διότι δεν υπάρχει λόγος ένα άθροισμα της μορφής $x_1 \cdot y_1 + x_2 \cdot y_2$ να είναι της μορφής $x \cdot y$, όπου $x_i, x \in I$ και $y_i, y \in J$, $i = 1, 2$. Όπως και πριν, για να διορθώσουμε αυτή την παθολογία, θεωρούμε το ακόλουθο υποσύνολο του R:

$$I_1 \cdot I_2 \cdots I_n = \{x_{1i_1} \cdot x_{1i_2} \cdots x_{1i_n} + x_{2i_1} \cdot x_{2i_2} \cdots x_{2i_n} + \cdots + x_{mi_1} \cdot x_{mi_2} \cdots x_{mi_n} \in R \mid x_{ki_j} \in I_j,\ 1 \leq j \leq n, n \in \mathbb{N}\}$$

Πρόταση 8.1.28. *Αν $\{I_k\}_{k=1}^n$ είναι μια πεπερασμένη οικογένεια ιδεωδών, το σύνολο $I_1 \cdot I_2 \cdots I_n$ είναι ένα ιδεώδες του R και μάλιστα είναι το μικρότερο ιδεώδες του R το οποίο περιέχει όλα τα γινόμενα $x_1 \cdot x_2 \cdots x_n$, όπου $x_k \in I_k$, $1 \leq k \leq n$.*

Απόδειξη. Το σύνολο $I_1 \cdot I_2 \cdots I_n$ προφανώς περιέχει όλα τα δυνατά γινόμενα στοιχείων της μορφής $x_1 \cdot x_2 \cdots x_n$, όπου $x_k \in I_k$, $1 \leq k \leq n$, και είναι εκ κατασκευής κλειστό στο άθροισμα ή τη διαφορά στοιχείων του. Επειδή τα I_k είναι αμφίπλευρα ιδεώδη του R, $1 \leq k \leq n$, το σύνολο $I_1 \cdot I_2 \cdots I_n$ είναι κλειστό στον πολλαπλασιασμό απο τα δεξιά και τα αριστερά με στοιχεία του δακτυλίου, και άρα είναι ένα ιδεώδες του R. Προφανώς, το ιδεώδες $I_1 \cdot I_2 \cdots I_n$ είναι το μικρότερο ιδεώδες του R το οποίο περιέχει τα στοιχεία $x_1 \cdot x_2 \cdots x_n$, όπου $x_k \in I_k$, $1 \leq k \leq n$. ■

Το ιδεώδες της Πρότασης 8.1.28 καλείται το **γινόμενο** των ιδεωδών $I_1, I_2, \cdots, I_n$. Αν έχουμε $I_1 = I_2 = \cdots = I_n := I$, τότε θα γράφουμε

$$I^n = \underbrace{I \cdot I \cdot \cdots \cdot I}_{n-\text{παράγοντες}}$$

και θα καλούμε το ιδέωδες I^n την n-**οστή δύναμη** του I. Παρατηρούμε ότι $I^n \subseteq I$, $\forall n \geq 1$.

Ένα ιδεώδες I καλείται **ταυτοδύναμο ιδεώδες** αν $I^2 = I$. Το ιδεώδες I καλείται **μηδενοδύναμο ιδεώδες**, αν υπάρχει θετικός ακέραιος n έτσι ώστε $I^n = 0$. Δύο ιδεώδη I και J καλούνται **ορθογώνια** αν $I \cdot J = \{0\}$. Ταυτοδύναμα και μηδενοδύναμα ιδεώδη παίζουν σημαντικό ρόλο στη θεωρία δακτυλίων. Εδώ, λόγω περιορισμένου χώρου, θα δούμε μόνο κάποια παραδείγματα.

Παράδειγμα 8.1.29. Θεωρούμε τον δακτύλιο

$$\mathsf{AT}_2(\mathbb{R}) = \left\{\begin{pmatrix} a_{11} & a_{12} \\ 0 & a_{22} \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a_{ij} \in \mathbb{R}\right\}$$

των 2×2 άνω τριγωνικών πινάκων υπεράνω του $\mathbb{R}$, και έστω το ιδεώδες:

$$I = \left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \in \mathsf{AT}_2(\mathbb{R}) \mid x, y \in \mathbb{R}\right\}$$

Τότε: $I^2 = I$. Πράγματι πάντα ισχύει $I^2 \subseteq I$, και αν $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right)$ είναι ένα στοιχείο του I, τότε $\left(\begin{smallmatrix} x & y \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & y \\ 0 & 0 \end{smallmatrix}\right) \in I^2$. Άρα $I \subseteq I^2$ και επομένως $I^2 = I$, δηλαδή το ιδεώδες I είναι ταυτοδύναμο.

Θεωρούμε τον δακτύλιο

$$\mathsf{AT}_3(\mathbb{R}) = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \mid a_{ij} \in \mathbb{R} \right\}$$

των 3×3 άνω τριγωνικών πινάκων υπεράνω του $\mathbb{R}$.

Εύκολα μπορούμε να δούμε ότι το υποσύνολα

$$I = \left\{ \begin{pmatrix} 0 & x & z \\ 0 & 0 & y \\ 0 & 0 & 0 \end{pmatrix} \in \mathsf{AT}_3(\mathbb{R}) \mid x, y, z \in \mathbb{R} \right\} \quad \text{και} \quad J = \left\{ \begin{pmatrix} 0 & 0 & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathsf{AT}_3(\mathbb{R}) \mid w \in \mathbb{R} \right\}$$

είναι ιδέωδη του $\mathsf{AT}_3(\mathbb{R})$. Τότε: $I^2 = J$ και $I^3 = 0$. Πράγματι, αν $\left(\begin{smallmatrix} 0 & x_1 & z_1 \\ 0 & 0 & y_1 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ και $\left(\begin{smallmatrix} 0 & x_2 & z_2 \\ 0 & 0 & y_2 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ είναι στοιχεία του I, τότε $\left(\begin{smallmatrix} 0 & x_1 & z_1 \\ 0 & 0 & y_1 \\ 0 & 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & x_2 & z_2 \\ 0 & 0 & y_2 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 & x_1 y_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in J$. Επειδή προφανώς πεπερασμένα αθροίσματα τέτοιων γινομένων ανήκουν στο ιδεώδες J, έπεται ότι $I^2 \subseteq J$. Αντίστροφα, αν $\left(\begin{smallmatrix} 0 & 0 & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$ είναι ένα στοιχείο του J, τότε θα έχουμε $\left(\begin{smallmatrix} 0 & 0 & w \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & w & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in I^2$. Επομένως $I^2 = J$. Επειδή $\left(\begin{smallmatrix} 0 & x_1 & z_1 \\ 0 & 0 & y_1 \\ 0 & 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & x_2 & z_2 \\ 0 & 0 & y_2 \\ 0 & 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & x_3 & z_3 \\ 0 & 0 & y_3 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 & x_1 y_2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)\cdot\left(\begin{smallmatrix} 0 & x_2 & z_3 \\ 0 & 0 & y_3 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)$, έπεται άμεσα ότι $I^3 = 0 = J^2$, δηλαδή τα ιδεώδη I, J είναι μηδενοδύναμα. $\surd$

Παράδειγμα 8.1.30. Έστω ότι R_1, R_2, $\cdots$, R_n είναι δακτύλιοι και θεωρούμε το ευθύ γινόμενό τους

$$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \le i \le n\}$$

Θεωρούμε τα ιδεώδη

$$\iota(e_i) = (e_i)_{\mathfrak{r}} = (e_i) = \Big\{ \underbrace{(0, \cdots, 0, r_i, 0, \cdots, 0)}_{i-\text{θέση}} \mid r_i \in R_i \Big\}, \qquad 1 \le i \le n$$

τα οποία παράγονται από τα στοιχεία e_i, όπου $e_i = (0, \cdots 0, 1_{R_i}, 0, \cdots, 0)$ (το στοιχείο 1_{R_i} είναι στην i-οστή θέση), $1 \le i \le n$, όπως στο Παράδειγμα 8.1.16. Τότε θα έχουμε:

$$i \neq j \implies (e_i)\cdot(e_j) = \{0\} \qquad \text{και} \qquad (e_i)\cdot(e_i) = (e_i)$$

Άρα η οικογένεια ιδεωδών $\{(e_i)\}_{i=1}^n$ είναι μια οικογένεια ταυτοδύναμων ανά δύο ορθογώνιων ιδεωδών του $R_1 \times R_2 \times \cdots \times R_n$ με άθροισμα $\sum_{i=1}^n (e_i) = (1_{\prod_{i=1}^n R_i}) = R_1 \times R_2 \times \cdots \times R_n$. $\surd$

Παράδειγμα 8.1.31. Στον δακτύλιο $\mathbb{Z}$ των ακεραίων θεωρούμε τα ιδεώδη $n\mathbb{Z}$ και $m\mathbb{Z}$, $n, m \ge 1$. Τότε

$$n\mathbb{Z} \cdot m\mathbb{Z} = (nm)\mathbb{Z}$$

Πραγματικά, επειδή ο δακτύλιος $\mathbb{Z}$ είναι μεταθετικός, θα έχουμε $n\{nx \in \mathbb{Z} \mid x \in \mathbb{Z}$, $m\{mx \in \mathbb{Z} \mid x \in \mathbb{Z}$ και $n\{nmx \in \mathbb{Z} \mid x \in \mathbb{Z}$. Ένα τυπικό στοιχείο του ιδεώδους $n\mathbb{Z} \cdot m\mathbb{Z}$ είναι πεπερασμένο άθροισμα στοιχείων της μορφής $nzmw = nmzw \in (nm)\mathbb{Z}$, όπου $z, w \in \mathbb{Z}$, και άρα ανήκει στο ιδεώδες $(nm)\mathbb{Z}$. Έτσι $n\mathbb{Z} \cdot m\mathbb{Z} \subseteq (nm)\mathbb{Z}$. Ακριβώς παρόμοια έχουμε $(nm)\mathbb{Z} \subseteq n\mathbb{Z} \cdot m\mathbb{Z}$, και άρα: $n\mathbb{Z} \cdot m\mathbb{Z} = (nm)\mathbb{Z}$. $\surd$

Κλείνουμε την παρούσα ενότητα αναλύοντας τη σχέση μεταξύ του γινομένου και της τομής μιας πεπερασμένης οικογένειας ιδεωδών ενός μεταθετικού δακτυλίου. Δύο ιδεώδη I και J του δακτυλίου R καλούνται **συμμέγιστα** αν: $I + J = R$. Μια πεπερασμένη οικογένεια ιδεωδών $\{I_k\}_{k=1}^n$ του δακτυλίου R αποτελείται από **ανά δύο συμμέγιστα ιδεώδη**, αν $I_i + I_j = R$, $1 \le i \neq j \le n$.

Πρόταση 8.1.32. *Αν $\{I_k\}_{k=1}^n$ είναι μια οικογένεια ιδεωδών ενός μεταθετικού δακτυλίου R, τότε:*

$$I_1 \cdot I_2 \cdots I_n \subseteq I_1 \cap I_2 \cap \cdots \cap I_n$$

Αν η οικογένεια $\{I_k\}_{k=1}^n$ αποτελείται από ανά δύο συμμέγιστα ιδεώδη, τότε: $I_1 \cdot I_2 \cdots I_n = I_1 \cap I_2 \cap \cdots \cap I_n$.

Απόδειξη. Έστω $n = 2$. Τότε τα στοιχεία του γινομένου ιδεωδών $I_1 \cdot I_2$ είναι πεπερασμένα αθροίσματα γινομένων $x = x_1 \cdot x_2$, όπου $x_k \in I_k$, $k = 1,2$. Όμως $x_1 \cdot x_2 \in I_1$ διότι $x_1 \in I_1$ και το I_1 είναι ιδεώδες του R και $x_1 \cdot x_2 \in I_2$ διότι $x_2 \in I_2$ και το I_2 είναι ιδεώδες του R. Άρα $x_1 \cdot x_2 \in I_1 \cap I_2$. Αυτό σημαίνει ότι $I_1 \cdot I_2 \subseteq I_1 \cap I_2$. Υποθέτουμε ότι το συμπέρασμα ισχύει για πλήθος ιδεωδών ίσο με $k < n$. Επειδή προφανώς $I_1 \cdot I_2 \cdots I_n = I_1 \cdot (I_2 \cdots I_n)$, θα έχουμε $I_1 \cdot I_2 \cdots I_n \subseteq I_1 \cap (I_2 \cdots I_n)$, οπότε από την επαγωγική υπόθεση θα έχουμε τελικά $I_1 \cdot I_2 \cdots I_n \subseteq I_1 \cap (I_2 \cdots I_n) \subseteq I_1 \cap (I_2 \cap \cdots \cap I_n)$.

Υποθέτουμε ότι $I_i + I_j = R$, όταν $1 \leq i \neq j \leq n$. Έστω ότι $n = 2$, οπότε $I_1 + I_2 = R$. Τότε μπορούμε να γράψουμε $1_R = s_1 + s_2$, όπου $s_i \in I_i$, $i = 1,2$. Τότε για κάθε $x \in I_1 \cap I_2$, θα έχουμε $x = x \cdot 1_R = x \cdot s_1 + x \cdot s_2 = s_1 \cdot x + x \cdot s_2 \in I_1 \cdot I_2$, διότι $s_1 \in I_1$, $x \in I_2$, $x \in I_1$, και $s_2 \in I_2$. Άρα $I_1 \cap I_2 \subseteq I_1 \cdot I_2$ και επομένως $I_1 \cdot I_2 = I_1 \cap I_2$. Υποθέτουμε ότι το συμπέρασμα ισχύει για πλήθος ιδεωδών ίσο με $k < n$. Τότε θα έχουμε: $I_1 + (I_2 \cdots I_n) = R$. Πράγματι, επειδή $I_1 + I_k = R$, $\forall k \geq 2$, μπορούμε να γράψουμε: $a_k + b_k = 1$, $\forall k \geq 2$, όπου $a_k \in I_1$, και $b_k \in I_k$, $\forall k \geq 2$. Θεωρούμε το στοιχείο

$$1_R = \prod_{k=2}^{n} (a_k + b_k) = (a_2 + b_2) \cdot (a_3 + b_3) \cdots (a_n + b_n)$$

το οποίο στο ανάπτυγμά του είναι άθροισμα γινομένων των στοιχείων a_k, b_k, και ο μόνος όρος του αναπτύγματος ο οποίος δεν περιέχει ως παράγοντα ένα από τα στοιχεία a_k, $2 \leq k \leq n$, είναι ο όρος

$$s_1 = \prod_{k=2}^{n} b_k \in I_2 \cdots I_n$$

Έτσι μπορούμε να γράψουμε $1_R = x_1 + s_1$, όπου $x_1 \in I_1$ και $s_1 \in I_2 \cdots I_n$. Άρα $\forall r \in R$, είναι $r = r \cdot x_1 + r \cdot s_1 \in I_1 + (I_2 \cdots I_n)$, και επομένως: $R = I_1 + (I_2 \cdots I_n)$. Από την από την περίπτωση $n = 2$ τότε θα έχουμε $I_1 \cap (I_2 \cdots I_n) = I_1 \cdot (I_2 \cdots I_n)$. Όμως από την επαγωγική υπόθεση θα έχουμε $I_2 \cdots I_n = I_2 \cap \cdots \cap I_n$, και επομένως τελικά θα έχουμε: $I_1 \cap I_2 \cap \cdots \cap I_n = I_1 \cdot I_2 \cdots I_n$. ■

Παράδειγμα 8.1.33. Γενικά η έγκλειση $I \cdot J \subseteq I \cap J$ είναι γνήσια. Για παράδειγμα, αν $I = J = n\mathbb{Z}$, $n \geq 2$. Τότε $I \cap J = n\mathbb{Z}$, αλλά $I \cdot J = n\mathbb{Z} \cdot n\mathbb{Z} = n^2\mathbb{Z}$, βλέπε το Παράδειγμα 8.1.31, και προφανώς $n\mathbb{Z} \neq n^2\mathbb{Z}$.

Από την άλλη πλευρά, αν ο δακτύλιος R δεν είναι μεταθετικός, τότε $I \cdot J \subseteq I \cap J$, αλλά υπάρχουν μη μεταθετικοί δακτύλιοι R, οι οποίοι περιέχουν ιδεώδη I και J έτσι ώστε $I + J = R$ και $I \cdot J \neq I \cap J$. √

8.1.3 Διαμερίσεις της Μονάδας

Έστω R ένας δακτύλιος με μονάδα. Υπενθυμίζουμε ότι ένα στοιχείο $e \in R$ καλείται **ταυτοδύναμο**, αν $e^2 = e$. Για παράδειγμα, τα στοιχεία $1, 0$ είναι ταυτοδύναμα στοιχεία του R, τα *τετριμμένα ταυτοδύναμα στοιχεία* του R. Δύο στοιχεία $r, s \in R$ καλούνται **ορθογώνια** αν $r \cdot s = 0 = s \cdot r$.

Ορισμός 8.1.34. *Μια πεπερασμένη οικογένεια στοιχείων $\mathscr{D} = \{e_k\}_{k=1}^n$ του δακτυλίου R καλείται* **διαμέριση της μονάδας** *του R, αν:*

1. *Τα στοιχεία της οικογένειεας $\mathscr{D}$ είναι ταυτοδύναμα στοιχεία και ανά δύο είναι ορθογώνια:*

$$\forall k = 1, 2, \cdots, n: \quad e_k^2 = e_k \quad \text{και} \quad e_k \cdot e_l = 0 = e_l \cdot e_k, \quad 1 \leq k \neq l \leq n$$

2. $1_R = \sum_{k=1}^n e_k = e_1 + e_2 + \cdots + e_n$.

Μια διαμέριση της μονάδας $\mathscr{D} = \{e_k\}_{k=1}^n$ του δακτυλίου R καλείται **κεντρική διαμέριση της μονάδας** *του R, αν τα στοιχεία της διαμέρισης είναι κεντρικά:*

$$\forall k = 1,2,\cdots,n: \quad e_k \in \mathsf{Z}(R)$$

Έστω $R_i = (R_i, +, \cdot)$, $1 \le i \le n$, μια πεπερασμένη ακολουθία δακτυλίων (χρησιμοποιούμε πάντα τα ίδια σύμβολα για τις πράξεις πρόσθεσης και πολλαπλασιασμού, για τα μηδενικά στοιχεία, και τις μονάδες των δακτυλίων R_i, $1 \le i \le n$), και θεωρούμε τον δακτύλιο ευθύ γινόμενο

$$R := \prod_{i=1}^n R_i = \left\{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \le i \le n\right\}$$

όπου οι πράξεις πρόσθεσης και πολλαπλασιασμού επί του $\prod_{i=1}^n R_i$ ορίζονται, «κατά συνιστώσα», ως εξής:

$$+ : \prod_{i=1}^n R_i \times \prod_{i=1}^n R_i \longrightarrow \prod_{i=1}^n R_i, \qquad (r_1, r_2, \cdots, r_n) + (r_1', r_2', \cdots, r_n') = (r_1 + r_1', r_2 + r_2', \cdots, r_n + r_n')$$

$$\cdot : \prod_{i=1}^n R_i \times \prod_{i=1}^n R_i \longrightarrow \prod_{i=1}^n R_i, \qquad (r_1, r_2, \cdots, r_n) \cdot (r_1', r_2', \cdots, r_n') = (r_1 \cdot r_1', r_2 \cdot r_2', \cdots, r_n \cdot r_n')$$

και το μηδενικό στοιχείο του δακτυλίου $\prod_{i=1}^n R_i$ είναι η n-άδα $0 = (0,0,\cdots,0)$ και η μονάδα του είναι η n-άδα $1 = (1,1,\cdots,1)$.

Θέτοντας $e_k = (\underbrace{0,0,\cdots,0,1_{R_k},0,\cdots,0,0}_{k-\text{θέση}})$, $1 \le k \le n$, αποκτούμε μια κεντρική διαμέριση της μονάδας $\mathscr{D} = \{e_k\}_{k=1}^n$ του δακτυλίου R. Πράγματι, θα έχουμε

$$1_R = (1,1,\cdots,1) = (1,0,\cdots,0) + (0,1,\cdots,0) + \cdots + (0,0,\cdots,1) = e_1 + e_2 + \cdots + e_n$$

$$e_k \cdot e_l = (0,0,\cdots,0), \ \text{ αν } \ k \ne l \qquad \text{και} \qquad e_k \cdot e_l = \underbrace{(0,\cdots,0,1_{R_k},0,\cdots,0)}_{k-\text{θέση}} = e_k, \ \text{ αν } \ k = l$$

και για κάθε στοιχείο $(r_1, r_2, \cdots, r_n) \in \mathsf{Z}(R)$:

$$e_k \cdot (r_1, r_2, \cdots, r_n) = \underbrace{(0,\cdots,0,1_{R_k} \cdot r_k,0,\cdots,0)}_{k-\text{θέση}} = \underbrace{(0,\cdots,0,r_k \cdot 1_{R_k},0,\cdots,0)}_{k-\text{θέση}} = (r_1, r_2, \cdots, r_n) \cdot e_k$$

δηλαδή κάθε στοιχείο e_k ανήκει στο κέντρο του R, $1 \le k \le n$.

Η ακόλουθη Πρόταση χαρακτηρίζει την ύπαρξη κεντρικής διαμέρισης της μονάδας ενός δακτυλίου.

Πρόταση 8.1.35. *Για έναν δακτύλιο R, τα ακόλουθα είναι ισοδύναμα:*

1. *Ο δακτύλιος R διαθέτει μια κεντρική διαμέριση $\mathscr{D} = \{e_k\}_{k=1}^n$ της μονάδας.*
2. *Ο δακτύλιος R είναι το ευθύ άθροισμα μιας πεπερασμένης οικογένειας ιδεωδών I_k του R, $1 \le k \le n$.*

$$R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

Αν μία από τις παραπάνω δύο ισοδύναμες συνθήκες είναι αληθής, τότε στο 2. μπορούμε να επιλέξουμε $I_k = e_k R = R e_k$, $1 \le k \le n$, και στο 1. μπορούμε να επιλέξουμε τα e_k ως τους προσθετέους στην (μοναδική) γραφή $1_R = e_1 + e_2 + \cdots + e_n$.

Απόδειξη. 1. Έστω $\mathscr{D} = \{e_k\}_{k=1}^n$ μια κεντρική διαμέριση της μονάδας του R. Για κάθε $k = 1,2,\cdots,n$, θέτουμε:

$$I_k = e_k R = \left\{e_k r \in R \mid r \in R\right\}$$

Επειδή το στοιχείο e_k είναι κεντρικό, θα έχουμε $e_k r = r e_k$, $\forall k = 1,2,\cdots n$. Το σύνολο I_k είναι ένα δεξιό ιδεώδες του R και επειδή $e_k \in \mathsf{Z}(R)$, θα έχουμε $e_k R = I_k = R e_k$, δηλαδή το I_k είναι και αριστερό ιδεώδες του R, έτσι κάθε I_k είναι ένα ιδεώδες του R. Θα δείξουμε ότι $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$.

Πράγματι, θα έχουμε $1_R = e_1 + e_2 + \cdots + e_n$ και επομένως, $\forall r \in R$:

$$r = 1_R \cdot r = (e_1 + e_2 + \cdots + e_n) \cdot r = e_1 r + e_2 r + \cdots + e_n r \ \in \ I_1 + I_2 + \cdots + I_n \quad \Longrightarrow \quad R = I_1 + I_2 + \cdots + I_n$$

Έστω $x = x_1 + x_2 + \cdots + x_n \in I_1 + I_2 + \cdots + I_n$, όπου $x_k \in I_k$, $1 \leq k \leq n$, και υποθέτουμε ότι $x = 0$. Τότε θα έχουμε $x_k = e_k r_k$ για κάποια στοιχεία $r_k \in R$ και τότε, χρησιμοποιώντας ότι τα στοιχεία e_k είναι ταυτοδύναμα και ανά δύο ορθογώνια, για κάθε $1 \leq l \leq n$, θα έχουμε:

$$0 = x = e_l x = e_l \cdot (e_1 r_1 + e_2 r_2 + \cdots + e_n r_n) = e_l e_1 r_1 + e_l e_2 r_2 + \cdots + e_l e_n r_n = e_l e_l r_l = e_l r_l = x_l$$

Επομένως από την Πρόταση 8.1.25 έπεται ότι το άθροισμα ιδεωδών $I_1 + I_2 + \cdots + I_n$ είναι ευθύ και άρα $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$.

2. Υποθέτουμε ότι ο δακτύλιος R είναι το ευθύ άθροισμα $R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$ ιδεωδών I_k, $1 \leq k \leq n$. Τότε για τη μονάδα 1_R του R θα έχουμε ότι υπάρχουν στοιχεία $e_k \in I_k$, $1 \leq k \leq n$, έτσι ώστε:

$$1_R = e_1 + e_2 + \cdots + e_n, \quad \text{όπου} \quad e_k \in I_k, \quad 1 \leq k \leq n$$

Τότε για κάθε στοιχείο $x_k \in I_k$, θα έχουμε

$$x_k = 1_R x_k = e_1 x_k + e_2 x_k + \cdots + e_{k-1} x_k + e_k x_k + e_{k+1} x_k + \cdots + e_n x_k$$

Επειδή τα I_k είναι ιδεώδη και $e_j \in I_j$, θα έχουμε $e_j x_k \in I_j$, $1 \leq j \leq n$ και τότε επειδή το άθροισμα $I_1 \oplus \cdots \oplus I_n$ είναι ευθύ, θα έχουμε $e_j x_k = 0$, $1 \leq j \neq k \leq n$, και $e_k x_k = x_k$. Ιδιαίτερα επιλέγοντας $x_k = e_k \in I_k$, θα έχουμε ότι τα στοιχεία e_k είναι ταυτοδύναμα και ανά δύο ορθογώνια. Επομένως το σύνολο $\mathscr{D} = \{e_k\}_{k=1}^n$ είναι μια διαμέριση της μονάδας του R, η οποία επιπλέον είναι κεντρική. Πράγματι, έστω $r \in R$. Τότε

$$r = r \cdot 1_R = re_1 + re_2 + \cdots re_n = e_1 r + e_2 r + \cdots + e_n r = 1_R r = r$$

Επειδή τα I_k είναι ιδεώδη, επειδή $e_k r, re_k \in I_k$, $1 \leq k \leq n$, από την μοναδικότητα της γραφής στο ευθύ άθροισμα ιδεωδών, θα έχουμε $e_k r = re_k$, $1 \leq k \leq n$. Επειδή το r επιλέχθηκε τυχαία, έπεται ότι $e_k \in \mathsf{Z}(R)$, $1 \leq k \leq n$. ■

Παρατήρηση 8.1.36. Όταν η διαμέριση της μονάδας δεν είναι απαραίτητα κεντρική, τότε η απόδειξη της Πρότασης 8.1.35 δείχνει ότι για έναν δακτύλιο R, τα ακόλουθα είναι ισοδύναμα:

1. Ο δακτύλιος R διαθέτει μια διαμέριση $\mathscr{D} = \{e_k\}_{k=1}^n$ της μονάδας.
2. Ο δακτύλιος R είναι το ευθύ άθροισμα μιας πεπερασμένης οικογένειας αριστερών ιδεωδών I_k του R, $1 \leq k \leq n$:
$$R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$$
3. Ο δακτύλιος R είναι το ευθύ άθροισμα μιας πεπερασμένης οικογένειας δεξιών ιδεωδών J_k του R, $1 \leq k \leq n$:
$$R = J_1 \oplus J_2 \oplus \cdots \oplus J_n$$

Αν μια από τις παραπάνω ισοδύναμες συνθήκες είναι αληθής, τότε:

$$I_k = Re_k \quad \text{και} \quad J_k = e_k R, \quad 1 \leq k \leq n \ \blacktriangle$$

Παράδειγμα 8.1.37. Έστω $e \in R$ ένα ταυτοδύναμο στοιχείο του δακτυλίου R. Επειδή $1_R = e + 1_R - e$ και

$$(1_R - e)^2 = (1_R - e) \cdot (1_R - e) = 1_R - e - e + e^2 = 1_R - e, \quad e \cdot (1_R - e) = e - e^2 = e - e = 0, \quad (1_R - e) \cdot e = e - e^2 = e - e = 0$$

έπεται ότι το σύνολο $\{e, 1_R - e\}$ είναι μια διαμέριση της μονάδας του R, και επομένως θα έχουμε ότι ο δακτύλιος R είναι ευθύ άθροισμα αριστερών ιδεωδών

$$R = Re \oplus R(1_R - e)$$

και ευθύ άθροισμα δεξιών ιδεώδων

$$R = eR \oplus (1_R - e)R$$

Αν το ταυτοδύναμο στοιχείο e είναι κεντρικό, τότε προφανώς και το ταυτοδύναμο στοιχείο $1_R - e$ είναι κεντρικό, και θα έχουμε $I := eR = Re$ και $J := (1_R - e)R = R(1_R - e)$. Έτσι ο δακτύλιος R είναι ευθύ άθροισμα ιδεωδών

$$R = I \oplus J \quad \surd$$

8.2 Ομομορφισμοί Δακτυλίων και Δακτύλιοι Πηλίκα

Στην παρούσα ενότητα θα μελετήσουμε την θεμελιώδη έννοια του ομομορφισμού δακτυλίων, η οποία θα μας επιτρέψει να συγκρίνουμε δύο δακτυλίους, και της θεμελιώδους κατασκευής του δακτυλίου πηλίκου ενός δακτυλίου ως προς ένα ιδεώδες.

8.2.1 Δακτύλιοι Πηλίκα

Έστω $R = (R, +, \cdot)$ ένας δακτύλιος και I μια υποομάδα της προσθετικής ομάδας $(R, +)$. Επειδή η ομάδα $(R, +)$ είναι αβελιανή, κάθε υποομάδα της είναι κανονική, και επομένως η υποομάδα $I \leq R$ είναι κανονική. Τότε ορίζεται η προσθετική ομάδα πηλίκο $(R/I, +)$ η οποία είναι αβελιανή, και τα στοιχεία της είναι (αριστερές) πλευρικές κλάσεις

$$R/I = \{r + I \subseteq R \mid r \in R\}$$

όπου

$$r + I = \{r + x \in R \mid x \in I\} \quad \text{και} \quad r + I = s + I \iff r - s \in I$$

Υπενθυμίζουμε ότι η πράξη πρόσθεσης στην ομάδα πηλίκο ορίζεται ως εξής:

$$+ : R/I \times R/I \longrightarrow R/I, \quad (r + I) + (s + I) = (r + s) + I \tag{8.4}$$

Καθώς ο δακτύλιος R είναι εφοδιασμένος με την πράξη του πολλαπλασιασμού, είναι εύλογο να αναρωτηθούμε αν η προσθετική ομάδα $(R/I, +)$ μπορεί να εφοδιαστεί με τη «φυσικά» επαγόμενη πράξη πολλαπλασιασμού

$$\cdot : R/I \times R/I \longrightarrow R/I, \quad (r + I) \cdot (s + I) = (r \cdot s) + I \tag{8.5}$$

έτσι ώστε η τριάδα $(R/I, +, \cdot)$ να είναι δακτύλιος. Σημειώνουμε ότι συμβολίζουμε με το ίδιο σύμβολο «$\cdot$» την πράξη πολλαπλασιασμού του δακτυλίου R και την ως άνω νέα πράξη επί της ομάδας πηλίκου R/I. Η παρακάτω παρατήρηση δίνει έναν επιπρόσθετο λόγο για τον οποίον τα ιδέωδη παίζουν σημαντικό ρόλο στη Θεωρία Δακτυλίων, ανάλογο με τον ρόλο που παίζουν οι κανονικές υποομάδες στη Θεωρία Ομάδων.

Η πράξη (8.5) είναι μια καλά ορισμένη πράξη επί της ομάδας $R/I \iff$ η υποομάδα I είναι ιδεώδες του R.

«$\Longrightarrow$» Υποθέτουμε ότι η πράξη (8.5) είναι μια καλά ορισμένη πράξη[1] επί της ομάδας πηλίκο R/I. Έστω $x \in I$ και $r \in R$. Τότε, επειδή $x \in I$, θα έχουμε $x + I = 0 + I = I$. Επειδή η πράξη «$\cdot$» είναι καλά ορισμένη, θα έχουμε:

$$x+I = 0+I \quad \text{και} \quad r+I = r+I \quad \Longrightarrow \quad x\cdot r+I = 0\cdot r+I = I \quad \text{και} \quad r\cdot x+I = r\cdot 0+I = I \quad \Longrightarrow \quad x\cdot r \in I \quad \text{και} \quad r\cdot x \in I$$

[1] Υπενθυμίζουμε ότι μια πράξη «$\cdot$» επί της ομάδας πηλίκου R/I είναι καλά ορισμένη αν και μόνο αν, $\forall r, r', s, s' \in R$:

$$r + I = r' + I \quad \text{και} \quad s + I = s' + I \quad \Longrightarrow \quad (r \cdot s) + I = (r' \cdot s') + I$$

και επομένως η υποομάδα I είναι ιδέωδες του R.

«$\Longleftarrow$» Υποθέτουμε ότι το I είναι ένα ιδεώδες του R, και έστω r, r', s, s' στοιχεία του R, έτσι ώστε:

$$r + I = r' + I \quad \text{και} \quad s + I = s' + I, \qquad \text{επομένως} \qquad r - r' \in I \quad \text{και} \quad s - s' \in I$$

Τότε, πολλαπλασιάζοντας την πρώτη διαφορά από τα δεξιά με το s και την δεύτερη διαφορά με το r' από τα αριστερά, και εκμεταλευόμενοι ότι το I είναι ιδεώδες, θα έχουμε:

$$(r - r') \cdot s = r \cdot s - r' \cdot s \in I \quad \text{και} \quad r' \cdot (s - s') = r' \cdot s - r' \cdot s' \in I \quad \Longrightarrow$$

$$(r \cdot s - r' \cdot s) + (r' \cdot s - r' \cdot s') = r \cdot s - r' \cdot s' \in I \quad \Longrightarrow \quad r \cdot s + I = r' \cdot s' + I$$

και άρα η πράξη «$\cdot$» επί της αβελιανής ομάδας R/I είναι καλά ορισμένη. ▲

Η παραπάνω ανάλυση μας επιτρέπει να διατυπώσουμε και να αποδείξουμε την ακόλουθη Πρόταση.

Πρόταση 8.2.1. *Έστω ότι $R = (R, +, \cdot)$ είναι ένας δακτύλιος και I είναι ένα ιδεώδες του R. Τότε η τριάδα $(R/I, +, \cdot)$, όπου:*

$$+ : \ R/I \times R/I \longrightarrow R/I, \qquad (r + I) + (s + I) = (r + s) + I$$

$$\cdot : \ R/I \times R/I \longrightarrow R/I, \qquad (r + I) \cdot (s + I) = (r \cdot s) + I$$

είναι ένας δακτύλιος με μηδενικό στοιχείο την πλευρική κλάση $0 + I = I$ και μονάδα την πλευρική κλάση $1_{R/I} = 1_R + I$.

Επιπλέον, αν ο δακτύλιος R είναι μεταθετικός, τότε και ο δακτύλιος R/I είναι μεταθετικός.

Απόδειξη. Σύμφωνα με την προηγηθείσα ανάλυση, επειδή το I είναι ιδεώδες του R, η πράξη (8.5) είναι μια καλά ορισμένη πράξη στην προσθετική ομάδα $(R/I, +)$. Έστω $r_1, r_2, r_3 \in R$. Τότε, χρησιμοποιώντας ότι ο πολλαπλασιασμός του R είναι προσεταιριστική πράξη, θα έχουμε:

$$(r_1 + I) \cdot \big((r_2 + I) \cdot (r_3 + I)\big) = (r_1 + I) \cdot \big((r_2 \cdot r_3) + I\big) = \big(r_1 \cdot (r_2 \cdot r_3)\big) + I = \big((r_1 \cdot r_2) \cdot r_3\big)\big) + I =$$

$$= \big((r_1 \cdot r_2) + I\big) \cdot (r_3 + I) = \big((r_1 + I) \cdot (r_2 + I)\big) \cdot (r_3 + I)$$

Άρα ο πολλαπλασιασμός του R/I είναι προσεταιριστική πράξη.

Επίσης, χρησιμοποιώντας ότι ο πολλαπλασιασμός του R ικανοποιεί την επιμεριστική ιδιότητα ως προς την πρόσθεση, θα έχουμε:

$$(r_1 + I) \cdot \big((r_2 + I) + (r_3 + I)\big) = (r_1 + I) \cdot \big((r_2 + r_3) + I\big) = \big(r_1 \cdot (r_2 + r_3)\big) + I = (r_1 \cdot r_2 + r_1 \cdot r_3) + I =$$

$$= \big((r_1 \cdot r_2) + I\big) + \big((r_1 \cdot r_3) + I\big) = \big((r_1 + I) \cdot (r_2 + I)\big) + \big((r_1 + I) \cdot (r_3 + I)\big)$$

και παρόμοια: $\big((r_1 + I) + (r_2 + I)\big) \cdot (r_3 + I) = \big((r_1 + I) \cdot (r_3 + I)\big) + \big((r_2 + I) \cdot (r_3 + I)\big)$. Επομένως ικανοποιείται η επιμεριστική ιδιότητα του πολλαπλασιασμού του R/I ως προς την πρόσθεση.

Τέλος, για κάθε στοιχείο $r + I \in R/I$ θα έχουμε:

$$(r + I) \cdot (1_R + I) = (r \cdot 1_R) + I = r + I = (1_R \cdot r) + I = (1_R + I) \cdot (r + I)$$

και επομένως η πλευρική κλάση $1_R + I$ είναι η μονάδα του R/I.

Αν ο δακτύλιος R είναι μεταθετικός, τότε από την ακόλουθη σχέση

$$(r + I) \cdot (s + I) = (r \cdot s) + I = (s \cdot r) + I = (s + I) \cdot (r + I)$$

έπεται ότι και ο δακτύλιος R/I είναι μεταθετικός. ■

Ορισμός 8.2.2. *Ο δακτύλιος R/I της πρότασης 8.2.1 καλείται ο* **δακτύλιος πηλίκο** *του δακτυλίου R ως προς το ιδεώδες I.*

Κάποιες ιδιότητες, όπως η μεταθετικότητα, κληρονομούνται από έναν δακτύλιο R στον δακτύλιο πηλίκο R/I ως προς ένα ιδεώδες I του R. Οι περισσότερες σημαντικές ιδιότητες όμως δεν κληρονομούνται από τον R στον R/I. Από την άλλη πλευρά υπάρχουν ιδιότητες του δακτυλίου πηλίκου R/I τις οποίες δεν ικανοποιεί ο δακτύλιος R. Τέτοιες ιδιότητες περιγράφονται στο ακόλουθο παράδειγμα. Αργότερα θα δούμε και άλλες τέτοιες ιδιότητες.

Παράδειγμα 8.2.3. Θεωρούμε το ιδεώδες $n\mathbb{Z} \subseteq \mathbb{Z}$ του δακτυλίου $\mathbb{Z}$ των ακεραίων, όπου $n \geq 2$. Τότε αποκτούμε τον δακτύλιο πηλίκο $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$.

1. Αν ο θετικός ακέραιος n είναι σύνθετος, τότε γνωρίζουμε από την Πρόταση 7.4.16 ότι ο δακτύλιος $\mathbb{Z}_n$ έχει διαιρέτες του μηδενός, και άρα δεν είναι ακέραια περιοχή, σε αντίθεση με τον δακτύλιο $\mathbb{Z}$ ο οποίος είναι ακέραια περιοχή.

2. Αν ο θετικός ακέραιος n είναι πρώτος, τότε γνωρίζουμε από την Πρόταση 7.4.16 ότι ο δακτύλιος $\mathbb{Z}_n$ είναι σώμα, σε αντίθεση με τον δακτύλιο $\mathbb{Z}$ ο οποίος δεν είναι σώμα. $\surd$

Στο παραπάνω παράδειγμα βλέπουμε ότι ξεκινώντας από τον δακτύλιο $\mathbb{Z}$ και ένα στοιχείο του $n \in \mathbb{Z}$, κατασκευάσαμε έναν νέο δακτύλιο, τον $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, στον οποίο το στοιχείο n, δηλαδή η πλευρική κλάση $n + n\mathbb{Z}$, είναι ίσο με μηδέν. Αυτή η συμπεριφορά είναι τυπική όταν θέλουμε να «μηδενίσουμε» στοιχεία ενός δακτυλίου, όπως δείχνει το ακόλουθο παράδειγμα. Αυτό μπορεί να γίνει εισάγοντας νέες σχέσεις σε έναν δακτύλιο. Επομένως *«ο δακτύλιος πηλίκο R/I προκύπτει τροποποιώντας τον αρχικό δακτύλιο R, εισάγοντας «σχέσεις» οι οποίες προκύπτουν από τα στοιχεία του ιδεώδους I»*.

Παράδειγμα 8.2.4. Έστω $a_1, a_2, \cdots, a_n$ στοιχεία ενός δακτυλίου R. Θέλουμε να κατασκευάσουμε με βέλτιστο τρόπο έναν δακτύλιο S στον οποίο τα στοιχεία $a_1, a_2, \cdots, a_n$ να «μηδενίζονται» με φυσικό τρόπο, δηλαδή να ικανοποιούνται οι σχέσεις: $a_1 = 0$, $a_2 = 0$, $\cdots$, $a_n = 0$ στον δακτύλιο S.

Θεωρούμε το (αμφίπλευρο) ιδεώδες $I = (a_1, a_2, \cdots, a_n)$ του R το οποίο παράγεται από τα στοιχεία $a_1, a_2, \cdots, a_n$, και έστω ο δακτύλιος πηλίκο

$$S = R/(a_1, a_2, \cdots, a_n)$$

Τότε, για κάθε $1 \leq i \leq n$, θέτοντας $\underline{a_i} = a_i + I$ θα έχουμε

$$\underline{a_i} = 0, \quad \underline{a_2} = 0, \cdots, \quad \underline{a_n} = 0, \qquad \text{στον δακτύλιο} \quad R/(a_1, a_2, \cdots, a_n)$$

Αν $x, y \in R$, τότε τα στοιχεία $\underline{x} = x + I$ και $\underline{y} = y + I$ είναι ίσα αν και μονον αν $x - y \in I$. Υποθέτοντας για ευκολία ότι ο δακτύλιος R είναι μεταθετικός, θα έχουμε $I = \left\{\sum_{i=1}^n r_i a_i \in R \mid r_i \in R,\ 1 \leq i \leq n\right\}$ και άρα $x - y \in I$ αν και μονον αν $x - y = \sum_{i=1}^n r_i a_i$, για κάποια στοιχεία $r_i \in R$, $1 \leq i \leq n$. Ιδιαίτερα θα έχουμε $\underline{x} = 0$ στον δακτύλιο S αν το στοιχείο x στον δακτύλιο R είναι της μορφής $x = \sum_{i=1}^n r_i a_i$, δηλαδή η σχέση $\underline{x} = 0$ είναι απόρροια των σχέσεων $\underline{a_i} = 0$, $1 \leq i \leq n$. $\surd$

Το επόμενο Παράδειγμα είναι χαρακτηριστικό για τη δομή του δακτυλίου πηλίκο (τα στοιχεία διαιρετότητας πολυωνύμων υπεράνω του $\mathbb{R}$ τα οποία θα χρησιμοποιήσουμε θεωρούνται γνωστά και θα επαναληφθούν σε μεγαλύτερη γενικότητα στο Κεφάλαιο 9).

Παράδειγμα 8.2.5. Στον δακτύλιο πολυωνύμων $\mathbb{R}[t]$ θεωρούμε το κύριο ιδεώδες (t^2+1) το οποίο παράγεται από το πολυώνυμο $t^2 + 1$:

$$(t^2+1) = \left\{P(t)(t^2+1) \in \mathbb{R}[t] \mid P(t) \in \mathbb{R}[t]\right\}$$

Ένα τυπικό στοιχείο του δακτυλίου πηλίκου $\mathbb{R}[t]/(t^2+1)$ είναι της μορφής $P(t) + (t^2+1)$. Από την Ευκλείδεια Διαίρεση του πολυωνύμου $P(t)$ με το πολυώνυμο $t^2 + 1$, θα έχουμε:

$$P(t) = Q(t)(t^2+1) + R(t), \quad \text{και:} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < 2$$

1. Αν $R(t) = 0$, τότε $P(t) = Q(t)(t^2+1) \in (t^2+1)$, και άρα το στοιχείο $P(t) + (t^2+1)$ είναι το μηδενικό στοιχείο του δακτυλίου πηλίκου $\mathbb{R}[t]/(t^2+1)$:

$$P(t) + (t^2+1) = (t^2+1)$$

2. Αν $\deg R(t) < 2$, θα έχουμε ότι το $R(t)$ είναι της μορφής $R(t) = a + bt$, όπου $a, b \in \mathbb{R}$ και $(a,b) \neq (0,0)$. Άρα
$$P(t) + (t^2+1) = a + bt + (t^2+1)$$
Ιδιαίτερα, επιλέγοντας το πολυώνυμο $P(t) = t^2$, θα έχουμε $t^2 = 1(t^2+1) - 1$, άρα σ' αυτή την περίπτωση $a = -1$ και $b = 0$, και επομένως
$$t^2 + (t^2+1) = -1 + (t^2+1) = -1_{\mathbb{R}[t]/(t^2+1)}$$
Επειδή
$$\big(t + (t^2+1)\big) \cdot \big(t + (t^2+1)\big) = t^2 + (t^2+1) = -1 + (t^2+1)$$
Θέτοντας $j = t + (t^2+1)$, η παραπάνω ανάλυση δείχνει ότι $j^2 = -1_{\mathbb{R}[t]/(t^2+1)}$, και κάθε στοιχείο του $\mathbb{R}[t]/(t^2+1)$ είναι της μορφής:
$$a + bt + (t^2+1) = \big(a + (t^2+1)\big) + \big(bt + (t^2+1)\big) = a\big(1 + (t^2+1)\big) + b\big(t + (t^2+1)\big) = a1_{\mathbb{R}[t]/(t^2+1)} + bj$$
$$j^2 = -1_{\mathbb{R}[t]/(t^2+1)}$$

Παραλείποντας την μονάδα $1_{\mathbb{R}[t]/(t^2+1)}$ του δακτυλίου $\mathbb{R}[t]/(t^2+1)$, έπεται ότι
$$\mathbb{R}[t]/(t^2+1) = \big\{a + bj \in \mathbb{R}[t]/(t^2+1) \mid a, b \in \mathbb{R}\big\}$$
η πρόσθεση και ο πολλαπλασιασμός των στοιχείων του $\mathbb{R}[t]/(t^2+1)$ παίρνουν τη μορφή:
$$(a+bj) + (c+dj) = (a+c) + (b+d)j$$
$$(a+bj) \cdot (c+dj) = ac + adj + bcj + bdj^2 = (ac - bd) + (ad + bc)j$$
Είναι τώρα φανερό ότι η αντιστοιχία
$$\mathbb{C} \ni a + bi \quad \longmapsto \quad a + bj \in \mathbb{R}[t]/(t^2+1)$$
είναι μια απεικόνιση η οποία είναι «1-1» και «επί», διατηρεί τις πράξεις πρόσθεσης και πολλαπλασιασμού στους δακτυλίους $\mathbb{C}$ και $\mathbb{R}[t]/(t^2+1)$, και στέλνει την μονάδα του $\mathbb{C}$ στην μονάδα του $\mathbb{R}[t]/(t^2+1)$. $\surd$

Απεικονίσεις του τύπου του Παραδείγματος 8.2.5 μεταξύ δακτυλίων καλούνται ισομορφισμοί δακτυλίων, και μας επιτρέπουν να ταυτίσουμε δύο δακτυλίους οι οποίοι έχουν τις ίδιες δομικές ιδιότητες, δηλαδή ιδιότητες οι οποίες απορρέουν από τα αξιώματα δακτυλίου. Η γενικότερη έννοια του ομομορφισμού δακτυλίων η οποία υπονοείται αποτελεί αντικείμενο της επόμενης υποενότητας.

8.2.2 Ομομορφισμοί Δακτυλίων

Θεωρούμε δύο δακτυλίους R και S. Όπως και στη θεωρία ομάδων, συμβολίζουμε τις πράξεις πρόσθεσης και πολλαπλασιασμού στους δακτυλίους R και S με τα ίδια σύμβολα, έτσι θα γράφουμε: $R = (R, +, \cdot)$ και $S = (S, +, \cdot)$. Ο πλέον φυσικός τρόπος να συγκρίνουμε ή να συσχετίσουμε τους δακτυλίους R και S είναι μέσω μιας απεικόνισης η οποία διατηρεί τις πράξεις μέσω των οποίων ορίζονται οι δακτύλιοι, καθώς και τις μονάδες αυτών.

Ορισμός 8.2.6. *Μια απεικόνιση $f\colon R \longrightarrow S$ καλείται* **ομομορφισμός δακτυλίων**, *αν, $\forall x, y \in R$:*
$$f(x+y) = f(x) + f(y), \qquad f(x \cdot y) = f(x) \cdot f(y), \qquad f(1_R) = 1_S$$

Ένας ομομορφισμός δακτυλίων καλείται:

1. **μονομορφισμός δακτυλίων**, *αν η απεικόνιση f είναι «1-1».*
2. **επιμορφισμός δακτυλίων**, *αν η απεικόνιση f είναι «επί».*

3. **ισομορφισμός δακτυλίων**, *αν η απεικόνιση f είναι «1-1» και «επί».*

Ένας ομομορφισμός δακτυλίων $f\colon R \longrightarrow R$ καλείται **ενδομορφισμός** του R, και ένας ισομορφισμός $f\colon R \longrightarrow R$ καλείται **αυτομορφισμός**. Σημειώνουμε ότι, για μια απεικόνιση $f\colon R \longrightarrow S$ μεταξύ δακτυλίων R και S, τα ακόλουθα είναι ισοδύναμα:

1. Η f είναι ένας ομομορφισμός δακτυλίων.
2. Η $f\colon (R,+) \longrightarrow (S,+)$ είναι ομομορφισμός των υποκείμενων προσθετικών ομάδων, και η απεικόνιση $f\colon (R,\cdot) \longrightarrow (S,\cdot)$ είναι ομομορφισμός των υποκείμενων πολλαπλασιαστικών μονοειδών.

Παρατήρηση 8.2.7. Για κάθε δακτύλιο R, η ταυτοτική απεικόνιση Id_R είναι ένας ενδομορφισμός του R.

Αντίθετα, αν R και S είναι δακτύλιοι, ο μηδενικός ομομορφισμός των αντίστοιχων προσθετικών ομάδων ομάδων $0\colon (R,+) \longrightarrow (S,+)$, $0(x) = 0_S$ **δεν είναι** ομομορφισμός δακτυλίων, εκτός αν $0_S = 1_S$, δηλαδή εκτός αν ο S είναι ο μηδενικός δακτύλιος.

Στην βιβλιογραφία συναντάται επίσης ο ορισμός ομομορφισμού δακτυλίου $f\colon R \longrightarrow S$ χωρίς να ικανοποιείται απαραίτητα η ιδιότητα $f(1_R) = 1_S$ (είτε οι δακτύλιοι έχουν μονάδα είτε όχι). Με αυτόν τον ορισμό ο μηδενικός ομομορφισμός παραπάνω είναι ομομορφισμός δακτυλίων. Στις παρούσες σημειώσεις δεν θα ακολουθήσουμε αυτόν τον πιο γενικό ορισμό.

Υπό προϋποθέσεις, μια απεικόνιση $f\colon R \longrightarrow S$ μεταξύ δακτυλίων R και S, η οποία ικανοποιεί τις δύο πρώτες ιδιότητες, $\forall x, y \in R$: $f(x+y) = f(x) + f(y)$ και $f(x\cdot y) = f(x)\cdot f(y)$, ικανοποιεί και την τρίτη ιδιότητα $f(1_R) = 1_S$, και άρα είναι ομομορφισμός δακτυλίων. Κάποιες από αυτές τις προϋποθέσεις είναι οι εξής:

1. Η απεικόνιση f είναι «επί».
2. $f \neq 0$, και ο δακτύλιος S είναι ακέραια περιοχή.

Η απόδειξη αφήνεται ως Άσκηση, βλέπε την Άσκηση 8.5.1. ▲

Στοιχειώδεις Ιδιότητες

Πριν περάσουμε στην ανάπτυξη και ανάλυση παραδειγμάτων ομομορφισμών δακτυλίων, θα δούμε κάποιες στοιχειώδεις ιδιότητες ομομορφισμών δακτυλίων. Επίσης θα μελετήσουμε συναφείς έννοιες οι οποίες προκύπτουν άμεσα από τον ορισμό ομομορφισμού δακτυλίων.

Πρόταση 8.2.8. 1. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Αν $x, y, x_1, \cdots, x_n \in R$, τότε:*

   (α΄) $f(0_R) = 0_S$, $f(x-y) = f(x) - f(y)$, $f(\sum_{k=1}^n x_k) = \sum_{k=1}^n f(x_k)$.

   (β΄) $f(x_1 \cdot x_2 \cdots x_n) = f(x_1)\cdot f(x_2)\cdots f(x_n)$.
   Ιδιαίτερα: $f(x^n) = f(x)^n$, $\forall n \geq 0$.

   (γ΄) Αν το στοιχείο $x \in R$ είναι αντιστρέψιμο, τότε και το στοιχείο $f(x) \in S$ είναι αντιστρέψιμο και:

$$f(x)^{-1} = f(x^{-1})$$

2. *Η σύνθεση ομομορφισμών δακτυλίων είναι ομομορφισμός δακτυλίων.*
3. *Αν $f\colon R \longrightarrow S$ είναι ένας ισομορφισμός δακτυλίων, τότε η αντίστροφη απεικόνιση $f^{-1}\colon S \longrightarrow R$, είναι ένας ισομορφισμός δακτυλίων.*
4. *Ένας ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$ είναι ισομορφισμός δακτυλίων αν και μονον αν υπάρχει ομομορφισμός δακτυλίων $f^{-1}\colon S \longrightarrow R$, έτσι ώστε:*

$$f \circ g = \mathrm{Id}_S \quad \text{και} \quad g \circ f = \mathrm{Id}_R$$

Απόδειξη. Χρησιμοποιούμε ότι ένας ομομορφισμός δακτυλίων είναι ιδιαίτερα ένας ομομορφισμός των υποκείμενων προσθετικών ομάδων, και των αντίστοιχων πολλαπλασιαστικών μονοειδών. Άρα ισχύουν τα συμπεράσματα των αντίστοιχων Προτάσεων 1.4.22, 1.4.34 και 2.8.8 από τη Θεωρία Μονοειδών και τη Θεωρία Ομάδων. Συνδυάζοντας αυτές τις προτάσεις, η απόδειξη των ισχυρισμών της Πρότασης είναι άμεση και αφήνεται ως Άσκηση στον αναγνώστη. ■

Αν $f\colon R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων, τότε από την Πρόταση 1.4.23, εφαρμοσμένη στον επαγόμενο ομομορφισμό πολλαπλασιαστικών μονοειδών $(R,\cdot)$ και $(S,\cdot)$, έπεται άμεσα η ακόλουθη συνέπεια.

Πόρισμα 8.2.9. *Ένας ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$ επάγει έναν ομομορφισμό ομάδων*

$$f\colon \mathsf{U}(R) \longrightarrow \mathsf{U}(S), \quad x \longmapsto f(x)$$

μεταξύ των ομάδων των αντιστρέψιμων στοιχείων των δακτυλίων R και S.

Πρόταση 8.2.10. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων.*

1. *Αν T είναι ένας υποδακτύλιος του R, τότε το υποσύνολο $f(T)$ είναι υποδακτύλιος του S.*
2. *Αν T είναι ένα ιδεώδες του R και η f είναι επιμορφισμός, τότε το υποσύνολο $f(T)$ είναι ιδεώδες του S.*
3. *Αν T είναι ένας υποδακτύλιος (ιδεώδες) του S, τότε το υποσύνολο $f^{-1}(T)$ είναι υποδακτύλιος (ιδεώδες) του R.*

Απόδειξη. 1. Έστω ότι T είναι ένας υποδακτύλιος του R, τότε $1_R \in T$ και τότε $1_S = f(1_R) \in f(T)$. Έστω $x, y \in f(T)$. Τότε $f(z) = x$ και $f(w) = y$, για κάποια $z, w \in T$. Επειδή το T είναι υποδακτύλιος του R, θα έχουμε $z - w \in T$ και $z \cdot w \in T$, και τότε:

$$x - y = f(z) - f(w) = f(z - w) \in f(T) \qquad \text{και} \qquad x \cdot y = f(z) \cdot f(w) = f(z \cdot w) \in f(T)$$

Άρα το υποσύνολο $f(T)$ είναι ένας υποδακτύλιος του S.

2. Αν T είναι ένα ιδεώδες του R, τότε $0_R \in T$ και άρα $0_S = f(0_R) \in f(T)$, και από το μέρος 1. το υποσύνολο $f(T)$ είναι υπομάδα της προσθετικής ομάδας $(S,+)$. Αν $s \in S$, τότε επειδή η f είναι επιμορφισμός, θα έχουμε $s = f(r)$, για κάποιο $r \in R$. Επειδή το υποσύνολο T είναι ιδεώδες του R, θα έχουμε $r \cdot x \in T$ και $x \cdot r \in T$, $\forall x \in T$. Τότε, για κάθε στοιχείο $x = f(z) \in f(T)$, όπου $z \in T$, θα έχουμε:

$$s \cdot x = f(r) \cdot f(z) = f(r \cdot z) \in f(T) \qquad \text{και} \qquad x \cdot s = f(z) \cdot f(r) = f(z \cdot r) \in f(T)$$

Άρα το υποσύνολο $f(T)$ είναι ιδεώδες του S.

3. Έστω ότι T είναι ένας υποδακτύλιος (ιδεώδες) του S. Τότε $0_S \in T$ και επειδή $f(0_R) = 0_S$, θα έχουμε $0_R \in f^{-1}(T)$. Έστω $r \in R$, και $x, y \in f^{-1}(T)$. Τότε $f(x), f(y) \in T$ και επειδή το T είναι υποδακτύλιος, αντίστοιχα ιδεώδες, του S, θα έχουμε $f(x) - f(y) \in T$ και $f(x) \cdot f(y) \in T$, αντίστοιχα $f(r) \cdot f(x) \in T$ και $f(x) \cdot f(r) \in T$. Τότε:

$$f(x) - f(y) = f(x - y) \in T \implies x - y \in f^{-1}(T) \quad \text{και} \quad f(x) \cdot f(y) = f(x \cdot y) \in T \implies x \cdot y \in f^{-1}(T)$$

$$f(r) \cdot f(x) = f(r \cdot y) \ \text{ και } \ f(x) \cdot f(r) = f(x \cdot r) \in T \implies r \cdot x \ \text{ και } \ x \cdot r \in f^{-1}(T)$$

Άρα το υποσύνολο $f^{-1}(T)$ είναι υποδακτύλιος (ιδεώδες) του R. ■

Όπως και στη Θεωρία Ομάδων, η Πρόταση 8.2.10 μας οδηγεί φυσιολογικά στον ακόλουθο ορισμό.

Ορισμός 8.2.11. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων.*

1. *Το υποσύνολο $f^{-1}(0_S) := \mathsf{Ker}(f)$ καλείται* **πυρήνας** *του ομομορφισμού f:*

$$\mathsf{Ker}(f) = \{x \in R \mid f(x) = 0_S\}$$

2. *Το υποσύνολο* $f(R) := \mathsf{Im}(f)$ *καλείται* **εικόνα** *του ομομορφισμού* f*:*

$$\mathsf{Im}(f) = \{f(x) \in S \mid x \in R\}$$

Ώς άμεση συνέπεια της Πρότασης 8.2.10 και της παρατήρησης ότι κάθε ομομορφισμός δακτυλίων είναι ομομορφισμός των υποκείμενων προσθετικών ομάδων, έχουμε το ακόλουθο Πόρισμα.

Πόρισμα 8.2.12. *Έστω* $f\colon R \longrightarrow S$ *ένας ομομορφισμός δακτυλίων.*

1. *Ο πυρήνας* $\mathsf{Ker}(f)$ *είναι ένα ιδεώδες του* R*.*
2. *Η εικόνα* $\mathsf{Im}(f)$ *του* f *είναι ένας υποδακτύλιος του* S*.*

Ο ομομορφισμός f *είναι μονομορφισμός, αντίστοιχα επιμορφισμός, αν και μόνο αν* $\mathsf{Ker}(f) = \{0_R\}$*, αντίστοιχα,* $\mathsf{Im}(f) = S$*.*

Παραδείγματα Ομομορφισμών Δακτυλίων

Το υπόλοιπο της παρούσας υποενότητας θα αφιερωθεί σε μια σειρά παραδειγμάτων ομομορφισμών δακτυλίων.

Παράδειγμα 8.2.13. Έτσω $S \subseteq R$ ένας υποδακτύλιος ενός δακτυλίου R. Τότε η απεικόνιση έγκλεισης

$$\iota_S\colon S \longrightarrow R, \quad \iota_S(x) = x$$

είναι ένας μονομορφισμός δακτυλιών, ο οποίος καλείται **μονομορφισμός κανονικής έγκλεισης**. $\surd$

Παράδειγμα 8.2.14. Για κάθε δακτύλιο R η απεικόνιση

$$\phi\colon \mathbb{Z} \longrightarrow R, \quad \phi(n) = n \cdot 1_R$$

είναι ένας ομομορφισμός δακτυλίων, και είναι μοναδικός με την έννοια ότι κάθε άλλος ομομορφισμός δακτυλίων $f\colon \mathbb{Z} \longrightarrow R$, συμπίπτει με τον ϕ.

Πράγματι, από τις Προτάσεις 7.1.4 και 7.1.5, θα έχουμε $\phi(1) = 1 \cdot 1_R = 1_R$, και:

$$\phi(n+m) = (n+m)\cdot 1_R = n\cdot 1_R + m \cdot 1_R = \phi(n) + \phi(m), \quad \phi(nm) = (nm)\cdot 1_R = (n\cdot 1_R)\cdot(m\cdot 1_R) = \phi(n)\cdot\phi(m)$$

και άρα η απεικόνιση ϕ είναι ομομορφισμός δακτυλίων. Άν $f\colon \mathbb{Z} \longrightarrow R$ είναι ένας άλλος ομομορφισμός δακτυλίων, τότε θα έχουμε $f(0) = 0_R = \phi(0)$. Επίσης θα έχουμε εξ ορισμού $f(1) = 1_R$, και αν $n \geq 1$, τότε χρησιμοποιώντας ότι ο f είναι ομομορφισμός δακτυλίων θα έχουμε:

$$f(n) = f(\underbrace{1+\cdots+1}_{n-\text{παράγοντες}}) = \underbrace{f(1)+\cdots+f(1)}_{n-\text{παράγοντες}} = \underbrace{1_R+\cdots+1_R}_{n-\text{παράγοντες}} = n\cdot 1_R = \phi(n)$$

Τέλος, αν $n < 0$, τότε $n = -m$, όπου $m > 0$, και τότε

$$f(n) = f(-m) = (-m)\cdot 1_R = (-1\cdot m)\cdot 1_R = (-1)\cdot m \cdot 1_R = (-1)\phi(m) = \phi(-m) = \phi(n)$$

Άρα $f(n) = \phi(n)$, $\forall n \in \mathbb{Z}$, και άρα $f = \phi$. $\surd$

Παράδειγμα 8.2.15. Έστω $n\mathbb{Z}$ το ιδεώδες του $\mathbb{Z}$, το οποίο παράγεται από τον θετικό ακέραιο $n \geq 1$. Έστω $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ο δακτύλιος πηλίκο. Θεωρούμε την απεικόνιση

$$\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \quad \pi(k) = [k]_n$$

Η απεικόνιση π είναι προφανώς «επί» και $\pi(1) = [1]_n = 1_{\mathbb{Z}/n\mathbb{Z}}$. Επιπλέον

$$\pi(k+l) = [k+l]_n = [k]_n + [l]_n = \pi(k) + \pi(l) \quad \text{και} \quad \pi(kl) = [kl]_n = [k]_n \cdot [l]_n = \pi(k)\cdot\pi(l)$$

Άρα η απεικόνιση π είναι ένας επιμορφισμός δακτυλίων. $\surd$

Γενικότερα:

Παράδειγμα 8.2.16. Για κάθε ιδεώδες I ενός δακτυλίου R, η απεικόνιση

$$\pi\colon R \longrightarrow R/I, \quad \pi(x) = x + I$$

είναι ένας επιμορφισμός από τον δακτύλιο R στον δακτύλιο πηλίκο R/I, ο οποίος καλείται ο **επιμορφισμός φυσικής** ή **κανονικής προβολής** του R στον R/I.

Πράγματι, η απεικόνιση π είναι προφανώς «επί» και $\pi(1_R) = 1_R + I = 1_{R/I}$. Επιπλέον

$$\pi(x+y) = (x+y) + I = (x+I) + (y+I) = \pi(x) + \pi(y) \quad \text{και} \quad \pi(x\cdot y) = (x\cdot y) + I = (x+I)\cdot(y+I) = \pi(x)\cdot\pi(y)$$

Άρα η απεικόνιση π είναι ένας επιμορφισμός δακτυλίων.

Για τον πυρήνα του π θα έχουμε:

$$\mathsf{Ker}(f) = \{x \in R \mid \pi(x) = 0_{R/I}\} = \{x \in R \mid x + I = I\} = \{x \in R \mid x \in I\} = I \quad \surd$$

Παράδειγμα 8.2.17. Η απεικόνιση

$$f\colon \mathbb{Q}[\sqrt{5}] \longrightarrow \mathbb{Q}[\sqrt{5}], \quad f(a + b\sqrt{5}) = a - b\sqrt{5}$$

είναι ένας αυτομορφισμός δακτυλίων.

Πράγματι θα έχουμε $f(1) = f(1 + 0\sqrt{5}) = 1$, και αν $a + b\sqrt{5}, c + d\sqrt{5} \in \mathbb{Q}[\sqrt{5}]$, θα έχουμε:

$$f\big((a + b\sqrt{5}) + (c + d\sqrt{5})\big) = f\big((a+c) + (b+d)\sqrt{5}\big) = (a+c) - (b+d)\sqrt{5} =$$

$$= (a - b\sqrt{5}) + (c - d\sqrt{5}) = f(a + b\sqrt{5}) + f(c + d\sqrt{5})$$

και παρόμοια:

$$f\big((a + b\sqrt{5})\cdot(c + d\sqrt{5})\big) = f\big((ac + 5bd) + (ad + bc)\sqrt{5}\big) = (ac + 5bd) - (ad + bc)\sqrt{5} =$$

$$= (a - b\sqrt{5})\cdot(c - d\sqrt{5}) = f\big(a + b\sqrt{5}\big)\cdot f\big(c + d\sqrt{5}\big)$$

Άρα η f είναι ενδομορφισμός του $\mathbb{Q}[\sqrt{5}]$ ο οποίος είναι αυτομορφισμός με αντίστροφο τον εαυτό του, διότι $f^2(a + b\sqrt{5}) = f(f(a + b\sqrt{5})) = f((a - b\sqrt{5}) = (a + b\sqrt{5})$, και άρα $f^2 = \mathrm{Id}_{\mathbb{Q}[\sqrt{5}]}$. $\surd$

Παράδειγμα 8.2.18. 1. Έστω ότι R είναι ένας μεταθετικός δακτύλιος. Τότε η απεικόνιση

$$f\colon R \longrightarrow R[t], \quad f(r) = \mathsf{r}$$

όπου r είναι το σταθερό πολυώνυμο $r \in R$, είναι προφανώς ένας μονομορφισμός δακτυλίων.

2. Έστω ότι R είναι ένας δακτύλιος. Τότε η απεικόνιση

$$f\colon R \longrightarrow \mathsf{M}_n(R), \quad f(r) = rI_n = \begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & r & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & r \end{pmatrix}$$

είναι προφανώς ένας μονομορφισμός δακτυλίων. $\surd$

Παράδειγμα 8.2.19 (Ομομορφισμός Εκτίμησης (I)). Έστω R ένας μεταθετικός δακτύλιος και έστω $R[t]$ ο δακτύλιος πολυωνύμων υπεράνω του R. Για κάθε $r \in R$, ορίζουμε απεικόνιση

$$\Phi_r : R[t] \longrightarrow R, \quad \Phi_r(P(t)) = P(r)$$

δηλαδή, αν $P(t) = a_0 + a_1 t + \cdots + a_n t^n$, τότε: $\Phi_r(P(t)) = P(r) = a_0 + a_1 \cdot r + a_2 \cdot r^2 + \cdots + a_n \cdot r^n$. Θα δείξουμε ότι ο Φ_r είναι ένας επιμορφισμός δακτυλίων, ο **επιμορφισμός εκτίμησης** στο $r \in R$.

Πράγματι, η απεικόνιση Φ_r είναι «επί», διότι, αν $s \in R$, τότε θεωρούμε το σταθερό πολυώνυμο $\mathsf{s} = s$, και τότε $\Phi_r(\mathsf{s}) = s$. Επιπλέον $\Phi_r(1) = 1_R$, όπου 1 είναι το σταθερό πολυώνυμο $1 = 1$. Έστω

$$P(t) = a_0 + a_1 t + \cdots + a_n t^n \qquad \text{και} \qquad Q(t) = b_0 + b_1 t + \cdots + b_m t^m$$

δύο πολυώνυμα υπεράνω του R. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $a_n \neq 0$, $b_m \neq 0$, και $n \leq m$ Τότε μπορούμε να γράψουμε $P(t) = a_0 + a_1 t + \cdots + a_n t^n + a_{n+1} t^{n+1} + \cdots + a_m t^m$, όπου $a_k = 0$, $n+1 \leq k \leq m$, και θα έχουμε:

$$\begin{aligned}
\Phi_r\big(P(t) + Q(t)\big)\big) &= \Phi_r\big((a_0 + b_0) + (a_1 + b_1)t + (a_2 + b_2)t^2 + \cdots + (a_m + b_m)t^m\big) \\
&= (a_0 + b_0) + (a_1 + b_1)r + (a_2 + b_2)r^2 + \cdots + (a_m + b_m)r^m \\
&= (a_0 + a_1 r + a_2 r^2 + \cdots + a_m r^m) + (b_0 + b_1 r + b_2 r^2 + \cdots + b_m r^m) \\
&= \Phi_r(P(t)) + \Phi_r(Q(t))
\end{aligned}$$

Για το γινόμενο των πολυωνύμων $P(t)$ και $Q(t)$ θα έχουμε $P(t) \cdot Q(t) = c_0 + c_1 t + c_2 t^2 + \cdots + c_{n+m} t^{n+m}$, όπου $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, $0 \leq k \leq n+m$. Τότε, χρησιμοποιώντας οτι ο δακτύλιος R είναι μεταθετικός, θα έχουμε:

$$(a_0 + a_1 r + a_2 r^2 + \cdots + a_n r^n) \cdot (b_0 + b_1 r + b_2 r^2 + \cdots + b_m r^m) =$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0) r + (a_0 b_2 + a_1 b_1 + a_2 b_0) r^2 + \cdots + \sum_{i=0}^{k} a_i b_{k-i} r^k + \cdots + a_n b_m t^{n+m}$$

και τότε

$$\begin{aligned}
\Phi_r\big(P(t) \cdot Q(t)\big)\big) &= \Phi_r\big(c_0 + c_1 t + c_2 t^2 + \cdots + c_{n+m} t^{n+m}\big) \\
&= c_0 + c_1 r + c_2 r^2 + \cdots + c_{n+m} r^{n+m} \\
&= (a_0 + a_1 r + a_2 r^2 + \cdots + a_n r^n) \cdot (b_0 + b_1 r + b_2 r^2 + \cdots + b_m r^m) \\
&= \Phi_r(P(t)) \cdot \Phi_r(Q(t))
\end{aligned}$$

Επομένως η απεικόνιση Φ_r είναι ένας επιμορφισμός δακτυλίων. Ο πυρήνας του Φ_r αποτελείται από όλα τα πολυώνυμα $P(t)$ για τα οποία $P(r) = 0$.

Προφανώς το πολυώνυμο $(t - r)$ είναι στοιχείο του $\mathsf{Ker}(\Phi_r)$, καθώς και κάθε πολλαπλάσιο του $Q(t)(t - r)$. Ας υποθέσουμε ότι ο δακτύλιος $R = \mathbb{K}$ είναι ένα σώμα. Τότε από την Ευκλείδεια Διαίρεση πολυωνύμων υπεράνω ενός σώματος, την οποία θα δούμε σε περισσότερο γενική μορφή στο επόμενο Κεφάλαιο 9, έπεται ότι υπάρχουν πολυώνυμα $Q(t), R(t) \in \mathbb{K}[t]$, έτσι ώστε: $P(t) = Q(t)(t-r) + R(t)$, όπου είτε $R(t) = 0$ είτε $\deg R(t) < 1$, δηλαδή το $R(t)$ είναι σταθερό μη μηδενικό πολυώνυμο, έστω $R(t) = \mathsf{c}$, όπου $c \in \mathbb{K} \setminus \{0\}$. Επομένως αν $0 \neq R(t)$ ανήκει στον πυρήνα $\mathsf{Ker}(\Phi_r)$, θα έχουμε $0 = P(r) = Q(r)(r - r) + c$ και άρα $c = 0$, δηλαδή $R(t) = 0$, το οποίο είναι άτοπο. Άρα $R(t) = 0$ και επομένως $P(t) = Q(t)(t - r)$. Συνοψίζοντας, δείξαμε ότι $\mathsf{Ker}(\Phi_r) = (t - r)$ είναι το κύριο ιδεώδες το οποίο παράγεται από το πολυώνυμο $(t - r)$. $\surd$

Παράδειγμα 8.2.20 (Πολυωνυμική Επέκταση Ομομορφισμού Δακτυλίων). Έστω $f : R \longrightarrow S$ ένας ομομορφισμός ματαθετικών δακτυλίων. Τότε ο ομομορφισμός δακτυλίων f επάγει έναν ομομορφισμό πολυωνυμικών δακτυλίων

$$\widetilde{f} : R[t] \longrightarrow S[t], \quad \widetilde{f}(a_0 + a_1 t + \cdots + a_n t^n) = f(a_0) + f(a_1)t + \cdots + f(a_n)t^n$$

Πράγματι, θα έχουμε $\widetilde{f}(1) = f(1_R) = 1_S = 1$, όπου συμβολίσαμε με 1 τα σταθερά πολυώνυμα $1 = 1_R$ και $1 = 1_S$ στους δακτυλίους $R[t]$ και $S[t]$ αντίστοιχα.

Έστω

$$P(t) = a_0 + a_1 t + \cdots + a_n t^n \qquad \text{και} \qquad Q(t) = b_0 + b_1 t + \cdots + b_m t^m$$

δύο πολυώνυμα υπεράνω του R. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $a_n \neq 0$, $b_m \neq 0$, και $n \leq m$ Τότε μπορούμε να γράψουμε $P(t) = a_0 + a_1 t + \cdots + a_n t^n + a_{n+1} t^{n+1} + \cdots + a_m t^m$, όπου $a_k = 0$, $n+1 \leq k \leq m$, και θα έχουμε:

$$\begin{aligned}
\widetilde{f}\big(P(t)+Q(t)\big) &= \widetilde{f}\big((a_0+b_0)+(a_1+b_1)t+(a_2+b_2)t^2+\ \cdots\ +(a_m+b_m)t^m\big)\\
&= f(a_0+b_0)+f(a_1+b_1)t+f(a_2+b_2)t^2+\ \cdots\ +f(a_m+b_m)t^m\\
&= f(a_0)+f(b_0)+(f(a_1)+f(b_1))t+(f(a_2)+f(b_2))t^2+\ \cdots\ +(f(a_m)+f(b_m))t^m\\
&= f(a_0)+f(a_1)t+f(a_2)t^2+\ \cdots\ +f(a_m)t^m\ +\ f(b_0)+f(b_1)t+f(b_2)t^2+\ \cdots\ +f(b_m)t^m\\
&= \widetilde{f}(P(t))+\widetilde{f}(Q(t))
\end{aligned}$$

Για το γινόμενο των πολυωνύμων $P(t)$ και $Q(t)$ θα έχουμε $P(t)\cdot Q(t) = c_0 + c_1 t + c_2 t^2 + \ \cdots\ + c_{n+m} t^{n+m}$, όπου $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, $0 \leq k \leq n+m$. Τότε, χρησιμοποιώντας οτι ο δακτύλιος R είναι μεταθετικός, θα έχουμε:

$$\begin{aligned}
\widetilde{f}\big(P(t)\cdot Q(t)\big) &= \widetilde{f}\big((a_0+a_1t+\ \cdots\ +a_nt^n)\cdot(b_0+b_1t+b_2t^2+\ \cdots\ +b_mt^m)\big)\\
&= \widetilde{f}\big(a_0b_0+(a_0b_1+a_1b_0)t+\cdots+\sum_{i=0}^{k}a_ib_{k-i}r^k+\cdots+a_nb_mt^{n+m}\big)\\
&= f(a_0b_0)+f(a_0b_1+a_1b_0)t+\cdots+f(\sum_{i=0}^{k}a_ib_{k-i})t^k+\cdots+f(a_nb_m)t^{n+m}\\
&= f(a_0)f(b_0)+\big(f(a_0)f(b_1)+f(a_1)f(b_0)\big)t+\cdots+\sum_{i=0}^{k}f(a_i)f(b_{k-i})t^k+\cdots+f(a_n)f(b_m)t^{n+m}\\
&= \big(f(a_0)+f(a_1)t+f(a_2)t^2+\ \cdots\ +f(a_n)t^n\big)\cdot\big(f(b_0)+f(b_1)t+f(b_2)t^2+\ \cdots\ ++f(b_m)t^m\big)\\
&= \widetilde{f}(P(t))\cdot\widetilde{f}(Q(t))
\end{aligned}$$

Άρα η απεικόνιση $\widetilde{f}$ είναι ένας ομομορφισμός δακτυλίων, ο οποίος καλείται η **πολυωνυμική επέκταση του ομομορφισμού** f. $\surd$

Παράδειγμα 8.2.21 (Ομομορφισμός Εκτίμησης (II))**.** Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός ματαθετικών δακτυλίων, και $s \in S$. Θεωρούμε την σύνθεση ομομορφισμών

$$\widetilde{\Phi}_s = \Phi_s \circ \widetilde{f}\ :\ R[t] \xrightarrow{\ \widetilde{f}\ } S[t] \xrightarrow{\ \Phi_s\ } S$$

δηλαδή της πολυωνυμικής επέκτασης $\widetilde{f}$ του ομομορφισμού f με τον ομομορφισμό εκτίμησης Φ_s στο $s \in S$.

Έτσι, αν $P(t) = a_0 + a_1 t + \cdots + a_n t^n \in R[t]$, τότε:

$$\widetilde{\Phi}_s(P(t)) = \widetilde{\Phi}_s\big(a_0 + a_1 t + \cdots + a_n t^n\big) = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n$$

Η απεικόνιση Φ_s, ως σύνθεση ομομορφισμών δακτυλίων, είναι ένας ομομορφισμός δακτυλίων. $\surd$

Λόγω της σπουδαιότητας του παραπάνω Παραδείγματος 8.2.21, το διατυπώνουμε γενικότερα ως εξής:

Πρόταση 8.2.22. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός ματαθετικών δακτυλίων, και $s \in S$. Τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων $f^*\colon R[t] \longrightarrow S$ έτσι ώστε:*

1. $f^*(t) = s$.
2. $f^*(\mathrm{r}) = f(r)$, $\forall r \in R$.

όπου $\mathsf{r} \in R[t]$ *είναι το σταθερό πολυώνυμο* $r \in R$.

Ο ομομορφισμός f^* *συμπίπτει με τον ομομορφισμό* $\widetilde{\Phi}_s$ *του Παραδείγματος 8.2.21:*

$$f^* = \widetilde{\Phi}_s = \Phi_s \circ \widetilde{f} : \ R[t] \xrightarrow{\widetilde{f}} S[t] \xrightarrow{\Phi_s} S, \quad \widetilde{\Phi}_s(P(t)) = \widetilde{\Phi}_s\big(a_0 + a_1 t + \cdots + a_n t^n\big) = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n$$

Απόδειξη. Γνωρίζουμε ότι η απεικόνιση $\widetilde{\Phi}_s := f^*$ είναι ένας ομομορφισμός δακτυλίων, και προφανώς $f^*(t) = s$, και $f^*(\mathsf{r}) = f(r)$, $\forall r \in R$.

Έστω $g\colon R[t] \longrightarrow S$ ένας ομομορφισμός δακτυλίων έτσι ώστε: $g(t) = s$ και $g(\mathsf{r}) = f(r)$, $\forall r \in R$. Τότε, επειδή το πολυώνυμο $r t^k$, όπου $r \in R$, είναι γινόμενο του σταθερού πολυωνύμου r με τιμή $r \in R$, και του πολυωνύμου t^k, θα έχουμε $g(r t^k) = g(r) \cdot g(t^k) = g(r) \cdot g(t)^k$. Τότε, χρησιμοποιώντας αυτές τις σχέσεις και την υπόθεση ότι ο g είναι ομομορφισμός δακτυλίων, θα έχουμε, $\forall P(t) = a_0 + a_1 t + \cdots + a_n t^n \in R[t]$:

$$g(P(t)) = g(a_0 + a_1 t + \cdots + a_n t^n) = g(a_0) + g(a_1)g(t) + \cdots + g(a_n)g(t^n) = f(a_0) + f(a_1)s + \cdots + f(a_n)s^n = f^*(P(t))$$

Επομένως θα έχουμε: $g = f^*$. ■

Επιλέγοντας ως ομομορφισμό $R \longrightarrow S[t]$ να είναι η σύνθεση $R \longrightarrow S \longrightarrow S[t]$, $r \longrightarrow f(r)$, όπου ταυτίζουμε το $f(r)$ με το σταθερό πολυώνυμο με την ίδια τιμή, και επιλέγοντας $s = t \in S[t]$, από την Πρόταση 8.2.22, θα έχουμε το ακόλουθο:

Πόρισμα 8.2.23. *Έστω* $f\colon R \longrightarrow S$ *ένας ομομορφισμός ματαθετικών δακτυλίων. Τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων* $f^*\colon R[t] \longrightarrow S[t]$ *έτσι ώστε:*

1. $f^*(t) = t$.
2. $f^*(\mathsf{r}) = f(r)$, $\forall r \in R$.

όπου $\mathsf{r} \in R[t]$ *είναι το σταθερό πολυώνυμο* $r \in R$, *ο οποίος ορίζεται ως εξής:*

$$f^* : \ R[t] \longrightarrow S[t], \quad f^*(P(t)) = f^*\big(a_0 + a_1 t + \cdots + a_n t^n\big) = f(a_0) + f(a_1)t + \cdots + f(a_n)t^n$$

Η Πρόταση 8.2.22 γενικεύεται και σε δακτυλίους πολυωνύμων πολλών μεταβλητών:

Πρόταση 8.2.24. *Έστω* $f\colon R \longrightarrow S$ *ένας ομομορφισμός ματαθετικών δακτυλίων, και* $u_1, u_2, \cdots, u_n \in S$. *Τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων* $f^*\colon R[t_1, t_2, \cdots, t_n] \longrightarrow S$ *έτσι ώστε:*

1. $f^*(t_i) = u_i$, $1 \le i \le n$.
2. $f^*(\mathsf{r}) = f(r)$, $\forall r \in R$.

όπου $\mathsf{r} \in R[t]$ *είναι το σταθερό πολυώνυμο* $r \in R$.

Ο ομομορφισμός f^* *ορίζεται ως εξής:*

$$f^*\colon R[t_1, t_2, \cdots, t_n] \longrightarrow S, \quad f^*(P(t_1, t_2, \cdots, t_n)) = f^*\Big(\sum_{(i)} r_{i_1 i_2 \cdots i_n} t_1^{k_1} t_2^{k_2} \cdots t_n^{k_n}\Big) = \sum_{(i)} f(r_{i_1 i_2 \cdots i_n}) u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}$$

όπου $(i) = (i_1, i_2, \cdots, i_n) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \cdots \times \mathbb{N}_0$.

Απόδειξη. Η απόδειξη είναι παρόμοια με την απόδειξη της Πρότασης 8.2.22 και παραλείπεται, βλέπε την Άσκηση 8.5.23. ■

Παράδειγμα 8.2.25. Η απεικόνιση $f\colon \mathbb{R} \longrightarrow \mathbb{C}$, $f(a) = a$, είναι προφανώς ένας ομομορφισμός δακτυλίων. Τότε θα έχουμε την πολυωνυμική επέκταση $\widetilde{f}\colon \mathbb{R}[t] \longrightarrow \mathbb{C}[t]$ του f, μέσω του οποίου μπορούμε να θεωρούμε κάθε πολυώνυμο υπεράνω του $\mathbb{R}$ ως πολυώνυμο υπεράνω του $\mathbb{C}$.

Θεωρούμε έναν μιγαδικό αριθμό $z \in \mathbb{C}$, και τότε θα έχουμε, σύμφωνα με το Παράδειγμα 8.2.21, τον ομομορφισμό

$$\widetilde{\Phi}_z(P(t)) = \widetilde{\Phi}_z\big(a_0 + a_1 t + \cdots + a_n t^n\big) = a_0 + a_1 z + \cdots + a_n z^n = P(z)$$

Για παράδειγμα, θέτοντας $z = i$ και $P(t) = t^2 + 1$, θα έχουμε

$$\widetilde{\Phi}_i(t^2 + 1) = 1 + i^2 = 1 + (-1) = 0 \quad \surd$$

Παράδειγμα 8.2.26. Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε ο ομομορφισμός δακτυλίων f επάγει έναν ομομορφισμό δακτυλίων πινάκων

$$\mathsf{M}_n(f)\colon \mathsf{M}_n(R) \longrightarrow \mathsf{M}_n(S), \quad \mathsf{M}_n(f)(A)_{ij} = (f(a_{ij})), \quad \text{όπου} \quad A = (a_{ij})$$

Η απόδειξη αφήνεται ως Άσκηση, βλέπε την Άσκηση 8.5.22. $\surd$

Παράδειγμα 8.2.27 (Ομομορφισμός Εκτίμησης (III))**.** Έστω X ένα μη κενό σύνολο και R ένας δακτύλιος. Θεωρούμε τον δακτύλιο

$$\mathscr{F}(X,R) = \{f\colon X \longrightarrow R \mid f\colon \text{απεικόνιση}\}$$

Για κάθε στοιχείο $a \in X$, ορίζουμε απεικόνιση

$$\Phi_a\colon \mathscr{F}(X,R) \longrightarrow R, \quad \Phi_a(f) = f(a)$$

Θα δείξουμε ότι η απεικόνιση Φ_a είναι ένας επιμορφισμός δακτυλίων. Υπενθυμίζουμε ότι η μονάδα του δακτυλίου $\mathscr{F}(X,R)$ είναι η σταθερή συνάρηση $1\colon X \longrightarrow R$, $1(x) = 1_R$. Έτσι θα έχουμε $\Phi_a(1) = 1(a) = 1_R$. Αν $r \in R$ τότε έστω $\mathsf{r}\colon X \longrightarrow R$, η σταθερή συνάρτηση $\mathsf{r}(x) = r$. Τότε $\Phi_a(\mathsf{r}) = \mathsf{r}(a) = r$, και άρα η Φ_r είναι επί.

Έστω $f, g \in \mathscr{F}(X,R)$. Θα έχουμε:

$$\Phi_a(f+g) = (f+g)(a) = f(a) + g(a) = \Phi_a(f) + \Phi_a(g) \quad \text{και} \quad \Phi_a(f\cdot g) = (f\cdot g)(a) = f(a)\cdot g(a) = \Phi_a(f)\cdot\Phi_a(g)$$

Άρα η Φ_a είναι επιμορφισμός δακτυλίων.

Έστω $X = [0,1] \subseteq \mathbb{R}$ και $R = \mathbb{R}$. Θεωρούμε τον υποδακτύλιο $\mathscr{C}([0,1],\mathbb{R}) \subseteq \mathscr{F}([0,1],\mathbb{R})$. Τότε για κάθε $r \in [0,1]$, ο περιορισμός της Φ_r στον υποδακτύλιο $\mathscr{C}([0,1],\mathbb{R})$

$$\Phi_r\colon \mathscr{C}([0,1],\mathbb{R}) \longrightarrow \mathbb{R}, \quad \Phi_r(f) = f(r)$$

είναι ένας επιμορφισμός δακτυλίων. $\surd$

Παράδειγμα 8.2.28. Θεωρούμε, όπως στο Παράδειγμα 8.1.30, τον δακτύλιο ευθύ γινόμενο

$$R_1 \times R_2 \times \cdots \times R_n = \{(r_1, r_2, \cdots, r_n) \mid r_i \in R_i,\ 1 \le i \le n\}$$

των δακτυλίων R_1, R_2, $\cdots$, R_n. Ορίζουμε απεικονίσεις, $1 \le k \le n$:

$$\pi_k \ :\ R_1 \times R_2 \times \cdots \times R_n \ \longrightarrow\ R_k, \quad \pi_k(r_1, r_2, \cdots, r_n) = r_k$$

Οι απεικονίσεις π_k, $1 \le k \le n$, είναι επιμορφισμοί δακτυλίων.

Πράγματι, προφανώς η απεικόνιση π_k είναι «επί», και θα έχουμε $\pi_k(1_{\prod_{i=1}^n R_i}) = \pi_k(1_{R_1}, 1_{R_2}, \cdots, 1_{R_n}) = 1_{R_k}$. Έστω $(r_1, r_2, \cdots, r_n), (s_1, s_2, \cdots, s_n) \in \prod_{i=1}^n R_i$. Τότε θα έχουμε:

$$\pi_k\big((r_1, r_2, \cdots, r_n) + (s_1, s_2, \cdots, s_n)\big) = \pi_k(r_1+s_1, r_2+s_2, \cdots, r_n+s_n) = r_k + s_k = \pi(r_1, r_2, \cdots, r_n) + \pi_k(s_1, s_2, \cdots, s_n)$$

$$\pi_k\big((r_1, r_2, \cdots, r_n)\cdot(s_1, s_2, \cdots, s_n)\big) = \pi_k(r_1\cdot s_1, r_2\cdot s_2, \cdots, r_n\cdot s_n) = r_k\cdot s_k = \pi(r_1, r_2, \cdots, r_n)\cdot\pi_k(s_1, s_2, \cdots, s_n)$$

Άρα η απεικόνιση π_k είναι επιμορφισμός δακτυλίων ο οποίος καλείται ο **επιμορφισμός κανονικής k-προβολής**.

Η απεικόνιση

$$\iota_k \ :\ R_k \ \longrightarrow\ R_1 \times R_2 \times \cdots \times R_n, \quad \iota_k(r) = (0, \cdots, 0, r, 0, \cdots, 0) \qquad (\text{το } r \text{ στην } k-\text{θέση})$$

αν και ικανοποιεί τις σχέσεις

$$\iota_k(r+s) = \iota_k(r) + \iota_k(s) \qquad \text{και} \qquad \iota_k(r\cdot s) = \iota_k(r)\cdot\iota_k(s)$$

δεν είναι ομομορφισμός δακτυλίων, διότι: $\iota_k(1_{R_k}) = (0,\cdots,0,1_{R_k},0,\cdots,0) \neq (1_{R_1},1_{R_2},\cdots,1_{R_n}) = 1_{\prod_{i=1}^n R_i}$, (το 1_{R_k} στην k-θέση). Θεωρούμε τα ιδεώδη

$$\iota(e_k) = (e_k)_{\mathfrak{r}} = (e_k) = \Big\{\underbrace{(0,\cdots,0,r_k,0,\cdots,0)}_{k-\text{θέση}} \mid r_k \in R_k\Big\}, \qquad 1 \leq k \leq n$$

τα οποία παράγονται από τα στοιχεία e_k, όπου $e_k = (0,\cdots 0,1_{R_k},0,\cdots,0)$ (το στοιχείο 1_{R_k} είναι στην k-οστή θέση), $1 \leq k \leq n$, όπως στο Παράδειγμα 8.1.16. Τότε εύκολα βέπουμε ότι τα ιδεώδη $R'_k := (e_k)$ είναι δακτύλιοι με μονάδα e_k, αλλά όχι υποδακτύλιοι του $\prod_{i=1}^n R_i$, και τότε η απεικόνιση

$$\iota_k : R_k \longrightarrow R'_k \subseteq \prod_{i=1}^n R_i, \quad \iota_k(r) = (0,\cdots,0,r,0,\cdots,0) \qquad (\text{το } r \text{ στην } k-\text{θέση})$$

είναι ένας ομομορφισμός δακτυλίων και μάλιστα είναι ισομορφισμός δακτυλίων. $\surd$

8.2.3 Διαμερίσεις της Μονάδας και Συνεκτικοί Δακτύλιοι

Το ακόλουθο βασικό Θεώρημα περιγράφει πότε ένας δακτύλιος είναι ισόμορφος με το ευθύ γινόμενο μιας πεπερασμένης οικογένειας δακτυλίων.

Θεώρημα 8.2.29. *Για έναν δακτύλιο R, τα ακόλουθα είναι ισοδύναμα:*

1. *Ο δακτύλιος R είναι ισόμορφος με το ευθύ γινόμενο μιας πεπερασμένης οικογένειας δακτυλίων $R_1,\cdots,R_n$:*
$$R \cong R_1 \times R_2 \times \cdots \times R_n$$
2. *Ο δακτύλιος R διαθέτει μια κεντρική διαμέριση $\mathscr{D} = \{e_k\}_{k=1}^n$ της μονάδας.*
3. *Ο δακτύλιος R είναι το ευθύ άθροισμα μιας πεπερασμένης οικογένειας ιδεωδών I_k του R, $1 \leq k \leq n$.*
$$R = I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

Απόδειξη. 1. «$\Longrightarrow$» 2. Όπως είδαμε στην συζήτηση πριν την απόδειξη της Πρότασης 8.1.35, θέτοντας

$$e_k = \underbrace{(0,0,\cdots,0,1_{R_k},0,\cdots,0,0)}_{k-\text{θέση}}, \quad 1 \leq k \leq n$$

αποκτούμε μια κεντρική διαμέριση της μονάδας $\mathscr{D} = \{e_k\}_{k=1}^n$ του δακτυλίου R.

2. «$\Longrightarrow$» 3. Αυτή η κατεύθυνση αποδείχθηκε στην Πρόταση 8.1.35.

3. «$\Longrightarrow$» 1. Όπως στην απόδειξη της Πρότασης 8.1.35, το σύνολο $\mathscr{D} = \{e_k\}_{k=1}^n$ είναι μια κεντρική διαμέριση της μονάδας του R. Επιπλέον, όπως είδαμε στην απόδειξη της Πρότασης 8.1.35, για κάθε στοιχείο $x_k \in I_k$, έχουμε $x_k = e_k x_k = x_k e_k$. Έτσι

$$(e_k x_k)e_k = x_k e_k e_k = x_k e_k = e_k x_k \qquad \text{και} \qquad e_k(x_k e_k) = e_k e_k x_k = e_k x_k = x_k e_k$$

Οι παραπάνω σχέσεις δείχνουν οτι το στοιχείο $e_k \in I_k$ είναι μονάδα του υποδακτυλίου I_k, $1 \leq k \leq n$. Έτσι έχουμε μια πεπερασμένη οικογένεια δακτυλίων με μονάδα $\{I_k\}_{k=1}^n$.

Θεωρούμε το ευθύ γινόμενο δακτυλίων $I_1 \times I_2 \times \cdots \times I_n$ και θέτουμε

$$f\colon R \longrightarrow I_1 \times I_2 \times \cdots \times I_n, \quad f(r) = (e_1 r, e_2 r, \cdots, e_n r)$$

Η απεικόνιση f είναι καλά ορισμένη διότι, καθώς τα I_k είναι ιδεώδη του R, $e_k r \in I_k$, $1 \leq k \leq n$.

(α') Θα έχουμε $f(1_R) = (e_1 \cdot 1_R, e_2 \cdot 1_R, \cdots, e_n \cdot 1_R) = (e_1, e_2, \cdots, e_n) = 1_{I_1 \times I_2 \times \cdots \times I_n}$.
Έστω $r, s \in R$. Τότε:

$$f(r+s) = \big(e_1(r+s), e_2(r+s), \cdots, e_n(r+s)\big) = (e_1 r + e_1 s, e_2 r + e_2 s, \cdots, e_n r + e_n s) =$$

$$= (e_1 r, e_2 r, \cdots, e_n r) + (e_1 s, e_2 s, \cdots, e_n s) = f(r) + f(s)$$

Και παρόμοια, χρησιμοποιώντας ότι τα στοιχεία e_k είναι ταυτοδύναμα και κεντρικά, θα έχουμε:

$$f(r \cdot s) = \big(e_1(r \cdot s), e_2(r \cdot s), \cdots, e_n(r \cdot s)\big) = (e_1 rs, e_2 rs, \cdots, e_n rs) = (e_1 e_1 rs, e_2 e_2 rs, \cdots, e_n e_n rs) =$$

$$= (e_1 r e_1 s, e_2 r e_2 s, \cdots, e_n r e_n s) = (e_1 r, e_2 r, \cdots, e_n r) \cdot (e_1 s, e_2 s, \cdots, e_n s) = f(r) \cdot f(s)$$

Οι παραπάνω σχέσεις δείχνουν ότι η απεικόνιση f είναι ομομορφισμός δακτυλίων.

(β') Έστω $f(r) = 0$. Τότε $(e_1 r, e_2 r, \cdots, e_n r) = (0, 0, \cdots, 0)$, και άρα $e_k r = 0$, $1 \leq k \leq n$. Τότε $r = 1_R \cdot r = (e_1 + e_2 r + \cdots + e_n) \cdot r = e_1 r + e_2 + \cdots + e_n r = 0$. Έτσι $\mathsf{Ker}(f) = \{0\}$, και άρα η απεικόνιση f είναι μονομορφισμός δακτυλίων.

(γ') Έστω $(x_1, x_2, \cdots, x_n) \in I_1 \times I_2 \times \cdots \times I_n$. Τότε θεωρούμε το στοιχείο $x = x_1 + x_2 + \cdots + x_n \in R$, και θα έχουμε:

$$f(x) = (e_1 x, e_2 x, \cdots, e_n x)$$

Όμως $e_k x = e_k \cdot (x_1 + x_2 + \cdots + x_n) = e_k x_1 + e_k x_2 + \cdots + e_k x_n$. Επειδή $e_k \in I_k$ και $x_j \in I_j$, έπεται ότι $e_k x_j \in I_k \cap I_j$, $1 \leq k, j \leq n$. Επειδή το άθροισμα $I_1 \oplus I_2 \oplus \cdots \oplus I_n$ των ιδεωδών $I_1, I_2, \cdots, I_n$ είναι ευθύ, θα έχουμε προφανώς $I_k \cap I_j = \{0\}$, αν $k \neq j$. Αυτό σημαίνει ιδιαίτερα ότι $e_k x = e_k x_k$, $1 \leq k \leq n$, και άρα $f(x) = (e_1 x_1, e_2 x_2, \cdots, e_n x_n)$. Από την άλλη πλευρά, $1_R = e_1 + e_2 + \cdots + e_n$ και άρα για κάθε $x_k \in I_k$, θα έχουμε ακριβώς παρόμοια ότι $x_k = 1_R x_k = e_1 x_k + e_2 x_k + \cdots + e_n x_k$ και το στοιχείο $e_j x_k \in I_j \cap I_k = \{0\}$, αν $j \neq k$. Έτσι $x_k = e_k x_k$, $1 \leq k \leq n$. Τότε θα έχουμε

$$f(x) = (e_1 x_1, e_2 x_2, \cdots, e_n x_n) = (x_1, x_2, \cdots, x_n)$$

Η παραπάνω σχέση δείχνει ότι η απεικόνιση f είναι «επί». Άρα η απεικόνιση f είναι ισομορφισμός δακτυλίων. ■

Παρατήρηση 8.2.30. Ένας δακτύλιος R καλείται **συνεκτικός**,[2] αν τα μόνα κεντρικά ταυτοδύναμα στοιχεία του είναι τα τετριμμένα: $0, 1$. Σύμφωνα με το Θεώρημα 8.2.29, ένας δακτύλιος R είναι συνεκτικός αν και μόνο αν δεν είναι ισόμορφος με ένα ευθύ γινόμενο $\prod_{k=1}^{n} R_k$ δακτυλίων R_k, με $k \geq 2$. Έτσι κάθε ακέραια περιοχή, ιδιαίτερα κάθε σώμα, είναι συνεκτικός δακτύλιος.

Θεωρούμε τον μη μεταθετικό δακτύλιο

$$\mathsf{AT}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \;\middle|\; a, b, c \in \mathbb{R} \right\}$$

των άνω τριγωνικών 2×2 πινάκων με στοιχεία από το σώμα $\mathbb{R}$ των πραγματικών αριθμών. Εύκολα υπολογίζουμε ότι $\mathsf{Z}(\mathsf{AT}_2(\mathbb{R})) = \left\{ aI_2 = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \mathsf{AT}_2(\mathbb{R}) \;\middle|\; a \in \mathbb{R} \right\}$. Επομένως ένα στοιχείο X του δακτυλίου $\mathsf{AT}_2(\mathbb{R})$ είναι κεντρικό και ταυτοδύναμο αν και μόνο αν $X = aI_2$ και $X^2 = a^2 I_2 = aI_2$, από όπου $a^2 = a$, δηλαδή $a = 0$ ή $a = 1$. Επομένως τα μόνα κεντρικά ταυτοδύναμα στοιχεία του $\mathsf{AT}_2(\mathbb{R})$ είναι τα τετριμμένα, και άρα ο δακτύλιος $\mathsf{AT}_2(\mathbb{R})$ είναι συνεκτικός. ▲

---

[2] Η ορολογία *συνεκτικός* δακτύλιος έχει τοπολογική προέλευση. Αν R είναι ένας μεταθετικός δακτύλιος, τότε το σύνολο $\mathsf{Spec}(R)$ των πρώτων ιδεωδών του R εφοδιασμένο με κατάλληλη τοπολογία, την τοπολογία Zariski, αποτελεί τοπολογικό χώρο, ο οποίος είναι συνεκτικός (με την έννοια της Τοπολογίας, δηλαδή ο τοπολογικός χώρος $\mathsf{Spec}(R)$ δεν μπορεί να γραφεί ως ξένη ένωση δύο ή περισσότερων μη κενών ανοιχτών υποσυνόλων του) αν και μόνο αν ο δακτύλιος R είναι συνεκτικός (με την έννοια των σημειώσεων).

Η τοπολογία Zariski του $\mathsf{Spec}(R)$ ορίζεται επιλέγοντας ως κλειστά υποσύνολα του $\mathsf{Spec}(R)$ τα σύνολα της μορφής $V(I) = \{P \in \mathsf{Spec}(R) \mid I \subseteq P\}$, όπου I είναι ένα ιδεώδες του R.

- Oscar Zariski (24 Ιανουαρίου 1899 - 4 Ιουλίου 1986) [https://en.wikipedia.org/wiki/Oscar_Zariski]: Σημαντικός Ρώσος μαθηματικός, ο οποίος έζησε και εργάστηκε στις ΗΠΑ, με θεμελιώδη συμβολή στην Άλγεβρα και ιδιαίτερα στην Αλγεβρική Γεωμετρία.

8.3 Τα Θεωρήματα Ισομορφισμών Δακτυλίων

Στην παρούσα ενότητα θα αποδείξουμε πέντε πολύ βασικά Θεωρήματα τα οποία αφορούν ισομορφισμούς δακτυλίων. Τα τρία βασικά Θεωρήματα Ισομορφισμών Δακτυλίων, το Θεώρημα αντιστοιχίας υποδακτυλίων και ιδεωδών, και το Κινεζικό Θεώρημα Υπολοίπων.

8.3.1 Το Πρώτο Θεώρημα Ισομορφισμών

Έστω $f: R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε ο πυρήνας $\mathsf{Ker}(f)$ του ομομορφισμού f είναι ένα ιδεώδες του R, και άρα ορίζεται ο δακτύλιος πηλίκο $R/\mathsf{Ker}(f)$. Από την άλλη πλευρά, όπως έχουμε δει, η εικόνα $\mathsf{Im}(f)$ του ομομορφισμού f είναι ένας υποδακτύλιος του S. Το πρώτο Θεώρημα Ισομορφισμών πιστοποιεί ότι οι δακτύλιοι $R/\mathsf{Ker}(f)$ και $\mathsf{Im}(f)$ είναι ισόμορφοι και μας επιτρέπει να αναλύσουμε κάθε ομομορφισμό δακτυλίων ως σύνθεση ενός επιμορφισμού, ενός ισομορφισμού και ενός μονομορφισμού δακτυλίων.

Θεώρημα 8.3.1 (1ο Θεώρημα Ισομορφισμών)**.** *Έστω $f: R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Τότε η απεικόνιση*

$$\widetilde{f}: R/\mathsf{Ker}(f) \longrightarrow \mathsf{Im}(f), \quad \widetilde{f}(x+\mathsf{Ker}(f)) = f(x)$$

ορίζει έναν ισομορφισμό δακτυλίων

$$\widetilde{f}: R/\mathsf{Ker}\, f \xrightarrow{\cong} \mathsf{Im}(f)$$

Απόδειξη. Από το Πόρισμα 8.2.12 γνωρίζουμε ότι ο πυρήνας $\mathsf{Ker}(f)$ του ομομορφισμού f είναι ένα ιδεώδες του R, και άρα ορίζεται ο δακτύλιος πηλίκο $R/\mathsf{Ker}(f)$, και η εικόνα $\mathsf{Im}(f)$ του ομομορφισμού f είναι ένας υποδακτύλιος του S. Θέτουμε για ευκολία $I = \mathsf{Ker}(f)$, και ορίζουμε απεικόνιση

$$\widetilde{f}: R/I \longrightarrow \mathsf{Im}(f), \quad \widetilde{f}(x+I) = f(x)$$

Θα δείξουμε ότι η $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση η οποία είναι ισομορφισμός δακτυλίων.

1. Η $\widetilde{f}$ ΕΙΝΑΙ ΚΑΛΑ ΟΡΙΣΜΕΝΗ: Έστω $x+I = y+I$, όπου $x, y \in R$. Τότε θα έχουμε:

$$x+I = y+I \implies x-y \in I = \mathsf{Ker}(f) \implies f(x-y) = 0_S \implies f(x)-f(y) = 0_S \implies f(x) = f(y) \implies$$
$$\widetilde{f}(x+I) = \widetilde{f}(y+I)$$

   Επομένως η $\widetilde{f}$ είναι μια καλά ορισμένη απεικόνιση.

2. Η $\widetilde{f}$ ΕΙΝΑΙ ΟΜΟΜΟΡΦΙΣΜΟΣ ΔΑΚΤΥΛΙΩΝ: Θα έχουμε $\widetilde{f}(1_R+I) = f(1_R) = 1_S$, και άρα η απεικόνιση $\widetilde{f}$ στέλνει την μονάδα του R/I στην μονάδα του υποδακτυλίου $\mathsf{Im}(f)$. Έστω $x+I, y+I \in R/I$. Τότε θα έχουμε:

$$\widetilde{f}\big((x+I)+(y+I)\big) = \widetilde{f}((x+y)+I) = f(x+y) = f(x)+f(y) = \widetilde{f}(x+I)+\widetilde{f}(y+I)$$
$$\widetilde{f}\big((x+I)\cdot(y+I)\big) = \widetilde{f}((x\cdot y)+I) = f(x\cdot y) = f(x)\cdot f(y) = \widetilde{f}(x+I)\cdot\widetilde{f}(y+I)$$

   Επομένως η $\widetilde{f}$ είναι ένας ομομορφισμός δακτυλίων.

3. Η $\widetilde{f}$ ΕΙΝΑΙ ΕΠΙΜΟΡΦΙΣΜΟΣ ΔΑΚΤΥΛΙΩΝ: Έστω $z \in \mathsf{Im}(f)$. Τότε υπάρχει $x \in R$ έτσι ώστε $f(x) = z$. Επειδή $\widetilde{f}(x+I) = f(x) = z$, έπεται ότι η απεικόνιση $\widetilde{f}$ είναι επιμορφισμός.

4. Η $\widetilde{f}$ ΕΙΝΑΙ ΜΟΝΟΜΟΡΦΙΣΜΟΣ ΔΑΚΤΥΛΙΩΝ: Θα υπολογίσουμε τον πυρήνα του ομομορφισμού $\widetilde{f}$:

$$\mathsf{Ker}(\widetilde{f}) = \{x+I \in R/I \mid \widetilde{f}(x+I) = 0_S\} = \{x+I \in R/I \mid f(x) = 0_S\} = \{x+I \in R/I \mid x \in I\} = I$$

   Επειδή η πλευρική κλάση I είναι το μηδενικό στοιχείο του δακτυλίου πηλίκου R/I, δηλαδή $I = 0_{R/I}$, έπεται ότι ο πυρήνας του ομομορφισμού $\widetilde{f}$ αποτελείται μόνο από το μηδενικό στοιχείο της προσθετικής ομάδας $(R/I, +)$. Αυτό, όπως γνωρίζουμε, δείχνει ότι ο ομομορφσιμός $\widetilde{f}$ είναι «1-1», και επομένως είναι μονομορφισμός δακτυλίων.

Συνδυάζοντας τα παραπάνω, βλέπουμε ότι η καλά ορισμένη απεικόνιση $\widetilde{f}$ είναι ένας ισομορφισμός δακτυλίων. ■

Παρατήρηση 8.3.2. Σημειώνουμε ότι τα μέρη 1., 3., 4., και το μισό του μέρους 2., της απόδειξης του παραπάνω Θεωρήματος προκύπτουν από το Πρώτο Θεώρημα Ισομορφισμών Ομάδων. Παρόμοια παρατήρηση ισχύει και για τα υπόλοιπα Θεωρήματα Ισομορφισμών Δακτυλίων. Στο παρόν εδάφιο, για λόγους έμφασης, δίνουμε πλήρεις αποδείξεις των Θεωρημάτων Ισομορφισμών Δακτυλίων, επαναλαμβάνοντας όπου χρειάζεται τα μέρη των αποδείξεων τα οποία έχουν ήδη καταγραφεί στην απόδειξη των αντίστοιχων Θεωρημάτων Ισομορφισμών Ομάδων. ▲

Τα ακόλουθα Πορίσματα είναι άμεσες συνέπειες του Θεωρήματος 6.3.1.

Πόρισμα 8.3.3. *Κάθε ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$ είναι σύνθεση $f = \mathsf{i}_f \circ \widetilde{f} \circ \pi_f$:*

1. *του μονομορφισμού $\mathsf{i}_f\colon \mathsf{Im}(f) \longrightarrow S,\ \mathsf{i}_f(y) = y$,*
2. *του ισομορφισμού $\widetilde{f}\colon R/\mathsf{Ker}(f) \longrightarrow \mathsf{Im}(f),\ \widetilde{f}(x+\mathsf{Ker}(f)) = f(x)$,*
3. *του επιμορφισμού $\pi_f\colon R \longrightarrow R/\mathsf{Ker}(f),\ \pi_f(x) = x+\mathsf{Ker}(f)$.*

Δηλαδή το ακόλουθο διάγραμμα είναι μεταθετικό

$$\begin{array}{ccc} R & \xrightarrow{\quad f \quad} & S \\ {\scriptstyle \pi_f}\downarrow & & \uparrow{\scriptstyle \mathsf{i}_f} \\ R/\mathsf{Ker}(f) & \xrightarrow[\cong]{\quad \widetilde{f} \quad} & \mathsf{Im}(f) \end{array} \qquad f = \mathsf{i}_f \circ \widetilde{f} \circ \pi_f$$

Απόδειξη. Στο Θεώρημα 8.3.1 δείξαμε ότι η απεικόνιση $\widetilde{f}$ είναι ισομορφισμός δακτυλίων. Από το Παράδειγμα 8.2.16 έπεται ότι η απεικόνιση π_f είναι επιμορφισμός δακτυλίων με πυρήνα $\mathsf{Ker}(\pi_f) = \mathsf{Ker}(f)$. Προφανώς η κανονική έγκλειση i_f είναι ένας μονομορφισμός δακτυλίων. Τέλος, $\forall\, x \in R$:

$$(\mathsf{i}_f \circ \widetilde{f} \circ \pi_f)(x) = \mathsf{i}_f(\widetilde{f}(\pi_f(x))) = \mathsf{i}_f(\widetilde{f}(x+\mathsf{Ker}(f))) = \mathsf{i}_f(f(x)) = f(x)$$

Επομένως $\mathsf{i}_f \circ \widetilde{f} \circ \pi_f = f$. ■

Πόρισμα 8.3.4. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων.*

1. *Αν ο f είναι μονομορφισμός, τότε ο ομομορφισμός $f\colon R \longrightarrow S$ ορίζει έναν ισομορφισμό δακτυλίων*

$$f'\colon R \xrightarrow{\ \cong\ } \mathsf{Im}(f), \quad f'(x) = f(x)$$

Δηλαδή ο δακτύλιος R είναι ισόμορφος με έναν υποδακτύλιο του S.

2. *Αν ο f είναι επιμορφισμός, τότε ο ομομορφισμός $f\colon R \longrightarrow S$ επάγει έναν ισομορφισμό*

$$R/\mathsf{Ker}(f) \xrightarrow{\ \cong\ } S$$

Δηλαδή ο δακτύλιος S είναι ισόμορφος με έναν δακτύλιο πηλίκο του R.

Απόδειξη. 1. Αν ο ομομορφισμός f είναι μονομορφισμός, τότε $\mathsf{Ker}(f) = \{0_R\}$ και τότε προφανώς θα έχουμε έναν ισομορφισμό δακτυλίων $R/\mathsf{Ker}(f) = R$ και άρα ο μονομορφισμός $f\colon R \longrightarrow S$ ορίζει έναν ισομορφισμό $f'\colon R \longrightarrow \mathsf{Im}(f),\ f'(x) = f(x)$.

2. Αν ο ομομορφισμός f είναι επιμορφισμός, τότε $\mathsf{Im}(f) = S$ και ο ισχυρισμός προκύπτει από το Θεώρημα 8.3.1. ■

Το ακόλουθο αποτέλεσμα παρουσιάζει μια περισσότερο γενική μορφή του Πρώτου Θεωρήματος Ισομορφισμών Δακτυλίων:

Θεώρημα 8.3.5 (1ο Θεώρημα Ισομορφισμών Δακτυλίων - Γενικευμένη Μορφή)**.** *Έστω $f: R \longrightarrow S$ ένας ομομορφισμός δακτυλίων, και έστω $I \subseteq R$ ένα ιδεώδες του δακτυλίου R. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. $I \subseteq \mathsf{Ker}(f)$.
2. *Υπάρχει μοναδικός ομομορφισμός δακτυλίων:*

$$\widetilde{f}: R/I \longrightarrow S, \quad \text{έτσι ώστε:} \quad \widetilde{f} \circ \pi_I = f \tag{†}$$

όπου $\pi_I: R \longrightarrow R/I$ είναι ο φυσικός επιμορφισμός κανονικής προβολής.

Επιπλέον:

(*a*) *Ο $\widetilde{f}$ είναι επιμορφισμός δακτυλίων αν και μόνο αν ο f είναι επιμορφισμός δακτυλίων.*

(*b*) *Ο $\widetilde{f}$ είναι μονομορφισμός δακτυλίων αν και μόνο αν $I = \mathsf{Ker}(f)$.*

(*c*) *Ο $\widetilde{f}$ είναι ισομορφισμός δακτυλίων αν και μόνο αν ο f είναι επιμορφισμός δακτυλίων και $I = \mathsf{Ker}(f)$.*

Απόδειξη. 1. $\Longrightarrow$ 2. Υποθέτουμε ότι $I \subseteq \mathsf{Ker}(f)$, και ορίζουμε μια απεικόνιση

$$\widetilde{f}: R/I \longrightarrow S \quad f(x+I) = f(x)$$

Δείχνουμε ότι η απεικόνιση $\widetilde{f}$ είναι καλά ορισμένη. Έστω $x+I, y+I \in R/I$. Τότε θα έχουμε:

$$x+I = y+I \implies x-y \in I \subseteq \mathsf{Ker}(f) \implies f(x-y) = 0_S \implies f(x) - f(y) = 0_S \implies f(x) = f(y) \implies$$

$$\widetilde{f}(x+I) = \widetilde{f}(y+I)$$

και επομένως πράγματι η απεικόνιση $\widetilde{f}$ είναι καλά ορισμένη. Όπως στην απόδειξη του Θεωρήματος 8.3.1, βλέπουμε ότι η $\widetilde{f}$ είναι ομομορφισμός δακτυλίων, και $\forall x \in R$ θα έχουμε:

$$(\widetilde{f} \circ \pi_I)(x) = \widetilde{f}(\pi_I(x)) = \widetilde{f}(x+I) = f(x)$$

Επομένως $f = \widetilde{f} \circ \pi_I$.

Αν $g: R/I \longrightarrow S$ είναι ένας άλλος ομομορφισμός δακτυλίων έτσι ώστε $f = g \circ \pi_I$. Τότε, $\forall x+I \in R/I$:

$$g(x+I) = g(\pi_I(x)) = (g \circ \pi_I)(x) = (\widetilde{f} \circ \pi_I)(x) = \widetilde{f}(\pi_I(x)) = \widetilde{f}(x+I)$$

Άρα $g = \widetilde{f}$.

2. $\Longrightarrow$ 1. Υποθέτουμε ότι η απεικόνιση (†) είναι ένας ομομορφισμός δακτυλίων με την ιδιότητα $\widetilde{f} \circ \pi_I = f$. Τότε, επειδή ο $\widetilde{f}$ είναι ομομορφισμός, επειδή η πλευρική κλάση I είναι το μηδενικό στοιχείο του δακτυλίου πηλίκο R/I, και επειδή ένας ομομορφισμός ομάδων στέλνει το ουδέτερο στοιχείο στο ουδέτερο στοιχείο, θα έχουμε:

$$f(I) = (\widetilde{f} \circ \pi_I)(I) = \widetilde{f}(\pi_I(I)) = \widetilde{f}(I) = 0_S$$

Αυτό σημαίνει ότι ο ομομορφισμός f στέλνει κάθε στοιχείο του ιδεώδους S στο ουδέτερο στοιχείο 0_S του δακτυλίου S. Επομένως $I \subseteq \mathsf{Ker}(f)$.

(*a*) Υποθέτουμε ότι ο ομομορφισμός $\widetilde{f}$ είναι επιμορφισμός. Επειδή $f = \widetilde{f} \circ \pi_I$, επειδή ο ομομορφισμός π_I είναι επιμορφισμός, και επειδή σύνθεση επιμορφισμών είναι επιμορφισμός, έπεται ότι ο ομομορφισμός f είναι επιμορφισμός.

Αντίστροφα, έστω ότι ο ομομορφισμός f είναι επιμορφισμός, και έστω $y \in S$. Τότε υπάρχει στοιχείο $x \in R$ έτσι ώστε $f(x) = y$. Τότε $\widetilde{f}(xH) = f(x) = y$ και επομένως ο ομομορφισμός $\widetilde{f}$ είναι επιμορφισμός.

(*b*) Υποθέτουμε πρώτα ότι ο ομομορφισμός $\widetilde{f}$ είναι μονομορφισμός, και έστω $x \in \mathsf{Ker}(f)$. Τότε $\widetilde{f}(\pi_I(x)) = (\widetilde{f} \circ \pi_I)(x) = f(x) = 0_S$. Επειδή η $\widetilde{f}$ είναι μονομορφισμός, θα έχουμε $\pi_I(x) = x + I = 0_{R/I} = I$ και άρα $x \in I$. Δηλαδή $\mathsf{Ker}(f) \subseteq I$ και επομένως $I = \mathsf{Ker}(f)$.

Αντίστροφα, αν $I = \mathsf{Ker}(f)$, τότε έστω $x + I \in \mathsf{Ker}(\widetilde{f})$. Τότε $\widetilde{f}(x + I) = f(x) = 0_S$ και άρα $x \in \mathsf{Ker}(f) = I$. Αυτό δείχνει ότι $x + I = I = 0_{R/I}$ και επομένως ο ομομορφισμός $\widetilde{f}$ είναι μονομορφισμός.

(*c*) Συνδυάζοντας τα (*a*) και (*b*), θα έχουμε: ο ομομορφισμός $\widetilde{f}$ είναι ισομορφισμός αν και ο μόνο αν ο ομομορφισμός f είναι επιμορφισμός και $I = \mathsf{Ker}(f)$. ■

Η επόμενη Παρατήρηση πιστοποιεί ότι επιμορφισμοί δακτυλίων οι οποίοι ξεκινούν από έναν δακτύλιο R και ιδέωδη του δακτυλίου R είναι «ισοδύναμες» έννοιες.

Παρατήρηση 8.3.6. «Με ακρίβεια ισομορφισμού», η αντιστοιχία

$$\Phi : \{\text{ιδεώδη } I \text{ του } R\} \longrightarrow \{\text{επιμορφισμοί δακτυλίων } f : R \longrightarrow S\}$$

$$\Phi(I) = \pi_I : R \longrightarrow R/I$$

είναι «1-1» και «επί», με αντίστροφη την αντιστοιχία

$$\Psi : \{\text{επιμορφισμοί δακτυλίων } f : R \longrightarrow S\} \longrightarrow \{\text{ιδεώδη } I \text{ του } R\}$$

$$\Psi(f) = \mathsf{Ker}(f)$$

Δηλαδή:

1. αν $I \subseteq R$ είναι ένα ιδεώδες του R, τότε η κανονική προβολή $\pi_I : R \longrightarrow R/I$ είναι επιμορφισμός δακτυλίων και $\mathsf{Ker}(\pi_I) = I$.
2. αν $f : R \longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων, τότε ο πυρήνας $\mathsf{Ker}(f)$ είναι ένα ιδεώδες του R και, χρησιμοποιώντας τον ισομορφισμό $R/\mathsf{Ker}(f) \cong S$ του Πρώτου Θεωρήματος Ισομορφισμών 8.3.1, ο επιμορφισμός δακτυλίων f «συμπίπτει» με τον φυσικό επιμορφισμό $\pi_f : R \longrightarrow R/\mathsf{Ker}(f)$ με την έννοια ότι $\pi_f \circ \widetilde{f} = f$ και ο ομομορφισμός $\widetilde{f}$ είναι ισομορφισμός.

Επομένως, υπό αυτή την οπτική γωνία, ιδεώδη του R, και επιμορφισμοί οι οποίοι εκκινούν από τον δακτύλιο R, είναι ισοδύναμες έννοιες. ▲

8.3.2 Το Δεύτερο Θεώρημα Ισομορφισμών

Αν S είναι ένας υποδακτύλιος του δακτυλίου R, και I είναι ένα ιδεώδες του R, τότε, όπως μπορούμε να δούμε εύκολα, το σύνολο

$$S + I = \{s + x \in R \mid s \in S \text{ και } x \in I\}$$

είναι ένας υποδακτύλιος του R ο οποίος περιέχει το I ως ιδεώδες. Έτσι ορίζεται ο δακτύλιος πηλίκο $S + I/I$. Από την άλλη πλευρά, ο υποδακτύλιος $S \cap I$ είναι ιδεώδες του S και έτσι ορίζεται ο δακτύλιος πηλίκο $S/S \cap I$. Το Δεύτερο Θεώρημα Ισομορφισμών δακτυλίων εξετάζει τη σχέση μεταξύ των δακτυλίων πηλίκων $S + I/I$ και $S/S \cap I$:

Θεώρημα 8.3.7 (2ο Θεώρημα Ισομορφισμών)**.** *Έστω R ένας δακτύλιος, και $S \subseteq R$ ένας υποδακτύλιος του R. Αν I είναι ένα ιδεώδες του R, τότε:*

1. *Το σύνολο $S + I$ είναι ένας υποδακτύλιος του R και το I είναι ένα ιδεώδες του $S + I$.*
2. *Το σύνολο $S \cap I$ είναι ένα ιδεώδες του S.*
3. *Υπάρχει ένας ισομορφισμός δακτυλίων:*

$$S + I \big/ I \;\cong\; S \big/ (S \cap I)$$

Απόδειξη. 1. Το σύνολο $S+I$ προφανώς περιέχει τη μονάδα $1_R = 1_S$ του δακτυλίου R και του υποδακτυλίου S. Επίσης, αν $s_1, s_2 \in S$ και $x_1, x_2 \in I$, τότε προφανώς θα έχουμε $s_1 + s_2 \in S$, και $x_1 + x_2 \in I$, και επομένως:

$$(s_1 + x_1) + (s_2 + x_2) = (s_1 + s_2) + (x_1 + x_2) \ \in \ S + I$$

Παρόμοια, $s_1 \cdot s_2 \in S$, και $x_1 \cdot x_2 \in I$. Επειδή το I είναι ιδεώδες του R, θα έχουμε και $s_1 \cdot x_2 \in I$ και $x_1 \cdot s_2 \in I$, και επομένως:

$$(s_1 + x_1) \cdot (s_2 + x_2) = s_1 \cdot s_2 + s_1 \cdot x_2 + x_1 \cdot s_2 + x_1 \cdot x_2 \ \in S + I$$

Άρα το $S+I$ είναι υποδακτύλιος του I. Το I είναι προφανώς υποδακτύλιος του $S+I$, Επειδή το I είναι ιδεώδες του R, θα έχουμε:

$$(s + x) \cdot y = s \cdot y + x \cdot y \ \in \ I \qquad \text{και} \qquad y \cdot (s + x) = y \cdot s + y \cdot x \ \in \ I$$

και άρα το I είναι ιδεώδες του $S+I$.

2. Επειδή το I είναι ιδεώδες του R, έπεται ότι θα είναι κλειστό στον πολλαπλασιασμό των στοιχείων του από τα δεξιά και τα αριστερά με στοιχεία του S. Επομένως, άμεσα βλέπουμε οτι η υποομάδα $S \cap I$ του S είναι ένα ιδεώδες του S. Παρακάτω θα δούμε έναν διαφορετικό τρόπο απόδειξης ότι το $S \cap I$ είναι ιδεώδες του S, καθώς το υποσύνολο $S \cap I$ είναι πυρήνας ομομορφισμού δακτυλίων.

3. Αν $s \in S$, τότε $s \in S \subseteq S + I$, και έτσι μπορούμε να ορίσουμε απεικόνιση

$$f : \ S \longrightarrow \ S + I/I, \qquad f(s) = s + I$$

Η απεικόνιση f είναι ομομορφισμός δακτυλίων, διότι $f(1_S) = 1_S + I = 1_{S+I} + I = 1_{S+I/I}$. Επιπλέον έστω $s_1, s_2 \in S$. Τότε

$$f(s_1 + s_2) = (s_1 + s_2) + I = (s_1 + I) + (s_2 + I) = f(s_1) + f(s_2)$$

$$f(s_1 \cdot s_2) = (s_1 \cdot s_2) + J = (s_1 + J) \cdot (s_2 + J) = f(s_1) \cdot f(s_2)$$

Η απεικόνιση f είναι επιμορφισμός, διότι έστω $(s + x) + I \in S + I/I$, όπου $s \in S$ και $x \in I$. Τότε, επειδή $x \in I$, θα έχουμε $x + I = I$ και τότε: $(s+x)+I = s+I+x+I = s+I+I = s+I = f(s)$. Τέλος, ας υπολογίσουμε τον πυρήνα της f:

$$\mathsf{Ker}(f) = \{s \in S \mid f(s) = 0_{S+I/I}\} = \{s \in S \mid s + I = I\} = \{s \in S \mid s \in I\} = S \cap I$$

Από το Πρώτο Θεώρημα Ισομορφισμών 8.3.1 θα έχουμε ότι ο επιμορφισμός f ορίζει έναν ισομορφισμό

$$\widetilde{f} : \ S/S \cap I \xrightarrow{\cong} \ S + I/I, \qquad \widetilde{f}(s + (S \cap I)) = s + I$$ ■

Παρατήρηση 8.3.8. Αν I και J είναι ιδεώδη ενός δακτυλίου R, τότε γνωρίζουμε ότι ορίζονται δύο επιπρόσθετα ιδεώδη του R: το άθροισμα $I + J$ και η τομή τους $I \cap J$. Τότε έχουμε εγκλείσεις ιδεωδών, και ιδιαίτερα εγκλείσεις υποδακτυλίων χωρίς μονάδα, του R: $J \subseteq I + J$ και $I \cap J \subseteq I$. Θεωρούμε τα ιδεώδη $I + J$ και I ως δακτυλίους χωρίς μονάδα, και τα ιδεώδη $J \subseteq I + J$ και $I \cap J \subseteq I$ ως ιδεώδη των δακτυλίων χωρίς μονάδα $I + J$ και I αντίστοιχα. Τότε οι προσθετικές αβελιανές ομάδες πηλίκα $I + J/J$ και $I/I \cap J$ αποκτούν με φυσικό τρόπο δομή δακτυλίων πηλίκων (χωρίς μοναδα). Μια εναλλακτική μορφή του Δεύτερου Θεωρήματος Ισομορφισμών δακτυλίων, με παρόμοια απόδειξη, η οποία εξετάζει τη σχέση μεταξύ των δακτυλίων πηλίκων $I + J/J$ και $I/I \cap J$, είναι η εξής:

Θεώρημα 8.3.9. *Αν I και J είναι ιδεώδη ενός δακτυλίου R, τότε υπάρχει ένας ισομορφισμός υποδακτυλίων πηλίκο (χωρίς μονάδα):*

$$I + J \big/ J \ \cong \ I \big/ (I \cap J) \quad ▲$$

8.3.3 Το Τρίτο Θεώρημα Ισομορφισμών

Αν I είναι ένα ιδεώδες του δακτυλίου R, τότε το Τρίτο Θεώρημα Ισομορφισμών περιγράφει τους δακτυλίους πηλίκα των ιδεωδών του δακτυλίου πηλίκου R/I.

Θεώρημα 8.3.10 (3ο Θεώρημα Ισομορφισμών Δακτυλίων)**.** *Έστω $I \subseteq R$ και $J \subseteq R$ ιδέωδη ενός δακτυλίου R, και υποθέτουμε οτι: $J \subseteq I$. Τότε η ομάδα πηλίκο I/J είναι ένα ιδεώδες του δακτυλίου πηλίκου R/J και υπάρχει ένας ισομορφισμός δακτυλίων:*

$$R/J\big/I/J \xrightarrow{\cong} R/I$$

Απόδειξη. Θεωρούμε τους δακτυλίους πηλίκα R/I και R/J, και οριζουμε απεικόνιση

$$f : R/J \longrightarrow R/I, \quad f(x+J) = x+I$$

Θα δείξουμε ότι η f είναι ένας καλά ορισμένος επιμορφισμός δακτυλίων με πυρήνα το ιδεώδες I/J.

1. Η f ΕΙΝΑΙ ΚΑΛΑ ΟΡΙΣΜΕΝΗ: Έστω $x+J = y+J$, όπου $x, y \in R$. Τότε επειδή $J \subseteq I$, θα έχουμε:

   $$x+J = y+J \implies x-y \in J \implies x-y \in I \implies x+I = y+I \implies f(x+J) = f(y+J)$$

   Επομένως η f είναι μια καλά ορισμένη απεικόνιση.

2. Η ΑΠΕΙΚΟΝΙΣΗ f ΕΙΝΑΙ ΟΜΟΜΟΡΦΙΣΜΟΣ ΔΑΚΤΥΛΙΩΝ: Προφανώς $f(1_{R/J}) = f(1_R + J) = 1_R + I = 1_{R/I}$. Έστω $x+J, y+J \in R/J$. Τότε θα έχουμε:

   $$f\big((x+J)+(y+J)\big) = f((x+y)+J) = (x+y)+I = (x+I)+(y+I) = f(x+J)+f(y+J)$$

   $$f\big((x+J)\cdot(y+J)\big) = f((x\cdot y)+J) = (x\cdot y)+I = (x+I)\cdot(y+I) = f(x+J)\cdot f(y+J)$$

   Επομένως η f είναι ένας ομομορφισμός δακτυλίων.

3. Ο ΟΜΟΜΟΡΦΙΣΜΟΣ f ΕΙΝΑΙ ΕΠΙΜΟΡΦΙΣΜΟΣ: Έστω $x+I \in R/I$. Τότε υπάρχει η πλευρική κλάση $x \in R/J$ είναι τέτοια ώστε $f(x+J) = x+I$. Επομένως η απεικόνιση f είναι επιμορφισμός.

4. $\mathsf{Ker}(f) = I/J$: Θα υπολογίσουμε τον πυρήνα του επιμορφισμού f:

   $$\mathsf{Ker}(f) = \big\{x+J \in R/J \mid f(x+J) = 0_{R/I}\big\} = \big\{x+J \in R/J \mid x+I = I\big\} = \big\{x+J \in R/J \mid x \in I\big\} = I/J$$

   Άρα $\mathsf{Ker}(f) = I/J$. Επειδή ο πυρήνας ενός ομομορφισμού δακτυλίων είναι πάντα ιδεώδες, έπεται ότι I/J είναι ένα ιδεώδες του δακτυλίου R/J.

Από το Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων 8.3.1, έπεται ότι ο επιμορφισμός f επάγει υπάρχει έναν ισομορφισμό μεταξύ των δακτυλίων $R/J\big/I/J$ και R/I. ■

8.3.4 Το Θεώρημα Αντιστοιχίας

Κλείνουμε την παρούσα υποενότητα με το ακόλουθο αποτέλεσμα το οποίο, δοθέντος ενός ομομορφισμού δακτυλίων $f : R \longrightarrow S$, μας δίνει μια «1-1» και «επί» αντιστοιχία μεταξύ των υποδακτυλίων του R οι οποίοι περιέχουν τον πυρήνα του f, και των υποδακτυλίων του S οι οποίοι περιέχονται στην εικόνα του f. Επιπρόσθετα, αυτή η αντιστοιχία διατηρεί ιδεώδη και συμπεριφέρεται καλά ως προς τους επαγόμενους δακτύλιους πηλίκα. Το ακόλουθο Θεώρημα αναφέρεται κάποιες φορές στη βιβλιογραφία και ως *Τέταρτο Θεώρημα Ισομορφισμών*.

Θεώρημα 8.3.11 (Θεώρημα Αντιστοιχίας Ι)**.** *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός δακτυλίων.*

1. *Η απεικόνιση*

$$\Phi : \{I : \text{ υποδακτύλιος του } R \mid \mathsf{Ker}(f) \subseteq I\} \longrightarrow \{K \text{ υποδακτύλιος του } S \mid K \subseteq \mathsf{Im}(f)\}, \quad \Phi(I) = f(I)$$

είναι «1-1» και «επί», με αντίστροφη την απεικόνιση:

$$\Psi : \{K \text{ υποδακτύλιος του } S \mid K \subseteq \mathsf{Im}(f)\} \longrightarrow \{I \text{ υποδακτύλιος του } R \mid \mathsf{Ker}(f) \subseteq I\}, \quad \Psi(K) = f^{-1}(K)$$

2. *Επιπλέον η απεικόνιση Ψ διατηρεί ιδεώδη, με άλλα λόγια:*

$$K : \text{ ιδεώδες του } S \implies \Psi(K) = f^{-1}(K) : \text{ ιδεώδες του } R$$

Αν ο ομομορφισμός δακτυλίων f είναι επιμορφισμός, τότε η απεικόνιση Φ διατηρεί ιδεώδη, δηλαδή:

$$I : \text{ ιδεώδες του } R \implies \Phi(I) = f(I) : \text{ ιδεώδες του } S$$

και ορίζει μια «1-1» και «επί» αντιστοιχία, με αντίστροφη την Ψ, ανάμεσα στα ιδεώδη του R τα οποία περιέχουν τον πυρήνα του f, και στα ιδεώδη του S τα οποία περιέχονται στην εικόνα του f.

3. *Έστω ότι ο f είναι επιμορφισμός δακτυλίων.*

   (α') Αν K είναι ένα ιδεώδες του S, τότε υπάρχει ένας ισομορφισμός δακτυλίων

$$R/f^{-1}(K) \xrightarrow{\cong} S/K$$

   (β') Αν I είναι ένα ιδεώδες του R, έτσι ώστε $\mathsf{Ker}(f) \subseteq I$, τότε υπάρχει ένας ισομορφισμός δακτυλίων

$$R/I \xrightarrow{\cong} S/f(I)$$

Απόδειξη. 1. Σύμφωνα με την Πρόταση 8.2.10, για κάθε υποδακτύλιο I του R, το υποσύνολο $\Phi(I) = f(I)$ είναι υποδακτύλιος του S και για κάθε υποδακτύλιο K του S, το υποσύνολο $\Psi(K) = f^{-1}(K)$ είναι υποδακτύλιος του R. Προφανώς $f(I) \subseteq \mathsf{Im}(f)$. Αν $K \subseteq \mathsf{Im}(f)$, τότε επειδή $\{0_S\} \subseteq K$, έπεται ότι θα έχουμε $\mathsf{Ker}(f) = f^{-1}(\{0_S\}) \subseteq f^{-1}(K)$.

Μένει να δείξουμε ότι, για κάθε υποδακτύλιο I του R και κάθε υποδακτύλιο K του S, έχουμε:

$$\mathsf{Ker}(f) \subseteq I \implies f^{-1}(f(I)) = I \quad \text{και} \quad K \subseteq \mathsf{Im}(f) \implies f(f^{-1}(K)) = K$$

Κατ' αρχήν, αν $x \in I$, τότε $f(x) \in f(I)$ και αυτό σημαίνει ότι $x \in f^{-1}(f(I))$. Άρα πάντα έχουμε $I \subseteq f^{-1}f(I))$. Έστω τώρα ότι $\mathsf{Ker}(f) \subseteq I$, και έστω $x \in f^{-1}(f(I))$. Τότε $f(x) \in f(I)$, και άρα $f(x) = f(y)$, για κάποιο $y \in I$. Τότε όμως θα έχουμε $f(x-y) = 0_S$, και άρα $x - y \in \mathsf{Ker}(f) \subseteq I$. Τότε $x - y = z \in I$ και άρα $x = y + z \in I$ διότι το I είναι ιδεώδες και $y, z \in I$. Άρα $f^{-1}(f(I)) \subseteq I$, και επομένως $I = f^{-1}(f(I))$.

Παρόμοια, αν $x \in f(f^{-1}(K))$, τότε $x = f(y)$ για κάποιο $y \in f^{-1}(K)$, και άρα $f(y) = x \in K$. Επομένως $f(f^{-1}(K)) \subseteq K$. Αντίστροφα, έστω $x \in K$. Επειδή $K \subseteq \mathsf{Im}(f)$, έπεται ότι υπάρχει $y \in R$ έτσι ώστε $x = f(y)$. Τότε $y \in f^{-1}(K)$ και άρα $x = f(y) \in f(f^{-1}(K))$. Άρα $K \subseteq f(f^{-1}(K))$ και επομένως: $K = f(f^{-1}(K))$.

2. Σύμφωνα με την Πρόταση 8.2.10, για κάθε ιδεώδες K του S, το υποσύνολο $\Psi(K) = f^{-1}(K)$ είναι ιδεώδες του R, και αν ο f ειναι επιμορφισμός, τότε για κάθε ιδέωδες I του R, το υποσύνολο $\Phi(I) = f(I)$ είναι ιδεώδες του S. Στην τελευταία περίπτωση προφανώς, όπως και στο μέρος 1., η απεικόνιση Φ ορίζει μια «1-1» και «επί» αντιστοιχία, με αντίστροφη την Ψ, ανάμεσα στα ιδεώδη του R τα οποία περιέχουν τον πυρήνα του f, και στα ιδεώδη του S τα οποία περιέχονται στην εικόνα του f.

3. Υποθέτουμε οτι ο f είναι επιμορφισμός.

(α') Ορίζουμε απεικόνιση

$$f^* : R \longrightarrow S/K, \quad f^*(x) = f(x) + K$$

Δηλαδή η f^* είναι η σύνθεση του επιμορφισμού f και του κανονικού επιμορφισμού $\pi_K : S \longrightarrow S/K$. Άρα η f^* είναι επιμορφισμός δακτυλίων. Υπολογίζουμε τον πυρήνα της f^*:

$$\mathsf{Ker}(f^*) = \{x \in R \mid f^*(x) = 0_{S/K}\} = \{x \in R \mid f(x) + K = K\} = \{x \in R \mid f(x) \in K\} = f^{-1}(K)$$

Από το Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων 8.3.1, έπεται ότι ο επιμορφισμός f^* επάγει έναν ισομορφισμό μεταξύ των δακτυλίων $R/f^{-1}(K)$ και S/K.

(β') Ορίζουμε απεικόνιση

$$f^\dagger : R \longrightarrow S/f(I), \quad f^\dagger(x) = f(x) + f(I)$$

Δηλαδή η f^* είναι η σύνθεση του επιμορφισμού f και του κανονικού επιμορφισμού $\pi_{f(I)} : S \longrightarrow S/f(I)$. Άρα η $f^\dagger$ είναι επιμορφισμός δακτυλίων. Όπως και παραπάνω, επειδή $\mathsf{Ker}(f) \subseteq I$, αν $f(x) \in f(I)$, τότε $x \in I$. Επομένως για τον υπολογισμό του πυρήνα της $f^\dagger$, θα έχουμε:

$$\mathsf{Ker}(f^\dagger) = \{x \in R \mid f^\dagger(x) = 0_{S/f(I)}\} = \{x \in R \mid f(x) + f(I) = f(I)\} = \{x \in R \mid f(x) \in f(I)\} = \{x \in R \mid x \in I\} = I$$

Από το Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων 8.3.1, έπεται ότι ο επιμορφισμός $f^\dagger$ επάγει έναν ισομορφισμό μεταξύ των δακτυλίων R/I και $S/f(I)$. ■

Ως πόρισμα έχουμε το ακόλουθο πολύ χρήσιμο αποτέλεσμα, το οποίο είναι γνωστό και ως Θεώρημα Αντιστοιχίας ιδεωδών, και το οποίο περιγράφει τα ιδεώδη ενός δακτυλίου πηλίκου.

Πόρισμα 8.3.12 (Θεώρημα Αντιστοιχίας II). *Έστω $I \subseteq R$ ένα ιδεώδες του δακτυλίου R. Τότε η απεικόνιση*

$$\Phi : \{\text{ιδεώδη } J \text{ του } R \text{ έτσι ώστε} : I \subseteq J\} \longrightarrow \{\text{ιδεώδη } K \text{ του } R/I\}$$

$$\Phi(J) = \pi_I(J) = J/I$$

είναι «1-1» και «επί».

Απόδειξη. Η απόδειξη είναι άμεση απόρροια του Θεωρήματος 8.3.11 όταν αυτό εφαρμοσθεί στον επιμορφισμό ομάδων $\pi_I : R \longrightarrow R/I$, του οποίου ο πυρήνας είναι το ιδεώδες I. ■

8.3.5 Το Κινεζικό Θεώρημα Υπολοίπων

Θα δούμε την γενική μορφή του Κινεζικού Θεωρήματος Υπολοίπων το οποίο είναι γνωστό από τη στοιχειώδη Θεωρία Αριθμών, όπου εκεί χρησιμοποιείται για την επίλυση συστημάτων γραμμικών ισοτιμιών. Εδώ θα προκύψει ως ειδική περίπτωση ενός γενικότερου θεωρήματος για δακτυλίους.

Θεώρημα 8.3.13. *Έστω $f_1 : R \longrightarrow S_1$ και $f_2 : R \longrightarrow S_2$ δύο ομομορφισμοί δακτυλίων. Τότε η απεικόνιση*

$$f : R \longrightarrow S_1 \times S_2, \quad f(r) = (f_1(r), f_2(r))$$

είναι ένας ομομορφισμός δακτυλίων με πυρήνα $\mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)$. Αν οι f_1 και f_2 είναι επιμορφισμοί και

$$\mathsf{Ker}(f_1) + \mathsf{Ker}(f_2) = R$$

τότε ο ομομορφισμός f είναι επιμορφισμός και επάγει έναν ισομορφισμό δακτυλίων:

$$R\big/\big((\mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)\big) \xrightarrow{\cong} S_1 \times S_2$$

Απόδειξη. Θα έχουμε $f(1_R) = (f_1(1_R), f_2(1_R)) = (1_{S_1}, 1_{S_2}) = 1_{S_1 \times S_2}$. Αν $r, r' \in R$, τότε θα έχουμε:

$$f(r+r') = (f_1(r+r'), f_2(r+r')) = (f_1(r)+f_1(r'), f_2(r)+f_2(r')) = (f_1(r), f_2(r)) + (f_1(r'), f_2(r')) = f(r)+f(r')$$

$$f(r\cdot r') = (f_1(r\cdot r'), f_2(r\cdot r')) = (f_1(r)\cdot f_1(r'), f_2(r)\cdot f_2(r')) = (f_1(r), f_2(r))\cdot(f_1(r'), f_2(r')) = f(r)\cdot f(r')$$

Άρα η f είναι ομομορφισμός δακτυλίων, και αν $r \in \mathsf{Ker}(f)$, τότε $(0,0) = f(r) = (f_1(r), f_2(r))$ και άρα $f_1(r) = 0$ και $f_2(r) = 0$, δηλαδή $r \in \mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)$. Αντίστροφα, αν $r \in \mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)$, τότε $f_1(r) = 0$ και $f_2(r) = 0$ από όπου άμεσα προκύπτει ότι $r \in \mathsf{Ker}(f)$. Επομένως

$$\mathsf{Ker}(f) = \mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)$$

Υποθέτουμε ότι οι ομομορφισμοί f_1 και f_2 είναι επιμορφισμοί και $\mathsf{Ker}(f_1) + \mathsf{Ker}(f_2) = R$. Τότε μπορούμε να γράψουμε $1_R = r_1 + r_2$, όπου $r_1 \in \mathsf{Ker}(f_1)$ και $r_2 \in \mathsf{Ker}(f_2)$. Έστω $z \in S_1$ και $w \in S_2$. Επειδή οι απεικονίσεις f_1 και f_2 είναι επιμορφισμοί, υπάρχουν $x, y \in R$, έτσι ώστε $f_1(x) = z$ και $f_2(y) = w$. Τότε:

$$f(r_1\cdot y + r_2\cdot x) = \big(f_1(r_1\cdot y + r_2\cdot x), f_2(r_1\cdot y + r_2\cdot x)\big) = \big(f_1(r_1)\cdot f_1(y) + f_1(r_2)\cdot f_1(x), f_2(r_1)\cdot f_2(y) + f_2(r_2)\cdot f_2(x)\big)$$

$$= \big(f_1(r_2)\cdot f_1(x), f_2(r_1)\cdot f_2(y)\big) = \big(f_1(x), f_2(y)\big) = (z, w)$$

όπου η προτελευταία ισότητα πρέκυψε διότι $f_1(r_2)\cdot f_1(x) = f_1(r_2\cdot x) = f_1(x)$ διότι $f_1(r_2\cdot x - x) = f_1\big((r_2-1)\cdot x\big) = f_1(r_1\cdot x) = f_1(r_1)\cdot f_1(x) = 0\cdot f_1(x) = 0$, και παρόμοια $f_2(r_1)\cdot f_2(y) = f_2(y)$. Άρα η απεικόνιση f είναι «επί».

Από το Πρώτο Θεώρημα Ισομορφισμών ο ομομορφισμός f επάγει έναν ισομορφισμό δακτυλίων

$$R\big/\big((\mathsf{Ker}(f_1) \cap \mathsf{Ker}(f_2)\big) \xrightarrow{\cong} S_1 \times S_2$$ ■

Πόρισμα 8.3.14 (Κινεζικό Θεώρημα Υπολοίπων)**.** *Έστω I, J δύο ιδεώδη του δακτυλίου R. Αν $I + J = R$, τότε η απεικόνιση $f\colon R \longrightarrow R/I \times R/J$, $f(r) = (r + I, r + J)$, επάγει έναν ισομορφισμό δακτυλίων:*

$$R\big/I \cap J \xrightarrow{\cong} R/I \times R/J$$

Απόδειξη. Η απόδειξη είναι άμεση συνέπεια του Θεωρήματος 8.3.13 εφαρμοσμένου στους κανονικούς επιμορφισμούς $R \longrightarrow R/I$ και $R \longrightarrow R/J$. ■

Υπενθυμίζουμε ότι μια πεπερασμένη οικογένεια ιδεωδών $\{I_k\}_{k=1}^n$ του δακτυλίου R αποτελείται από ανά δύο συμμέγιστα ιδεώδη, αν $I_i + I_j = R$, $1 \le i \ne j \le n$.

Θεώρημα 8.3.15 (Κινεζικό Θεώρημα Υπολοίπων - Γενική Μορφή)**.** *Έστω $\{I_k\}_{k=1}^n$ μια οικογένεια ανά δύο συμμέγιστων ιδεωδών του δακτυλίου R. Τότε υπάρχει ένας ισομορφισμός δακτυλίων*

$$R\Big/\bigcap_{k=1}^{n} I_k \xrightarrow{\cong} R/I_1 \times \cdots \times R/I_n$$

Απόδειξη. Θα κατασκευάσουμε έναν επιμορφισμό δακτυλίων $f\colon R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n$ με πυρήνα $\mathsf{Ker}(f) = \bigcap_{k=1}^n I_k$.

Θεωρούμε την απεικόνιση

$$f\colon R \longrightarrow R/I_1 \times R/I_2 \times \cdots \times R/I_n, \quad f(r) = (r + I_1, r + I_2, \cdots, r + I_n)$$

Η απεικόνιση f είναι ομομορφισμός δακτυλίων διότι $f(1_R) = (1_R + I_1, \cdots, 1_R + I_n) = 1_{\prod_{k=1}^n R/I_k}$. Επιπλέον, αν $r, s \in R$, τότε:

$$f(r+s) = (r+s+I_1, \cdots, r+s+I_n) = (r+I_1, \cdots, r+I_n) + (s+I_1, \cdots, s+I_n) = f(r)+f(s)$$

$$f(r\cdot s) = (r\cdot s+I_1, \cdots, r\cdot s+I_n) = (r+I_1, \cdots, r+I_n)\cdot(s+I_1, \cdots, s+I_n) = f(r)\cdot f(s)$$

Άρα η απεικόνιση f είναι ομομορφισμός δακτυλίων, και

$$\mathsf{Ker}(f) = \left\{r \in R \mid f(r) = 0_{\prod_{k=1}^n R/I_k}\right\} = \left\{r \in R \mid (r+I_1, r+I_2, \cdots, r+I_n) = (I_1, I_2, \cdots, I_n)\right\} =$$

$$= \left\{r \in R \mid r \in I_k,\ 1 \le k \le n\right\} = \bigcap_{k=1}^n I_k$$

Από το Πρώτο Θεώρημα Ισομορφισμών, ο ομομορφισμός f επάγει έναν μονομορφισμό δακτυλίων

$$\widetilde{f}:\ R\Big/\bigcap_{k=1}^n I_k \longrightarrow R/I_1 \times \cdots \times R/I_n, \quad \widetilde{f}(r + \cap_{k=1}^n I_k) = f(r)$$

και επομένως αρκεί να δείξουμε ότι ο $\widetilde{f}$ ή ισοδύναμα η f, είναι «επί».

- Ισχυρισμός: *Υπάρχουν στοιχεία $s_1, s_2, \cdots, s_n \in R$, έτσι ώστε:*

$$\forall\, k = 1, 2, \cdots, n: \quad s_k + I_k = 1_R + I_k \quad \text{και} \quad s_k + I_j = I_j, \quad \forall\, j:\ 1 \le j \ne k \le n$$

Πράγματι, επειδή τα ιδεώδη $I_1, I_2, \cdots, I_n$ είναι ανά δύο συμμέγιστα, θα έχουμε ότι $I_i + I_j = R$, $1 \le i \ne j \le n$. Ιδιαίτερα θα έχουμε, για κάθε $k \ge 1$:

$$I_1 + I_k = R \implies \exists\ a_k \in I_1 \quad \text{και} \quad \exists\ b_k \in I_k: \quad a_k + b_k = 1_R$$

Θεωρούμε το στοιχείο

$$1_R = \prod_{k=2}^n (a_k + b_k) = (a_2 + b_2) \cdot (a_3 + b_3) \ \cdots\ (a_n + b_n)$$

το οποίο, όπως στην Πρόταση 8.1.32, στο ανάπτυγμά του είναι άθροισμα γινομένων των στοιχείων a_k, b_k, και ο μόνος όρος του αναπτύγματος ο οποίος δεν περιέχει ως παράγοντα ένα από τα στοιχεία a_k, $2 \le k \le n$, είναι ο όρος

$$s_1 = \prod_{k=2}^n b_k \in I_2 \ \cdots\ I_n$$

Έτσι μπορούμε να γράψουμε $1_R = x_1 + s_1$, όπου $x_1 \in I_1$ και $s_1 \in I_2 \ \cdots\ I_n \subseteq \bigcap_{k=2}^n I_k$, βλέπε την Πρόταση 8.1.32. Τότε, επειδή $x_1 \in I_1$, θα έχουμε $s_1 + I_1 = x_1 + s_1 + I_1 = 1_R + I_1$, και $s_1 + I_k = I_k$, $\forall\, k \ge 2$. Άρα δείξαμε την ύπαρξη του ζητούμενου στοιχείου s_1 με τις επιθυμητές ιδιότητες. Εργαζόμενοι ακριβώς ανάλογα, αποδεικνύουμε την ύπαρξη στοιχείων s_k, $k \ge 2$, με τις επιθυμητές ιδιότητες.

Έστω τώρα $(r_1 + I_1, r_2 + I_2, \cdots, r_n + I_n) \in \prod_{k=1}^n R/I_k$ ένα τυχαίο στοιχείο του δακτυλίου $\prod_{k=1}^n R/I_k$. Θεωρούμε το στοιχείο του R:

$$r = r_1 s_1 + r_2 s_2 + \cdots + r_n s_n$$

Τότε, χρησιμοποιώντας τον Ισχυρισμό, για κάθε $k \ge 1$, θα έχουμε:

$$(r_1 s_1 + r_2 s_2 + \cdots + r_n s_n) + I_k = r_k s_k + I_k = (r_k + I_k) \cdot (s_k + I_k) = (r_k + I_k) \cdot (1_R + I_k) = r_k + I_k$$

Επομένως

$$f(r) = f(r_1 s_1 + r_2 s_2 + \cdots + r_n s_n) = \big((r_1 s_1 + r_2 s_2 + \cdots + r_n s_n) + I_1,\ \big((r_1 s_1 + r_2 s_2 + \cdots + r_n s_n) + I_1\big)\big) =$$

$$= (r_1 + I_1, \cdots, r_n + I_n)$$

και άρα η f είναι επιμορφισμός. Επομένως η f επάγει έναν ισομορφισμό δακτυλίων

$$\widetilde{f}:\ R\Big/\bigcap_{k=1}^n I_k \xrightarrow{\ \cong\ } R/I_1 \times \cdots \times R/I_n$$

■

8.4 Εφαρμογές των Θεωρημάτων Ισομορφισμών

Στην παρούσα ενότητα θα δούμε διάφορα παραδείγματα και εφαρμογές των Θεωρημάτων Ισομορφισμών για Δακτυλίους.

8.4.1 Παραδείγματα

Παράδειγμα 8.4.1. Από το Παράδειγμα 8.2.19, έπεται ότι για κάθε μεταθετικό δακτύλιο R και κάθε στοιχείο $r \in R$, ορίζεται ο ομομορφισμός εκτίμησης

$$\Phi_r : R[t] \longrightarrow R, \quad \Phi_r(P(t)) = P(r)$$

ο οποίος είναι επιμορφισμός δακτυλίων. Ο πυρήνας $\mathsf{Ker}(\Phi_r)$ αποτελείται από όλα τα πολυώνυμα $P(t)$ για τα οποία $P(r) = 0$. Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε έναν ισομορφισμό δακτυλίων

$$R[t]/\mathsf{Ker}(\Phi_r) \xrightarrow{\cong} R \quad \surd$$

Παράδειγμα 8.4.2. Από την Πρόταση 8.2.22, έπεται ότι, αν $f : R \longrightarrow S$ είναι ένας ομομορφισμός μεταθετικών δακτυλίων, και $u \in R$, τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων $f^* : R[t] \longrightarrow S$ έτσι ώστε: $f^*(t) = u$, και $f^*(\mathsf{r}) = f(r)$, $\forall r \in R$. όπου $\mathsf{r} \in R[t]$ είναι το σταθερό πολυώνυμο $r \in R$. Ο ομομορφισμός f^* ορίζεται ως:

$$f^* : R[t] \longrightarrow S, \quad f^*(P(t)) = f^*\left(a_0 + a_1 t + \cdots + a_n t^n\right) = f(a_0) + f(a_1)u + \cdots + f(a_n)u^n$$

Τότε ο πυρήνας $\mathsf{Ker}(f^*)$ αποτελείται από όλα τα πολυώνυμα $P(t) \in R[t]$ έτσι ώστε $f^*(P(t)) = 0$, και:

$$\mathsf{Im}(f^*) = \left\{s_0 + s_1 u + s_2 u^2 + \cdots + s_n u^n \in S \mid s_k \in \mathsf{Im}(f),\ n \geq 0\right\}$$

Αν ο ομομορφισμός f είναι η κανονική έγκλειση $\iota : R \subseteq S$ ενός υποδακτυλίου του S και $u \in S$, τότε

$$\mathsf{Im}(\iota^*) = \left\{r_0 + r_1 u + r_2 u^2 + \cdots + r_n u^n \in S \mid r_k \in R,\ n \geq 0\right\} = R[u]$$

είναι ο υποδακτύλιος του S ο οποίος παράγεται υπεράνω του R από το u, και $\mathsf{Ker}(\iota^*) = \left\{P(t) \in R[t] \mid P(r) = 0\right\}$. Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε τότε:

$$R[t]/\mathsf{Ker}(\iota^*) \xrightarrow{\cong} R[u] \quad \surd$$

Παράδειγμα 8.4.3 (Το «Κλασικό» Κινεζικό Θεώρημα Υπολοίπων)**.** Θεωρούμε τον δακτύλιο $\mathbb{Z}_n$, όπου $n \geq 2$, και έστω

$$n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$$

η πρωτογενής ανάλυση του n, δηλαδή οι αριθμοί p_i είναι ανά δύο διαφορετικοί πρώτοι και $m, a_i \geq 1$. Θεωρούμε τα κύρια ιδεώδη $I_k = (p_k^{a_k})$ τα οποία παράγονται από τις δυνάμεις πρώτων $p_k^{a_k}$, $1 \leq k \leq m$. Επειδή οι αριθμοί $p_1^{a_1}$, $p_2^{a_2}$, $\cdots$, $p_m^{a_m}$ είναι ανά δύο πρώτοι μεταξύ τους, τα ιδεώδη I_k, $\leq k \leq m$ είναι ανά δύο συμμέγιστα, και τότε από τα Παραδείγματα 8.1.10 και 8.1.31, θα έχουμε:

$$(p_1^{a_1}) \cap (p_2^{a_2}) \cap \cdots \cap (p_m^{a_m}) = (p_1^{a_1}) \cdot (p_2^{a_2}) \cdots (p_m^{a_m}) = (p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m})\mathbb{Z} = n\mathbb{Z}$$

Τέλος, από το Θεώρημα 8.3.15, θα έχουμε:

$$\mathbb{Z}/n\mathbb{Z} \ \cong \ \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_m^{a_m}}$$

Γενικότερα, αν $\left\{n_i\right\}_{i=1}^k$ είναι ανά δύο πρώτοι μεταξύ τους θετικοί ακέραιοι, $(n_i, n_j) = 1$, $1 \leq i \neq j \leq k$, και $n = n_1 n_2 \cdots n_k$, τότε όπως παραπάνω θα έχουμε:

$$\mathbb{Z}/n\mathbb{Z} \ \cong \ \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

μέσω του ισομορφισμού $a+n\mathbb{Z} \longmapsto \big(a+n_1\mathbb{Z},\, a+n_2\mathbb{Z},\, \cdots,\, a+n_k\mathbb{Z}\big)$. Με άλλα λόγια, αν έχουμε ένα σύστημα γραμμικών ισοτιμιών

$$x \equiv a_1 \bmod n_1, \qquad x \equiv a_1 \bmod n_1, \cdots, \quad x \equiv a_k \bmod n_k, \qquad a_i \in \mathbb{Z},\ \ 1 \le i \le k \tag{Σ}$$

όπου $(n_i, n_j) = 1$, $1 \le i \ne j \le k$, και $n = n_1 n_2 \cdots n_k$, τότε έχουμε ένα στοιχείο

$$\big(a_1 + n_1\mathbb{Z},\, a_2 + n_2\mathbb{Z},\, \cdots,\, a_k + n_k\mathbb{Z}\big) \ \in\ \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$$

και άρα από τον παραπάνω ισομορφισμό υπάρχει στοιχείο $a \in \mathbb{Z}$ έτσι ώστε:

$$\big(a+n_1\mathbb{Z},\, a+n_2\mathbb{Z},\, \cdots,\, a+n_k\mathbb{Z}\big) = \big(a_1+n_1\mathbb{Z},\, a_2+n_2\mathbb{Z},\, \cdots,\, a_k+n_k\mathbb{Z}\big)$$

Αυτό σημαίνει ότι το σύστημα γραμμικών ισοτιμιών (Σ) έχει λύση την $a \bmod n_i$, $1 \le i \le k$, η οποία είναι μοναδική $\bmod n$. $\surd$

Παράδειγμα 8.4.4. 1. Θεωρούμε τον δακτύλιο $\mathbb{Z}$ των ακεραίων ως υποδακτύλιο του $\mathbb{C}$. Από το Παράδειγμα 8.4.2, επιλέγοντας $u = i$, έπεται ότι θα έχουμε έναν ισομορφισμό δακτυλίων $\mathbb{Z}[t]/\operatorname{Ker}(\iota^*) \cong \mathbb{Z}[i]$, όπου $\mathbb{Z}[i]$ είναι ο δακτύλιος των ακεραίων του Gauss. Το ιδεώδες $\operatorname{Ker}(\iota^*)$ αποτελείται από όλα τα πολυώνυμα $P(t) \in \mathbb{Z}[t]$, έτσι ώστε $P(i) = 0$. Όπως και στο Παράδειγμα 8.2.5, μπορούμε να δούμε ότι $\operatorname{Ker}(\iota^*) = (t^2+1)$, και επομένως από το Πρώτο Θεώρημα ισομορφισμών θα έχουμε:

$$\mathbb{Z}[t]/(t^2+1) \xrightarrow{\ \cong\ } \mathbb{Z}[i]$$

Παρόμοια εργαζόμενοι, θα έχουμε έναν ισομορφισμό δακτυλίων

$$\mathbb{Q}[t]/(t^2+1) \xrightarrow{\ \cong\ } \mathbb{Q}[i] \qquad \text{και} \qquad \mathbb{R}[t]/(t^2+1) \xrightarrow{\ \cong\ } \mathbb{R}[i] = \mathbb{C}$$

2. Θεωρούμε το σώμα $\mathbb{Q}$ των ρητών ως υποδακτύλιο του $\mathbb{R}$. Από το Παράδειγμα 8.4.2, επιλέγοντας $u = \sqrt{5}$, έπεται ότι θα έχουμε έναν ισομορφισμό δακτυλίων $\mathbb{Q}[t]/\operatorname{Ker}(\iota^*) \cong \mathbb{Q}[\sqrt{5}]$, όπου $\mathbb{Q}[\sqrt{5}] = \big\{a + b\sqrt{5} \in \mathbb{R} \mid a, b \in \mathbb{Q}\big\}$ Το ιδεώδες $\operatorname{Ker}(\iota^*)$. αποτελείται από όλα τα πολυώνυμα $P(t) \in \mathbb{Q}[t]$, έτσι ώστε $P(\sqrt{5}) = 0$. Όπως και στο Παράδειγμα 8.2.5, μπορούμε να δούμε ότι $\operatorname{Ker}(\iota^*) = (t^2-5)$, και επομένως από το Πρώτο Θεώρημα ισομορφισμών θα έχουμε:

$$\mathbb{Q}[t]/(t^2-5) \xrightarrow{\ \cong\ } \mathbb{Q}[\sqrt{5}]$$

3. Θεωρούμε το πολυώνυμο $t^2 - 4 \in \mathbb{R}[t]$. Θα περιγράψουμε τον δακτύλιο πηλίκο $\mathbb{R}[t]/(t^2-4)$. Ορίζουμε απεικόνιση

$$f\colon \mathbb{R}[t] \longrightarrow \mathbb{R} \times \mathbb{R}, \quad f(P(t)) = (P(2), P(-2))$$

Τότε $f(1) = (1,1) = 1_{\mathbb{R}\times\mathbb{R}}$. Η απεικόνιση f είναι ομομορφισμός δακτυλίων. Πράγματι, έχουμε τους ομομορφισμούς εκτίμησης $f_1\colon \mathbb{R}[t] \longrightarrow \mathbb{R}$, $f_1(P(t)) = P(2)$ και $f_2\colon \mathbb{R}[t] \longrightarrow \mathbb{R}$, $f_2(P(t)) = P(-2)$, οι οποίοι επάγουν, σύμφωνα με το Θεώρημα 8.3.13, έναν ομομορφισμό δακτυλίων ο οποίος συμπίπτει με τον f. Επειδή προφανώς $\operatorname{Ker}(f_1) = (t-2)$ και $\operatorname{Ker}(f_2) = (t+2)$, θα έχουμε

$$\operatorname{Ker}(f) = \operatorname{Ker}(f_1) \cap \operatorname{Ker}(f_2) = (t-2) \cap (t+2) = \big((t-2)\cdot(t+2)\big) = (t^2-4)$$

Από την άλλη πλευρά, οι ομομορφισμοί f_1 και f_2 είναι επιμορφισμοί, και επειδή $\frac{1}{4}(t+2) - \frac{1}{4}(t-2) = 1$, έπεται ότι για κάθε πολυώνυμο $P(t) \in \mathbb{R}[t]$ θα έχουμε:

$$P(t) = (-\frac{1}{4}P(t)(t-2) + \frac{1}{4}P(t)(t+2) \in \operatorname{Ker}(f_1) + \operatorname{Ker}(f2) \quad \Longrightarrow \quad \mathbb{R}[t] = \operatorname{Ker}(f_1) + \operatorname{Ker}(f2)$$

Επομένως από το Θεώρημα 8.3.13 θα έχουμε έναν ισομορφισμό $\mathbb{R}[t]/(t^2-4) \cong \mathbb{R} \times \mathbb{R}$. $\surd$

Παράδειγμα 8.4.5. Έστω το πολυώνυμο $t^2+at+b \in \mathbb{R}[t]$. Θα περιγράψουμε τον δακτύλιο πηλίκο

$$\mathbb{R}[t]/(t^2+at+b)$$

Ειδικότερα θα δείξουμε ότι:

1. Αν $a^2-4b>0$, τότε:
$$\mathbb{R}[t]/(t^2+at+b) \xrightarrow{\cong} \mathbb{R}\times\mathbb{R}$$
2. Αν $a^2-4b=0$, τότε:
$$\mathbb{R}[t]/(t^2+at+b) \xrightarrow{\cong} \mathbb{R}[t]\big(t^2\big)$$
3. Αν $a^2-4b<0$, τότε:
$$\mathbb{R}[t]/(t^2+at+b) \xrightarrow{\cong} \mathbb{C}$$

1. Υποθέτουμε ότι $\Delta = a^2-4b>0$, δηλαδή η διακρίνουσα Δ του τριωνύμου t^2+at+b είναι θετική και άρα το t^2+at+b έχει δύο διακεκριμένες ρίζες, έστω $\rho,\sigma\in\mathbb{R}$. Έτσι θα έχουμε $t^2+at+b=(t-\rho)(t-\sigma)$. Θεωρούμε τους ομομορφισμούς εκτίμησης
$$f_1\colon \mathbb{R}[t]\longrightarrow\mathbb{R},\quad f_1(P(t))=P(\rho) \qquad \text{και} \qquad f_2\colon \mathbb{R}[t]\longrightarrow\mathbb{R},\quad f_2(P(t))=P(\sigma)$$
Από το Παράδειγμα 8.2.19 θα έχουμε $\mathsf{Ker}(f_1)=(t-\rho)$ και $\mathsf{Ker}(f_2)=(t-\sigma)$ και ισομορφισμούς δακτυλίων:
$$\mathbb{R}[t]/(t-\rho) \xrightarrow{\cong} \mathbb{R} \xleftarrow{\cong} \mathbb{R}[t]/(t-\sigma)$$
Όπως στο Θεώρημα 8.3.13, θεωρούμε τον επαγόμενο ομομορφισμό δακτυλίων
$$f\colon \mathbb{R}[t]\longrightarrow\mathbb{R}\times\mathbb{R},\quad f(P(t))=\big(P(\rho),P(\sigma)\big)$$
με πυρήνα $\mathsf{Ker}(f_1)\cap\mathsf{Ker}(f_2)=(t-\rho)\cap(t-\sigma)$. Δείχνουμε ότι $(t-\rho)\cap(t-\sigma)=\big((t-\rho)(t-\sigma)\big)$. Προφανώς $(t-\rho)(t-\sigma)\subseteq(t-\rho)\cap(t-\sigma)$. Έστω $P(t)\in(t-\rho)\cap(t-\sigma)$. Τότε θα έχουμε $P(t)=Q_1(t)(t-\rho)=Q_2(t)(t-\sigma)$. Τότε $Q_2(\rho)(\rho-\sigma)=0$, απ' όπου $Q_2(\rho)=0$, διότι $\rho\neq\sigma$. Αυτό, όπως και πριν, σημαίνει ότι $Q_2(t)=Q_3(t)(t-\rho)$ και άρα $P(t)=Q_2(t)(t-\sigma)=Q_3(t)(t-\rho)(t-\sigma)\in\big((t-\rho)(t-\sigma)\big)$. Έτσι, $\mathsf{Ker}(f)=\big((t-\rho)(t-\sigma)\big)$.
Δείχνουμε ότι $\mathsf{Ker}(f_1)+\mathsf{Ker}(f_2)=\mathbb{R}[t]$. Πράγματι, επειδή $\rho\neq\sigma$, μπορούμε να γράψουμε:
$$\frac{1}{\sigma-\rho}(t-\rho)+\frac{-1}{\sigma-\rho}(t-\sigma)=1 \implies \forall P(t)\in\mathbb{R}[t]\colon\quad P(t)=\frac{P(t)}{\sigma-\rho}(t-\rho)+\frac{-P(t)}{\sigma-\rho}(t-\sigma)\ \in\ (t-\rho)+(t-\sigma)$$
και επομένως $\mathsf{Ker}(f_1)+\mathsf{Ker}(f_2)=\mathbb{R}[t]$. Τότε, από το Θεώρημα 8.3.13, η απεικόνιση f επάγει έναν ισομορφισμό
$$f\colon \mathbb{R}[t]\big/(t^2+at+b) \xrightarrow{\cong} \mathbb{R}\times\mathbb{R},\quad f(P(t))=\big((P(\rho),P(\sigma)\big)$$

2. Υποθέτουμε ότι $\Delta=a^2-4b=0$, δηλαδή η διακρίνουσα Δ του τριωνύμου t^2+at+b είναι μηδέν και άρα το t^2+at+b έχει μια διπλή πραγματική ρίζα ρ. Έτσι θα έχουμε $t^2+at+b=(t-\rho)^2$. Θα δείξουμε ότι
$$\mathbb{R}[t]\big/(t-\rho)^2 \xrightarrow{\cong} \big/\mathbb{R}[t]/(t^2)$$
Από την Πρόταση 8.2.22, έπεται ότι η κανονική έγκλειση $\mathbb{R}\longrightarrow\mathbb{R}[t]$, επεκτείνεται μοναδικά σε έναν ομομορφισμό δακτυλίων
$$f\colon \mathbb{R}[t]\longrightarrow\mathbb{R}[t],\quad f(P(t))=P(t+\rho)$$
έτσι ώστε $f(t)=t+\rho$ και $f(r)=r$, $\forall t\in\mathbb{R}$. Προφανώς ο ομομορφισμός f είναι ισομορφισμός με αντίστροφο τον ισομορφισμό
$$g\colon \mathbb{R}[t]\longrightarrow\mathbb{R}[t],\quad g(P(t))=P(t-\rho)$$

Πράγματι $g(f(P(t)) = g(P(t+\rho)) = P(t-\rho+\rho)) = P(t)$ και παρόμοια $f(g(P(t)) = f(P(t-\rho)) = P(t+\rho-\rho)) = P(t)$. Μέσω αυτών των ισομορφισμών θα έχουμε $f((t-\rho)^2) = t^2$ και $g(t^2) = (t-\rho)^2$. Ως άμεση συνέπεια θα έχουμε ότι η απεικόνιση

$$\widetilde{f}\colon \mathbb{R}[t]/(t^2+at+b) \xrightarrow{\cong} \mathbb{R}[t]/(t^2), \quad \widetilde{f}\big(P(t)+(t^2+at+b)\big) = P(t+\rho)+(t^2)$$

είναι ισομορφισμός δακτυλίων. Για μια διαφορετική περιγραφή του δακτυλίου $\mathbb{R}[t]/(t^2)$ ως δακτυλίου δυϊκών αριθμών παραπέμπουμε στο Παράδειγμα 8.4.12.

3. Υποθέτουμε ότι $a^2-4b<0$, δηλαδή η διακρίνουσα $\Delta = a^2-4b<0$ του τριωνύμου t^2+at+b είναι αρνητική και άρα το t^2+at+b δεν έχει πραγματικές ρίζες, αλλά τις μιγαδικές ρίζες

$$\rho = \frac{-a+i\sqrt{4b-a^2}}{2} \quad \text{και} \quad \overline{\rho} = \frac{-a-i\sqrt{4b-a^2}}{2}$$

Από την Πρόταση 8.2.22, έπεται ότι η κανονική έγκλειση $f\colon \mathbb{R} \longrightarrow \mathbb{C}$, επεκτείνεται μοναδικά σε έναν ομομορφισμό δακτυλίων

$$f\colon \mathbb{R}[t] \longrightarrow \mathbb{C}, \quad f(P(t)) = P(\rho)$$

έτσι ώστε $f(t)=\rho$ και $f(r)=r$, $\forall\, t\in\mathbb{R}$. Προφανώς $(t^2+at+b)\subseteq \mathsf{Ker}(f)$, διότι στο σώμα των μιγαδικών αριθμών έχουμε $\rho^2+a\rho+b=0$. Αν $P(t)\in\mathsf{Ker}(f)$, τότε $P(t)=Q(t)(t^2+at+b)+R(t)$, όπου είτε $R(t)=0$ είτε $R(t)=k+lt$, $k,l\in\mathbb{R}$, $(k,l)\neq(0,0)$. Στην δεύτερη περίπτωση θα έχουμε $0=P(\rho)=Q(\rho)(\rho^2+a\rho+b)+(k+l\rho)$, από όπου $k+l\rho=0$, και αυτό είναι άτοπο διότι $\rho\in\mathbb{C}$. Άρα $R(t)=0$ και επομένως $P(t)=Q(t)(t^2+at+b)\in(t^2+at+b)$. Έτσι, τελικά θα έχουμε: $\mathsf{Ker}(f)=(t^2+at+b)$.

Έτσι ο ομομορφισμός f επάγει έναν μονομορφισμό δακτυλίων

$$\widetilde{f}\colon \mathbb{R}[t]/(t^2+at+b) \longrightarrow \mathbb{C}, \quad \widetilde{f}\big(P(t)+(t^2+at+b)\big) = f(P(t)) = P(\rho)$$

και όπως παραπάνω $P(t)=Q(t)(t^2+at+b)+(k+lt)$, οπότε $P(t)+(t^2+at+b)=k+lt+(t^2+at+b)$ και $P(\rho)=k+l\rho$. Τέλος, δείχνουμε ότι η f είναι «επί». Έστω $r+si\in\mathbb{C}$, όπου $r,s\in\mathbb{R}$. Τότε αναζητούμε πολυώνυμο $k+lt$ έτσι ώστε $P(\rho)=k+l\rho=r+is$. Αναλύοντας αυτή τη σχέση θα έχουμε

$$k+l\rho=r+si \implies k+l\frac{-a+i\sqrt{4b-a^2}}{2}=r+si \implies k-\frac{al}{2}+\frac{l\sqrt{4b-a^2}}{2}i=r+si \implies$$
$$\implies l=\frac{2s}{\sqrt{4b-a^2}} \quad \text{και} \quad k=r+\frac{as}{\sqrt{4b-a^2}}$$

Τότε προφανώς $\widetilde{f}\big(k+lt+(t^2+at+b)\big)=r+si$ και η $\widetilde{f}$ είναι «επί» και άρα θα είναι ισομορφισμός

$$\widetilde{f}\colon \mathbb{R}[t]/(t^2+at+b) \xrightarrow{\cong} \mathbb{C}, \quad \widetilde{f}\big(P(t)+(t^2+at+b)\big) = f(P(t)) = P(\rho)$$

Οι δακτύλιοι $\mathbb{R}\times\mathbb{R}$, $\mathbb{R}[t]/(t^2)$, και $\mathbb{C}$, έχουν θεμελιώδεις διαφορές. Οι δύο πρώτοι δεν είναι ακέραιες περιοχές, ο τρίτος είναι σώμα, ο πρώτος δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία (είναι «ημιαπλός» δακτύλιος), και ο δεύτερος έχει μη μηδενικά μηδενοδύναμα στοιχεία (δεν είναι «ημιαπλός» δακτύλιος). $\surd$

Παράδειγμα 8.4.6. (Ι) Θα προσδιορίσουμε τον δακτύλιο πηλίκο $\mathbb{Z}[i]/(1+5i)$, όπου $(1+5i)=\{(a+bi)(1+5i)\in\mathbb{Z}[i] \mid a+bi\in\mathbb{Z}[i]\}$ είναι το κύριο ιδεώδες του $\mathbb{Z}[i]$ το οποίο παράγεται από το στοιχείο $1+5i$, δείχνοντας ότι:

$$\mathbb{Z}[i]/(1+5i) \xrightarrow{\cong} \mathbb{Z}_{26}$$

Θεωρούμε την απεικόνιση

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Z}[i]/(1+5i), \quad f(x)=x+(1+5i)$$

η οποία είναι ομομορφισμός ως σύνθεση της κανονικής έγκλεισης $\mathbb{Z}\longrightarrow\mathbb{Z}[i]$, $x\longmapsto x$, και της κανονικής προβολής $\mathbb{Z}[i]\longrightarrow\mathbb{Z}[i]/(1+5i)$, $a+bi\longmapsto a+bi+(1+5i)$.

1. Έστω $x \in \mathsf{Ker}(f)$. Τότε $f(x) = 0_{\mathbb{Z}[i]/(1+5i)}$, δηλαδή $x + (1+5i) = (1+5i)$, και άρα $x \in (1+5i)$. Επομένως υπάρχει $a+bi \in \mathbb{Z}[i]$, έτσι ώστε: $x = (a+bi)(1+5i) = (a-5b) + (5a+b)i$. Επειδή $x \in \mathbb{Z}$, έπεται ότι $5a+b = 0$, δηλαδή $b = -5a$. Τότε $x = a-5b = a-5(-5a) = a+25a = 26a$. Αυτό σημαίνει ότι $x \in 26\mathbb{Z}$ και επομένως $\mathsf{Ker}(f) \subseteq 26\mathbb{Z}$. Αντίστροφα, αν $x \in 26\mathbb{Z}$, τότε $x = 26a$ για κάποιο $a \in \mathbb{Z}$ και τότε $f(x) = 26a + (1+5i) = (1+5i)$ διότι $26a = (a-5ai)(1+5i) \in (1+5i)$. Άρα $x \in \mathsf{Ker}(f)$ και επομένως:

$$\mathsf{Ker}(f) = 26\mathbb{Z}$$

2. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφισμών, η απεικόνιση f επάγει έναν ισομορφισμό δακτυλίων

$$\widetilde{f}\colon \mathbb{Z}_{26} = \mathbb{Z}/26\mathbb{Z} \xrightarrow{\cong} \mathsf{Im}(f) \subseteq \mathbb{Z}[i]/(1+5i), \quad \widetilde{f}(x+26\mathbb{Z}) = f(x) + (1+5i) = x + (1+5i)$$

Έστω $a+bi+(1+5i) \in \mathbb{Z}[i]/(1+5i)$. Τότε υπάρχει ακέραιος $x \in \mathbb{Z}$ έτσι ώστε $f(x) = a+bi+(1+5i)$, δηλαδή $x+(1+5i) = a+bi+(1+5i)$, αν και μόνο αν $x-a-bi \in (1+5i)$, δηλαδή αν και μόνο αν υπάρχουν ακέραιοι $k,l \in \mathbb{Z}$ έτσι ώστε

$$x-a-bi = (k+li)(1+5i) \implies x-a-bi = k-5l+(5k+l)i \implies x-a = k-5l \quad \text{και} \quad -b = 5k+l$$

$$\implies x-a = k-5(-b-5k) = 26k+5b \implies x = a+5b+26k \implies x+26\mathbb{Z} = a+5b+26\mathbb{Z}$$

στον δακτύλιο $\mathbb{Z}/26\mathbb{Z}$. Τότε θα έχουμε

$$\widetilde{f}((a+5b)+26\mathbb{Z}) = a+5b+(1+5i) = a+bi+(1+5i) \quad \text{διότι} \quad a+5b-a-bi = 5b-bi = (-bi)(1+5i)$$

Άρα για το τυχόν στοιχείο $a+bi+(1+5i)$ προσδιορίσαμε στοιχείο $x+26\mathbb{Z} = a+5b+26\mathbb{Z}$, έτσι ώστε $\widetilde{f}(x+26\mathbb{Z}) = a+bi+(1+5i)$, και επομένως $\mathsf{Im}(\widetilde{f}) = \mathbb{Z}[i]/(1+5i)$, δηλαδή η απεικόνιση $\widetilde{f}$ είναι ισομορφισμός δακτυλίων:

$$\widetilde{f}\ :\ \mathbb{Z}[i]\big/(1+5i) \xrightarrow{\cong} \mathbb{Z}_{26}$$

(II) Θα προσδιορίσουμε τον δακτύλιο πηλίκο $\mathbb{Z}[i]\big/(2+i)$ κατασκευάζοντας έναν ισομορφισμό δακτυλίων

$$\mathbb{Z}[i]\big/(2+i) \xrightarrow{\cong} \mathbb{Z}_5$$

Εργαζόμενοι όπως παραπάνω βλέπουμε ότι η απεικόνιση

$$f\colon \mathbb{Z} \longrightarrow \mathbb{Z}[i](2+i), \quad f(x) = x+(2+i)$$

είναι ένας ομομορφισμός δακτυλίων.

1. Έστω $x \in \mathsf{Ker}(f)$. Τότε $f(x) = 0_{\mathbb{Z}[i]/(2+i)}$, δηλαδή $x+(2+i) = (2+i)$, και άρα $x \in (2+i)$. Επομένως υπάρχει $a+bi \in \mathbb{Z}[i]$, έτσι ώστε: $x = (a+bi)(2+i) = (2a-b) + (a+2b)i$. Επειδή $x \in \mathbb{Z}$, έπεται ότι $a+2b = 0$, δηλαδή $a = -2b$. Τότε $x = 2(-2b) - b = a-5(-5a) = -5b$. Αυτό σημαίνει ότι $x \in 5\mathbb{Z}$ και επομένως $\mathsf{Ker}(f) \subseteq 5\mathbb{Z}$. Αντίστροφα, αν $x \in b\mathbb{Z}$, τότε $x = 5a$ για κάποιο $a \in \mathbb{Z}$ και τότε $f(x) = 5a + (2+i) = (2+i)$ διότι $5a = (2a-ai)(2+i) \in (2+i)$. Άρα $x \in \mathsf{Ker}(f)$ και επομένως:

$$\mathsf{Ker}(f) = 5\mathbb{Z}$$

2. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφισμών, η απεικόνιση f επάγει έναν ισομορφισμό δακτυλίων

$$\widetilde{f}\colon \mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z} \xrightarrow{\cong} \mathsf{Im}(f) \subseteq \mathbb{Z}[i]/(2+i), \quad \widetilde{f}(x+2\mathbb{Z}) = f(x) + (2+i) = x + (2+i)$$

Έστω $a+bi+(2+i) \in \mathbb{Z}[i]/(2+i)$. Τότε υπάρχει ακέραιος $x \in \mathbb{Z}$ έτσι ώστε $f(x) = a+bi+(2+i)$, δηλαδή $x+(2+i) = a+bi+(2+i)$, αν και μόνο αν $x-a-bi \in (2+i)$, δηλαδή αν και μόνο αν υπάρχουν ακέραιοι $k,l \in \mathbb{Z}$ έτσι ώστε

$$x-a-bi = (k+li)(2+i) \implies x-a-bi = 2k-l+(k+2l)i \implies x-a = 2k-l \quad \text{και} \quad -b = k+2l$$

$$\Longrightarrow \quad x-a=2(-b-2l)-l=-2b-5l \quad \Longrightarrow \quad x=a-2b+5(-l) \quad \Longrightarrow \quad x+5\mathbb{Z}=a-2b+5\mathbb{Z}$$

στον δακτύλιο $\mathbb{Z}/5\mathbb{Z}$. Τότε θα εχουμε

$$\widetilde{f}((a-2b)+5\mathbb{Z})=a-2b+(2+i)=a+bi+(2+i) \quad \text{διότι} \quad -2b-bi=(-b)(2+i)\in(2+i)$$

Άρα για το τυχόν στοιχείο $a+bi+(2+i)$ προσδιορίσαμε στοιχείο $x+5\mathbb{Z}=a-2b+5\mathbb{Z}$, έτσι ώστε $\widetilde{f}(x+5\mathbb{Z})=a+bi+(2+i)$, και επομένως $\mathsf{Im}(\widetilde{f})=\mathbb{Z}[i]/(2+i)$, δηλαδή η $\widetilde{f}$ είναι ισομορφισμός δακτυλίων:

$$\widetilde{f}\ :\ \mathbb{Z}[i]\big/(2+i)\ \xrightarrow{\cong}\ \mathbb{Z}_5 \quad \surd$$

8.4.2 Πρωτοδακτύλιοι και Πρωτοσώματα

Υπενθυμίζουμε ότι, σύμφωνα με το Παράδειγμα 8.2.14, για κάθε δακτύλιο R υπάρχει μοναδικός ομομορφισμός δακτυλίων

$$\phi\colon \mathbb{Z}\longrightarrow R, \quad \phi(m)=m\cdot 1_R$$

Ο πυρήνας $\mathsf{Ker}(\phi)$ του ϕ είναι τότε ένα ιδεώδες του $\mathbb{Z}$. Από την Πρόταση 8.1.4, έπεται ότι θα έχουμε: $\mathsf{Ker}(\phi)=n\mathbb{Z}$, για κάποιον μη αρνητικό ακέραιο $n=0,1,2,\cdots$, και άρα

$$\mathsf{Ker}(\phi)=\{k\in\mathbb{Z}\mid k1_R=0_R\}=\langle n\rangle=n\mathbb{Z}$$

Η εικόνα του ϕ είναι

$$\mathsf{Im}(\phi)=\{n1_R\in R\mid n\in\mathbb{Z}\}=\mathbb{Z}1_R$$

είναι ένας υποδακτύλιος του R, και μάλιστα ο πρωτοδακτύλιος του R.

Θα έχουμε $n=\mathsf{char}(R)$. Προφανώς, αν $n=1$, τότε $1_R=0_R$ και τότε ο R είναι ο μηδενικός δακτύλιος. Αν $n=0$, δεν υπάρχει θετικός ακέραιος k με την ιδιότητα $k1_R=0_R$, και άρα ο R έχει χαρακτηριστική ίση με 0. Αν $n\geq 2$, τότε ο R έχει θετική χαρακτηριστική ίση με n. Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε

$$\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n\ \xrightarrow{\cong}\ \mathbb{Z}1_R\ \subseteq\ R$$

Θεώρημα 8.4.7. *Ο πρωτοδακτύλιος $\mathbb{Z}1_R$ ενός δακτυλίου R είναι ισόμορφος:*

1. *είτε με τον δακτύλιο $\mathbb{Z}$ των ακεραίων, αν* $\mathsf{char}(R)=0$.
2. *είτε με τον δακτύλιο $\mathbb{Z}_n$ των κλάσεων υπολοίπων* mod n, *αν* $\mathsf{char}(R)=n>0$.

Αν ο δακτύλιος R είναι ακέραια περιοχή, τότε γνωρίζουμε ότι η χαρακτηριστική του $\mathsf{char}(R)$ θα είναι είτε ίση με 0 είτε ίση με έναν πρώτο αριθμό p. Αυτό προκύπτει και από το ότι στην δεύτερη περίπτωση ο πρωτοδακτύλιος $\mathbb{Z}1_R\cong\mathbb{Z}_n\subseteq R$ θα είναι ακέραια περιοχή ως υποδακτύλιος της ακέραιας περιοχής R, και τότε αναγκαστικά θα έχουμε ότι ο n είναι πρώτος.

Στρέφουμε τώρα την προσοχή μας στην περίπτωση κατά την οποία ο δακτύλιος είναι ένα σώμα F. Τότε, επειδή κάθε σώμα είναι ακέραια περιοχή, ο πρωτοδακτύλιος $\mathbb{Z}1_F$ του F, δηλαδή ο υποδακτύλιος του F ο οποίος παράγεται από την μονάδα 1_F του F, θα είναι ισόμορφος είτε με το πεπερασμένο σώμα $\mathbb{Z}_p$, όπου p είναι ένας πρώτος αριθμός, αν $\mathsf{char}(F)>0$, είτε με τον δακτύλιο $\mathbb{Z}$ των ακεραίων, αν $\mathsf{char}(F)=0$. Ας αναλύσουμε περισσότερο την τελευταία περίπτωση.

Λήμμα 8.4.8. *Έστω F ένα σώμα χαρακτηριστικής* 0. *Τότε ο μοναδικός μονομορφισμός δακτυλίων $\phi\colon\mathbb{Z}\longrightarrow F$ επεκτείνεται μοναδικά σε έναν μονομορφισμό σωμάτων*

$$\phi^*:\mathbb{Q}\longrightarrow F, \quad \phi^*\Big(\frac{a}{b}\Big)=\phi(a)\phi(b)^{-1}$$

Απόδειξη. Επειδή η απεικόνιση ϕ είναι «1-1» και $b \neq 0$, έπεται ότι $\phi(b) \neq 0$ και άρα υπάρχει το στοιχείο $\phi(b)^{-1}$ διότι το F είναι σώμα. Αν $\frac{a}{b} = \frac{c}{d}$ στο σώμα $\mathbb{Q}$, τότε στον δακτύλιο $\mathbb{Z}$ των ακεραίων θα έχουμε $ad = bc$ και επομένως θα έχουμε $\phi(ad) = \phi(a)\phi(d) = \phi(b)\phi(c) = \phi(bc)$ στο σώμα F. Τότε θα έχουμε $\phi^*\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1} = \phi(c)\phi(c)^{-1} = \phi^*\left(\frac{c}{d}\right)$, και επομένως η απεικόνιση ϕ^* είναι καλά ορισμένη. Η απεικόνιση ϕ^* είναι «1-1» διότι, αν $\phi^*\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1} = 0$, τότε $\phi(a) = 0 \cdot \phi(b) = 0$, και άρα $a = 0$ διότι η ϕ είναι «1-1». Άρα $\mathsf{Ker}(\phi^*) = \{0\}$ και έτσι η ϕ^* είναι «1-1». Επιπλέον $\phi^*(1) = \phi^*(\frac{1}{1}) = \phi(1)\phi(1)^{-1} = 1_F \cdot 1_F^{-1} = 1_F$.

Έστω $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$. Τότε θα έχουμε:

$$\phi^*\left(\frac{a}{b} + \frac{c}{d}\right) = \phi^*\left(\frac{ad+bc}{bd}\right) = \phi(ad+bc)\phi(bd)^{-1} = \big(\phi(a)\phi(d) + \phi(b)\phi(c)\big)\phi(b)^{-1}\phi(d)^{-1} =$$

$$= \phi(a)\phi(d)\phi(b)^{-1}\phi(d)^{-1} + \phi(b)\phi(c)\phi(b)^{-1}\phi(d)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1} = \phi^*\left(\frac{a}{b}\right) + \phi^*\left(\frac{c}{d}\right)$$

Παρόμοια

$$\phi^*\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \phi^*\left(\frac{ac}{bd}\right) = \phi(ac)\phi(bd)^{-1} = \phi(a)\phi(c) \cdot \phi(bd)^{-1} = \phi(a)\phi(c) \cdot \phi(b)^{-1}\phi(d)^{-1} = \phi^*\left(\frac{a}{b}\right) \cdot \phi^*\left(\frac{c}{d}\right)$$

Οι παραπάνω σχέσεις δείχνουν ότι η ϕ^* είναι ένας μονομορφισμός σωμάτων.

Αν $f\colon \mathbb{Q} \longrightarrow F$ είναι ένας άλλος μονομορφισμός σωμάτων έτσι ώστε $f|_{\mathbb{Z}} = \phi$, δηλαδή η σύνθεση της f με την κανονική έγκλειση $\mathbb{Z} \longrightarrow \mathbb{Q}$, $n \longmapsto \frac{n}{1}$ συμπίπτει με την ϕ, επομένως $f\left(\frac{n}{1}\right) = \phi(n)$, $\forall n \in \mathbb{Z}$, τότε θα δείξουμε ότι $f = \phi^*$. Πράγματι, χρησιμοποιώντας ότι η f είναι μονομορφισμός σωμάτων, θα έχουμε, $\forall \frac{a}{b} \in \mathbb{Q}$:

$$f\left(\frac{a}{b}\right) = f\left(a \cdot b^{-1}\right) = f(a) \cdot f(b^{-1}) = f(a)f(b)^{-1} = \phi(a)\phi(b)^{-1} = \phi^*\left(\frac{a}{b}\right)$$

Επομένως $\phi^* = f$. ■

Από το Λήμμα 8.4.8, έπεται ότι κάθε σώμα F χαρακτηριστικής ίσης με μηδέν, περιέχει ως υποδακτύλιο, και μάλιστα ως τον πρωτοδακτύλιό του, το σώμα των ρητών. Σ' αυτό το πλαίσιο, υπενθυμίζουμε ότι ο πρωτοδακτύλιος ενός δακτυλίου R είναι η τομή όλων των υποδακτυλίων του R, και έτσι είναι ο μικρότερος υποδακτύλιος του R. Όταν ο δακτύλιος είναι ένα σώμα F, τότε ορίζουμε ως **υπόσωμα** του σώματος F έναν υποδακτύλιο $K \subseteq F$ έτσι ώστε $\forall k \in K \setminus \{0\}$: $k^{-1} \in K$. Είναι άμεσο ότι ένα υπόσωμα ενός σώματος είναι σώμα και εύκολα έπεται ότι η τομή υποσωμάτων ενός σώματος F είναι υπόσωμα του F, βλέπε την Άσκηση 8.5.34. Κατ' αναλογία με τον ορισμό πρωτοδακτυλίων, ορίζουμε ως το **πρωτόσωμα** ενός σώματος F να είναι η τομή όλων των υποσωμάτων του F. Είναι προφανές ότι το πρωτόσωμα ενός σώματος είναι το μικρότερο υπόσωμα του F.

Με βάση την παραπάνω ανάλυση και ορολογία, μπορούμε να διατυπώσουμε και να αποδείξουμε το ακόλουθο σημαντικό αποτέλεσμα, μέσω του οποίου τα σώματα χωρίζονται σε δύο μεγάλες κατηγορίες ανάλογα με την χαρακτηριστική τους.

Θεώρημα 8.4.9. *Έστω F ένα σώμα και $P(F)$ το πρωτόσωμά του. Τότε:*

1. *Αν $\mathsf{char}(F) = 0$, τότε υπάρχει ένας ισομορφισμός σωμάτων*

$$P(F) \cong \mathbb{Q}$$

2. *Αν $\mathsf{char}(F) = p$, όπου p είναι πρώτος, τότε υπάρχει ένας ισομορφισμός σωμάτων*

$$P(F) \cong \mathbb{Z}_p$$

Απόδειξη. 1. Το πρωτόσωμα $P(F)$ του F είναι υποδακτύλιος τους F και άρα περιέχει τον μικρότερο υποδακτύλιο του F ο οποίος, επειδή $\mathsf{char}(F) = 0$, είναι ισόμορφος με τον δακτύλιο $\mathbb{Z}$ των ακεραίων. Έτσι η εικόνα του μοναδικού μονομορφισμού δακτυλίων $\phi\colon \mathbb{Z} \longrightarrow F$ περιέχεται στο $P(F)$. Από το Λήμμα 8.4.8, ο ϕ επεκτείνεται μοναδικά σε έναν μονομορφισμό σωμάτων $\phi^*\colon \mathbb{Q} \longrightarrow F$, $\phi^*\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1}$. Επειδή $\mathsf{Im}(\phi) \subseteq P(F)$ και το $P(F)$ είναι υπόσωμα, έπεται ότι $\phi(b)^{-1} \in P(F)$, $\forall b \in \mathbb{Z} \setminus \{0\}$. Ως συνέπεια,

$\phi^*\left(\frac{a}{b}\right) \in P(F)$, $\forall \frac{a}{b} \in \mathbb{Q}$, και επομένως $\mathbb{Q} \cong \mathsf{Im}(\phi^*) \subseteq P(F)$. Επειδή το $\mathbb{Q}$ είναι σώμα, έπεται ότι $\mathsf{Im}(\phi^*)$ είναι υπόσωμα του F. Επειδή το πρωτόσωμα $P(F)$ είναι το μικρότερο υπόσωμα του F και $\mathsf{Im}(\phi^*) \subseteq P(F)$, έπεται ότι $\mathsf{Im}(\phi^*) = P(F)$. Επομένως ο μονομορφισμός ϕ^* επάγει έναν ισομορφισμό σωμάτων

$$\phi^* \colon \mathbb{Q} \xrightarrow{\cong} P(F)$$

2. Όπως και στο μέρος 1., το πρωτόσωμα $P(F)$ του F είναι υποδακτύλιος του F και άρα περιέχει τον μικρότερο υποδακτύλιο του F ο οποίος, επειδή το F είναι σώμα και $\mathsf{char}(F) = p$, είναι ισόμορφος με το σώμα $\mathbb{Z}_p$ των ακεραίων mod p. Έτσι $\mathbb{Z}_p \cong \mathsf{Im}(\phi^*)$, όπου ο μονομορφισμός $\phi^* \colon \mathbb{Z}_p \longrightarrow F$ επάγεται από τον μοναδικό ομομορφισμό $\phi \colon \mathbb{Z} \longrightarrow F$. Άρα θα έχουμε $\mathsf{Im}(\phi^*) \subseteq P(F)$. Επειδή το πρωτόσωμα $P(F)$ είναι το μικρότερο υπόσωμα του F και $\mathsf{Im}(\phi^*) \subseteq P(F)$, έπεται ότι $\mathsf{Im}(\phi^*) = P(F)$. Επομένως ο μονομορφισμός ϕ^* επάγει έναν ισομορφισμό σωμάτων

$$\phi^* \colon \mathbb{Z}_p \xrightarrow{\cong} P(F)$$ ■

Αντίστροφα, αν ένα σώμα F περιέχει έναν υποδακτύλιο R ο οποίος είναι ισόμορφος με το σώμα $\mathbb{Q}$ των ρητών, τότε $\mathsf{char}(F) = 0$. Πράγματι, έστω $f \colon \mathbb{Q} \longrightarrow R$ ένας ισομορφισμός δακτυλίων. Αν υπάρχει $k \in \mathbb{N}$ έτσι ώστε $k1_F = 0$, τότε επειδή $1_F \in R = f(\mathbb{Q})$ θα είχαμε $f(k1) = 0$, από όπου $k = 0$, διότι η f είναι «1-1». Επειδή αυτό είναι άτοπο, έπεται οτι $\mathsf{char}(F) = 0$.

Ανάλογο επιχείρημα δείχνει ότι, αν ένα σώμα F περιέχει έναν υποδακτύλιο R ο οποίος είναι ισόμορφος με το σώμα $\mathbb{Z}_p$, όπου p είναι πρώτος, τότε $\mathsf{char}(F) = p$.

8.4.3 Εμφυτεύοντας Δακτυλίους Χωρίς Μονάδα σε Δακτυλίους (με Μονάδα)

Έστω S ένας δακτύλιος χωρίς μονάδα. Θα δούμε έναν τρόπο να «εμφυτεύσουμε» τον S σε έναν δακτύλιο με μονάδα R, δηλαδή ο S είναι ισόμορφος με έναν υποδακτύλιο χωρίς μονάδα του R. Η κατασκευή που θα περιγράψουμε χρησιμοποιείται για την αναγωγή αρκετών προβλημάτων που αφορούν δακτυλίους χωρίς μονάδα, σε προβλήματα δακτυλίων (με μονάδα).

Έστω $S = (S, +, \cdot)$ ένας δακτύλιος χωρίς μονάδα. Θεωρούμε το ευθύ γινόμενο $\mathbb{Z} \times S$ των προσθετικών αβελιανών ομάδων $(\mathbb{Z}, +)$ και $(S, +)$:

$$\mathbb{Z} \times S = \left\{(n, s) \in \mathbb{Z} \times S \mid n \in \mathbb{Z},\ s \in S\right\}$$

Υπενθυμίζουμε ότι η πράξη της πρόσθεσης «+» στην αβελιανή ομάδα $\mathbb{Z} \times S$ ορίζεται ως εξής:

$$(n_1, s_1) + (n_2, s_2) = (n_1 + n_2, s_1 + s_2)$$

Γράφοντας ως συνήθως ns να είναι το άθροισμα $s + \cdots + s$ (n-παράγοντες) στην προσθετική αβελιανή ομάδα $(S, .+)$, ορίζουμε μια πράξη πολλαπλασιασμού «$\cdot$» στην αβελιανή ομάδα $(\mathbb{Z} \times S, +)$ ως εξής:

$$(n_1, s_1) \cdot (n_2, s_2) = (n_1 n_2, n_1 s_2 + n_2 s_1 + s_1 \cdot s_2)$$

Θεώρημα 8.4.10. *Με τις παραπάνω πράξεις, η τριάδα $R = (\mathbb{Z} \times S, +, \cdot)$ αποτελεί δακτύλιο με μονάδα το στοιχείο $1_R = (1, 0_S)$. Επιπλέον η απεικόνιση*

$$f \colon S \longrightarrow R = \mathbb{Z} \times S, \quad f(s) = (0, s)$$

είναι ένας μονομορφισμός δακτυλίων χωρίς μονάδα ο οποίος επάγει έναν ισομορφισμό $S \cong \mathsf{Im}(f)$ δακτυλίων χωρίς μονάδα, και η εικόνα $\mathsf{Im}(f)$ του f είναι ένα ιδεώδες του R.

Απόδειξη. 1. Ελέγχουμε την προσεταιριστικότητα του πολλαπλασιασμού. Έστω $(n_1, s_1), (n_2, s_2), (n_3, s_3) \in R$. Τότε:

$$(n_1, s_1) \cdot \big((n_2, s_2) \cdot (n_3, s_3)\big) = (n_1, s_1) \cdot (n_2 n_3, n_2 s_3 + n_3 s_2 + s_2 \cdot s_3) =$$

$$= \big((n_1 n_2 n_3, n_2 n_3 s_1 + n_1(n_2 s_3 + n_3 s_2 + s_2 \cdot s_3) + s_1 \cdot (n_2 s_3 + n_3 s_2 + s_2 \cdot s_3)\big) =$$

$$= \big(n_1n_2n_3, n_2n_3s_1 + n_1n_2s_3 + n_1n_3s_2 + n_1s_2 \cdot s_3 + n_2s_1 \cdot s_3 + n_3s_1 \cdot s_2 + s_1 \cdot s_2 \cdot s_3\big)$$

Παρόμοια:

$$\big((n_1, s_1) \cdot (n_2, s_2)\big) \cdot (n_3, s_3) = \big(n_1n_2, n_1s_2 + n_2s_1 + s_1 \cdot s_2\big) \cdot (n_3, s_3) =$$

$$= \big(n_1n_2n_3, n_1n_2s_3 + n_3(n_1s_2 + n_2s_1 + s_1 \cdot s_2) + (n_1s_2 + n_2s_1 + s_1 \cdot s_2) \cdot s_3)\big) =$$

$$= \big(n_1n_2n_3, n_1n_2s_3 + n_1n_3s_2 + n_2n_3s_1 + n_3s_1 \cdot s_2 + n_1s_2 \cdot s_3 + n_2s_1 \cdot s_3 + s_1 \cdot s_2 \cdot s_3\big)$$

Άρα: $(n_1, s_1) \cdot \big((n_2, s_2) \cdot (n_3, s_3)\big) = \big((n_1, s_1) \cdot (n_2, s_2)\big) \cdot (n_3, s_3)$, και επομένως ικανοποιείται η προσεταιριστική ιδιότητα του πολλαπλασιασμού «$\cdot$».

2. Για την επιμεριστική ιδιότητα, θα έχουμε:

$$(n_1, s_1) \cdot \big((n_2, s_2) + (n_3, s_3)\big) = (n_1, s_1) \cdot (n_2 + n_3, s_2 + s_3) = \big(n_1(n_2 + n_3), n_1(s_2 + s_3) + (n_2 + n_3)s_1 + s_1 \cdot (s_2 + s_3)\big) =$$

$$= \big(n_1n_2 + n_1n_3, n_1s_2 + n_1s_3 + n_2s_1 + n_3s_1 + s_1 \cdot s_2 + s_1 \cdot s_3\big)$$

και

$$(n_1, s_1) \cdot (n_2, s_2) + (n_1, s_1) \cdot (n_3, s_3) = (n_1n_2, n_1s_2 + n_2s_1 + s_1 \cdot s_2) + (n_1n_3, n_1s_3 + n_3s_1 + s_1 \cdot s_3) =$$

$$= \big(n_1n_2 + n_1n_3, n_1s_2 + n_2s_1 + n_1s_3 + n_3s_1 + s_1 \cdot s_3 + s_1 \cdot s_2\big)$$

Άρα: $(n_1, s_1) \cdot \big((n_2, s_2) + (n_3, s_3)\big) = (n_1, s_1) \cdot (n_2, s_2) + (n_1, s_1) \cdot (n_3, s_3)$.

Επίσης

$$\big((n_1, s_1) + (n_2, s_2)\big) \cdot (n_3, s_3) = (n_1 + n_2, s_1 + s_2) \cdot (n_3, s_3) = \big((n_1 + n_2)n_3, n_3(s_1 + s_2) + (n_1 + n_2)s_3 + (s_1 + s_2) \cdot s_3)\big) =$$

$$= \big(n_1n_3 + n_2n_3, n_1s_3 + n_2s_3 + n_3s_1 + n_3s_2 + s_1 \cdot s_3 + s_2 \cdot s_3\big)$$

και

$$(n_1, s_1) \cdot (n_3, s_3) + (n_2, s_2) \cdot (n_3, s_3) = (n_1n_3, n_1s_3 + n_3s_1 + s_1 \cdot s_3) + (n_2n_3, n_2s_3 + n_3s_2 + s_2 \cdot s_3) =$$

$$= (n_1n_3 + n_2n_3, n_1s_3 + n_3s_1 + n_2s_3 + n_3s_2 + s_2 \cdot s_3 + s_1 \cdot s_3)$$

Άρα: $\big((n_1, s_1) + (n_2, s_2)\big) \cdot (n_3, s_3) = (n_1, s_1) \cdot (n_3, s_3) + (n_2, s_2) \cdot (n_3, s_3)$.

Οι παραπάνω σχέσεις δείχνουν ότι ισχύει η επιμεριστική ιδιότητα του πολλαπλασιασμού ως προς την πρόσθεση.

3. Δείχνουμε ότι το στοιχείο $(1, 0) = (1, 0_S)$ είναι μονάδα του R. Πράγματι, για κάθε $(n, s) \in R$, θα έχουμε:

$$(1, 0_S) \cdot (n, s) = (n, 1s + n0_S + 0_S \cdot s) = (n, s) \qquad \text{και} \qquad (n, s) \cdot (1, 0_S) = (n, n0_S + 1s + s \cdot 0_S) = (n, s)$$

Άρα το στοιχείο $(1, 0)$ είναι μονάδα του R, και άρα η τριάδα $(R, +, \cdot)$ είναι ένας δακτύλιος με μονάδα.

4. Για την απεικόνιση $f\colon S \longrightarrow R = \mathbb{Z} \times S$, $f(s) = (0, s)$, θα έχουμε:

$$f(s_1 + s_2) = (0, s_1 + s_2) = (0, s_1) + (0, s_2) = f(s_1) + f(s_2)$$

$$f(s_1 \cdot s_2) = (0, s_1 \cdot s_2) \quad \text{και} \quad f(s_1) \cdot f(s_2) = (0, s_1) \cdot (0, s_2) = (s_1 \cdot s_2, 0)$$

Άρα η απεικόνιση f διατηρεί την πρόσθεση και τον πολλαπλασιασμό και έτσι είναι ένας ομομορφισμός δακτυλίων χωρίς μονάδα. Προφανώς, αν $f(s) = (0, 0_S)$, τότε $s = 0$, και άρα η απεικόνιση f είναι μονομορφισμός δακτυλίων χωρίς μονάδα.

Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε τότε ότι ο f επάγει έναν ισομορφισμό δακτυλίων χωρίς μονάδα: $S \cong \mathsf{Im}(f)$ και η εικόνα $\mathsf{Im}(f)$ του f είναι ένας υποδακτύλιος χωρίς μονάδα του R.

5. Ο υποδακτύλιος $\mathsf{Im}(f) = \big\{(0, s) \in R \mid s \in S\big\}$ είναι ιδεώδες του R διότι, για κάθε $(0, s) \in \mathsf{Im}(f)$ και κάθε $(n, s') \in R$, θα έχουμε:

$$(0, s) \cdot (n, s') = (0, ns + s \cdot s') \in \mathsf{Im}(f) \qquad \text{και} \qquad (n, s') \cdot (0, s) = (0, ns + s' \cdot s) \in \mathsf{Im}(f)$$ ■

Μετατρέποντας έναν διανυσματικό χώρο σε μηδενοδύναμο ιδεώδες

Έστω $\mathbb{K}$ ένα σώμα και $\mathcal{V}$ ένας διανυσματικός χώρος υπεράνω του $\mathbb{K}$. Μια παραλλαγή της παραπάνω θεώρησης είναι η «μετατροπή» του $\mathcal{V}$ σε ένα ιδεώδες υπεράνω κατάλληλου δακτυλίου. Πιο αναλυτικά, αυτή η μετατροπή συνίσταται στην κατασκευή ενός δακτυλίου με μονάδα $\mathbb{K} \ltimes \mathcal{V}$, ο οποίος περιέχει ένα ιδεώδες I το οποίο είναι και $\mathbb{K}$-διανυσματικός χώρος, έτσι ώστε $I^2 = 0$ και ο $\mathcal{V}$ είναι ισόμορφος, ως διανυσματικός χώρος, με το ιδεώδες $I \subseteq \mathbb{K} \ltimes \mathcal{V}$.

Έστω $\mathbb{K}$ ένα σώμα, και $\mathcal{V}$ ένας διανυσματικός χώρος υπεράνω του $\mathbb{K}$. Υπενθυμίζουμε από τη Γραμμική Άλγεβρα ότι η τριάδα $(\mathcal{V}, +, \cdot)$, είναι ένας $\mathbb{K}$-*διανυσματικός χώρος*, αν το ζεύγος $(\mathcal{V}, +)$ είναι αβελιανή ομάδα και $\cdot \colon \mathbb{K} \times \mathcal{V} \longrightarrow \mathcal{V}$, $(k, \vec{x}) \longmapsto k \cdot \vec{x}$ είναι μια εξωτερική πράξη, ο *βαθμωτός πολλαπλασιασμός* του $\mathbb{K}$ επί του $\mathcal{V}$, για την οποία ισχύουν τα εξής: (α) $k \cdot (\vec{x} + \vec{y}) = k \cdot \vec{x} + k \cdot \vec{y}$, (β) $(k + l) \cdot \vec{x} = k \cdot \vec{x} + l \cdot \vec{x}$, (γ) $(kl) \cdot \vec{x} = k \cdot (l \cdot \vec{x})$, (δ) $1 \cdot \vec{x} = \vec{x}$, όπου $\vec{x}, \vec{y} \in \mathcal{V}$ και $k, l \in \mathbb{K}$. Από τώρα και στο εξής θα γράφουμε: $\vec{x} \cdot k = k \cdot \vec{x}$.

Θεωρούμε την προσθετική αβελιανή ομάδα

$$\mathbb{K} \times \mathcal{V} = \left\{ (k, \vec{x}) \in \mathbb{K} \times \mathcal{V} \mid k \in \mathbb{K},\ \vec{x} \in \mathcal{V} \right\}$$

όπου η πρόσθεση «+» ορίζεται ως εξής:

$$(k_1, \vec{x}) + (k_2, \vec{y}) = (k_1 + k_2, \vec{x} + \vec{y})$$

Ορίζουμε μια πράξη πολλαπλασιασμού «·» στην αβελιανή ομάδα $\mathbb{K} \times \mathcal{V}$ ως εξής:

$$(k_1, \vec{x}) \cdot (k_2, \vec{y}) = (k_1 k_2, k_1 \vec{y} + k_2 \vec{x})$$

Πρόταση 8.4.11. *Η τριάδα $(\mathbb{K} \ltimes \mathcal{V}, +, \cdot)$ είναι ένας δακτύλιος με μονάδα ο οποίος είναι και διανυσματικός χώρος υπεράνω του $\mathbb{K}$. Η απεικόνιση*

$$g \colon \mathbb{K} \ltimes \mathcal{V} \longrightarrow \mathbb{K}, \quad g(k, \vec{x}) = k$$

είναι ένας επιμορφισμός δακτυλίων με πυρήνα το ιδεώδες $I = \mathsf{Ker}(g) = \left\{ (0, \vec{x}) \in \mathbb{K} \ltimes \mathcal{V} \mid \vec{x} \in \mathcal{V} \right\}$, και έχουμε έναν ισομορφισμό δακτυλίων:

$$(\mathbb{K} \ltimes \mathcal{V}) / I \xrightarrow{\cong} \mathbb{K}$$

Το ιδεώδες I είναι $\mathbb{K}$-διανυσματικός χώρος, υπάρχει ισομορφισμός $\mathbb{K}$-διανυσματικών χώρων $\mathcal{V} \cong I$ και:

$$I^2 = 0$$

Απόδειξη. Χρησιμοποιώντας τα αξιώματα διανυσματικού χώρου υπεράνω του $\mathbb{K}$ και εργαζόμενοι όπως στο Θεώρημα 8.4.10, βλέπουμε ότι η τριάδα $(\mathbb{K} \ltimes \mathcal{V}, +, \cdot)$ είναι ένας δακτύλιος με μονάδα το στοιχείο $(1, \vec{0})$.

Για την απεικόνιση f θα έχουμε $f(1) = (1, \vec{0})$ και $g(1, \vec{0}) = 1$, και αν $k, l \in \mathbb{K}$, και $(k, \vec{x}), (l, \vec{y}) \in \mathbb{K} \ltimes \mathcal{V}$, τότε:

$$f(k + l) = (k + l, \vec{0}) = (k, \vec{0}) + (l, \vec{0}) = f(k) + f(l)$$

$$g\big((k, \vec{x}) + (l, \vec{y})\big) = g(k + l, \vec{x} + \vec{y}) = k + l = g(k, \vec{x}) + g(l, \vec{y})$$

και

$$f(kl) = (kl, \vec{0}) = (k, \vec{0}) \cdot (l, \vec{0}) = f(k) \cdot f(l)$$

$$g\big((k, \vec{x}) \cdot (l, \vec{y})\big) = g(kl, k\vec{y} + l\vec{x}) = kl = g(k, \vec{x}) \cdot g(l, \vec{y})$$

Άρα οι απεικονίσεις f, g είναι ομομορφισμοί δακτυλίων, και επιπλέον $(g \circ f)(k) = g(f(k)) = g(k, \vec{0}) = k$, άρα $g \circ f = \mathrm{Id}_{\mathbb{K}}$. Προφανώς θα έχουμε ότι το $I = \mathsf{Ker}(f) = \left\{ (0, \vec{x}) \in \mathbb{K} \ltimes \mathcal{V} \mid \vec{x} \in \mathcal{V} \right\}$ είναι ένα ιδεώδες του $\mathbb{K} \ltimes \mathcal{V}$, και από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε:

$$(\mathbb{K} \ltimes \mathcal{V}) / I \xrightarrow{\cong} \mathbb{K}$$

Για κάθε $(0, \vec{x}), (0, \vec{y}) \in I$, θα έχουμε $(0, \vec{x}) \cdot (0, \vec{y}) = (0, 0\vec{y} + 0\vec{x}) = (0, \vec{0})$. Επομένως άμεσα θα έχουμε $I^2 = 0$.

Τέλος, η απεικόνιση $h \colon \mathcal{V} \longrightarrow I$, $h(\vec{x}) = (0, \vec{x})$ είναι προφανώς «1-1» και «επί» και εύκολα βλέπουμε ότι είναι και $\mathbb{K}$-γραμμική, δηλαδή είναι ένας ισομορφισμός $\mathbb{K}$-διανυσματικών χώρων. ■

Παράδειγμα 8.4.12. Στην παραπάνω Πρόταση, έστω $\mathcal{V} = \mathbb{K}$. Τότε ο δακτύλιος $\mathbb{K} \ltimes \mathbb{K}$ καλείται ο **δακτύλιος των δυϊκών αριθμών** υπεράνω του $\mathbb{K}$. Έτσι κάθε σώμα $\mathbb{K}$ γίνεται ιδεώδες I, έτσι ώστε $I^2 = 0$, στον δακτύλιο των δυϊκών αριθμών $\mathbb{K} \ltimes \mathbb{K}$.

Εδώ θα δείξουμε ότι ο δακτύλιος $\mathbb{K} \ltimes \mathbb{K}$ των δυϊκών αριθμών υπεράνω του $\mathbb{K}$, και ο δακτύλιος πηλίκο $\mathbb{K}[t]/(t^2)$ των πολυωνύμων υπεράνω του $\mathbb{K}$ ως προς το κύριο ιδεώδες το οποίο παράγεται από το πολυώνυμο t^2, είναι ισόμορφοι:

$$\mathbb{K} \ltimes \mathbb{K} \xrightarrow{\cong} \mathbb{K}[t]/(t^2)$$

Πράγματι θεωρούμε την απεικόνιση

$$f : \mathbb{K} \ltimes \mathbb{K} \longrightarrow \mathbb{K}[t]/(t^2), \quad f(k_0, k_1) = (k_0 + k_1 t) + (t^2)$$

Τότε θα έχουμε $f(1_{\mathbb{K} \ltimes \mathbb{K}}) = f(1,0) = 1 + (t^2) = 1_{\mathbb{K}[t]/(t^2)}$, και αν $(k_0, k_1), (l_0, l_1) \in \mathbb{K} \ltimes \mathbb{K}$, θα έχουμε:

$$f\big((k_0, k_1) + (l_0, l_1)\big) = f(k_0 + l_0, k_1 + l_1) = (k_0 + l_0) + (k_1 + l_1)t + (t^2) = (k_0 + k_1 t) + (t^2) + (l_0 + l_1 t) + (t^2) =$$

$$= f(k_0, k_1) + f(l_0, l_1)$$

$$f\big((k_0, k_1) \cdot (l_0, l_1)\big) = f(k_0 l_0, k_0 l_1 + k_1 l_0) = (k_0 l_0) + (k_0 l_1 + k_1 l_0)t + (t^2) = \big((k_0 + k_1 t) + (t^2)\big) \cdot \big((l_0 + l_1 t) + (t^2)\big) =$$

$$= f(k_0, k_1) \cdot f(l_0, l_1)$$

όπου παραπάνω ο όρος $k_1 l_1 t^2$ δεν εμφανίζεται διότι ανήκει στο ιδεώδες (t^2). Επομένως η απεικόνιση f είναι ομομορφισμός δακτυλίων. Επιπλέον:

$$\mathsf{Ker}(f) = \big\{(k_0, k_1) \in \mathbb{K} \ltimes \mathbb{K} \mid f(k_0, k_1) = 0_{\mathbb{K}[t]/(t^2)}\big\} = \big\{(k_0, k_1) \in \mathbb{K} \ltimes \mathbb{K} \mid (k_0 + k_1 t) + (t^2) = (t^2)\big\} =$$

$$= \big\{(k_0, k_1) \in \mathbb{K} \ltimes \mathbb{K} \mid (k_0 + k_1 t) \in (t^2)\big\}$$

Η σχέση $k_0 + k_1 t \in (t^2)$ σημαίνει ότι το πολυώνυμο $k_0 + k_1 t$ είναι πολλαπλάσιο του πολυωνύμου t^2, και προφανώς αυτό είναι εφικτό μόνο αν $k_0 = k_1 = 0$. Τότε $\mathsf{Ker}(f) = \{0_{\mathbb{K} \ltimes \mathbb{K}}\}$, και άρα η f είναι μονομορφισμός. Τέλος, αν $P(t) + (t^2)$ είναι ένα τυπικό στοιχείο του δακτυλίου $\mathbb{K}[t]/(t^2)$, τότε από την Ευκλείδεια Διαίρεση του πολυωνύμου $P(t)$ με το πολυώνυμο t^2 θα έχουμε: $P(t) = Q(t)t^2 + R(t)$, όπου $R(t) = 0$ ή $\deg R(t) < 2$. Άρα $R(t) = k_0 + k_1 t$, όπου $k_0, k_1 \in \mathbb{K}$, και τότε

$$P(t) + (t^2) = (k_0 + k_1 t) + Q(t)t^2 + (t^2) = (k_0 + k_1 t) + (t^2) = f(k_0, k_1)$$

Δηλαδή η f είναι επιμορφισμός και άρα ισομορφισμός δακτυλίων.

Ο δακτύλιος $\mathbb{R}[t]/(t^2)$ έχει και μια παράσταση ως δακτύλιος πινάκων. Πράγματι, το υποσύνολο $\big\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R}\big\}$ είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{R})$, και υπάρχει ένας ισομορφισμός δακτυλίων

$$\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R}\right\} \xrightarrow{\cong} \mathbb{R}[t]/(t^2)$$

βλέπε την Άσκηση 8.5.27 $\surd$

8.4.4 Δακτύλιοι Ενδομορφισμών και το Θεώρημα του Cayley

Όπως με τα μονοειδή και τις ομάδες, υπάρχει εκδοχή του Θεωρήματος του Cayley και για δακτυλίους. Στο παρόν πλαίσιο το ακόλουθο Θεώρημα δείχνει ότι κάθε δακτύλιος μπορεί να θεωρηθεί ως υποδακτύλιος του δακτυλίου ενδομορφισμών της υποκείμενης προσθετικής του αβελιανής ομάδας. Έτσι οι δακτύλιοι ενδομορφισμών αβελιανών ομάδων διαδραματίζουν στη θεωρία δακτυλίων αντίστοιχα ρόλο με τον ρόλο των συμμετρικών ομάδων στη θεωρία ομάδων.

Θεώρημα 8.4.13 (Θεώρημα Cayley για Δακτυλίους)**.** *Κάθε δακτύλιος είναι ισόμορφος με έναν υποδακτύλιο του δακτυλίου ενδομορφισμών μιας αβελιανής ομάδας. Αναλυτικότερα, η απεικόνιση*

$$\Phi : R \longrightarrow \mathsf{End}_{\mathbb{Z}}(R), \quad r \longmapsto \Phi(r) := \Phi_r, \quad \text{όπου} \quad \Phi_r : R \longrightarrow R, \quad \Phi_r(s) = r \cdot s$$

είναι ένας μονομορφισμός δακτυλίων.

Απόδειξη. Κατ' αρχήν δείχνουμε ότι, για κάθε $r \in R$, η απεικόνιση Φ_r είναι ομομορφισμός της προσθετικής αβελιανής ομάδας $(R,+)$. Έστω $r, s_1, s_2 \in R$. Τότε:

$$\Phi_r(s_1+s_2) = r\cdot(s_1+s_2) = r\cdot s_1 + r\cdot s_2 = \Phi_r(s_1)+\Phi_r(s_2)$$

Άρα για κάθε $r \in R$, θα έχουμε $\Phi_r \in \mathsf{End}_{\mathbb{Z}}(R)$. Θα έχουμε $\Phi_{1_R}(s) = \Phi_{1_R}(s) = 1_R \cdot s = s = \mathrm{Id}_R(s)$ και επομένως $\Phi(1_R) = \mathrm{Id}_R = 1_{\mathsf{End}_{\mathbb{Z}}(R)}$. Έστω $r_1, r_r \in R$. Τότε θα έχουμε:

$$\Phi_{r_1+r_2}(s) = (r_1+r_2)\circ s = r_1\cdot s + r_2\cdot s = \Phi_{r_1}(s)+\Phi_{r_2}(s) \quad \Longrightarrow \quad \Phi(r_1+r_2) = \Phi_{r_1+r_2} = \Phi_{r_1}+\Phi_{r_2} = \Phi(r_1)+\Phi(r_2)$$

$$\Phi_{r_1\cdot r_2}(s) = (r_1\cdot r_2)\cdot s = r_1\cdot(r_2\cdot s) = r_1\cdot\Phi_{r_2}(s) = \Phi_{r_1}(\Phi_{r_2}(s)) \quad \Longrightarrow \quad \Phi(r_1\cdot r_2) = \Phi_{r_1\cdot r_2} = \Phi_{r_1}\circ\Phi_{r_2} = \Phi(r_1)\circ\Phi(r_2)$$

Οι παραπάνω σχέσεις δείχνουν ότι η απεικόνιση Φ είναι ομομορφσιμός δακτυλίων. Για τον πυρήνα του Φ θα έχουμε:

$$\mathsf{Ker}(\Phi) = \left\{r\in R \mid \Phi(r) = 0_{\mathsf{End}_{\mathbb{Z}}(R)}\right\} = \left\{r\in R \mid \Phi(r)(s) = 0(s),\ \forall s\in R\right\} = \left\{r\in R \mid r\cdot s = 0_R,\ \forall s\in R\right\} =$$

$$= \left\{r\in R \mid r = r\cdot 1_R = 0_R\right\} = \left\{0_R\right\}$$

και άρα η Φ είναι μονομορφισμός. ■

Ορισμός 8.4.14. *Ο μονομορφισμός δακτυλίων $\Phi\colon R \longrightarrow \mathsf{End}_{\mathbb{Z}}(R)$, καλείται η* **αριστερή κανονική αναπαράσταση** *του R.*

Παρατήρηση 8.4.15. Δακτύλιοι για τους οποίους η αριστερή κανονική αναπαράσταση τους είναι ισομορφισμός είναι πολύ ειδικοί, και η κλάση τους είναι πολύ μικρή. Για παράδειγμα, αυτό συμβαίνει για τους δακτυλίους $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$, $\forall n \geq 1$. Είναι εύκολο να δειχθεί ότι δακτύλιοι R των οποίων η αριστερή κανονική αναπαράσταση είναι ισομορφισμός είναι μεταθετικοί και, αν επιπρόσθετα η προσθετική ομάδα $(R,+)$ είναι πεπερασμένα παραγόμενη, τότε είτε $R=\mathbb{Z}$ είτε $R=\mathbb{Z}_n$, βλέπε τις Άσκήσεις 8.5.28 και 8.5.31.

Συμβολίζουμε με

$$\mathsf{End}_{\mathsf{Ring}}(R) = \left\{f\colon R\longrightarrow R \mid f : \text{ομομορφισμός δακτυλίων}\right\}$$
$$\mathsf{Hom}_{\mathsf{Ring}}(R,S) = \left\{f\colon R\longrightarrow S \mid f : \text{ομομορφισμός δακτυλίων}\right\}$$

Πρόταση 8.4.16. *Υπάρχουν ισομορφισμοί δακτυλίων:*

$$\mathsf{End}_{\mathsf{Ring}}(\mathbb{Z}) = \left\{\mathrm{Id}_{\mathbb{Z}}\right\} \quad \textit{και} \quad \mathsf{End}_{\mathsf{Ring}}(\mathbb{Z}_p) = \left\{\mathrm{Id}_{\mathbb{Z}_p}\right\} \quad (p : \textit{πρώτος}) \quad \textit{και} \quad \mathsf{End}_{\mathsf{Ring}}(\mathbb{Q}) = \left\{\mathrm{Id}_{\mathbb{Q}}\right\}$$

Απόδειξη. 1. Έστω $f\colon \mathbb{Z}\longrightarrow\mathbb{Z}$ ένας ομομορφισμός δακτυλίων. Τότε ο f είναι ιδιαίτερα ενδομορφισμός της προσθετικής ομάδας $(\mathbb{Z},+)$. Από το Θεώρημα 6.4.6 γνωρίζουμε ότι $f = f_k$, όπου $k\in\mathbb{Z}$ και $f_k\colon\mathbb{Z}\longrightarrow\mathbb{Z}$, $f_k(x) = kx$. Επειδή ο f είναι ομομορφισμός δακτυλίων, θα έχουμε $1 = f_k(1) = k$. Άρα $f = \mathrm{Id}_{\mathbb{Z}}$.

2. Έστω $f\colon\mathbb{Z}_p\longrightarrow\mathbb{Z}_p$ ένας ομομορφισμός δακτυλίων. Τότε ο f είναι ιδιαίτερα ενδομορφισμός της προσθετικής ομάδας $(\mathbb{Z},+)$. Από το Λήμμα 6.4.11 γνωρίζουμε ότι το σύνολο των ενδομορφισμών της προσθετικής ομάδας $(\mathbb{Z}_p,+)$ είναι μια κυκλική ομάδα τάξης p, με στοιχεία $f_k\colon\mathbb{Z}_p\longrightarrow\mathbb{Z}_p$, $f_k([x]_p) = [kx]_p$. $0\leq k\leq p-1$. Επομένως θα έχουμε $f = f_k$, για κάποιο $k = 0,1,\cdots,p-1$. Προφανώς $k\neq 0$, διότι διαφορετικά $f = f_0$ θα είναι ο μηδενικός ομομορφισμός και αυτό είναι άτοπο. Επειδή ο f είναι ομομορφισμός δακτυλίων, θα έχουμε: $f_k([1]_p) = [1]_p$ από όπου $[k]_p = [1]_p$, δηλαδή $p \mid k-1$ και τότε $k-1=0$ διότι διαφορετικά θα είχαμε $k < p \leq k-1$, το οποίο είναι άτοπο. Έτσι $k=1$ και επομένως $f = f_1 = \mathrm{Id}_{\mathbb{Z}_p}$. Επομένως ο ταυτοτικός ενδομορφισμός είναι ο μοναδικός ενδομορφισμός του δακτυλίου $\mathbb{Z}_p$.

3. Έστω $f\colon\mathbb{Q}\longrightarrow\mathbb{Q}$ ένας ομομορφισμός δακτυλίων. Έστω $\frac{a}{b}\in\mathbb{Q}$ ένα τυχόν στοιχείο. Χρησιμοποιώντας ότι ο f είναι ιδιαίτερα ενδομορφισμός της προσθετικής ομάδας $(\mathbb{Q},+)$ και στέλνει την μονάδα στην μονάδα, $f(1)=1$, θα έχουμε:

$$bf\left(\frac{a}{b}\right) = f\left(b\frac{a}{b}\right) = f(a) = af(1) = a \quad \Longrightarrow \quad f\left(\frac{a}{b}\right) = \frac{a}{b}$$

Επομένως $f = \mathrm{Id}_{\mathbb{Q}}$. ■

Παρατήρηση 8.4.17. Σύμφωνα με το Παράδειγμα 8.2.14, για κάθε δακτύλιο R υπάρχει μοναδικός ομομορφισμός δακτυλίων $\phi\colon \mathbb{Z} \longrightarrow R$, όπου $\phi(m) = m\cdot 1_R$. Επίσης, σύμφωνα με το Θεώρημα 8.4.9, για κάθε σώμα F, υπάρχουν μοναδικοί ομομορφισμοί σωμάτων $\mathbb{Q} \longrightarrow F$ (αν $\mathsf{char}(F) = 0$) και $\mathbb{Z}_p \longrightarrow F$ (αν $\mathsf{char}(F) = p > 0$, όπου p: πρώτος). Επομένως, θέτοντας $R = \mathbb{Z}$, $F = \mathbb{Q}$ και $F = \mathbb{Z}_p$, έχουμε μια διαφορετική απόδειξη της παραπάνω πρότασης. ▲

Πρόταση 8.4.18. *Υπάρχει ένας ισομορφισμός δακτυλίων:*

$$\mathsf{End}_{\mathsf{Ring}}(\mathbb{R}) = \{\mathrm{Id}_{\mathbb{R}}\}$$

Αν $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ είναι ένας ομομορφισμός δακτυλίων ο οποίος ικανοποιεί την συνθήκη $f(r) = r$, $\forall r \in \mathbb{R}$, τότε:

$$\text{είτε } f = \mathrm{Id}_{\mathbb{C}} \text{ είτε } f = {}^{-}, \text{ όπου } {}^{-}\colon \mathbb{C} \longrightarrow \mathbb{C},\ z \longmapsto \overline{z}$$

Απόδειξη. 1. Έστω $f\colon \mathbb{R} \longrightarrow \mathbb{R}$ ένας ομομορφισμός δακτυλίων. Τότε ο f είναι ιδιαίτερα ενδομορφισμός της προσθετικής ομάδας $(\mathbb{Z}, +)$, και, εργαζόμενοι όπως στην παραπάνω Πρόταση, βλέπουμε ότι $f(q) = q$, $\forall q \in \mathbb{Q}$. Θα δείξουμε ότι $x \le y$ συνεπάγεται ότι $f(x) \le f(y)$, για κάθε δύο $x, y \in \mathbb{R}$. Πράγματι, θα έχουμε $y - x \ge 0$ και επειδή κάθε μη αρνητικός αριθμός έχει τετραγωνική ρίζα, έπεται ότι υπάρχει $z \in \mathbb{R}$ έτσι ώστε $z^2 = y - x$. Τότε $f(y) - f(x) = f(y - x) = f(z^2) = f(zz) = f(z)f(z) \ge 0$.

Έστω ότι υπάρχει $x \in \mathbb{R}$ έτσι ώστε $f(x) \neq x$. Χρησιμοποιούμε ότι μεταξύ δύο πραγματικών αριθμών $a, b \in \mathbb{R}$ με $a < b$ υπάρχει πάντα ρητός $q \in \mathbb{Q}$: $a < q < b$. Αν $f(x) < x$, έστω $q \in \mathbb{Q}$ έτσι ώστε $f(x) < q < x$. Τότε θα έχουμε $f(f(x)) \le f(q) \le f(x)$, δηλαδή $f(f(x)) \le q \le f(x)$, το οποίο είναι άτοπο διότι $q \le f(x)$. Αν $x < f(x)$, έστω $q \in \mathbb{Q}$ έτσι ώστε $x < q < f(x)$. Τότε θα έχουμε $f(x) \le f(q) \le f(f(x))$, δηλαδή $f(x) \le q \le f(f(x))$, το οποίο είναι άτοπο διότι $q < f(x)$. Άρα αναγκαστικά $f(x) = x$ και επομένως $f = \mathrm{Id}_{\mathbb{R}}$.

2. Έστω $f\colon \mathbb{C} \longrightarrow \mathbb{C}$ ένας ομομορφισμός δακτυλίων. Τότε:

$$-1 = -f(1) = f(-1) = f(i^2) = f(i\cdot i) = f(i)\cdot f(i) \quad \Longrightarrow \quad f(i) = \pm i$$

Από την άλλη πλευρά για κάθε μιγαδικό αριθμό $z = a + bi$, όπου $a, b \in \mathbb{R}$, θα έχουμε: $f(z) = f(a+bi) = f(a) + f(bi) = f(a) + f(b)f(i) = a + bf(i)$. Αν $f(i) = i$, τότε προφανώς $f = \mathrm{Id}_{\mathbb{C}}$. Αν $f(i) = -i$ τότε $f(z) = \overline{z}$. Άρα θα έχουμε ότι είτε $f = \mathrm{Id}_{\mathbb{C}}$ είτε $f = {}^{-}$. ■

Παρατήρηση 8.4.19. Σε αντίθεση με το τι συμβαίνει στους δακτυλίους $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$, και $\mathbb{R}$, υπάρχει, εκτός του ταυτοτικού και του αυτομορφισμού συζυγίας, μη αριθμήσιμο πλήθος ενδομορφισμών, και μάλιστα αυτομορφισμών, του $\mathbb{C}$. Οι αυτομορφισμοί αυτοί καλούνται «άγριοι», ως απεικονίσεις είναι μη συνεχείς, και η ύπαρξή τους εξασφαλίζεται με προχωρημένες συνολοθεωρητικές μεθόδους. Έτσι η απόδειξη ξεφεύγει από το πλαίσιο των σημειώσεων αυτών. Στην παραπάνω Πρόταση δείξαμε ότι αν περιοριστούμε σε ενδομορφισμούς του $\mathbb{C}$ οι οποίοι αφήνουν σταθερά τα στοιχεία του $\mathbb{R}$, τότε υπάρχουν μόνο δύο ενδομορφισμοί, ο ταυτοτικός και ενδομορφισμός συζυγίας. ▲

Παράδειγμα 8.4.20. Θεωρούμε την αριστερή κανονική αναπαράσταση του R:

$$\Phi\colon R \longrightarrow \mathsf{End}_{\mathbb{Z}}(R), \quad r \longmapsto \Phi(r) := \Phi_r, \quad \text{όπου} \quad \Phi_r\colon R \longrightarrow R, \quad \Phi_r(s) = r\cdot s$$

Τότε η εικόνα $\mathsf{Im}(\Phi) = \{\Phi_r \in \mathsf{End}_{\mathbb{Z}}(R) \mid r \in R\}$ είναι ένας υποδακτύλιος του $\mathsf{End}_{\mathbb{Z}}(R)$. Θα προσδιορίσουμε τον κεντροποιητή

$$\mathsf{C}_{\mathsf{End}_{\mathbb{Z}}(R)}(\mathsf{Im}(\Phi)) = \{f \in \mathsf{End}_{\mathbb{Z}}(R) \mid f\circ\Phi_r = \Phi_r \circ f,\ \forall r \in R\}$$

Για κάθε $r \in R$ και κάθε $x \in R$, θα έχουμε

$$(f\circ\Phi_r)(x) = f(\Phi_r(x)) = f(rx) \qquad \text{και} \qquad (\Phi_r\circ f)(x) = \Phi_r(f(x) = rf(x)$$

Άρα:

$$\mathsf{C}_{\mathsf{End}_{\mathbb{Z}}(R)}(\mathsf{Im}(\Phi)) = \{f \in \mathsf{End}_{\mathbb{Z}}(R) \mid f(rx) = rf(x),\ \forall r, x \in R\} \quad \surd$$

Παρατήρηση 8.4.21. Θεωρούμε την απεικόνιση:

$$\Psi : R \longrightarrow \mathsf{End}_{\mathbb{Z}}(R), \quad r \longmapsto \Psi(r) := \Psi_r, \quad \text{όπου} \quad \Psi_r : R \longrightarrow R, \quad \Psi_r(s) = s \cdot r$$

Εύκολα βλέπουμε ότι η απεικόνιση Ψ ικανοποιεί τις ακόλουθες σχέσεις: $\Psi(1_R) = \mathrm{Id}_R$, $\Psi(r_1 + r_2) = \Psi(r_1) + \Psi(r_2)$, και $\Psi(r_1 \cdot r_2) = \Psi(r_2) \circ \Psi(r_1)$, $\forall r_1, r_2 \in R$. Άρα η απεικόνιση $\Psi : R \longrightarrow \mathsf{End}_{\mathbb{Z}}(R)$ δεν είναι ομομορφισμός δακτυλίων, αλλά είναι ομομορφισμός δακτυλίων

$$\Psi : R^{\mathsf{op}} \longrightarrow \mathsf{End}_{\mathbb{Z}}(R), \quad r \longmapsto \Psi(r) := \Psi_r, \quad \text{όπου} \quad \Psi_r : R \longrightarrow R, \quad \Psi_r(s) = s \cdot r$$

όπου R^{op} είναι ο αντίθετος δακτύλιος του R. Υπενθυμίζουμε ότι $R^{\mathsf{op}} = (R, +, \cdot^{\mathsf{op}})$, όπου $r_1 \cdot^{\mathsf{op}} r_2 = r_2 \cdot r_1$.

Ο ομομορφισμός δακτυλίων $\Psi : R^{\mathsf{op}} \longrightarrow \mathsf{End}_{\mathbb{Z}}(R)$, $\Psi(r)(x) = x \cdot r$, καλείται η **δεξιά κανονική αναπαράσταση** του R. $\surd$

8.5 Ασκήσεις

Άσκηση 8.5.1. *Έστω $f : R \longrightarrow S$ μια απεικόνιση μεταξύ δακτυλίων R και S, για την οποία ισχύει ότι, $\forall x, y \in R$:*

$$f(x + y) = f(x) + f(y) \quad \text{και} \quad f(x \cdot y) = f(x) \cdot f(y)$$

1. *Να δειχθεί ότι το στοιχείο $f(1_R)$ είναι μονάδα στον υποδακτύλιο χωρίς μονάδα $f(R)$ αλλά όχι απαραίτητα στον δακτύλιο S.*

2. *Να δειχθεί ότι η απεικόνιση f ικανοποιεί και την ιδιότητα $f(1_R) = 1_S$, και άρα είναι ομομορφισμός δακτυλίων, αν $f \neq 0$ και ικανοποιείται μια από τις ακόλουθες τρεις προϋποθέσεις:*

(α) *Ο ομομορφισμός f είναι επιμορφισμός.*

(β) *Ο δακτύλιος S είναι δακτύλιος διαίρεσης.*

(γ) *Ο δακτύλιος S δεν έχει διαιρέτες του μηδενός.*

3. *Αν ισχύει $f(1_R) = 1_S$, τότε να δειχθεί ότι:*

(α) *για κάθε αντιστρέψιμο στοιχείο $x \in R$, το στοιχείο $f(x) \in S$ είναι αντιστρέψιμο και $f(x)^{-1} = f(x^{-1})$, και*

(β) *ο ομομορφισμός δακτυλίων $f : R \longrightarrow S$ επάγει έναν ομομορφισμό ομάδων $f : \mathsf{U}(R) \longrightarrow \mathsf{U}(S)$ μεταξύ των (πολλαπλασιαστικών) ομάδων των δακτυλίων R και S αντίστοιχα.*

Άσκηση 8.5.2. *Να δώσετε παράδειγμα ομομορφισμού δακτυλίων $f : R \longrightarrow S$, όπου R και S είναι δακτύλιοι με μονάδα, έτσι ώστε:*

1. *$f(1_R) \neq 1_S$.*
2. *ο δακτύλιος R περιέχει αντιστρέψιμο στοιχείο x και το στοιχείο $f(x) \in S$ δεν είναι αντιστρέψιμο.*

Άσκηση 8.5.3.

1. *Είναι δυνατόν ένας δακτύλιος με μονάδα να περιέχει ταυτόχρονα δύο υποδακτύλιους ισόμορφους με τους $\mathbb{Z}_n$ και $\mathbb{Z}_m$, όπου $m \neq n$; Αν είναι, δώστε ένα παράδειγμα. Αν όχι, αποδείξτε το.*
2. *Είναι δυνατόν ένας δακτύλιος με μονάδα να περιέχει ταυτόχρονα δύο υποδακτύλιους ισόμορφους προς τα σώματα $\mathbb{Z}_p$ και $\mathbb{Z}_q$, όπου p και q είναι δύο διαφορετικοί πρώτοι; Δώστε παράδειγμα ή δείξτε ότι είναι αδύνατον.*

Άσκηση 8.5.4. *Αν R είναι ένα μεταθετικός δακτύλιος και I, J, και K είναι ιδεώδη του R, τότε να δειχθούν τα ακόλουθα:*

$$I+(J+K)=(I+J)+K, \quad (0)+I=I=I+(0), \quad I+J=J+I, \quad R+I=R=I+R$$

με άλλα λόγια το σύνολο $\mathsf{Ideal}(R)$ όλων των ιδεωδών του R με πράξη το άθροισμα ιδεωδών αποτελεί ένα μεταθετικό μονοειδές.

Άσκηση 8.5.5. *Αν R είναι ένας μεταθετικός δακτύλιος και I, J, και K είναι ιδεώδη του R, τότε να δειχθούν τα ακόλουθα:*

$$I\cdot(J\cdot K)=(I\cdot J)\cdot K, \quad R\cdot I=I=I\cdot R, \quad I\cdot J=J\cdot I$$

με άλλα λόγια το σύνολο $\mathsf{Ideal}(R)$ όλων των ιδεωδών του R με πράξη το γινόμενο ιδεωδών αποτελεί ένα μεταθετικό μονοειδές.

Άσκηση 8.5.6. *Έστω ότι R είναι ένας μεταθετικός δακτύλιος και ότι I, J, και K είναι ιδεώδη του R. Τότε:*

$$(I\cap J)+(I\cap K)\subseteq I\cap(J+K), \quad I+(J\cap K)\subseteq(I+J)\cap(I+K), \quad I\cdot(J+K)=I\cdot J+I\cdot K, \quad I\cdot(J\cap K)\subseteq(I\cdot J)\cap(I\cdot K)$$

Άσκηση 8.5.7. *Αν R είναι μια μεταθετική ακέραια περιοχή στην οποία κάθε ιδεώδες είναι κύριο, να δειχθεί ότι το σύνολο $\mathsf{Ideal}^*(R)$ όλων των μη μηδενικών ιδεωδών του R με πράξη το γινόμενο ιδεωδών, είναι ένα μεταθετικό μονοειδές για το οποίο ισχύει ο Νόμος Διαγραφής, $\forall I,J,K\in\mathsf{Ideal}^*(R)$:*

$$I\cdot J=I\cdot K \quad\Longrightarrow\quad J=K$$

Άσκηση 8.5.8. *Άν $f,g\colon\mathbb{Q}\longrightarrow R$ είναι μομομορφσιμοί δακτυλίων και ισχύει ότι $f(n)=g(n)$, $\forall n\in\mathbb{Z}$, να δειχθεί ότι $f=g$.*

Άσκηση 8.5.9.

1. *Να προσδιοριστούν όλοι οι ομομορφισμοί δακτυλίων $\mathbb{Z}\longrightarrow\mathbb{Z}$.*
2. *Να προσδιοριστούν όλοι οι ομομορφισμοί δακτυλίων $\mathbb{Z}\longrightarrow\mathbb{Q}$.*
3. *Να προσδιοριστούν όλοι οι ομομορφισμοί δακτυλίων $\mathbb{Z}_n\longrightarrow\mathbb{Z}_n$.*
4. *Να προσδιοριστούν όλοι οι ομομορφισμοί δακτυλίων $\mathbb{Z}_n\longrightarrow\mathbb{Z}_m$, όπου $n,m\geq 2$.*

Άσκηση 8.5.10. *Να δείξετε ότι ένας ομομορφισμός δακτυλίων $f:R\longrightarrow S$, όπου R είναι σώμα, είναι είτε ο μηδενικός (οπότε $0_S=1_S$) ή είναι μονομορφισμός. Επίσης να δείξετε ότι ο f δεν είναι απαραίτητα επιμορφισμός.*

Να δείξετε ότι ο δακτύλιος πηλίκο R/I ενός σώματος R ως προς ένα ιδεώδες I είναι είτε ο μηδενικός δακτύλιος με ένα στοιχείο ή είναι ισόμορφος με το σώμα R.

Άσκηση 8.5.11.

1. *Να δοθεί παράδειγμα μη μεταθετικού δακτυλίου R, ο οποίος περιέχει ένα ιδεώδες I έτσι ώστε ο δακτύλιος πηλίκο R/I να είναι μεταθετικός.*
2. *Να δοθεί παράδειγμα δακτυλίου R χωρίς μονάδα, ο οποίος περιέχει ένα ιδεώδες I έτσι ώστε ο δακτύλιος πηλίκο R/I να έχει μονάδα.*
3. *Να δοθεί παράδειγμα δακτυλίου R με διαιρέτες του μηδενός, ο οποίος περιέχει ένα ιδεώδες I έτσι ώστε ο δακτύλιος πηλίκο R/I να μην έχει διαιρέτες του μηδενός.*
4. *Να δοθεί παράδειγμα δακτυλίου R χωρίς διαιρέτες του μηδενός, ο οποίος περιέχει ένα ιδεώδες I έτσι ώστε ο δακτύλιος πηλίκο R/I να έχει διαιρέτες του μηδενός.*
5. *Βρείτε έναν υποδακτύλιο του δακτυλίου $\mathbb{Z}\times\mathbb{Z}$, ο οποίος να μην είναι ιδεώδες του $\mathbb{Z}\times\mathbb{Z}$.*

Άσκηση 8.5.12. *1. Δείξτε ότι η απεικόνιση*

$$f : \mathbb{C} \longrightarrow \mathsf{M}_2(\mathbb{R}), \quad f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

είναι μονομορφισμός δακτυλίων.

2. Θεωρούμε τον υποδακτύλιο

$$\mathbb{Q}[\sqrt{5}] = \{a + b\sqrt{5} \in \mathbb{R} \mid a, b \in \mathbb{Q}\}$$

του σώματος $\mathbb{R}$ των πραγματικών αριθμών. Να δειχθεί ότι το υποσύνολο $\mathbb{Q}[\sqrt{5}]$ είναι σώμα και η απεικόνιση

$$f : \mathbb{Q}[\sqrt{5}] \longrightarrow \mathbb{Q}[\sqrt{5}], \quad f(a+b\sqrt{5}) = a - b\sqrt{5}$$

είναι ισομορφισμός δακτυλίων.

Άσκηση 8.5.13. *Να δειχθεί ότι η απεικόνιση*

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5, \quad f(x) = ([x]_3, [x]_5)$$

είναι επιμορφισμός δακτυλίων και να προσδιοριστεί ο πυρήνας του.

Άσκηση 8.5.14. *Για έναν μη μηδενικό ακέραιο d ο οποίος είναι ελεύθερος τετραγώνου (δηλαδή δεν υπάρχει πρώτος το τετράγωνο του οποίου διαιρεί τον d), να δειχθεί ότι το υποσύνολο*

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$$

είναι ένας υποδακτύλιος του $\mathbb{C}$ και να βρεθούν τα στοιχεία $x \in \mathbb{Z}[\sqrt{d}]$ για τα οποία η απεικόνιση $\mathbb{Z} \longrightarrow \mathbb{Z}[\sqrt{d}]/(x)$, $a \longmapsto a + (x)$ είναι επιμορφισμός δακτυλίων. Αν x είναι ένα τέτοιο στοιχείο, να δειχθεί ότι υπάρχει ένας ισομορφισμός δακτυλίων

$$\mathbb{Z}/\mathbb{Z} \cap (x) \xrightarrow{\cong} \mathbb{Z}[\sqrt{d}]/(x)$$

Άσκηση 8.5.15. *Έστω ο δακτύλιος πολυωνύμων $\mathbb{R}[t]$ υπεράνω του $\mathbb{R}$. Έστω τα κύρια ιδεώδη του $\mathbb{R}[t]$*

$$I = (t^2 + 2) \quad \text{και} \quad J = (t^2 - 9)$$

τα οποία παράγονται από τα πολυώνυμα $t^2 + 2$ και $t^2 - 9$. Να περιγραφούν οι δακτύλιοι πηλίκα $\mathbb{R}[t]/I$ και $\mathbb{R}[t]/J$. Τι παρατηρείτε;

Άσκηση 8.5.16. *Να βρεθούν όλα τα ιδεώδη του υποδακτυλίου*

$$\mathsf{AT}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b, c \in \mathbb{R} \right\} \subseteq \mathsf{M}_2(\mathbb{R})$$

των 2×2 άνω τριγωνικών πινάκων υπεράνω του $\mathbb{R}$.

Άσκηση 8.5.17. *Έστω $\mathbb{K}$ ένα σώμα. Να δειχθεί ότι τα μόνα ιδεώδη του δακτυλίου πινάκων $\mathsf{M}_2(\mathbb{K})$ είναι το μηδενικό ιδεώδες και ο ίδιος ο δακτύλιος. Να εξεταστεί αν αυτός ο ισχυρισμός είναι αληθής όταν $n > 2$.*

Άσκηση 8.5.18. *Έστω R ένας δακτύλιος με μονάδα. Να δειχθεί ότι ένα υποσύνολο A του δακτυλίου πινάκων $\mathsf{M}_n(R)$ είναι ιδεώδες του $\mathsf{M}_n(R)$ αν και μόνο αν υπάρχει ιδεώδες I του R έτσι ώστε:*

$$A = \mathsf{M}_n(I) := \left\{ A = (a_{ij}) \in \mathsf{M}_n(R) \mid a_{ij} \in I, \ \ 1 \leq i, j \leq n \right\}$$

Επιπλέον να δειχθεί ότι η απεικόνιση

$$\Phi : \{\text{ιδεώδη } I \text{ του } R\} \longrightarrow \{\text{ιδεώδη } A \text{ του } \mathscr{M}_n(R)\}, \quad \Phi(I) = \mathsf{M}_n(I)$$

είναι «1-1» και «επί».

Άσκηση 8.5.19. *1. Βρείτε όλα τα ιδεώδη N του δακτυλίου $\mathbb{Z}_{12}$. Σε κάθε περίπτωση να περιγράψετε του δακτύλιο πηλίκο $\mathbb{Z}_{12}/N$, δηλαδή βρείτε γνωστό δακτύλιο με τον οποίο είναι ισόμορφος ο δακτύλιος πηλίκο $\mathbb{Z}_{12}/N$.*

2. Να δείξετε ότι το υποσύνολο $8\mathbb{Z}$ είναι ιδεώδες του δακτυλίου $2\mathbb{Z}$, και να συμπληρώσετε τους πίνακες πρόσθεσης και πολλαπλασιασμού του δακτύλιου πηλίκου $2\mathbb{Z}/8\mathbb{Z}$. Είναι οι δακτύλιοι $2\mathbb{Z}/8\mathbb{Z}$ και $\mathbb{Z}_4$ ισόμορφοι;

Άσκηση 8.5.20. *Έστω $\{I_k\}_{k=1}^n$ ένα σύνολο δεξιών, αριστερών ή αμφίπλευρων ιδεώδωνμ ενός δακτύλιου. Να δειχθεί ότι αν $I_i \cap I_j = \{0\}$, $1 \leq i \neq j \leq n$, τότε το άθροισμα $I_1 + I_2 + \cdots + I_n$ δεν είναι απαραίτητα ευθύ.*

Άσκηση 8.5.21. *Να δοθεί παράδειγμα ομομορφισμού δακτυλίων $f\colon R \longrightarrow S$ και ιδεώδους I του R έτσι ώστε το υποσύνολο $f(I)$ να μην είναι ιδεώδες του S.*

Άσκηση 8.5.22. *Έστω $f\colon R \longrightarrow S$ ένας ομομορφισμός δακτυλίων. Να δειχθεί ότι ο ομομορφισμός δακτυλίων f επάγει έναν ομομορφισμό δακτυλίων πινάκων*

$$\mathsf{M}_n(f)\colon \mathsf{M}_n(R) \longrightarrow \mathsf{M}_n(S), \quad A = (a_{ij}) \longmapsto \mathsf{M}_n(f)(A), \quad \text{όπου} \quad \mathsf{M}_n(f)(A)_{ij} = (f(a_{ij}))$$

Άσκηση 8.5.23. *Να αποδειχθεί η Πρόταση 8.2.24.*

Άσκηση 8.5.24. *Να δειχθεί ότι κάθε δακτύλιος R μπορεί να εμφυτευθεί ταυτόχρονα ως υποδακτύλιος S και ως ιδεώδες I σε έναν δακτύλιο $\widetilde{R}$, έτσι ώστε $I^2 = 0$.*

Υπόδειξη: Στην αβελιανή ομάδα $R \times R$ να θεωρήστε πολλαπλασιασμό $(r_1, r_2)\cdot(r_1', r_2') = (r_1 \cdot r_1', r_1 \cdot r_2' + r_2 \cdot r_1')$.

Άσκηση 8.5.25. *Να περιγραφεί ο δακτύλιος πηλίκο $\mathbb{Z}[t]/(2,t)$ ως ισόμορφος με έναν γνωστό σας δακτύλιο.*

Άσκηση 8.5.26. *Αν p είναι ένας πρώτος αριθμός, να περιγραφεί ο δακτύλιος πηλίκο $\mathbb{Z}[t]/(p, t^2+1)$ ως ισόμορφος με έναν γνωστό σας δακτύλιο.*

Άσκηση 8.5.27. *Να δειχθεί ότι το υποσύνολο $\left\{\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right) \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R}\right\}$ είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{R})$, και υπάρχει ένας ισομορφισμός δακτυλίων*

$$\left\{\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R}\right\} \xrightarrow{\cong} \mathbb{R}[t]/(t^2)$$

Άσκηση 8.5.28. *Να δειχθεί ότι αν για έναν δακτύλιο R η αριστερή κανονική αναπαράσταση είναι ισομορφισμός, τότε ο δακτύλιος R είναι μεταθετικός.*

Άσκηση 8.5.29. *Να βρεθεί η αριστερή κανονική αναπαράστση των δακτυλίων $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$.*

Άσκηση 8.5.30. *Να βρεθεί η αριστερή κανονική αναπαράσταση (α) του δακτυλίου $\mathsf{M}_2(\mathbb{R})$ των 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς, και (β) του δακτυλίου $\mathsf{AT}_2(\mathbb{R})$ των 2×2 άνω τριγωνικών πινάκων με στοιχεία πραγματικούς αριθμούς.*

Άσκηση 8.5.31. *Έστω R ένας δακτύλιος και υποθέτουμε ότι η προσθετική ομάδα του $(R,+)$ είναι κυκλική. Τι συμπέρασμα μπορείτε να εξαγάγετε για την δομή του δακτυλίου R;*

Άσκηση 8.5.32. *Στον δακτύλιο* $\mathscr{C}([0,1],\mathbb{R}) = \{f : [0,1] \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$, *να δειχθεί ότι το υποσύνολο*

$$I_r = \{f \in \mathscr{C}([0,1],\mathbb{R}) \mid f(r) = 0\} \quad (r \in [0,1])$$

είναι ένα ιδεώδες το οποίο δεν είναι πεπερασμένα παραγόμενο.

Άσκηση 8.5.33. *Να δείξετε ότι στην αβελιανή προσθετική ομάδα του Klein* $V = \{e,a,b,c\}$ *μπορούμε να ορίσουμε μια πράξη πολλαπλασιασμού* $\cdot$ *έτσι ώστε η τριάδα* $(V,+,\cdot)$ *να είναι ένας μεταθετικός δακτύλιος με μονάδα. Να δείξετε ότι ο δακτύλιος* $(V,+,\cdot)$ *είναι ισόμορφος με τον δακτύλιο ευθύ γινόμενο* $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Άσκηση 8.5.34. *Υπενθυμίζουμε ότι ένα μη κενό υποσύνολο* $\mathbb{F}$ *ενός σώματος* $\mathbb{K}$ *καλείται υπόσωμα, αν:* (α) $a-b \in \mathbb{K}$, $\forall a,b \in \mathbb{K}$, *και* (β) $ab^{-1} \in \mathbb{K}$, $\forall a,b \in \mathbb{K}$, $b \neq 0$.

1. *Να δείξετε ότι, με τις επαγόμενες πράξεις του σώματος, ένα υπόσωμα είναι σώμα.*
2. *Να δείξετε ότι η τομή υποσωμάτων ενός σώματος είναι υπόσωμα.*
3. *Να δείξετε ότι υπάρχει μεταθετικός δακτύλιος με μονάδα* R *ο οποίος περιέχει δύο υποδακτυλίους* S *και* T *οι οποίοι είναι σώματα, αλλά ο υποδακτύλιος* $S \cap T$ *δεν είναι σώμα.*

Άσκηση 8.5.35. *Έστω ο δακτύλιος πολυωνύμων* $\mathbb{R}[t]$ *υπεράνω του* $\mathbb{R}$. *Να δείξετε ότι τα υποσύνολα*

$$I = \{P(t)(t^2-1) \in \mathbb{R}[t] \mid P(t) \in \mathbb{R}[t]\} \quad \text{και} \quad I = \{P(t)(t^2-5t+6) \in \mathbb{R}[t] \mid P(t) \in \mathbb{R}[t]\}$$

είναι ιδεώδη του $\mathbb{R}[t]$ *και να περιγραφούν οι δακτύλιοι πηλίκα* $\mathbb{R}[t]/I$ *και* $\mathbb{R}[t]/J$.

Άσκηση 8.5.36. 1. *Δείξτε ότι η απεικόνιση*

$$f : \mathbb{C} \longrightarrow \mathbb{H}, \quad f(z) = \begin{pmatrix} z & 0 \\ 0 & \overline{z} \end{pmatrix}$$

είναι μονομορφισμός δακτυλίων, όπου

$$\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix} \in \mathsf{M}_2(\mathbb{C}) \mid z,w \in \mathbb{C} \right\}$$

είναι ο δακτύλιος διαίρεσης των τετρανίων του Hamilton.

2. *Έστω* $\mathbb{F}$ *ένα σώμα χαρακτηριστικής* $p > 0$. *Να δείξετε ότι η απεικόνιση Frobenius*[3]

$$F : \mathbb{F} \longrightarrow \mathbb{F}, \quad F(a) = a^p$$

είναι ομομορφισμός δακτυλίων.

Άσκηση 8.5.37. *Να δοθεί παράδειγμα υποδακτυλίου* $S \subseteq R$ *ενός δακτυλίου* R *και ενός ιδεώδους* $I \subseteq S$ *του* S *έτσι ώστε το* I *να μην είναι ιδεώδες του* R.

Υπενθυμίζουμε ότι ένα στοιχείο $r \in R$ ενός δακτυλίου R καλείται **μηδενοδύναμο**, αν υπάρχει $n \geq 1$ έτσι ώστε $r^n = 0$.

[3] Ferdinand Georg Frobenius (26 Οκτωβρίου 1849 - 3 Αυγούστου 1917) [https://en.wikipedia.org/wiki/Ferdinand_Georg_Frobenius]: Γερμανός μαθηματικός, με σημαντική συμβολή στην Άλγεβρα, ιδιαίτερα στη Θεωρία Ομάδων, στην Ανάλυση, ιδιαίτερα στις διαφορικές εξισώσεις και στη θεωρία ελλειπτικών συναρτήσεων, και στη Θεωρία Αριθμών.

Άσκηση 8.5.38. *Αν ο δακτύλιος R είναι μεταθετικός, να δειχθεί ότι το σύνολο $\mathsf{Nil}(R)$ όλων των μηδενοδύναμων στοιχείων του R είναι ένα ιδεώδες*[4] *του R και ο δακτύλιος πηλίκο $R/\mathsf{Nil}(R)$ δεν έχει μη μηδενικά μηδενοδύναμα στοιχεία.*

Επιπλέον να υπολογίσετε το ιδεώδες $\mathsf{Nil}(R)$ στις ακόλουθες περιπτώσεις: $R=\mathbb{Z}$, $R=\mathbb{Z}_{12}$, $R=\mathbb{Z}_{32}$, και $R=\mathbb{K}[t]$, όπου $\mathbb{K}$ είναι ένα σώμα.

Άσκηση 8.5.39. *Να δοθεί παράδειγμα ενός μη μεταθετικού δακτυλίου R ο οποίος περιέχει ένα γνήσιο ιδεώδες I έτσι ώστε ο δακτύλιος πηλίκο R/I να είναι μεταθετικός.*

Άσκηση 8.5.40. *Έστω R_1 και R_2 δύο δακτύλιοι. Στον δακτύλιο ευθύ γινόμενο $R=R_1\times R_2$ να δείξετε ότι τα υποσύνολα*

$$R_1^* = \big\{(x,0)\in R \mid x\in R_1\big\} \qquad \text{και} \qquad R_1^* = \big\{(0,y)\in R \mid y\in R_2\big\}$$

είναι ιδεώδη και υπάρχουν ισομορφισμοί δακτυλίων, $i=1,2$:

$$R_i^* \xrightarrow{\cong} R_i \qquad \text{και} \qquad R/R_1^* \xrightarrow{\cong} R_2 \qquad \text{και} \qquad R/R_2^* \xrightarrow{\cong} R_1$$

Να γενικευθούν οι παραπάνω ισχυρισμοί για ευθύ γινόμενο δακτυλίων $R=R_1\times R_2\times\cdots\times R_n$, $n>2$.

Άσκηση 8.5.41. *Έστω $\mathscr{F}=\big\{f\colon [0,1]\longrightarrow\mathbb{R} \mid f \text{ είναι συνάρτηση}\big\}$ ο (μεταθετικός με μονάδα) δακτύλιος των συναρτήσεων από το κλειστό διάστημα $[0,1]\subseteq\mathbb{R}$ στο $\mathbb{R}$.*

Έστω

$$\mathscr{C}([0,1],\mathbb{R}) = \big\{f\colon [0,1]\longrightarrow\mathbb{R} \mid f \text{ είναι συνεχής συνάρτηση}\big\} \subseteq \mathscr{F}$$

1. *Να δειχθεί ότι το υποσύνολο $\mathscr{C}([0,1],\mathbb{R})$ είναι υποδακτύλιος του $\mathscr{F}$.*
2. *Για κάθε $r\in[0,1]$, να δειχθεί ότι το σύνολο*

$$M_r = \big\{f\in\mathscr{C}([0,1],\mathbb{R}) \mid f(r)=0\big\}$$

είναι ένα ιδεώδες του $\mathscr{C}([0,1],\mathbb{R})$ και υπάρχει ένας ισομορφισμός δακτυλίων

$$\mathscr{C}([0,1],\mathbb{R})\Big/M_r \;\cong\; \mathbb{R}$$

Άσκηση 8.5.42. 1. *Να δειχθεί ότι το ιδεώδες $I=(2,t)$ του δακτυλίου $\mathbb{Z}[t]$ το οποίο παράγεται από το σύνολο $\{2,t\}\subseteq\mathbb{Z}[t]$ δεν είναι κύριο.*

2. *Να δειχθεί ότι το ιδεώδες (t_1,t_2) του δακτυλίου $\mathbb{K}[t_1,t_2]$, όπου $\mathbb{K}$ είναι ένα σώμα, το οποίο παράγεται από το σύνολο $\{t_1,t_2\}\subseteq\mathbb{K}[t_1,t_2]$ δεν είναι κύριο.*

Άσκηση 8.5.43. *Έστω ότι $f\colon R\longrightarrow S$ είναι ένας επιμορφισμός δακτυλίων και I και J είναι ιδεώδη του S. Να δειχθεί ότι:*

$$f^{-1}(I+J) = f^{-1}(I)+f^{-1}(J)$$

Άσκηση 8.5.44. *Έστω ότι $f\colon R\longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων, ότι I είναι ένα ιδεώδες του R, και ότι $\{K_i\}_{i\in I}$ είναι μια οικογένεια ιδεωδών του S. Να δειχθεί ότι:*

$$f^{-1}(f(I)) = I+\mathsf{Ker}(f) \qquad \text{και} \qquad f^{-1}\Big(\bigcap_{i\in I}K_i\Big)=\bigcap_{i\in I}f^{-1}(K_i)$$

[4] Το ριζικό $\mathsf{Nil}(R)$ του μεταθετικού δακτυλίου R καλείται το **μηδενοριζικό** του R.

Άσκηση 8.5.45. *Στην Πρόταση 8.1.35 να δειχθεί ότι κάθε ιδεώδες* $I_k = e_kR = Re_k = e_kRe_k$ *είναι δακτύλιος με μονάδα* e_k, $1 \le k \le n$.

Άσκηση 8.5.46. *Έστω ότι* $f: R \longrightarrow S$ *είναι ένας ομομορφισμός δακτυλίων. Αν* $x \in R$ *και* $x^2 = 2 \cdot 1_R$, *τότε* $f(x)^2 = 2 \cdot 1_S$. *Χρησιμοποιώντας αυτή την ιδιότητα να δειχθεί ότι οι δακτύλιοι* $\mathbb{Z}[\sqrt{2}]$ *και* $\mathbb{Z}[\sqrt{3}]$ *δεν είναι ισόμορφοι.*

Άσκηση 8.5.47. *Έστω* R *ένας δακτύλιος με μονάδα* 1_R. *Τότε η απεικόνιση*

$$f: \mathbb{Z} \longrightarrow R, \quad f(n) = n \cdot 1_R$$

είναι ομομορφισμός δακτυλίων και $\mathsf{Ker}(f) = \{kp \in \mathbb{Z} | k \in \mathbb{Z}\} = (p)$, *όπου* $p = \mathsf{char}(R)$.

Ο f *είναι ο μοναδικός ομομορφισμός δακτυλίων* $\mathbb{Z} \longrightarrow R$ *με την ιδιότητα* $f(1) = 1_R$. *Επιπλέον:*

1. *Αν* $p > 0$, *τότε ο δακτύλιος* R *περιέχει έναν υποδακτύλιο ισόμορφο με τον δακτύλιο* $\mathbb{Z}_p$.
2. *Αν* $p = 0$, *τότε ο δακτύλιος* R *περιέχει έναν υποδακτύλιο ισόμορφο με τον δακτύλιο* $\mathbb{Z}$.

Άσκηση 8.5.48. *Να δειχθεί ότι, αν* $f: R \longrightarrow S$ *είναι ένας ομομορφισμός μεταξύ δύο δακτυλίων διαίρεσης, τότε:* $\mathsf{char}(R) = \mathsf{char}(S)$.

Άσκηση 8.5.49. *Αν* I *είναι ένα ιδεώδες του δακτυλίου* R, *να δειχθεί ότι υπάρχει ένας ισομορφισμός δακτυλίων*

$$\mathsf{M}_n(R)/\mathsf{M}_n(I) \xrightarrow{\cong} \mathsf{M}_n(R/I)$$

όπου $\mathsf{M}_n(I)$ *είναι το ιδεώδες* $\mathsf{M}_n(I) = \{A = (a_{ij}) \in \mathsf{M}_n(R) \mid a_{ij} \in I,\ 1 \le i, j \le n\}$.

Άσκηση 8.5.50. *Να δειχθεί ότι, αν* A *και* B *είναι δύο σύνολα και* $|A| = |B|$, *τότε οι δακτύλιοι* $\mathscr{P}(A)$ *και* $\mathscr{P}(B)$, *βλέπε την Άσκηση 7.6.26 είναι ισόμορφοι.*

Άσκηση 8.5.51. *Έστω* $A = [0,1] \subseteq \mathbb{R}$, *και θεωρούμε του δακτύλιο* $\mathscr{P}(A)$ *της Άσκησης 7.6.26. Να περιγραφούν τα ιδεώδη* (X), (Y), *και* (X,Y) *τα οποία παράγονται από τα υποσύνολα* $X = [0, \frac{1}{2}]$, $Y = \{\frac{1}{4}\}$ *και* $\{X, Y\}$ *του* $A = [0,1]$, *καθώς και το ιδεώδες γινόμενο* $(A) \cdot (B)$.

Άσκηση 8.5.52. *Έστω* A *ένα μη κενό σύνολο,* $X \subseteq A$ *ένα υποσύνολο του* A, *και θεωρούμε του δακτύλιο* $\mathscr{P}(A)$ *της Άσκησης 7.6.26.*

1. *Να δειχθεί ότι το σύνολο* $\mathscr{P}(X)$ *είναι ένα ιδεώδες του* $\mathscr{P}(A)$ *και υπάρχει ένας ισομορφισμός δακτυλίων*

$$\mathscr{P}(A \setminus X) \xrightarrow{\cong} \mathscr{P}(A)/\mathscr{P}(X)$$

2. *Αν το σύνολο* A *είναι πεπερασμένο, να δειχθεί ότι κάθε ιδεώδες του δακτυλίου* $\mathscr{P}(A)$ *είναι της μορφής* $\mathscr{P}(X)$, *για κάποιο υποσύνολο* $X \subseteq A$.
3. *Να δοθεί παράδειγμα ενός άπειρου συνόλου* A, *έτσι ώστε ο δακτύλιος* $\mathscr{P}(A)$ *να περιέχει ένα ιδεώδες* I *το οποίο δεν είναι της μορφής* $\mathscr{P}(Y)$, *όπου* $Y \subseteq A$.

Άσκηση 8.5.53. *Έστω* R *ένας, όχι απαραίτητα μεταθετικός, δακτύλιος. Υπενθυμίζουμε ότι μια υποομάδα* I *της προσθετικής ομάδας* $(R,+)$ *καλείται αριστερό, αντίστοιχα δεξιό, ιδεώδες, αν:* $rx \in I$, *αντίστοιχα* $xr \in I$, $\forall r \in R$, $\forall x \in I$.

1. *Αν ο δακτύλιος R έχει μονάδα, τότε ο R είναι δακτύλιος διαίρεσης αν και μόνο αν τα μόνα αριστερά (δεξιά) ιδεώδη του R είναι τα $\{0\}$ και R.*

2. *Αν ο δακτύλιος R δεν έχει απαραίτητα μονάδα και τα μόνα αριστερά (δεξιά) ιδεώδη του R είναι τα $\{0\}$ και R, τότε είτε ο R είναι δακτύλιος διαίρεσης είτε το πλήθος των στοιχείων του R είναι ένας πρώτος αριθμός p, και: $rs = 0,\ \forall r, s \in R$.*

Άσκηση 8.5.54. *Θεωρούμε τον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων του Gauss.*

1. *Να περιγραφεί το ιδεώδες (i) το οποίο παράγεται από το στοιχείο i.*

2. *Να εξεταστεί, αν το σύνολο $I = \{m + mi \in \mathbb{Z}[i] \mid m \in \mathbb{Z}\}$ είναι ιδεώδες του $\mathbb{Z}[i]$.*

3. *Θεωρούμε το ιδεώδες $J = (1 + i)$ το οποίο παράγεται από το στοιχείο $1 + i$.*

   (α') Να δειχθεί ότι $2 \in J$.

   (β') Να υπολογιστούν όλα τα στοιχεία του δακτυλίου $\mathbb{Z}[i]/J$.

Άσκηση 8.5.55. *Να δειχθεί ότι, αν $\mathbb{F}$ είναι ένα πεπερασμένο σώμα χαρακτηριστικής p, τότε $p - 1 \mid |\mathbb{F}| - 1$. Να συμπεράνετε ότι, αν το πλήθος των στοιχείων του $\mathbb{F}$ είναι άρτιο, τότε $\mathsf{char}(\mathbb{F}) = 2$.*

Άσκηση 8.5.56. *Να προσδιοριστεί ο πυρήνας των ακόλουθων ομομορφισμών εκτίμησης*

$$f : \mathbb{R}[t] \longrightarrow \mathbb{C}, \quad f(t) = f(2 + i) \qquad \text{και} \qquad g : \mathbb{Z}[t] \longrightarrow \mathbb{R}, \quad g(t) = g(1 + \sqrt{2})$$

Άσκηση 8.5.57. *Έστω ότι R είναι ένας δακτύλιος και ότι I, J, και K είναι ιδεώδη του R.*

1. *Να δειχθεί ότι: $I \cdot J \subseteq I \cap J$.*

2. *Να δοθεί παράδειγμα δακτυλίου R και ιδεωδών I και J του R έτσι ώστε: $I \cdot J \neq I \cap J$.*

3. *Να δειχθεί ότι $I \cdot J = I \cap J$, αν $I + J = R$.*

4. *Να εξεταστεί αν: $I \cdot (J + K) = I \cdot J + I \cdot K$.*

Άσκηση 8.5.58. *Έστω ότι R είναι ένας δακτύλιος και ότι I, J είναι ιδεώδη του R έτσι ώστε: $I + J = R$ και $I \cdot J = (0)$. Να δειχθεί ότι υπάρχει ένας ισομορφισμός δακτυλίων*

$$R \xrightarrow{\cong} R/I \times R/J$$

Άσκηση 8.5.59. *Έστω I, J, και K είναι ιδεώδη ενός δακτυλίου R και υποθέτουμε ότι $I \subseteq K$. Να δειχθεί ότι:*

$$(I + J) \cap K = I + (J \cap K)$$

Να εξεταστεί αν η παραπάνω ισότητα ισχύει στην περίπτωση κατά την οποία $I \nsubseteq K$.

Άσκηση 8.5.60. *Να προσδιοριστούν όλα τα ιδεώδη των δακτυλίων $\mathbb{K} \times \mathbb{K}$, όπου $\mathbb{K}$ είναι ένα σώμα, και $\mathbb{Z} \times \mathbb{Z}$, και ακολούθως να περιγραφούν οι αντίστοιχοι δακτύλιοι πηλίκα.*

Άσκηση 8.5.61. *Αν I είναι ένα αριστερό ιδεώδες και J είναι ένα δεξιό ιδεώδες σε έναν δακτύλιο R, να εξεταστεί αν το σύνολο $I \cap J$ είναι πάντα ιδεώδες του R.*

Άσκηση 8.5.62. *Έστω ότι $\mathbb{K}$ και $\mathbb{L}$ είναι δύο σώματα με χαρακτηριστική $\neq 2,3$ και έστω ότι $f:\mathbb{K}\longrightarrow\mathbb{L}$ είναι μια απεικόνιση έτσι ώστε, $\forall\, x,y\in\mathbb{K}$:*

$$f(x+y)=f(x)+f(y)\qquad \text{και}\qquad f(1_{\mathbb{K}})=1_{\mathbb{L}}$$

Να δειχθεί ότι η απεικόνιση f είναι ομομορφισμός αν και μόνο αν $f(x^3)=f(x)^3$, $\forall\, x\in\mathbb{K}$.

Άσκηση 8.5.63. *Να δειχθεί ότι κάθε μη μηδενικό ιδεώδες του δακτυλίου $\mathbb{Z}[i]$ των ακεραίων του Gauss περιέχει πάντα έναν θετικό ακέραιο.*

Άσκηση 8.5.64. *Έστω I ένα ιδεώδες ενός μεταθετικού δακτυλίου R. Το* **ριζικό** *του I ορίζεται να είναι το σύνολο*

$$\sqrt{I}=\left\{r\in R\mid \exists n\in\mathbb{N}:\ r^n\in I\right\}$$

1. *Να δειχθεί ότι το σύνολο $\sqrt{I}$ είναι ένα ιδεώδες του R.*
2. *Ισχύουν οι εξής σχέσεις:*

$$\sqrt{\sqrt{I}}=I,\qquad \sqrt{I\cap J}=\sqrt{I}\cap\sqrt{J},\qquad \sqrt{I+J}=\sqrt{\sqrt{I}+\sqrt{J}}$$

3. *Να δειχθεί ότι $\sqrt{(0)}=\mathsf{Nil}(R)$.*

Άσκηση 8.5.65. *Με ποιους γνωστούς σας δακτύλιους είναι ισόμορφοι οι δακτύλιοι: (α) $\mathbb{Z}[t]/(t^2+3,p)$, όπου $p=2$ ή $p=3$, και (β) $\mathbb{Z}[i]/(2+i)$;*

Άσκηση 8.5.66. *Για κάθε πρώτο αριθμό p, θεωρούμε το ακόλουθο σύνολο*

$$\mathbb{Q}^{(p)}=\left\{\frac{a}{b}\in\mathbb{Q}\mid (p,b)=1\right\}$$

1. *Να δειχθεί ότι το σύνολο $\mathbb{Q}^{(p)}$ είναι ένας υποδακτύλιος του $\mathbb{Q}$.*
2. *Για κάθε ρητό $x\in\mathbb{Q}$, ισχύει: είτε $x\in\mathbb{Q}^{(p)}$ είτε $x^{-1}\in\mathbb{Q}^{(p)}$.*
3. *Δεν υπάρχει υποδακτύλιος R του $\mathbb{Q}$ έτσι ώστε: $\mathbb{Q}^{(p)}\subsetneqq R\subsetneqq\mathbb{Q}$.*
4. *Τα ιδεώδη του δακτυλίου $\mathbb{Q}^{(p)}$ είναι κύρια της μορφής (p^n), όπου $n\geq 0$.*
5. *Αν $\mathbb{P}$ είναι τό σύνολο όλων των πρώτων αριθμών τότε*

$$\bigcap_{p\in\mathbb{P}}\mathbb{Q}^{(p)}=\mathbb{Z}$$

Άσκηση 8.5.67. *Να δειχθεί ότι το ακόλουθο σύνολο*

$$R=\left\{\begin{pmatrix}a+2b & 3b\\ 2b & a-2b\end{pmatrix}\in \mathsf{M}_2(\mathbb{Q})\;\middle|\; a,b\in\mathbb{Q}\right\}$$

είναι ένας υποδακτύλιος του $\mathsf{M}_2(\mathbb{Q})$ ο οποίος είναι σώμα και υπάρχει ένας ισομορφισμός σωμάτων

$$R\xrightarrow{\cong}\mathbb{Q}[\sqrt{10}]=\left\{a+b\sqrt{10}\in\mathbb{R}\mid a,b\in\mathbb{Q}\right\}$$

Άσκηση 8.5.68. *Να δειχθεί ότι το σύνολο*

$$R = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \in \mathbb{Q} \mid a, b \in \mathbb{Q} \right\}$$

είναι ένας μη μεταθετικός υποδακτύλιος χωρίς μονάδα του δακτυλίου $\mathsf{M}_2(\mathbb{Q})$. *Αν* $I = \{A \in R \mid A^2 = 0\}$, *να δειχθεί ότι το σύνολο* I *είναι ένα ιδεώδες του* R *και υπάρχει ένας ισομορφισμός δακτυλίων*

$$R/I \xrightarrow{\cong} \mathbb{Q}$$

Άρα υπάρχουν μη μεταθετικοί δακτύλιοι χωρίς μονάδα οι οποίοι περιέχουν ιδεώδη, έτσι ώστε ο δακτύλιος πηλίκο να είναι μεταθετικός δακτύλιος με μονάδα.

Άσκηση 8.5.69. *Έστω* $q \in \mathbb{Q}$ *ένας ρητός αριθμός. Θεωρούμε του ακόλουθο υποδακτύλιο του* $\mathbb{Q}$, *βλέπε την Άσκηση 8.5.69:*

$$R_q = \left\{ \begin{pmatrix} a & b \\ qb & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{Q}) \mid a, b \in \mathbb{Q} \right\}$$

Να δειχθεί ότι, αν ο ακέραιος d *είναι ελεύθερος τετραγώνου, τότε ο δακτύλιος* R_q *είναι σώμα και είναι ισόμορφος με το σώμα*

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{q} \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

Άσκηση 8.5.70. *Να δειχθεί ότι η προσθετική ομάδα* $(\mathbb{K}, +)$ *ενός σώματος* $\mathbb{K}$ *και η πολλαπλασιαστική ομάδα του* $(\mathbb{K}^*, \cdot)$ *δεν είναι ισόμορφες.*

Άσκηση 8.5.71. *Έστω ότι* $\mathbb{K}$ *είναι ένα σώμα. Στο σύνολο* $\mathbb{K} \times \mathbb{K}$ *ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» ως εξής,* $\forall\, a, b, c, d \in \mathbb{K}$*:*

$$(a, b) + (c, d) = (a + c, b + d) \qquad \text{και} \qquad (a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

1. *Να δειχθεί ότι η τριάδα* $R := (\mathbb{K} \times \mathbb{K}, +, \cdot)$ *είναι ένας δακτύλιος.*
2. *Να δειχθεί ότι ο δακτύλιος* R *είναι σώμα αν και μόνο αν δεν υπάρχει στοιχείο* $k \in \mathbb{K}$ *έτσι ώστε* $k^2 = -1$.
3. *Να δειχθεί ότι, αν υπάρχει στοιχείο* $k \in \mathbb{K}$ *έτσι ώστε* $k^2 = -1$, *και* $\mathsf{char}(\mathbb{K}) \neq 2$, *τότε υπάρχει ένας ισομορφισμός δακτυλίων*

$$R \xrightarrow{\cong} \mathbb{K} \times \mathbb{K}$$

Κεφάλαιο 9

Δακτύλιοι Πολυωνύμων και Σώματα Κλασμάτων

Στο παρόν Κεφάλαιο θα μελετήσουμε διεξοδικότερα τις βασικές ιδιότητες του δακτυλίου πολυωνύμων, κυρίως μιας μεταβλητής, με στοιχεία από έναν μεταθετικό δακτύλιο, ιδιαίτερα με στοιχεία από ένα σώμα. Στην τελευταία περίπτωση θα αναλύσουμε την δομή των ιδεωδών του δακτυλίου πολυωνύμων μιας μεταβλητής. Επιπρόσθετα θα δούμε ότι κάθε ακέραια περιοχή μπορεί να εμφυτευθεί με μοναδικό τρόπο σε ένα σώμα, το σώμα κλασμάτων της. Ως σημαντική ειδική περίπτωση της παραπάνω κατασκευής προκύπτει το σώμα των ρητών συναρτήσεων, ως το σώμα κλασμάτων του δακτυλίου πολυωνύμων υπεράνω ενός σώματος.

9.1 Δακτύλιοι Πολυωνύμων

Έστω $R = (R, +, \cdot)$ ένας μεταθετικός δακτύλιος. Υπενθυμίζουμε ότι ο **δακτύλιος** $R[\![t]\!] = (R[\![t]\!], +, \cdot)$ **των τυπικών δυναμοσειρών** υπεράνω του R

$$R[\![t]\!] = \left\{ \mathsf{a} = (a_n)_{n\geq 0} \mid a_n \in R, \;\; n \geq 0 \right\}$$

έχει ως στοιχεία ακολουθίες $\mathsf{a} = (a_n)_{n\geq 0}$ στοιχείων του R, όπου δύο ακολουθίες $\mathsf{a} = (a_n)_{n\geq 0}, \mathsf{b} = (b_n)_{n\geq 0}$ είναι ίσες αν και μόνο αν $a_n = b_n$, $\forall\, n \geq 0$. Η πρόσθεση «+» και ο πολλαπλασιασμός «·» ορίζονται ως εξής:

$$+ : R[\![t]\!] \times R[\![t]\!] \longrightarrow R[\![t]\!], \quad \mathsf{a} + \mathsf{b} = \mathsf{c} = (c_n)_{n\geq 0}, \quad \text{όπου} \quad c_n = a_n + b_n, \;\; \forall\, n \geq 0$$

$$\cdot : R[\![t]\!] \times R[\![t]\!] \longrightarrow R[\![t]\!], \quad \mathsf{a} \cdot \mathsf{b} = \mathsf{d} = (d_n)_{n\geq 0}, \quad \text{όπου} \quad d_n = \sum_{k=0}^{n} a_k b_{n-k}, \;\; \forall\, n \geq 0$$

Γνωρίζουμε τότε ότι η τριάδα $(R[\![t]\!], +, \cdot)$ είναι ένας δακτύλιος με μονάδα, την ακολουθία $1 = (1, 0, 0, \cdots, 0, \cdots)$. Το μηδενικό στοιχείο είναι η μηδενική ακολουθία $0 = (0, 0, \cdots, 0, \cdots)$, και το αντίθετο στοιχείο της ακολουθίας $\mathsf{a} = (a_n)_{n\geq 0}$ είναι η ακολουθία $-\mathsf{a} = (-a_n)_{n\geq 0}$. Επειδή ο δακτύλιος R είναι μεταθετικός, ο πολλαπλασιασμός του $R[\![t]\!]$ δείχνει ότι ο δακτύλιος $R[\![t]\!] = (R[\![t]\!], +, \cdot)$ είναι επίσης μεταθετικός.

Υπενθυμίζουμε ότι ο **δακτύλιος** $R[t]$ **των πολυωνύμων υπεράνω του** R ορίζεται ως ο υποδακτύλιος

$$R[t] = \left\{ \mathsf{a} = (a_n)_{n\geq 0} \in R[\![t]\!] \mid \exists n \geq 0 : \; a_k = 0, \; \forall\, k > n \right\}$$

του δακτυλίου $R[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του R. Συμβολίζοντας:

$$t^0 := \left(1, 0, 0, \cdots, 0, \cdots\right), \quad t := \left(0, 1, 0, \cdots, 0, \cdots\right), \quad \text{και γενικότερα:} \quad t^n := \underbrace{\left(0, 0, \cdots, \; 0, 1, 0, \cdots, 0, \cdots\right)}_{\text{το } 1 \text{ στην } (n+1)-\text{θέση}}, \quad \forall\, n \geq 0$$

θα έχουμε ότι οι ακολουθίες t^n, $n \geq 0$, είναι πολυώνυμα υπεράνω του R και παρατηρούμε ότι το πολυώνυμο t^n είναι η n-οστή δύναμη του πολυωνύμου t ως προς την πράξη του πολλαπλασιασμού πολυωνύμων: $t^n = t \cdot t \cdots t$ (n-παράγοντες).

Επίσης, για κάθε στοιχείο $r \in R$, γράφοντας:

$$r\mathsf{a} = (ra_n)_{n\geq 0} = \left(ra_0, ra_1, \cdots, ra_n, \cdots\right)$$

για το γινόμενο της ακολουθίας $\mathsf{r} = (r, 0, \cdots, 0, \cdots)$ με την ακολουθία $\mathsf{a} = (a_0, a_1, \cdots, a_n, \cdots)$, όπως στο παράδειγμα 7.2.14, κάθε στοιχείο $\mathsf{a} = (a_n)_{n\geq 0}$, καλείται **τυπική δυναμοσειρά** υπεράνω του R, και μπορεί να εκφραστεί και να γραφεί ως εξής:

$$P(t) = \sum_{n=0}^{\infty} a_n t^n = a_0 1 + a_1 t + a_2 t^2 + \cdots a_n t^n + \cdots$$

Αν η τυπική δυναμοσειρά $P(t) = \sum_{n=0}^{\infty} a_n t^n$ ανήκει στον υποδακτύλιο $R[t]$, τότε υπάρχει $n \geq 0$ έτσι ώστε $a_n = 0$, $\forall k > n$. Τότε η τυπική δυναμοσειρά καλείται **πολυώνυμο** υπεράνω του R, και μπορεί να εκφραστεί και να γραφεί ως εξής:

$$P(t) = \sum_{k=0}^{n} a_n t^n = a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n$$

Χάριν απλότητας η ακολουθία (πολυώνυμο) 1 παραλείπεται από τις παραπάνω εκφράσεις. Παρατηρούμε ότι ο δακτύλιος πολυωνύμων $R[t]$ είναι ο υποδακτύλιος του $R[\![t]\!]$ ο οποίος παράγεται υπεράνω του R από το στοιχείο του t, και συνήθως καλείται ο **δακτύλιος πολυωνύμων μιας μεταβλητής** t.

Έστω $R_1 = R[t_1]$ ο δακτύλιος πολυωνύμων μιας μεταβλητής t_1 υπεράνω του R. Επειδή ο δακτύλιος R_1 είναι μεταθετικός, έπεται ότι μπορούμε να επαναλάβουμε τη διαδικασία και να θεωρήσουμε τον δακτύλιο πολυωνύμων $R_2 = R_1[t_2] = R[t_1][t_2]$, (εισάγουμε νέο σύμβολο t_2 για να μην υπάρχει σύγχυση με το σύμβολο t_1), ο οποίος είναι μεταθετικός, συμβολίζεται με $R[t_1, t_2]$ και καλείται ο *δακτύλιος των πολυωνύμων στις δύο μεταβλητές* t_1 και t_2. Επειδή ο δακτύλιος $R[t_1, t_2]$ είναι μεταθετικός, μπορούμε να επαναλάβουμε την διαδικασία για ένα πεπερασμένο πλήθος, ας πούμε n, βημάτων, και να αποκτήσουμε τον **δακτύλιο πολυωνύμων** $R[t_1, t_2, \cdots, t_n]$ **στις** n **μεταβλητές** t_1, t_2, $\cdots$, t_n:

$$R[t_1, t_2] = (R[t_1])[t_2], \quad R[t_1, t_2, t_3] = (R[t_1, t_2])[t_3], \ \cdots, \quad R[t_1, t_2, \cdots, t_n] = (R[t_1, t_2, \cdots, t_{n-1}])[t_n]$$

και τα στοιχεία του οποίου είναι πεπερασμένα αθροίσματα γινομένων στοιχείων του δακτυλίου R με γινόμενα μη αρνητικών δυνάμεων των στοιχείων $t_1, t_2, \cdots, t_n$:

$$R[t_1, t_2, \cdots, t_n] = \left\{ \sum_{(i)} r_{i_1 i_2 \cdots i_n} t_1^{k_{i_1}} t_2^{k_{i_2}} \cdots t_n^{k_{i_n}} \ \in \ S \ \middle| \ r_{i_1 i_2 \cdots i_n} \in R, \ \ k_{i_j} \geq 0, \ \ 1 \leq j \leq n \right\}$$

όπου $(i) = (i_1, i_2, \cdots, i_n) \in \mathbb{N}_0 \times \mathbb{N}_0 \times \cdots \times \mathbb{N}_0$.

9.1.1 Βασικές Ιδιότητες Πολυωνυμικών Δακτυλίων

Έστω $R[t]$ ο δακτύλιος πολυωνύμων μιας μεταβλητής t υπεράνω του μεταθετικού δακτυλίου R. Αν $0 \neq P(t)$ είναι ένα μη-μηδενικό πολυώνυμο, τότε υπάρχει $n \geq 0$ έτσι ώστε το $P(t)$ είναι της μορφής

$$P(t) = \sum_{k=0}^{n} a_n t^n = a_0 1 + a_1 t + a_2 t^2 + \cdots + a_n t^n, \qquad a_k \in R, \ \ 0 \leq k \leq n \quad \text{και} \quad a_n \neq 0 \tag{9.1}$$

Ο θετικός ή ίσος με μηδέν ακέραιος n καλείται ο **βαθμός** του πολυωνύμου $P(t)$ και συμβολίζεται με $\deg P(t)$:

$$\deg P(t) = \max\left\{ r \geq 0 \mid a_r \neq 0, \text{ όπου } 0 \neq P(t) = \sum_{k=0}^{m} a_k t^k \right\}$$

Το στοιχείο a_n καλείται ο **συντελεστής του μεγιστοβάθμιου όρου** ή **οδηγών συντελεστής** του $P(t)$. Αν ο οδηγών συντελεστής του πολυωνύμου $P(t)$ είναι το 1, το πολυώνυμο $P(t)$ καλείται **μονικό**. Στο μηδενικό πολυώνυμο δεν αποδίδουμε βαθμό.[1] Ένα πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k$ καλείται **σταθερό πολυώνυμο**, αν

[1] Στην βιβλιογραφία συχνά στο μηδενικό πολυώνυμο 0 αποδίδεται ως βαθμός το σύμβολο $\deg 0 = -\infty$, με την σύμβαση ότι: $n > -\infty$, $\forall n \in \mathbb{Z}$, και συμφωνώντας ότι: $(-\infty) + (-\infty) = -\infty = n + (-\infty)$, $\forall n \in \mathbb{Z}$.

$a_k = 0$, $\forall k \geq 1$, δηλαδή $P(t) = a_0 = a_0 1$. Ένα μη μηδενικό πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k$ έχει βαθμό $\deg P(t) = 0$, αν $a_0 \neq 0$ και $a_k = 0$, $\forall k \geq 1$. Δηλαδή το $P(t)$ είναι ένα μη μηδενικό σταθερό πολυώνυμο. Αντίστροφα κάθε μη-μηδενικό σταθερό πολυώνυμο έχει βαθμό ίσο με μηδέν. Συνήθως θα γράφουμε $\deg P(t) \leq n$, όπου $n \geq 0$, εννοώντας ότι είτε το πολυώνυμο $P(t)$ είναι το μηδενικό πολυώνυμο ή ότι το $P(t)$ είναι ένα μη μηδενικό πολυώνυμο με βαθμό το πολύ n. Αν $r \in R$, τότε συχνά, προς αποφυγή σύγχυσης, θα συμβολίζουμε το σταθερό πολυώνυμο r, δηλαδή το πολυώνυμο $r1$, με r.

Προφανώς η απεικόνιση

$$f\colon R \longrightarrow R[t], \quad f(a) = \mathsf{a} = a1 \quad \text{ή γενικότερα η απεικόνιση} \quad f\colon R \longrightarrow R[t_1, t_2, \cdots, t_n], \quad f(a) = \mathsf{a} = a1$$

είναι ένας μονομορφισμός δακτυλίων με εικόνα $\mathsf{Im}(f)$ το σύνολο των σταθερών πολυωνύμων υπεράνω του R.

Από τώρα και στο εξής θα ταυτίζουμε τα στοιχεία του R με τα σταθερά πολυώνυμα του δακτυλίου $R[t_1, t_2, \cdots, t_n]$, $\forall r \geq 1$, μέσω του παραπάνω μονομορφισμού δακτυλίων.

Λήμμα 9.1.1. *Έστω $P(t), Q(t) \in R[t]$ δύο μη μηδενικά πολυώνυμα. Τότε:*

1. $\deg\big(P(t) + Q(t)\big) \leq \max\big\{\deg P(t), \deg Q(t)\big\}$, *και η ισότητα ισχύει, εκτός αν* $\deg P(t) = \deg Q(t)$.
2. *Αν ο μεγιστοβάθμιος συντελεστής είτε του $P(t)$ είτε του $Q(t)$ δεν είναι διαιρέτης του μηδενός του R, τότε:* $\deg\big(P(t)Q(t)\big) = \deg P(t) + \deg Q(t)$.

Απόδειξη. Έστω $\deg P(t) = n$ και $\deg Q(t) = m$, όπου $P(t) = \sum_{k=0}^{n} a_k t^k$ και $Q(t) = \sum_{l=0}^{m} b_l t^l$, οπότε $a_n \neq 0 \neq b_m$.

1. Υποθέτουμε πρώτα ότι $n < m$. Τότε

$$P(t) + Q(t) = \sum_{k=0}^{m} (a_k + b_k) t^k, \quad a_l = 0 \quad \text{αν} \quad n+1 \leq l \leq m$$

Έτσι ο συντελεστής του μεγιστοβάθμιου όρου του πολυωνύμου $P(t) + Q(t)$ είναι ο $b_m \neq 0$ και άρα $\deg\big(P(t) + Q(t)\big) = m = \deg Q(t) = \max\big\{\deg P(t), \deg Q(t)\big\}$.

Ακριβώς ανάλογα, αν $m < n$, ο συντελεστής του μεγιστοβάθμιου όρου του πολυωνύμου $P(t)+Q(t)$ είναι ο $a_n \neq 0$ και άρα $\deg\big(P(t) + Q(t)\big) = n = \deg P(t) = \max\big\{\deg P(t), \deg Q(t)\big\}$.

Τέλος, αν $n = m$, τότε, επειδή ενδέχεται ο συντελεστής $a_n + b_m$ του $P(t)+Q(t)$ να είναι μηδέν, θα έχουμε προφανώς $\deg\big(P(t) + Q(t)\big) \leq n = \max\big\{\deg P(t), \deg Q(t)\big\}$, ή μπορεί $P(t) + Q(t) = 0$, οπότε $\deg\big(P(t) + Q(t)\big) = \deg 0 = -\infty < \max\big\{\deg P(t), \deg Q(t)\big\}$.

2. Θα έχουμε:

$$P(t)Q(t) = \sum_{k=0}^{n+m} c_k t^k, \quad \text{όπου:} \quad c_0 = a_0 b_0, \;\; c_1 = a_0 b_1 + a_1 b_0, \;\; \cdots, \;\; c_{n+m} = a_n b_m$$

Τότε $c_{n+m} = a_n b_m \neq 0$. Διαφορετικά, αν $a_n b_m = 0$, τότε, επειδή το στοιχείο a_n ή το στοιχείο b_m δεν είναι διαιρέτης του μηδενός, θα έχουμε άτοπο. Άρα $c_{n+m} \neq 0$, το οποίο σημαίνει ότι $\deg\big(P(t)Q(t)\big) = n + m = \deg P(t) + \deg Q(t)$. ■

Ως άμεση συνέπεια των ιδιοτήτων βαθμού πολυωνύμων υπεράνω ακέραιων περιοχών έχουμε το ακόλουθο σημαντικό αποτέλεσμα.

Πρόταση 9.1.2. *Έστω R ακέραια περιοχή, και $n \geq 1$ ένας θετικός ακέραιος.*

1. *Ο δακτύλιος πολυώνυμων $R[t_1, t_2, \cdots, t_n]$ είναι ακέραια περιοχή.*
2. $\mathsf{U}\big(R[t_1, t_2, \cdots, t_n]\big) = \mathsf{U}(R)$.

Απόδειξη. 1. Υποθέτουμε ότι $P(t)Q(t)=0$ στον πολυωνυμικό δακτύλιο $R[t]$, και θα δείξουμε ότι είτε $P(t)=0$ είτε $Q(t)=0$. Αν $P(t)=0$ ή $Q(t)=0$, τότε δεν έχουμε τίποτα να αποδείξουμε. Έτσι υποθέτουμε ότι $P(t)\neq 0\neq Q(t)$. Τότε σύμφωνα με το Λήμμα 9.1.1, έπεται ότι $\deg\{P(t)Q(t)\}=\deg P(t)+\deg Q(t)\geq 0$ και ιδιαίτερα το πολυώνυμο $P(t)Q(t)$ δεν μπορεί να είναι το μηδενικό πολυώνυμο, το οποίο είναι άτοπο. Άρα είτε $P(t)=0$ είτε $Q(t)=0$, και επομένως ο μεταθετικός δακτύλιος $R[t]$ είναι ακέραια περιοχή.

Αν $n\geq 1$, επειδή ο R είναι ακέραια περιοχή, όπως παραπάνω θα έχουμε ότι ο $R[t_1]$ είναι ακέραια περιοχή. Παρόμοια, ο δακτύλιος $R[t_1,t_2]=(R[t_1])[t_2]$ είναι ακέραια περιοχή, και επαγωγικά προκύπτει άμεσα ότι ο δακτύλιος $R[t_1,t_2,\cdots,t_n]$ είναι ακέραια περιοχή.

2. Προφανώς, αν $a\in\mathsf{U}(R)$ είναι ένα αντιστρέψιμο στοιχείο του R, τότε το σταθερό πολυώνυμο $P(t)=a$ είναι αντιστρέψιμο στοιχείο του πολυωνυμικού δακτυλίου $R[t]$. Αντίστροφα, αν $P(t)\in\mathsf{U}(R[t])$, τότε υπάρχει πολυώνυμο $Q(t)$ έτσι ώστε $P(t)Q(t)=1$. Τότε θα έχουμε: $0=\deg 1=\deg\big(P(t)Q(t)\big)=\deg P(t)+\deg Q(t)$. Αυτό σημαίνει ότι $\deg P(t)=0=Q(t)$ και άρα τα $P(t)=a$ και $Q(t)=b$ είναι σταθερά πολυώνυμα, το οποίο προφανώς δεν είναι τα μηδενικά, διότι έχουμε $P(t)Q(t)=ab1=1_R1$. Τότε όμως στον δακτύλιο R θα έχουμε $ab=1_R$ και επομένως $P(t)=a$, όπου $a\in\mathsf{U}(R)$. Επομένως μέσω του μονομορφισμού $R\longrightarrow R[t]$, $a\longmapsto a1$, μπορούμε να ταυτίσουμε $\mathsf{U}(R)=\mathsf{U}(R[t])$.

Αν $n\geq 1$, τότε θα έχουμε $\mathsf{U}(R)=\mathsf{U}(R[t_1])$. Παρόμοια $\mathsf{U}(R[t_1,t_2])=\mathsf{U}(R[t_1])=\mathsf{U}(R)$. Επαγωγικά προκύπτει άμεσα ότι $\mathsf{U}(R[t_1,t_2,\cdots,t_n])=\mathsf{U}(R[t_1,t_2,\cdots,t_{n-1}])=\cdots=\mathsf{U}(R[t_1,t_2])=\mathsf{U}(R[t_1])=\mathsf{U}(R)$. ■

9.1.2 Η Ευκλείδεια Διαίρεση Πολυωνύμων

Έστω όπως και πριν R ένας μεταθετικός δακτύλιος και $R[t]$ ο δακτύλιος πολυωνύμων μιας μεταβλητής υπεράνω του R. Στην παρούσα υποενότητα, θα υπενθυμίσουμε βασικές ιδιότητες διαιρετότητας πολυωνύμων, εστιάζοντας περισσότερο στην Ευκλείδεια διαίρεση.

Έστω $P(t),Q(t)\in R[t]$ δύο πολυώνυμα. Θα λέμε ότι το $P(t)$ **διαιρεί** το $Q(t)$, ή ότι το $Q(t)$ είναι *πολλαπλάσιο* του $P(t)$, και θα γράφουμε $P(t)\,|\,Q(t)$ αν υπάρχει πολυώνυμο $A(t)\in R[t]$ έτσι ώστε: $Q(t)=P(t)A(t)$. Η ακόλουθη βοηθητική πρόταση περιγράφει βασικές ιδιότητες διαιρετότητας πολυωνύμων.

Λήμμα 9.1.3. *Έστω $P(t),Q(t),S(t),R(t)\in R[t]$. Τότε:*

1. *$P(t)\,|\,P(t)$ και $P(t)\,|\,0$. Αντίστροφα: $0\,|\,P(t)$ αν και μόνο αν $P(t)=0$.*
2. *Αν $P(t)\,|\,Q(t)$ και $Q(t)\,|\,R(t)$, τότε: $P(t)\,|\,R(t)$.*
3. *Αν $P(t)\,|\,Q(t)$ και $P(t)\,|\,R(t)$, τότε: $P(t)\,|\,(Q(t)+R(t))$.*
4. *Αν $P(t)\,|\,S(t)$ και $Q(t)\,|\,R(t)$, τότε: $P(t)Q(t)\,|\,S(t)R(t)$.*
5. *Αν $P(t)\,|\,Q(t)$ και $Q(t)\neq 0$, και αν ο συντελεστής του μεγιστοβάθμιου όρου του $P(t)$ ή του $Q(t)$ δεν είναι διαιρέτης του μηδενός στον δακτύλιο R, τότε:*
   (α΄) $\deg P(t)\leq\deg Q(t)$.
   (β΄) *$P(t)\,|\,Q(t)$ και $Q(t)\,|\,P(t)$ αν και μόνο αν υπάρχει $r\in\mathsf{U}(R)$: $P(t)=rQ(t)$ και $Q(t)=r^{-1}P(t)$.*

Απόδειξη. 1. $P(t)\,|\,P(t)$ διότι $P(t)=1P(t)$, και $P(t)\,|\,0$ διότι $0=0P(t)$. Αν $0\,|\,P(t)$, τότε για κάποιο πολυώνυμο $R(t)$ θα έχουμε $P(t)=0R(t)=0$. Αντίστροφα, αν $P(t)=0$, τότε προφανώς $0\,|\,P(t)$.

2. Επειδή $P(t)\,|\,Q(t)$, θα έχουμε $Q(t)=P(t)A(t)$ και επειδή $Q(t)\,|\,R(t)$, τότε $R(t)\,|\,Q(t)B(t)$, όπου $A(t),B(t)\in R[t]$. Τότε:

$$R(t)=Q(t)B(t)=(P(t)A(t))B(t)\quad\Longrightarrow\quad P(t)\,|\,R(t)$$

3. Αν $P(t)\,|\,Q(t)$ και $P(t)\,|\,R(t)$, τότε θα έχουμε $Q(t)=A(t)P(t)$ και $R(t)=B(t)P(t)$, για κάποια $A(t),B(t)\in R[t]$. Τότε

$$Q(t)+R(t)=A(t)P(t)+B(t)P(t)=(A(t)+B(t))P(t)\quad\Longrightarrow\quad P(t)\,|\,(Q(t)+R(t))$$

4. Αν $P(t) \mid S(t)$ και $Q(t) \mid R(t)$, τότε θα έχουμε $S(t) = A(t)P(t)$ και $R(t) = B(t)Q(t)$, για κάποια $A(t), B(t) \in R[t]$. Τότε:

$$S(t)R(t) = A(t)P(t)B(t)Q(t) = A(t)B(t)P(t)Q(t) \quad \Longrightarrow \quad P(t)Q(t) \mid R(t)S(t)$$

5. (α') Αν $P(t) \mid Q(t)$, τότε $Q(t) = P(t)A(t)$, για κάποιο $A(t) \in R[t]$. Προφανώς τα πολυώνυμα $P(t)$ και $A(t)$ δεν είναι τα μηδενικά πολυώνυμα και άρα από το Λήμμα 9.1.1 θα έχουμε $\deg Q(t) = \deg\big(P(t)A(t)\big) = \deg P(t) + \deg A(t)$. Επομένως $\deg P(t) \leq \deg Q(t)$.

   (β') Υποθέτουμε ότι $P(t) \mid Q(t)$ και $Q(t) \mid P(t)$. Τότε από το μέρος (a) θα έχουμε $\deg P(t) \leq \deg Q(t)$ και $\deg Q(t) \leq \deg P(t)$, οπότε $\deg P(t) = \deg Q(t)$. Επιπλέον θα έχουμε $Q(t) = A(t)P(t)$, και επομένως $\deg Q(t) = \deg\big(A(t)P(t)\big) = \deg A(t) + \deg P(t) = \deg A(t) + \deg Q(t)$, από όπου $\deg A(t) = 0$, δηλαδή $A(t)$ είναι ένα σταθερό πολυώνυμο $A(t) = r$, όπου $r \in R$ και $r \neq 0$, διότι $Q(t) \neq 0$. Παρόμοια θα έχουμε $P(t) = B(t)Q(t)$, και επομένως $\deg P(t) = \deg\big(B(t)Q(t)\big) = \deg B(t) + \deg Q(t) = \deg B(t) + \deg P(t)$, από όπου $\deg B(t) = 0$, δηλαδή $B(t)$ είναι ένα σταθερό πολυώνυμο $B(t) = s$, όπου $s \in R$ και $s \neq 0$, διότι $P(t) \neq 0$. Έτσι θα έχουμε $Q(t) = rP(t)$ και $P(t) = sQ(t)$, και επομένως:

$$P(t) = srP(t) \quad \text{και} \quad Q(t) = rsQ(t)$$

   Έστω $P(t) = \sum_{k=1}^{n} a_k t^k$. Τότε $rsP(t) = \sum_{k=1}^{n} (rsa_k)t^k$, από όπου η ισότητα πολυωνύμων δίνει:

$$a_0 = a_0 sr, \quad a_1 = a_1 sr, \quad a_2 = a_2 sr, \quad \cdots, \quad a_n = a_n sr$$

   Η τελευταία σχέση δίνει $a_n(1_R - sr) = 0$. Επειδή ο μεγιστοβάθμιος όρος a_n του $P(t)$ δεν είναι διαιρέτης του μηδενός, έπεται ότι $1_R - sr = 0$, δηλαδή $sr = 1_R$, και επειδή ο δακτύλιος R είναι μεταθετικός, έπεται ότι το στοιχείο r είναι αντιστρέψιμο με αντίστροφο το στοιχείο s. Επομένως $Q(t) = rP(t)$ και $P(t) = r^{-1}Q(t)$.

■

Μπορούμε να αποδείξουμε τώρα το ακόλουθο σημαντικό αποτέλεσμα το οποίο περιγράφει την Ευκλείδεια διαίρεση πολυωνύμων.

Θεώρημα 9.1.4 (Ευκλείδεια Διαίρεση (Ι)). *Έστω $P(t), Q(t) \in R[t]$, όπου $Q(t) \neq 0$, και υποθέτουμε ότι $\deg Q(t) = m$. Αν b_m είναι ο συντελεστής του μεγιστοβάθμιου όρου του $Q(t)$, τότε υπάρχει θετικός ακέραιος $k \in \mathbb{N}$ και πολυώνυμα $S(t), R(t) \in R[t]$ έτσι ώστε:*

$$b_m^k P(t) = S(t)Q(t) + R(t), \quad \textit{και} \quad \textit{είτε} \quad R(t) = 0 \quad \textit{είτε} \quad \deg R(t) < \deg Q(t)$$

Απόδειξη. Αν $P(t) = 0$, τότε μπορούμε να θέσουμε $S(t) = 0 = R(t)$. Αν $P(t) \neq 0$, και $\deg P(t) < \deg Q(t)$, τότε μπορούμε να θέσουμε $S(t) = 0$ και $R(t) = P(t)$.

Έστω $P(t) = \sum_{k=0}^{n} a_k t^k$ και $Q(t) = \sum_{k=0}^{m} b_k t^k$.

Υποθέτουμε ότι: $\deg P(t) \geq \deg Q(t) = m$, και έστω $\deg P(t) = n$. Θα δείξουμε την ζητούμενη σχέση με χρήση της Αρχής Μαθηματικής Επαγωγής στον βαθμό $n \geq 0$ του $P(t)$. Αν $n = 0$, τότε $m = 0$, και τα πολυώνυμα $P(t) = r$ και $Q(t) = s$ είναι σταθερά μη μηδενικά πολυώνυμα, όπου $r, s \in R \setminus \{0\}$. Τότε $b_0 = s$, θέτοντας $k = 1$, $S(t) = r$ και $R(t) = 0$, έχουμε ότι η ζητούμενη σχέση, η οποία τώρα είναι της μορφής $sr = rs$, είναι αληθής.

Υποθέτουμε ότι η ζητούμενη σχέση ισχύει για όλα τα πολυώνυμα $P_1(t)$ με βαθμό $\deg P_1(t) < \deg P(t) = n$. Θεωρούμε το πολυώνυμο

$$P_1(t) = b_m P(t) - a_n t^{n-m} Q(t)$$

Ο συντελεστής του όρου t^n των πολυωνύμων $b_m P(t)$ και $a_n t^{n-m} Q(t)$ είναι προφανώς $a_n b_m$, από όπου έπεται άμεσα ότι $\deg P_1(t) < P(t)$. Από την Επαγωγική Υπόθεση, έπεται ότι υπάρχει $k-1 \in \mathbb{N}$ και πολυώνυμα $S_1(t), R(t) \in R[t]$ έτσι ώστε:

$$b_m^{k-1} P_1(t) = S_1(t)Q(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg Q(t)$$

Τότε θα έχουμε:

$$b_m^{k-1}\big(b_m P(t) - a_n t^{n-m} Q(t)\big) = S_1(t)Q(t) + R(t) \quad \Longrightarrow \quad b_m^k P(t) = \big(b_m^{k-1} a_n t^{n-m} + S_1(t)\big)Q(t) + R(t)$$

Θέτοντας $S(t) = b_m^{k-1} a_n t^{n-m} + S_1(t)$, επειδή είτε $R(t) = 0$ είτε $\deg R(t) < \deg Q(t)$ θα έχουμε τη ζητούμενη σχέση. ■

Θα δούμε κάποιες ενδιαφέρουσες περιπτώσεις του Θεωρήματος 9.1.4.

Πρόταση 9.1.5 (Ευκλείδεια Διαίρεση (II)). *Αν ο δακτύλιος R είναι σώμα, τότε για τυχόντα πολυώνυμα $P(t), Q(t) \in R[t]$, όπου $Q(t) \neq 0$, υπάρχουν μοναδικά πολυώνυμα $S(t), R(t) \in R[t]$ έτσι ώστε:*

$$P(t) = S(t)Q(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg Q(t)$$

Απόδειξη. Από το Θεώρημα 9.1.4, έπεται ότι υπάρχει θετικός ακέραιος $k \in \mathbb{N}$ και πολυώνυμα $S_1(t), R_1(t) \in R[t]$ έτσι ώστε:

$$b_m^k P(t) = S(t)Q(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg Q(t)$$

όπου b_m είναι ο συντελεστής του μεγιστοβάθμιου όρου του $Q(t)$, και $\deg Q(t) = m$. Επειδή ο δακτύλιος R είναι σώμα, το στοιχείο b^m, άρα και το στοιχείο b_m^k είναι αντιστρέψιμο, και τότε θέτοντας: $S(t) = b_m^{-k} S_1(t)$ και $R(t) = b_m^{-k} R_1(t)$, και τότε προφανώς θα έχουμε ότι είτε $R_1 = R_t = 0$ είτε $\deg R_1(t) = \deg R(t) < \deg Q(t)$. Συνοψίζοντας, θα έχουμε:

$$P(t) = S(t)Q(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg Q(t)$$

Υποθέτουμε ότι υπάρχουν πολυώνυμα $A(t), B(t) \in R[t]$, έτσι ώστε:

$$P(t) = A(t)Q(t) + B(t), \quad \text{και} \quad \text{είτε} \quad B(t) = 0 \quad \text{είτε} \quad \deg B(t) < \deg Q(t)$$

Τότε οι δύο τελευταίες σχέσεις δίνουν

$$\big(S(t) - A(t)\big)Q(t) = B(t) - R(t)$$

Αν τα πολυώνυμα $B(t)$ και $R(t)$ είναι το μηδενικό πολυώνυμο ή αν $B(t) = R(t)$, τότε, επειδή το $Q(t) \neq 0$ και επειδή ο δακτύλιος $R[t]$ είναι ακέραια περιοχή, θα έχουμε $S(t) = A(t)$. Έστω ότι ένα εκ των $R(t)$ και $B(t)$ δεν είναι το μηδενικό πολυώνυμο, και η διαφορά $B(t) - R(t)$ δεν είναι το μηδενικό πολυώνυμο. Αν το πολυώνυμο $S(t) - A(t)$ δεν είναι το μηδενικό, τότε ο βαθμός $m := \deg\big((S(t) - A(t))Q(t)\big)$ του γινομένου $\big(S(t) - A(t)\big)Q(t)$ είναι $\geq m$, και από την άλλη πλευρά ο βαθμός $\deg\big(B(t) - R(t)\big)$ της διαφοράς $B(t) - R(t)$ είναι $< m$, διότι $\deg B(t) < m$ και $R(t) < m$. Αυτή η αντίφαση συνεπάγεται ότι $S(t) = A(t)$ και επομένως $R(t) = B(t)$. ■

Υπενθυμίζουμε ότι για κάθε μεταθετικό δακτύλιο R, και στοιχείο $r \in R$, υπάρχει μοναδικός ομομορφισμός δακτυλίων $\mathsf{e}_r : R[t] \longrightarrow R$, έτσι ώστε $\mathsf{e}_r(t) = r$ και $\mathsf{e}_r(s) = s$, $\forall s \in R$, όπου το $s \in R$ θεωρείται ως σταθερό πολυώνυμο. Προφανώς θα έχουμε $\mathsf{e}_r(P(t)) = P(r)$.

Όταν σε μια σχέση μεταξύ πολυωνύμων του $R[t]$ αναφέρουμε ότι

«αντικαθιστούμε τη μεταβλητή t με το στοιχείο $\rho \in R$»

εννοούμε ότι εφαρμόζουμε στην εν λόγω σχέση τον ομομορφισμό εκτίμησης e_ρ και έτσι προκύπτει η ανάλογη σχέση μεταξύ στοιχείων του R. Ιδιαίτερα η σχέση $P(\rho) = 0$ σημαίνει ότι, αν $P(t) = \sum_{k=0}^n a_k t^k$, τότε το στοιχείο $P(\rho) = \sum_{k=0}^n a_k \rho^k$ του δακτυλίου R είναι το μηδενικό.

Πόρισμα 9.1.6. *Έστω $P(t) \in R[t]$ ένα πολυώνυμο και $r \in R$. Τότε υπάρχει μοναδικό πολυώνυμο $S(t) \in R[t]$ έτσι ώστε:*

$$P(t) = (t - r)S(t) + P(r)$$

Απόδειξη. Εφαρμόζουμε το Θεώρημα 9.1.4, θέτοντας $Q(t) = t - r$, το οποίο είναι μη μηδενικό με μεγιστοβάθμιο όρο τη μονάδα του R, και θα έχουμε:

$$P(t) = (t-r)S(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg(t-r) = 1$$

Άρα το πολυώνυμο $R(t)$ είναι σταθερό. Αν $R(t) \neq 0$, τότε, αντικαθιστώντας στην παραπάνω σχέση το πολυώνυμο t με το στοιχείο r, δηλαδή εφαρμόζοντας στην παραπάνω σχέση τον ομομορφισμό εκτίμησης $\mathsf{e}_r : R[t] \longrightarrow R$, $A(t) \longmapsto A(r)$, θα έχουμε: $P(r) = (r-r)S(r) + R(r) = R(r)$, από όπου προκύπτει η ζητούμενη σχέση. Το πολυώνυμο $S(t)$ είναι μοναδικό διότι, αν είχαμε επίσης $P(t) = (t-r)A(t) + P(r)$, τότε θα προέκυπτε ότι $(t-r)(S(t) - A(t)) = 0$. Αν $S(t) - A(t) \neq 0$, τότε ο βαθμός του πολυωνύμου $(t-r)(S(t) - A(t))$ θα ήταν προφανώς ≥ 1 και αυτό είναι άτοπο. Άρα $S(t) = A(t)$. ■

Πόρισμα 9.1.7. *Έστω $P(t) \in R[t]$ και $r \in R$. Τότε:*

$$(t-r) \mid P(t) \iff P(r) = 0$$

Απόδειξη. Αν $(t-r) \mid P(t)$, τότε υπάρχει πολυώνυμο $S(t) \in R[t]$, έτσι ώστε: $P(t) = (t-r)S(t)$, και τότε αντικαθιστώντας το πολυώνυμο t με το στοιχείο $r \in R$, θα έχουμε: $P(r) = (r-r)S(r) = 0$. Αντίστροφα, αν $P(r) = 0$, τότε από το Πόρισμα 9.1.6 έπεται ότι $P(t) = (t-r)S(t)$ για κάποιο πολυώνυμο $S(t) \in R[t]$. Επομένως $(t-r) \mid P(t)$. ■

Ένα στοιχείο $a \in \mathbb{R}$, όπου R είναι ένας μεταθετικός δακτύλιος, καλείται **ρίζα** του πολυωνύμου $P(t) \in R[t]$, αν $P(a) = 0$. Από το Πόρισμα 9.1.7, έπεται ότι αν το στοιχείο $a \in R$ είναι ρίζα του $P(t) \in R[t]$, τότε μπορούμε να γράψουμε $P(t) = (t-a)A(t)$, για κάποιο πολυώνυμο $A(t) \in R[t]$, και επομένως το πολυώνυμο $P(t)$ απλοποιείται ως προς την παραγοντοποίηση πολυωνύμων στον δακτύλιο $R[t]$. Ποια είναι, στο πλαίσιο της παραγοντοποίησης πολυωνύμων, τα πολυώνυμα με την «απλούστερη» δυνατή μορφή; Η απάντηση βρίσκεται στην έννοια του ανάγωγου πολυωνύμου.

Ανάγωγα Πολυώνυμα

Υπενθυμίζουμε ότι ένας θετικός ακέραιος $p \in \mathbb{Z}$ καλείται *πρώτος* αν $p \neq 1$ και αν $p = nm$, όπου $n, m \in \mathbb{N}$, τότε είτε $n = 1$ (και άρα $m = p$) είτε $n = p$ (και άρα $m = 1$). Η ανάλογη έννοια στο πλαίσιο του δακτυλίου πολυωνύμων μιας μεταβλητής με στοιχεία από ένα σώμα είναι η εξής:

Ορισμός 9.1.8. *Ένα πολυώνυμο $P(t) \in \mathbb{K}[t]$, όπου $\mathbb{K}$ είναι ένα σώμα, καλείται* **ανάγωγο**, *αν το πολυώνυμο $P(t)$ είναι θετικού βαθμού και δεν μπορεί να γραφεί ως γινόμενο $P(t) = A(t)B(t)$, πολυωνύμων $A(t), B(t) \in \mathbb{K}[t]$ θετικού βαθμού.*

Το αν ένα πολυώνυμο είναι ανάγωγο ή όχι εξαρτάται από το σώμα επί του οποίου είναι ορισμένο, δηλαδή στο σώμα στο οποίο ανήκουν οι συντελεστές του. Για παράδειγμα, το πολυώνυμο $P(t) = t^2 + 1$ μπορεί να θεωρηθεί ως πολυώνυμο υπεράνω του $\mathbb{R}$ και ως πολυώνυμο υπεράνω του $\mathbb{C}$. Το $P(t)$ είναι ανάγωγο υπεράνω του $\mathbb{R}$ (διότι δεν μπορεί να γραφεί ως γινόμενο δύο πολυωνύμων θετικού βαθμού με πραγματικούς συντελεστές) αλλά δεν είναι ανάγωγο υπεράνω του $\mathbb{C}$ (διότι $P(t) = (t-i)(t+i)$).

Η επόμενη Παρατήρηση συνοψίζει κάποιες στοιχειώδεις ιδιότητες ανάγωγων πολυωνύμων υπεράνω ενός σώματος.

Παρατήρηση 9.1.9. Έστω $\mathbb{K}$ ένα σώμα, και $P(t) \in \mathbb{K}[t]$.

1. Αν $\deg P(t) = n \geq 1$, τότε το $P(t)$ είναι ανάγωγο αν και μόνο αν ο βαθμός κάθε διαιρέτη του $P(t)$ στον δακτύλιο $\mathbb{K}[t]$ είναι 0 ή n.

2. Αν $\deg P(t) = 1$, τότε το $P(t)$ είναι ανάγωγο υπεράνω του $\mathbb{K}$ και έχει ρίζα στο $\mathbb{K}$.

3. Αν $\deg P(t) \geq 2$ και το $P(t)$ είναι ανάγωγο υπεράνω του $\mathbb{K}$, τότε το $P(t)$ δεν έχει ρίζα στο $\mathbb{K}$. Πράγματι, αν $\rho \in \mathbb{K}$ είναι μια ρίζα του $P(t)$, τότε από το Πόρισμα 9.1.7 θα είχαμε $P(t) = (t-\rho)A(t)$, για κάποιο πολυώνυμο $A(t) \in \mathbb{K}[t]$ και αναγκαστικά $\deg A(t) \geq 1$ (διότι $\deg P(t) \geq 2$), δηλαδή το $P(t)$ δεν είναι ανάγωγο και αυτό είναι άτοπο.

   Άρα ένα ανάγωγο πολυώνυμο υπεράνω ενός σώματος $\mathbb{K}$ βαθμού ≥ 2 δεν έχει καμία ρίζα στο $\mathbb{K}$.

   Το αντίστροφο δεν ισχύει: υπάρχουν μη ανάγωγα πολυώνυμα υπεράνω ενός σώματος τα οποία δεν έχουν καμία ρίζα στο σώμα. Για παράδειγμα, το πολυώνυμο $t^4+2t^2+1 = (t^2+1)(t^2+1) \in \mathbb{R}[t]$ έχει αυτή την ιδιότητα, και το ίδιο συμβαίνει για το πολυώνυμο $t^4-4 = (t^2-2)(t^2+2) \in \mathbb{Q}[t]$.

4. *Αν $\deg P(t) = 2$ ή 3, τότε το $P(t)$ είναι ανάγωγο υπεράνω του $\mathbb{K}$ αν και μόνο αν το $P(t)$ δεν έχει καμία ρίζα στο $\mathbb{K}$.*

   Πράγματι, υποθέτουμε ότι το $P(t)$ δεν έχει καμία ρίζα στο $\mathbb{K}$ και έστω $P(t) = A(t)B(t)$, όπου τα πολυώνυμα $A(t), B(t)$ είναι βαθμού ≥ 1. Τότε προφανώς είτε το $A(t)$ είτε το $B(t)$ είναι πρωτοβάθμιο, και επομένως έχει μια ρίζα στο $\mathbb{K}$, η οποία είναι και ρίζα του $P(t)$. Αυτό είναι άτοπο και επομένως το $P(t)$ είναι ανάγωγο. ▲

Θα μελετήσουμε αναλυτικότερα επιπρόσθετες ιδιότητες ανάγωγων πολυωνύμων στο Κεφάλαιο 11 στο πλαίσιο της θεωρίας διαιρετότητας σε περιοχές κυρίων ιδεωδών.

Πλήθος Ριζών Πολυωνύμων και Πρωταρχικές Ρίζες mod p

Θα χρησιμοποιήσουμε το Πόρισμα 9.1.7 για να αποδείξουμε ότι ένα πολυώνυμο θετικού βαθμού υπεράνω ενός σώματος $\mathbb{K}$ έχει το πολύ $\deg P(t)$ διακεκριμένες ρίζες στο σώμα $\mathbb{K}$.

Θεώρημα 9.1.10. *Έστω $\mathbb{K}$ ένα σώμα και $P(t) \in \mathbb{K}[t]$ ένα πολυώνυμο βαθμού $\deg P(t) = n \geq 1$. Τότε το $P(t)$ έχει το πολύ n ρίζες στο σώμα $\mathbb{K}$.*

Ιδιαίτερα αν ένα πολυώνυμο έχει πλήθος ριζών μεγαλύτερο από τον βαθμό του, τότε είναι το μηδενικό πολυώνυμο.

Απόδειξη. Αν $\deg P(t) = 1$, τότε το $P(t)$ είναι της μορφής $P(t) = a_0 + a_1 t$, όπου $a_0, a_1 \in \mathbb{K}$ και $a_1 \neq 0$. Τότε προφανώς το $P(t)$ έχει ακριβώς μια ρίζα στο $\mathbb{K}$ την $\rho = -\frac{a_0}{a_1}$.

Υποθέτουμε ότι κάθε πολυώνυμο υπεράνω του $\mathbb{K}$ βαθμού $n \geq 2$ έχει το πολύ n ρίζες στο $\mathbb{K}$, και έστω $P(t)$ ένα πολυώνυμο βαθμού $n+1$ υπεράνω του $\mathbb{K}$. Αν το $P(t)$ δεν έχει καμία ρίζα στο $\mathbb{K}$, τότε δεν έχουμε να αποδείξουμε τίποτα. Αν $\rho \in \mathbb{K}$ είναι μια ρίζα του $P(t)$ στο $\mathbb{K}$, τότε, σύμφωνα με το Πόρισμα 9.1.7, θα έχουμε $(t-\rho) \mid P(t)$ και άρα μπορούμε να γράψουμε

$$P(t) = (t-\rho)Q(t)$$

όπου $Q(t)$ είναι ένα πολυώνυμο υπεράνω του $\mathbb{K}$ και προφανώς $\deg Q(t) = n$. Από την επαγωγική υποθεση, έπεται ότι το πολυώνυμο $Q(t)$ έχει το πολύ n ρίζες στο $\mathbb{K}$. Αν a είναι μια ρίζα του $P(t)$, τότε $0 = P(a) = (a-\rho)Q(a)$ και επομένως, επειδή ο δακτύλιος $\mathbb{K}$ είναι σώμα, έπεται ότι είτε $a = \rho$ είτε $Q(a) = 0$ δηλαδή το a είναι ρίζα του $Q(t)$. Επειδή το πολυώνυμο $Q(t)$ έχει το πολύ n ρίζες στο $\mathbb{K}$, αυτό σημαίνει ότι το πολυώνυμο $P(t)$ έχει το πολύ $n+1$ ρίζες στο $\mathbb{K}$: την ρίζα ρ και τις k το πλήθος ρίζες του $Q(t)$, όπου $0 \leq k \leq n$. Από την Αρχή Μαθηματικής Επαγωγής έπεται τότε ότι κάθε πολυώνυμο βαθμού $n \geq 1$ έχει το πολύ n το πλήθος ρίζες στο σώμα $\mathbb{K}$.

Αν $P(t)$ είναι ένα πολυώνυμο το οποίο έχει περισσότερες ρίζες από τον βαθμό του, τότε σύμφωνα με την παραπάνω ανάλυση θα πρέπει $\deg P(t) = 0$, δηλαδή $P(t) = r$ είναι ένα σταθερό πολυώνυμο, όπου $r \in \mathbb{K}$. Αν $r \neq 0$, τότε το $P(t)$ δεν έχει καμία ρίζα στο $\mathbb{K}$ και αυτό είναι άτοπο διότι το πλήθος των ριζών του $P(t)$ είναι $> 0 = \deg P(t)$. Άρα αναγκαστικά $r = 0$, και αυτό σημαίνει ότι το πολυλωνυμο $P(t)$ είναι το μηδενικό πολυώνυμο. ■

Το ακόλουθο παράδειγμα δείχνει ότι το Θεώρημα 9.1.10 δεν ισχύει για πολυώνυμα υπεράνω (μεταθετικών) δακτυλίων οι οποίοι δεν είναι σώματα.

Παράδειγμα 9.1.11. Θεωρούμε τον μεταθετικό δακτύλιο $\mathbb{Z}_8$, ο οποίος δεν είναι σώμα ούτε ακέραια περιοχή. Θεωρούμε το πολυώνυμο $P(t) = t^2 - 1 \in \mathbb{Z}_8[t]$. Το πολυώνυμο $P(t)$ είναι βαθμού 2 υπεράνω του $\mathbb{Z}_8$, αλλά έχει 4 ρίζες στον δακτύλιο $\mathbb{Z}_8$, τις κλάσεις ισοτιμίας mod 8: $[1]_8$, $[-1]_8$, $[2]_8$, και $[-3]_8$. $\surd$

Παρατήρηση 9.1.12. Με χρήση του Θεωρήματος 9.1.10, είδαμε στο Θεώρημα 4.2.9 ότι κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος είναι κυκλική.

Αυτό το αποτέλεσμα δεν ισχύει αν ο δακτύλιος δεν είναι σώμα, αλλά είναι, για παράδειγμα, δακτύλιος διαίρεσης. Πράγματι η ομάδα $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ των τετρανίων του Hamilton είναι μια πεπερασμένη μη κυκλική ομάδα της πολλαπλασιαστικής ομάδας του δακτυλίου διαίρεσης των τετρανίων του Hamilton (η ομάδα Q τάξης 8 δεν είναι κυκλική διότι δεν διαθέτει στοιχείο τάξης 8). ▲

Ιδιαίτερα από το Θεώρημα 4.2.9 έπεται το ακόλουθο.

Θεώρημα 9.1.13. *Αν $\mathbb{K}$ είναι ένα πεπερασμένο σώμα, τότε η ομάδα $\mathsf{U}(\mathbb{K}) = \mathbb{K}^*$ είναι κυκλική.*

Υπενθυμίζουμε ότι μια κλάση ισοτιμίας $[k]_n \in \mathbb{Z}_n$ καλείται **πρωταρχική ρίζα** mod n αν η κλάση $[k]_n$ είναι γεννήτορας της ομάδας $\mathsf{U}(\mathbb{Z}_n)$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_n$. Επίσης υπενθυμίζουμε ότι το πλήθος των γεννητόρων σε μια κυκλική ομάδα τάξης n είναι ίσο με $\phi(n)$, όπου ϕ είναι η συνάρτηση του Euler.

Πόρισμα 9.1.14. *Αν p είναι ένας πρώτος αριθμός, τότε η πολλαπλασιαστική ομάδα $\mathsf{U}(\mathbb{Z}_p) = \mathbb{Z}_p^*$ είναι κυκλική. Επομένως υπάρχουν πρωταρχικές ρίζες* mod p*, και το πλήθος τους είναι ίσο με $\phi(p-1)$.*

Παράδειγμα 9.1.15. Θεωρούμε το σώμα $\mathbb{Z}_7$. Τότε η ομάδα $\mathsf{U}(\mathbb{Z}_7) = \mathbb{Z}_7^* = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$ είναι κυκλική με γεννήτορα την κλάση ισοτιμίας $[5]_7$.

Αντίθετα, η ομάδα $\mathsf{U}(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ των αντιστρέψιμων στοιχείων του δακτυλίου $\mathbb{Z}_8$ δεν είναι κυκλική, καθώς κάθε στοιχείο της, εκτός του ταυτοτικού, έχει τάξη 2. Προφανώς η ομάδα $\mathsf{U}(\mathbb{Z}_8)$ είναι ισόμορφη με την ομάδα $\mathcal{V}_4$ των τεσσάρων στοιχείων του Klein. ▲

9.2 Ιδεώδη του δακτυλίου $\mathbb{K}[t]$

Αν $\mathbb{K}$ είναι ένα σώμα, τότε η δομή των ιδεωδών του δακτυλίου πολυωνύμων $\mathbb{K}[t]$ είναι σχετικά απλή. Πράγματι το επόμενο Θεώρημα πιστοποιεί ότι κάθε ιδεώδες του $\mathbb{K}[t]$ είναι **κύριο**, δηλαδή παράγεται από ένα πολυώνυμο.

Θεώρημα 9.2.1. *Αν $\mathbb{K}$ είναι ένα σώμα, τότε κάθε ιδεώδες του δακτυλίου πολυωνύμων $\mathbb{K}[t]$ είναι κύριο.*

Απόδειξη. Έστω $I \subseteq \mathbb{K}[t]$ ένα ιδεώδες του $\mathbb{K}[t]$. Αν I είναι το μηδενικό ιδεώδες, τότε προφανώς το I είναι κύριο, καθώς παράγεται από το μηδενικό πολυώνυμο. Αν $I = \mathbb{K}[t]$, τότε το I είναι κύριο, καθώς παράγεται από την μονάδα του δακτυλίου $\mathbb{K}[t]$, δηλαδή το σταθερό πολυώνυμο 1.

Υποθέτουμε ότι το I είναι ένα μη μηδενικό και γνήσιο ιδεώδες του $\mathbb{K}[t]$. Τότε το I περιέχει πολυώνυμα βαθμού ≥ 1. Πράγματι, επειδή $I \neq \{0\}$, το I περιέχει ένα μη μηδενικό πολυώνυμο, και άρα περιέχει ένα πολυώνυμο βαθμού ≥ 0. Αν κάθε μη μηδενικό πολυώνυμο του I είναι βαθμού μηδέν, τότε το I περιέχει ένα σταθερό μη μηδενικό πολυώνυμο. Επειδή κάθε τέτοιο πολυώνυμο είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$, έπεται ότι το I περιέχει ένα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$ και άρα $I = \mathbb{K}[t]$. Αυτό είναι άτοπο διότι το I είναι γνήσιο.

Έστω $Q(t)$ το πολυώνυμο με τον μικρότερο βαθμό ≥ 1 το οποίο ανήκει στο I. Επειδή το I είναι ιδεώδες του $\mathbb{K}[t]$, θα έχουμε $(Q(t)) \subseteq I$. Έστω $P(t)$ ένα τυχόν μη μηδενικό πολυώνυμο το οποίο ανήκει στο I. Από την Ευκλείδεια διαίρεση, θα έχουμε ότι υπάρχουν πολυώνυμα $S(t), R(t) \in \mathbb{K}[t]$, έτσι ώστε:

$$P(t) = S(t)Q(t) + R(t), \quad \text{και:} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg Q(t)$$

Τότε θα έχουμε $R(t) = P(t) - S(t)Q(t) \in I$ διότι $P(t), Q(t) \in I$ και το I είναι ιδεώδες του $\mathbb{K}[t]$. Αν $R(t) \neq 0$, τότε το I περιέχει ένα μη μηδενικό ιδεώδες $R(t)$ με βαθμό $\deg R(t) < \deg Q(t)$. Αυτό είναι άτοπο διότι το $Q(t)$ επιλέχθηκε να είναι το πολυώνυμο με τον μικρότερο βαθμό το οποίο ανήκει στο I. Επομένως $R(t) = 0$ και τότε $P(t) = S(t)Q(t) \in I$. Αυτό σημαίνει ότι $I \subseteq (Q(t))$ και τελικά θα έχουμε $I = (Q(t))$, δηλαδή το I είναι κύριο και παράγεται από το $Q(t)$. ■

Παρατήρηση 9.2.2. Το αποτέλεσμα του Θεωρήματος 9.2.1 αφορά δακτυλίους πολυωνύμων $\mathbb{K}[t]$ μιας μεταβλητής με συντελεστές υπεράνω ενός σώματος $\mathbb{K}$ και δεν γενικεύεται σε δακτυλίους πολυωνύμων πολλών μεταβλητών $\mathbb{K}[t_1, t_2, \cdots, t_n]$, $n \geq 2$, ή σε δακτυλίους πολυωνύμων μιας μεταβλητής $R[t]$, όπου ο μεταθετικός δακτύλιος R δεν είναι σώμα:

1. Το ιδεώδες $I = (t_1, t_2) \subseteq \mathbb{K}[t_1, t_2]$ το οποίο παράγεται από τα πολυώνυμα t_1, t_2 δεν είναι κύριο.

   Πράγματι, έστω ότι το ιδεώδες I είναι κύριο και επομένως υπάρχει πολυώνυμο $P(t_1, t_2)$ έτσι ώστε $(P(t_1, t_2)) = I$. Τότε, επειδή $t_1, t_2 \in I$, υπάρχουν πολυώνυμα $A(t_1, t_2), B(t_1, t_2) \in \mathbb{K}[t_1, t_2]$ έτσι ώστε:

   $$t_1 = P(t_1, t_2)A(t_1, t_2) \qquad \text{και} \qquad t_2 = P(t_1, t_2)B(t_1, t_2)$$

   Από την πρώτη σχέση έπεται ότι ο βαθμός ως προς t_1 του πολυωνύμου $P(t_1, t_2)$, δηλαδή ο βαθμός του πολυωνύμου $P(t_1, t_2)$ θεωρούμενου ως πολυώνυμο του δακτυλίου $(\mathbb{K}[t_2])[t_1]$ με συντελεστές στον δακτύλιο πολυωνύμων $\mathbb{K}[t_2]$, είναι το πολύ ίσος με 1. Επομένως υπάρχουν πολυώνυμα $C(t_2), D(t_2) \in \mathbb{K}[t_2]$ έτσι ώστε:

   $$P(t_1, t_2) = C(t_2) + D(t_2)t_1$$

   Πρόμοια έπεται ότι ο βαθμός ως προς t_2 του πολυωνύμου $P(t_1, t_2)$, δηλαδή ο βαθμός του πολυωνύμου $P(t_1, t_2)$ θεωρούμενου ως πολυώνυμο του δακτυλίου $(\mathbb{K}[t_1])[t_2]$ με συντελεστές στον δακτύλιο πολυωνύμων $\mathbb{K}[t_1]$, είναι το πολύ ίσος με 1. Επομένως ο βαθμός των πολυωνύμων $C(t_2), D(t_2)$ είναι το πολύ ίσος με 1 και επομένως θα έχουμε $C(t_2) = a_{00} + a_{01}t_2$ και $D(t_2) = b_{00} + b_{01}t_2$, όπου $a_{00}, b_{00}, a_{01}, b_{01} \in \mathbb{K}$. Τότε:

   $$P(t_1, t_2) = C(t_2) + D(t_2)t_1 = a_{00} + a_{01}t_2 + (b_{00} + b_{01}t_2)t_1 = a_{00} + b_{00}t_1 + a_{01}t_2 + b_{01}t_1t_2$$

   Από τη σχέση $t_1 = \big(a_{00} + b_{00}t_1 + a_{01}t_2 + b_{01}t_1t_2\big)A(t_1, t_2)$ έπεται άμεσα ότι $b_{01} = 0$. Από την άλλη πλευρά, επειδή προφανώς το πολυώνυμο $b_{00}t_1 + a_{01}t_2 \in I = (t_1, t_2)$, θα έχουμε ότι $a_{00} = 0$. Άρα $t_1 = \big(b_{00}t_1 + a_{01}t_2\big)A(t_1, t_2)$, από όπου $a_{01} = 0$. Παρόμοια, από τη σχέση $t_2 = b_{00}t_1B(t_1, t_2)$, θα έχουμε $b_{00} = 0$. Έτσι $P(t_1, t_2) = 0$, το οποίο είναι άτοπο. Άρα το ιδεώδες $I = (t_1, t_2)$ δεν είναι κύριο.

2. Το ιδεώδες $I = (2, t) \subseteq \mathbb{Z}[t]$ το οποίο παράγεται από το σταθερό πολυώνυμο 2 και το πολυώνυμο t δεν είναι κύριο.

   Πράγματι, έστω ότι το ιδεώδες I είναι κύριο και επομένως θα έχουμε $I = (P(t))$, για ένα πολυώνυμο $P(t) = \sum_{k=0}^{n} d_k t^k$, όπου $d_k \in \mathbb{Z}$, $0 \leq k \leq n$. Προφανώς θα έχουμε:

   $$I = (2, t) = \big\{2A(t) + tB(t) \in \mathbb{Z}[t] \mid A(t), B(t) \in \mathbb{Z}[t]\big\}$$

   Αν $A(t) = \sum_{k=0}^{m} a_k t^k$ και $B(t) = \sum_{k=0}^{l} b_k t^k$, τότε ένα τυπικό στοιχείο του I θα είναι της μορφής $2A(t) + tB(t) = 2\sum_{k=0}^{m} a_k t^k + t\sum_{k=0}^{l} b_k t^k = 2a_0 + (2a_1 + b_0)t + \cdots$, και επομένως έπεται άμεσα ότι:

   $$I = \big\{C(t) \in \mathbb{Z}[t] \mid C(0): \text{ άρτιος}\big\}$$

   δηλαδή το I αποτελείται από όλα τα πολυώνυμα του $\mathbb{Z}[t]$ με άρτιο σταθερό όρο. Έτσι ο σταθερός όρος d_0 του $P(t)$ είναι άρτιος, δηλαδή $d_0 = 2d_0'$, όπου $d_0' \in \mathbb{Z}$. Επειδή $2, t \in I = (P(t))$, υπάρχουν πολυώνυμα $Q(t) = \sum_{k=0}^{r} c_k t^k$ και $R(t) = \sum_{k=0}^{s} e_k t^k$ του $\mathbb{Z}[t]$, έτσι ώστε:

   $$2 = P(t)A(t) \qquad \text{και} \qquad t = P(t)B(t)$$

   Από τις παραπάνω σχέσεις βλέπουμε άμεσα ότι:

   $$2 = d_0c_0 = 2d_0'c_0 \implies 1 = d_0'c_0 \qquad \text{και} \qquad 1 = d_0e_1 + d_1e_0 = 2d_0'e_1 + d_1e_0$$

Τότε $d_0' = \pm 1$ και $c_0 = \pm 1$. Επίσης έχουμε $0 = d_1c_0 + d_0c_1 = d_1c_0 + 2d_0'c_1$ και άρα $d_1c_0 = -2d_0'c_1$. Επειδή $c_0 = \pm 1$, έπεται ότι $2 \mid d_1$ και άρα $d_1 = 2d_1'$, για κάποιο $d_1' \in \mathbb{Z}$. Τότε θα έχουμε $1 = 2d_0'e_1 + d_1e_0 = 2d_0'e_1 + 2d_1'e_0 = 2(d_0'e_1 + d_1'e_0)$, το οποίο είναι άτοπο. Άρα το ιδεώδες I δεν είναι κύριο. ▲

Παρατήρηση 9.2.3. Έστω $I \subseteq \mathbb{K}[t]$ ένα μη-μηδενικό ιδεώδες του δακτυλίου $\mathbb{K}[t]$. Τότε $I = (P(t))$, για ένα μη μηδενικό πολυώνυμο $P(t) \in \mathbb{K}[t]$. Έστω $P(t) = \sum_{k=0}^{n} a_k t^k$, όπου $a_n \neq 0$ και άρα $\deg P(t) = n$. Αν $a_n \neq 1$, τότε το πολυώνυμο $Q(t) = a_n^{-1}P(t) = a_0a_n^{-1} + a_1a_n^{-1}t + a_2a_n^{-1}t^2 + \cdots a_{n-1}a_n^{-1}t^{n-1} + t^n$ προφανώς έχει την ιδιότητα $I = (Q(t))$ και ο γεννήτορας $Q(t)$ έχει ως συντελεστή του μεγιστοβάθμιου όρου το 1, δηλαδή το $Q(t)$ είναι μονικό πολυώνυμο. Αν $Q'(t) = b_0 + b_1t + b_2t^2 + \cdots + b_{m-1}t^{m-1} + t^m$ είναι ένα μονικό πολυώνυμο το οποίο είναι γεννήτορας του I, τότε $Q(t) = Q'(t)$. Πράγματι, χωρίς βλάβη της γενικότητας, έστω $n \leq m$. Θα έχουμε $Q(t) = A(t)Q'(t)$ και $Q'(t) = B(t)Q(t)$ για κάποια, προφανώς μη μηδενικά, πολυώνυμα $A(t), B(t) \in \mathbb{K}[t]$. Τότε θα έχουμε $n = \deg Q(t) = \deg A(t) + \deg Q'(t) = \deg A(t) + m$ και $m = \deg Q'(t) = \deg B(t) + \deg Q(t) = \deg B(t) + n$, από όπου έπεται ότι $\deg A(t) = 0 = \deg B(t)$ και $n = m$. Ιδιαίτερα θα έχουμε $A(t) = a$ και $B(t) = b$, όπου $a, b \in \mathbb{K} \setminus \{0\}$. Από τις παραπάνω σχέσεις τότε θα έχουμε $a = 1 = b$ και άρα $A(t) = B(t) = 1$, δηλαδή $Q(t) = Q'(t)$. ▲

Επομένως κάθε μη μηδενικό ιδεώδες I του $\mathbb{K}[t]$, $\mathbb{K}$ είναι σώμα, είναι της μορφής $I = (Q(t))$, για ένα μοναδικό μονικό πολυώνυμο $Q(t)$, το οποίο καλείται ο **μονικός γεννήτορας** του I.

Πότε ο δακτύλιος $R[u]$ είναι σώμα;

Θα χρησιμοποιήσουμε τη γνώση της δομής των ιδεωδών του $\mathbb{K}[t]$ για να απαντήσουμε στο παραπάνω ερώτημα όταν ο δακτύλιος R είναι ένα σώμα $\mathbb{K}$.

Έστω R ένας υποδακτύλιος ενός μεταθετικού δακτυλίου S, και έστω $u \in S$ ένα τυχόν στοιχείο του S. Τότε, αν $\iota\colon R \longrightarrow S$, $\iota(r) = r$, είναι η κανονική έγκλειση, γνωρίζουμε ότι υπάρχει μοναδικός ομομορφισμός δακτυλίων $\iota^*\colon R[t] \longrightarrow S$ έτσι ώστε: $\iota^*(\mathsf{r}) = \iota(r) = r$ και $\iota^*(t) = u$, όπου r είναι το σταθερό πολυώνυμο r. Υπενθυμίζουμε ότι

$$R[u] = \{r_0 + r_1u + r_2u^2 + \cdots + r_nu^n \in S \mid r_i \in R,\ 0 \leq i \leq n,\ n \in \mathbb{N}\}$$

είναι ο υποδακτύλιος του S ο οποίος παράγεται υπεράνω του R από το στοιχείο $u \in S$.

Η παρακάτω Πρόταση δίνει μια διαφορετική περιγραφή του δακτυλίου $R[u]$.

Πρόταση 9.2.4. *Με τους παραπάνω συμβολισμούς υπάρχει ένας ισομορφισμός δακτυλίων*

$$R[t]/\mathsf{Ker}(\iota^*) \ \cong\ R[u] \qquad \textit{και} \qquad \mathsf{Ker}(\iota^*) \cap R = \{0\}$$

Αντίστροφα, έστω ότι $I \subseteq R[t]$ είναι ένα ιδεώδες του δακτυλίου $R[t]$ έτσι ώστε $I \cap R = \{0\}$. Θέτοντας $S = R[t]/I$, η απεικόνιση $\phi\colon R \longrightarrow S = R[t]/I$, $\phi(r) = \mathsf{r} + I$, όπου r είναι το σταθερό πολυώνυμο r, είναι μονομορφισμός δακτυλίων, και άρα ο δακτύλιος $R \cong \phi(R) \subseteq S$ μπορεί να θεωρηθεί ως υποδακτύλιος του S. Επιπλέον έχουμε έναν ισομορφισμό δακτυλίων $R[t]/I \cong R[u]$, όπου $u = t + I$.

Απόδειξη. Ο ομομορφισμός δακτυλίων $\iota^*\colon R[t] \longrightarrow S$ έτσι ώστε: $\iota^*(\mathsf{r}) = \iota(r) = r$ και $\iota^*(t) = u$, όπου r είναι το σταθερό πολυώνυμο r, έχει την ιδιότητα

$$\iota^*\Big(\sum_{k=0}^{n} a_kt^k\Big) = \sum_{k=0}^{n} a_ku^k$$

από όπου αμέσως βλέπουμε ότι $\mathsf{Im}(\iota^*) = R[u]$. Τότε από το Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων, θα έχουμε έναν ισομορφισμό δακτυλίων $R[t]/\mathsf{Ker}(\iota^*) \cong R[u]$. Αν $P(t) = \sum_{k=0}^{n} a_kt^k \in \mathsf{Ker}(\iota^*) \cap R$, τότε το $P(t)$ είναι προφανώς το σταθερό πολυώνυμο $P(t) = a_0$, και τότε επειδή $P(t) \in \mathsf{Ker}(\iota^*)$, θα έχουμε $\iota^*(P(t)) = a_0 = 0$. Άρα $P(t) = 0$ και επομένως $\mathsf{Ker}(\iota^*) \cap R = \{0\}$.

Θεωρούμε την απεικόνιση

$$\phi\colon R \longrightarrow R[t]/I, \quad \phi(r) = \mathsf{r} + I$$

η οποία είναι ένας ομομορφισμός δακτυλίων ως σύνθεση της κανονικής έγκλεισης $R \longrightarrow R[t]$ και της κανονικής προβολής $R[t] \longrightarrow R[t]/I$. Αν $\phi(r) = 0_{R[t]/I}$, τότε $r + I = 0 + I$, από όπου έπεται ότι $r \in I$. Τότε $r \in \mathsf{Ker}(\iota^*) \cap R = \{0\}$, και αυτό σημαίνει ότι ο ομομορφισμός ϕ είναι μονομορφισμός. Έτσι ο δακτύλιος $R \cong \phi(R) \subseteq S$ μπορεί να θεωρηθεί ως υποδακτύλιος του $S = R[t]/I$, μέσω του μονομορφισμού ϕ. Αν ϕ^* ο μοναδικός μονομορφισμός δακτυλίων $\phi\colon R[t] \longrightarrow S$, έτσι ώστε $\phi^*(r) = \phi(r)$, $\forall r \in R$, και $\phi^*(t) = u$, όπου $u = t + I$, τότε προφανώς $\phi^* = \pi_I\colon R[t] \longrightarrow R[t]/I$, $\pi_I(P(t)) = P(t) + I$ είναι η κανονική προβολή. Προφανώς θα έχουμε

$$\phi^*\big(\sum_{k=0}^{n} a_k t^k\big) = \sum_{k=0}^{n} (a_k + I)(t + I)^k = \sum_{k=0}^{n} (a_k + I)(t^k + I) = \sum_{k=0}^{n} (a_k + I)u^k$$

και $\mathsf{Im}(\phi^*) = R[u]$, όπου ταυτίσαμε τον δακτύλιο R με τον υποδακτύλιο $\phi(R) \subseteq S$. Επομένως ο ομομορφισμός $\phi^*\colon R[t] \longrightarrow R[t]/I$ είναι επιμορφισμός δακτυλίων και $\mathsf{Ker}(\phi^*) = I$. Άρα θα έχουμε έναν ισομορφισμό δακτυλίων $R[t]/I \cong R[u]$. ■

Για την μελέτη δακτυλίων της μορφής $R[u]$ χρειαζόμαστε τον ακόλουθο ορισμό ο οποίος εισάγει σημαντικές ιδιότητες τις οποίες μπορεί να έχει το στοιχείο u υπεράνω του R.

Ορισμός 9.2.5. *Έστω R ένας υποδακτύλιος ενός μεταθετικού δακτυλίου S, και έστω $u \in S$ ένα τυχόν στοιχείο του S. Έστω $\iota^*\colon R[t] \longrightarrow S$ ο μοναδικός ομομορφισμός δακτυλίων έτσι ώστε: $\iota^*(r) = \iota(r) = r$ και $\iota^*(t) = u$, όπου r είναι το σταθερό πολυώνυμο r.*

1. *Το στοιχείο $u \in S$ καλείται* **αλγεβρικό υπεράνω του** *R αν: $\mathsf{Ker}(\iota^*) \neq \{0\}$.*
2. *Το στοιχείο $u \in S$ καλείται* **υπερβατικό υπεράνω του** *R αν: $\mathsf{Ker}(\iota^*) = \{0\}$.*

Επομένως το στοιχείο $u \in S$ είναι αλγεβρικό υπεράνω του R αν υπάρχει μη μηδενικό πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k \in R[t]$ με $\iota^*(P(t)) = 0$, δηλαδή: $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$, και τα στοιχεία $a_k \in R$, $0 \leq k \leq n$, δεν είναι όλα ταυτόχρονα μηδέν. Ανάλογα, το στοιχείο u είναι υπερβατικό υπεράνω του R, αν: $a_k \in R$, $0 \leq k \leq n$, και $a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^n = 0$, τότε: $a_k = 0$, $0 \leq k \leq n$.

Αν το στοιχείο $u \in S$ είναι αλγεβρικό υπεράνω του υποδακτυλίου $\mathbb{K} \subseteq S$ και ο υποδακτύλιος $\mathbb{K}$ είναι σώμα, τότε το μη μηδενικό ιδεώδες $\mathsf{Ker}(\iota^*) \subseteq \mathbb{K}[t]$ έχει έναν μονικό γεννήτορα $Q_u(t)$, ο οποίος καλείται το **ελάχιστο πολυώνυμο** του u υπεράνω του $\mathbb{K}$.

Σύμφωνα με την παραπάνω ανάλυση, το πολυώνυμο $Q_u(t)$ είναι το μονικό πολυώνυμο με τον μικρότερο βαθμό υπεράνω του $\mathbb{K}$ το οποίο έχει το στοιχείο u σαν ρίζα.

Παράδειγμα 9.2.6.

1. Έστω $\mathbb{K}$ ένα σώμα, το οποίο θεωρούμε ως υποδακτύλιο του δακτυλίου πολυωνύμων $\mathbb{K}[t]$, μέσω του κανονικού μονομορφισμού $\iota\colon \mathbb{K} \longrightarrow \mathbb{K}[t]$, $\iota(k) = k$, όπου k είναι το σταθερό πολυώνυμο k. Προφανώς τότε $\iota^*\colon \mathbb{K}[t] \longrightarrow \mathbb{K}[t]$ είναι η ταυτοτική απεικόνιση. Ισχυριζόμαστε ότι το πολυώνυμο $t \in \mathbb{K}[t]$ είναι υπερβατικό υπεράνω του $\mathbb{K}$. Πράγματι, αν το t ήταν αλγεβρικό, θα είχαμε $a_0 + a_1 t + \cdots + a_n t^n = 0$, για κάποια στοιχεία $a_k \in \mathbb{K}$, $0 \leq k \leq n$. Αυτό όμως μπορεί να συμβεί μόνο αν το πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k$ είναι το μηδενικό πολυώνυμο. Άρα το πολυώνυμο t είναι υπερβατικό στοιχείο του $\mathbb{K}[t]$ υπεράνω του $\mathbb{K}$.
2. Θεωρούμε το σώμα $\mathbb{Q}$ των ρητών ως υπόσωμα του σώματος $\mathbb{R}$ των πραγματικών αριθμών, και έστω το στοιχείο $u = \sqrt{2} \in \mathbb{R}$. Τότε το $\sqrt{2}$ είναι αλγεβρικό υπεράνω του $\mathbb{Q}$ διότι $P(\sqrt{2}) = 0$, όπου $P(t) = t^2 - 2 \in \mathbb{Q}[t]$. Προφανώς το $t^2 - 2$ είναι το ελάχιστο πολυώνυμο του $\sqrt{2}$ υπεράνω του $\mathbb{Q}$. $\surd$

Μπορούμε τώρα να χαρακτηρίσουμε πότε ο υποδακτύλιος $\mathbb{K}[u] \subseteq S$ του σώματος S, ο οποίος παράγεται υπεράνω του σώματος $\mathbb{K} \subseteq S$ από ένα στοιχείο $u \in S$, είναι σώμα.

Θεώρημα 9.2.7. *Έστω $\mathbb{K}$ ένας υποδακτύλιος ενός δακτυλίου S, και έστω $u \in S$ ένα τυχόν στοιχείο του S. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Ο υποδακτύλιος $\mathbb{K}[u]$ του S είναι σώμα.*
2. *Το στοιχείο $u \in S$ είναι αλγεβρικό υπεράνω του $\mathbb{K}$ και το ελάχιστο πολυώνυμο $Q_u(t) \in \mathbb{K}[t]$ του u είναι ανάγωγο.*

Αν ο δακτύλιος $\mathbb{K}[u]$ *είναι σώμα, τότε*

$$\mathbb{K}[u] = \left\{a_0 + a_1 u + a_2 u^2 + \cdots + a_n u^{n-1} \in S \mid a_i \in \mathbb{K},\ 0 \leq i \leq n-1,\ n = \deg Q_u(t)\right\}$$

Απόδειξη. Θεωρούμε την κανονική έγκλειση δακτυλίων $\iota\colon \mathbb{K} \longrightarrow S$. Τότε, όπως στην Πρόταση 9.2.4, θα έχουμε έναν ισομορφισμό δακτυλίων $\mathbb{K}[t]/I \cong \mathbb{K}[u]$, όπου $I = \mathsf{Ker}(\iota^*)$ και ι^* είναι ο μοναδικός ομομορφισμός δακτυλίων $\iota^*\colon \mathbb{K}[t] \longrightarrow S$ έτσι ώστε: $\iota^*(\mathsf{k}) = \iota(k) = k$ και $\iota^*(t) = u$, όπου k είναι το σταθερό πολυώνυμο $k \in \mathbb{K}$.

1. «$\Longrightarrow$» 2. Υποθέτουμε ότι ο υποδακτύλιος $\mathbb{K}[u]$ είναι σώμα, και άρα ο δακτύλιος πηλίκο $\mathbb{K}[t]/I$ είναι σώμα. Έστω $I = (Q(t))$, όπου $Q(t) \in \mathbb{K}[t]$. Προφανώς $Q(t) \neq 0$, διότι διαφορετικά θα είχαμε $\mathbb{K}[u] \cong \mathbb{K}[t]/\{0\} \cong \mathbb{K}[t]$, το οποίο είναι άτοπο διότι ο δακτύλιος $\mathbb{K}[t]$ δεν είναι σώμα. Επίσης $\deg Q(t) \geq 1$ διότι διαφορετικά θα είχαμε ότι το πολυώνυμο $Q(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο, και άρα είναι ένα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$. Τότε όμως $I = \mathbb{K}[t]$ και άρα ο δακτύλιος πηλίκο $\mathbb{K}[t]/I \cong \mathbb{K}[u]$ θα είναι ο τετριμμένος δακτύλιος. Αυτό είναι άτοπο διότι ο δακτύλιος $\mathbb{K}[u]$ είναι σώμα. Άρα πράγματι $\deg Q(t) := n \geq 1$. Έστω $Q(t) = \sum_{k=0}^{n} a_k t^k$. Τότε $0 = \iota^*(Q(t)) = \sum_{k=0}^{n} a_k u^k$ και άρα το στοιχείο u είναι αλγεβρικό υπεράνω του $\mathbb{K}$. Έστω $Q_u(t) = \sum_{k=0}^{n-1} a_k t^k + t^n$ το ελάχιστο πολυώνυμο του u υπεράνω του $\mathbb{K}$. Αν $Q_u(t) = Q_1(t)Q_2(t)$, όπου $0 \neq Q_i(t) \in \mathbb{K}[t]$, $i = 1, 2$, τότε $n = \deg Q_u(t) = \deg Q_1(t) + \deg Q_2(t)$, και άρα $\deg Q_i(t) \leq n = \deg Q_u(t)$. Τότε:

$$0 = \iota^*(Q_u(t))\iota^*\big(Q_1(t)Q_2(t)\big) = \iota^*(Q_1(t))\iota^*(Q_2(t)) \ \in\ \mathbb{K}[t]/(Q_u(t)) \ \cong\ \mathbb{K}[u]$$

Επειδή ο δακτύλιος $\mathbb{K}[u]$ είναι σώμα, έπεται ότι είτε $\iota^*(Q_1(t)) = 0$ είτε $\iota^*(Q_2(t)) = 0$. Σε κάθε περίπτωση, αποκτούμε ένα μη μηδενικό πολυώνυμο το οποίο ανήκει στο ιδεώδες $\mathsf{Ker}(\iota^*) = (Q_u(t))$ με βαθμό μικρότερο ή ίσο από τον βαθμό του μονικού γεννήτορα $Q_u(t)$. Επειδή το $Q_u(t)$ είναι το μονικό πολυώνυμο με τον μικρότερο βαθμό το οποίο ανήκει στο ιδεώδες $\mathsf{Ker}(\iota^*)$, έπεται ότι είτε $\deg Q_1(t) = 0$ είτε $\deg Q_2(t)$. Άρα είτε το $Q_1(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο, και άρα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$, είτε το $Q_2(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο, και άρα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$. Αυτό σημαίνει ότι το ελάχιστο πολυώνυμο $Q_u(t)$ του u υπεράνω του $\mathbb{K}$ είναι ανάγωγο.

2. «$\Longrightarrow$» 1. Υποθέτουμε ότι το στοιχείο $u \in S$ είναι αλγεβρικό υπεράνω του $\mathbb{K}$ και το ελάχιστο πολυώνυμο $Q_u(t) \in \mathbb{K}[t]$ του u είναι ανάγωγο. Επειδή το u είναι αλγεβρικό υπεράνω του $\mathbb{K}$, έπεται ότι θα έχουμε έναν ισομορφισμό $\mathbb{K}[t]/(Q_u(t)) \cong \mathbb{K}[u]$, και αρκεί να δείξουμε ότι ο δακτύλιος πηλίκο $\mathbb{K}[t]/(Q_u(t))$ είναι σώμα. Σύμφωνα με την Πρόταση 8.1.17, αυτό συμβαίνει αν και μόνο αν ο δακτύλιος $\mathbb{K}[t]/(Q_u(t))$ είναι απλός, δηλαδή τα μόνα ιδεώδη του είναι το μηδενικό και ο ίδιος ο δακτύλιος. Έστω $K \subseteq \mathbb{K}[t]/(Q_u(t))$ ένα ιδεώδες του $\mathbb{K}[t]/(Q_u(t))$. Από το Πόρισμα 8.3.12, έπεται ότι $K = I/(Q_u(t))$, όπου I είναι ένα ιδεώδες του $\mathbb{K}[t]$ έτσι ώστε $(Q_u(t)) \subseteq I$. Επειδή κάθε ιδεώδες του $\mathbb{K}[t]$ είναι κύριο, θα έχουμε $I = (P(t))$, για ένα πολυώνυμο $P(t) \in \mathbb{K}[t]$. Τότε $Q_u(t) \in (Q_u(t)) \subseteq (P(t))$ και επομένως $Q_u(t) = P(t)A(t)$. Επειδή το πολυώνυμο $Q_u(t)$ είναι ανάγωγο, έπεται ότι είτε το $P(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο είτε το $A(t)$ είναι ένα σταθερό μη μηδενικό πολυώνυμο. Στην πρώτη περίπτωση, το $P(t)$ είναι ένα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$ και επομένως θα έχουμε $I = (P(t)) = \mathbb{K}[t]$, και τότε $K = \mathbb{K}[t]/(Q_u(t))$. Στην δεύτερη περίπτωση, θα έχουμε ότι το $A(t)$ είναι ένα αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$ και επομένως, επειδή $Q_u(t) = P(t)A(t)$, έπεται ότι τα ιδεώδη $(Q_u(t))$ και $I = (P(t))$ συμπίπτουν και άρα $K = \left\{0_{\mathbb{K}[t]/(Q_u(t))}\right\}$. Επομένως ο δακτύλιος $\mathbb{K}[t]/(Q_u(t))$ έχει ακριβώς δύο ιδεώδη, τα τετριμμένα, και έτσι είναι σώμα.

Υποθετουμε ότι ο δακτύλιος $\mathbb{K}[u]$ είναι σώμα, δηλαδή το στοιχείο u είναι αλγεβρικό υπεράνω του $\mathbb{K}$ και το ελάχιστο πολυώνυμο του $Q_u(t)$ είναι ανάγωγο, και έχει βαθμό $n = \deg Q_u(t)$. Έστω $r = \sum_{k=0}^{m} b_k u^m \in \mathbb{K}[u]$. Αν $r = 0$ ή $m \leq n$, τότε δεν έχουμε να αποδείξουμε τίποτα. Έστω $r \neq 0$ και $m > n$. Θεωρούμε το πολυώνυμο $P(t) = \sum_{k=0}^{m} b_k t^k$. Από την Ευκλείδεια Διαίρεση του $P(t)$ με το $Q_u(t)$, θα έχουμε $P(t) = Q_u(t)A(t) + B(t)$, όπου είτε $B(t) = 0$ είτε $\deg B(t) < n$. Αν $B(t) = 0$, τότε $P(t) = Q_u(t)A(t)$ και άρα $r = P(u) = Q_u(u)A(u) = 0$, το οποίο είναι άτοπο. Αν $l := \deg B(t) < n$, τότε $r = P(u) = Q_u(u)A(u) + B(u) = B(u)$. Δηλαδή $r = c_0 + c_1 u + \cdots + c_{n-1}u^{n-1} \in \mathbb{K}[u]$, όπου $c_i \in \mathbb{K}$, $0 \leq i \leq n-1$, το οποίο ήταν ο ισχυρισμός που θέλαμε να δείξουμε. ∎

Η ακόλουθη Πρόταση εξετάζει την περίπτωση κατά την οποία το στοιχείο u είναι υπερβατικό.

Πρόταση 9.2.8. *Έστω $\mathbb{K}$ ένας υποδακτύλιος ενός δακτυλίου S, και έστω $u \in S$ ένα τυχόν στοιχείο του S. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Το στοιχείο u είναι υπερβατικό υπεράνω του $\mathbb{K}$.*
2. *Η κανονική έγκλειση $\iota\colon \mathbb{K} \longrightarrow S$ επάγει έναν ισομορφισμό δακτυλίων*

$$\mathbb{K}[u] \cong \mathbb{K}[t]$$

Απόδειξη. Θεωρούμε την κανονική έγκλειση δακτυλίων $\iota\colon \mathbb{K} \longrightarrow S$. Τότε, όπως στην Πρόταση 9.2.4, θα έχουμε έναν ισομορφισμό δακτυλίων $\mathbb{K}[t]/I \cong \mathbb{K}[u]$, όπου $I = \mathsf{Ker}(\iota^*)$ και ι^* είναι ο μοναδικός ομομορφισμός δακτυλίων $\iota^*\colon \mathbb{K}[t] \longrightarrow S$ έτσι ώστε: $\iota^*(\mathsf{k}) = \iota(k) = k$ και $\iota^*(t) = u$, όπου k είναι το σταθερό πολυώνυμο $k \in \mathbb{K}$.

1. «$\Longrightarrow$» 2. Υποθέτουμε ότι το στοιχείο u είναι υπερβατικό υπεράνω του $\mathbb{K}$. Τότε το ιδεώδες $I = \mathsf{Ker}(\iota^*) = \{0\}$, και επομένως θα έχουμε έναν ισομορφισμό

$$\iota^*\colon \mathbb{K}[t] \xrightarrow{\cong} \mathbb{K}[u], \quad \iota^*(t) = u$$

2. «$\Longrightarrow$» 1. Υποθέτουμε ότι η κανονική έγκλειση $\iota\colon \mathbb{K} \longrightarrow S$ επάγει έναν ισομορφισμό δακτυλίων $\iota^*\colon \mathbb{K}[u] \cong \mathbb{K}[t]$, και επομένως θα έχουμε $\iota^*(t) = u$ και $\iota^*(\mathsf{k}) = k$, $\forall k \in \mathbb{K}$. Αν το στοιχείο u ήταν αλγεβρικό υπεράνω του $\mathbb{K}$, τότε θα υπήρχε μη μηδενικό πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k$, έτσι ώστε $P(u) = 0$. Τότε όμως, επειδή ο ομομορφισμός ι^* είναι μονομορφισμός, θα έχουμε:

$$0 = P(u) = \iota^*(P(t)) \quad \Longrightarrow \quad P(t) \in \mathsf{Ker}(\iota^*) = \{0\}$$

Άρα το $P(t)$ είναι το μηδενικό πολυώνυμο, και αυτό είναι άτοπο. Άρα το στοιχείο u είναι αλγεβρικό υπεράνω του $\mathbb{K}$. ■

Παράδειγμα 9.2.9. 1. Θεωρούμε το υπόσωμα $\mathbb{Q}$ του σώματος $\mathbb{R}$ και έστω το στοιχείο $u = \sqrt[3]{2} \in \mathbb{R}$.

Αν $P(t) = t^3 - 2$, τότε προφανώς $P(u) = P(\sqrt[3]{2}) = (\sqrt[3]{2})^3 - 2 = 2 - 2 = 0$. Επομένως το στοιχείο u είναι αλγεβρικό υπεράνω του $\mathbb{Q}$. Το πολυώνυμο $P(t) = t^3 - 2$ είναι μονικό, μηδενίζει το στοιχείο $\sqrt[3]{2}$ και προφανώς είναι ανάγωγο υπεράνω του $\mathbb{Q}$. Άρα το $t^3 - 2$ είναι το ελάχιστο πολυώνυμο του $\sqrt[3]{2}$ υπεράνω του $\mathbb{Q}$ και επομένως θα έχουμε ότι ο δακτύλιος

$$\mathbb{Q}[t]/(t^3 - 2) \cong \mathbb{Q}[\sqrt[3]{2}] = \left\{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \in \mathbb{R} \mid a, b, c \in \mathbb{Q}\right\}$$

είναι σώμα.

2. Έστω $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ μια (πρωταρχική) κυβική ρίζα της μονάδας. Τότε $P(\omega) = 0$, όπου $P(t) = t^2 + t + 1 \in \mathbb{Q}[t]$, και άρα το ω είναι αλγεβρικό στοιχείο υπεράνω του $\mathbb{Q}$. Το $P(t)$ είναι μονικό, έχει το ω ως ρίζα, η άλλη ρίζα είναι η $\omega^2 = \frac{-1-i\sqrt{3}}{2}$, και ανάγωγο υπεράνω του $\mathbb{Q}$ και προφανώς είναι το ελάχιστο πολυώνυμο του ω. Επομένως θα έχουμε ότι ο δακτύλιος

$$\mathbb{Q}[t]/(t^2 + t + 1) \cong \mathbb{Q}[\omega] = \left\{a + b\omega + c\omega^2 \in \mathbb{C} \mid a, b, c \in \mathbb{Q}\right\}$$

είναι σώμα. $\surd$

9.3 Πολυωνυμικές Συναρτήσεις

Έστω R ένας μεταθετικός δακτύλιος. Θεωρούμε τον δακτύλιο $(\mathscr{F}(R,R), +\cdot)$

$$\mathscr{F}(R,R) = \left\{f\colon R \longrightarrow R \mid f : \text{απεικόνιση}\right\}$$

όπου η πρόσθεση «+» και ο πολλαπλασιασμός «·» ορίζονται ως εξής:

$$+ : \mathscr{F}(R,R)\times\mathscr{F}(R,R)\longrightarrow\mathscr{F}(R,R),\quad (f,g)\longmapsto f+g\colon R\longrightarrow R,\quad (f+g)(r)=f(r)+g(r)$$

$$\cdot : \mathscr{F}(R,R)\times\mathscr{F}(R,R)\longrightarrow\mathscr{F}(R,R),\quad (f,g)\longmapsto f\cdot g\colon R\longrightarrow R,\quad (f\cdot g)(r)=f(r)g(r)$$

Γνωρίζουμε τότε ότι η τριάδα $(\mathscr{F}(R,R),+,\cdot)$ είναι ένας δακτύλιος με μονάδα την απεικόνιση $1\colon R\longrightarrow R$, $1(r)=1_R$. Το μηδενικό στοιχείο είναι η μηδενική απεικόνιση $0\colon R\longrightarrow R$, $0(r)=0_R$, και το αντίθετο στοιχείο της απεικόνισης f είναι η απεικόνιση $-f\colon R\longrightarrow R$, $(-f)(r)=-f(r)$. Επειδή ο δακτύλιος R είναι μεταθετικός, ο πολλαπλασιασμός του $\mathscr{F}(R,R)$ δείχνει ότι ο δακτύλιος $\mathscr{F}(R,R)=(\mathscr{F}(R,R),+,\cdot)$ είναι επίσης μεταθετικός.

Ο δακτύλιος $\mathscr{F}(R,R)$ περιέχει κάποιες σημαντικές απεικονίσεις: τις σταθερές απεικονίσεις και την ταυτοτική συνάρτηση. Αναλυτικότερα, για κάθε $r\in R$, ορίζεται η σταθερή απεικόνιση $\mathsf{r}\colon R\longrightarrow R$, $\mathsf{r}(x)=r$. Γενικότερα μια απεικόνιση $f\in\mathscr{F}(R,R)$ καλείται *σταθερή απεικόνιση*, αν υπάρχει $r\in R$, έτσι ώστε $f=\mathsf{r}$. Προφανώς η απεικόνιση

$$\phi\colon R\longrightarrow\mathscr{F}(R,R),\quad r\longmapsto\phi(r)=\mathsf{r}\colon R\longrightarrow R,\quad \mathsf{r}(x)=r$$

είναι ένας μονομορφισμός δακτυλίων, με εικόνα $\mathsf{Im}(\phi)$ το σύνολο των σταθερών απεικονίσεων. Από τώρα και στο εξής, αν δεν υπάρχει κίνδυνος σύγχυσης, θα ταυτίζουμε τον δακτύλιο R με τον υποδακτύλιο $\mathsf{Im}(\phi)$ του $\mathscr{F}(R,R)$ ο οποίος αποτελείται από τις σταθερές απεικονίσεις.

Επιπρόσθετα, στον δακτύλιο $\mathscr{F}(R,R)$ ανήκει και η ταυτοτική συνάρτηση $\mathrm{Id}_R\colon R\longrightarrow R$, $\mathrm{Id}_R(r)=r$. Για παραδοσιακούς λόγους και χάριν ευκολίας του συμβολισμού, από τώρα και στο εξής, η ταυτοτική απεικόνιση Id_R θα συμβολίζεται με s, έτσι:

$$\mathsf{s}\colon R\longrightarrow R,\quad r\longmapsto\mathsf{s}(r)=r$$

Οι δυνάμεις της ταυτοτικής απεικόνισης s ορίζονται ως εξής, $\forall\, n\geq 0$:

$$\mathsf{s}^n\colon R\longrightarrow R,\quad \mathsf{s}^n(x)=\big(\mathsf{s}\cdot\mathsf{s}\cdots\mathsf{s}\big)(x)=\mathsf{s}(x)\cdot\mathsf{s}(x)\cdots\mathsf{s}(x)=x\cdot x\cdots x=x^n$$

Θεωρώντας τον μεταθετικό δακτύλιο R ως υποδακτύλιο του δακτυλίου $\mathscr{F}(R,R)$ (ισόμορφο με τον υποδακτύλιο των σταθερών απεικονίσεων μέσω του μονομορφισμού ϕ), θεωρούμε τον υποδακτύλιο $R[\mathsf{s}]$ ο οποίος παράγεται υπεράνω του R από την ταυτοτική συνάρτηση s. Σύμφωνα με την Πρόταση 7.3.5, θα έχουμε:

$$R[\mathsf{s}]=\big\{r_0+r_1\mathsf{s}+r_2\mathsf{s}^2+\cdots+r_n\mathsf{s}^n\in\mathscr{F}(R,R)\mid r_i\in R,\quad n\geq 0\big\}$$

Δηλαδή η απεικόνιση $r_0+r_1\mathsf{s}+r_2\mathsf{s}^2+\cdots+r_n\mathsf{s}^n\in R[\mathsf{s}]$ ορίζεται ως

$$r_0+r_1\mathsf{s}+r_2\mathsf{s}^2+\cdots+r_n\mathsf{s}^n\colon R\longrightarrow R,\quad x\longmapsto r_0+r_1x+r_2x^2+\cdots+r_nx^n$$

Θεωρώντας το πολυώνυμο $P(t)=r_0+r_1t+r_2t^2+\cdots+r_nt^n\in R[t]$, έπεται ότι η παραπάνω απεικόνιση $r_0+r_1\mathsf{s}+r_2\mathsf{s}^2+\cdots+r_n\mathsf{s}^n\colon R\longrightarrow R$, είναι της μορφής $x\longmapsto P(x)$. Έτσι προκύπτει φυσιολογικά ο ακόλουθος ορισμός και ορολογία.

Ορισμός 9.3.1. *Ο υποδακτύλιος $R[\mathsf{s}]$ του $\mathscr{F}(R,R)$, ο οποίος παράγεται υπεράνω του R από την ταυτοτική απεικόνιση s του R, καλείται ο δακτύλιος των* **πολυωνυμικών συναρτήσεων** *επί του R.*

Θεωρούμε την απεικόνιση

$$\Phi\colon R[t]\longrightarrow\mathscr{F}(R,R),\quad P(t)\longmapsto\Phi(P(t))\colon R\longrightarrow R,\quad \Phi(P(t))(x)=P(x)$$

Με άλλα λόγια, η απεικόνιση Φ συμπίπτει με τον ομομορφισμό εκτίμησης ο οποίος επάγεται μοναδικά, όπως στην Πρόταση 8.2.22, από τον ομομορφισμό $\phi\colon R\longrightarrow\mathscr{F}(R,R)$, $\phi(r)=\mathsf{r}$ και το στοιχείο $\mathsf{s}\in\mathscr{F}(R,R)$. Επομένως η απεικόνιση Φ είναι ο μοναδικός ομομορφισμός δακτυλίων $\Phi\colon R[t]\longrightarrow\mathscr{F}(R,R)$ έτσι ώστε $\Phi(t)=\mathsf{s}$ και $\Phi(r)=\mathsf{r}$.

Προφανώς $\mathsf{Im}(\Phi)=R[\mathsf{s}]$, και επομένως ο ομομορφισμός Φ είναι επιμορφισμός δακτυλίων, και άρα επάγει έναν ισομορφισμό δακτυλίων

$$R[t]/\,\mathsf{Ker}(\Phi)\ \cong\ R[\mathsf{s}]$$

όπου

$$\mathsf{Ker}(\Phi)=\big\{P(t)\in R[t]\mid\Phi(P(t))=0\big\}=\big\{P(t)\in R[t]\mid P(x)=0,\ \forall\, x\in R\big\}$$

Πότε ο ομομορφισμός Φ είναι ισομορφισμός δακτυλίων;

Πρόταση 9.3.2. *Αν $R = \mathbb{K}$ είναι ένα σώμα, τότε ο επιμορφισμός δακτυλίων*

$$\Phi\colon \mathbb{K}[t] \longrightarrow \mathbb{K}[\mathsf{s}], \quad P(t) \longmapsto \Phi(P(t))\colon \mathbb{K} \longrightarrow \mathbb{K}, \ \ \Phi(P(t))(x) = P(x)$$

είναι ισομορφισμός αν και μόνο αν το σώμα $\mathbb{K}$ είναι άπειρο.

Απόδειξη. Υποθέτουμε ότι το σώμα $\mathbb{K}$ είναι άπειρο. Έστω $P(t)$ ένα πολυώνυμο το οποίο ανήκει στον πυρήνα $\mathsf{Ker}(\Phi)$ του επιμορφισμού Φ. Τότε η πολυωνυμική συνάρτηση $\Phi(P(t))\colon \mathbb{K} \longrightarrow \mathbb{K}$ είναι η μηδενική, δηλαδή $\Phi(P(t))(x) = P(x) = 0$, $\forall\, x \in \mathbb{K}$, δηλαδή κάθε στοιχείο x του σώματος $\mathbb{K}$ είναι ρίζα του $P(t)$. Αν $\deg P(t) \geq 1$, τότε, σύμφωνα με το Θεώρημα 9.1.10, το πολυώνυμο έχει το πολύ $\deg P(t)$ ρίζες στο σώμα $\mathbb{K}$. Άρα, επειδή κάθε στοιχείο του άπειρου σώματος $\mathbb{K}$ είναι ρίζα του $P(t)$, το $P(t)$ είναι σταθερό πολυώνυμο, έστω $P(t) = r_0 \in R$. Τότε, $\forall\, x \in R$, θα έχουμε $0 = P(x) = r_0$, και αυτό σημαίνει ότι το $P(t)$ είναι το μηδενικό πολυώνυμο. Έτσι δείξαμε ότι $\mathsf{Ker}(\Phi) = \{0\}$ και επομένως ο επιμορφισμός Φ είναι ισομορφισμός.

Αντίστροφα, αν το σώμα $\mathbb{K}$ είναι πεπερασμένο, έστω $\mathbb{K} = \{x_1, x_2, \cdots, x_k\}$, τότε θεωρούμε το πολυώνυμο

$$P(t) = (t - x_1)(t - x_2)\cdots(t - x_k)$$

το οποίο προφανώς είναι ένα μη μηδενικό πολυώνυμο βαθμού k. Η εικόνα $\Phi(P(t))$ του πολυωνύμου $P(t)$ μέσω του επιμορφισμού Φ, είναι η πολυωνυμική συνάρτηση

$$\Phi(P(t))\colon \mathbb{K} \longrightarrow \mathbb{K}, \quad x \longmapsto \Phi(P(t))(x) = P(x) = (x - x_1)(x - x_2)\cdots(x - x_k)$$

Επειδή το $x \in \mathbb{K}$ είναι ένα εκ των $\{x_1, x, \cdots, x_k\}$, έπεται ότι $\Phi(P(t))(x) = 0$, $\forall\, x \in \mathbb{K}$, και άρα η πολυωνυμική συνάρτηση $\Phi(P(t))$ είναι η μηδενική. Αυτό σημαίνει ότι $0 \neq P(t) \in \mathsf{Ker}(\Phi)$ και άρα ο επιμορφισμός Φ δεν είναι ισομορφισμός. Επομένως, αν ο επιμορφισμός Φ είναι ισομορφισμός, έπεται ότι το σώμα $\mathbb{K}$ είναι άπειρο. ■

Η παραπάνω Πρόταση μας επιτρέπει να ταυτίσουμε ένα πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k$ υπεράνω ενός άπειρου σώματος $\mathbb{K}$, π.χ. $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, με την αντίστοιχη πολυωνυμική συνάρτηση η οποία ορίζεται με «πολυωνυμικό τύπο» $: \mathbb{K} \longrightarrow \mathbb{K}$, $x \longmapsto \sum_{k=0}^{n} a_k x^k$.

Αν το σώμα $\mathbb{K}$ είναι πεπερασμένο, τότε γνωρίζουμε ότι $\mathsf{Ker}(\Phi) \neq \{0\}$. Η ακόλουθη Πρόταση περιγράφει το ιδεώδες $\mathsf{Ker}(\Phi)$:

Πρόταση 9.3.3. *Έστω $\mathbb{K}$ ένα σώμα με πλήθος στοιχείων ίσο με $|\mathbb{K}| = q < \infty$. Τότε $\mathsf{Ker}(\Phi) = (t^q - t)$, και άρα θα έχουμε έναν ισομορφισμό δακτυλίων*

$$\mathbb{K}[t]\big/(t^q - t) \ \cong \ \mathbb{K}[\mathsf{s}]$$

Απόδειξη. Θεωρούμε την πολλαπλασιαστική ομάδα $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ του πεπερασμένου σώματος $\mathbb{K}$ η οποία έχει τάξη $q-1$. Τότε, από γνωστή συνέπεια του Θεωρήματος του Lagrange, θα έχουμε $x^{q-1} = 1$, $\forall\, x \in \mathbb{K}^*$, και άρα $x^q = x$, $\forall\, x \in \mathbb{K}$. Θεωρούμε το πολυώνυμο $t^q - t \in \mathbb{K}[t]$, το οποίο είναι προφανώς μη μηδενικό και ανήκει στον πυρήνα $\mathsf{Ker}(\Phi)$ του επιμορφισμού Φ, διότι: $\Phi(t^q - t)(x) = x^q - x = 0$, $\forall\, x \in \mathbb{K}$. Άρα $(t^q - t) \subseteq \mathsf{Ker}(\Phi)$. Αντίστροφα, αν $P(t)$ είναι ένα πολυώνυμο το οποίο ανήκει στον πυρήνα $\mathsf{Ker}(\Phi)$, τότε από την Ευκλείδεια διαίρεση του $P(t)$ με το $t^q - t$ θα έχουμε:

$$P(t) = (t^q - t)Q(t) + R(t), \quad \text{και} \quad \text{είτε} \quad R(t) = 0 \quad \text{είτε} \quad \deg R(t) < \deg(t^q - t) = q$$

Επειδή $P(t) \in \mathsf{Ker}(\Phi)$, έπεται ότι η επαγόμενη πολυωνυμική συνάρτηση είναι η μηδενική, και το ίδιο συμβαίνει και με το πολυώνυμο $t^q - t$. Επομένως, για κάθε $x \in \mathbb{K}$, θα έχουμε

$$P(x) = (x^q - x)Q(x) + R(x) \quad \Longrightarrow \quad 0 = 0Q(x) + R(x) \quad \Longrightarrow \quad R(x) = 0$$

Άρα το πολυώνυμο $R(t)$ έχει πλήθος διακεκριμένων ριζών ίσο με $q > \deg R(t)$. Σύμφωνα με το Θεώρημα 9.1.10, αυτό μπορεί να συμβαίνει μόνο όταν το $R(t)$ είναι σταθερό πολυώνυμο $R(t) = r_0 \in R$, και τότε προφανώς r_0 διότι $0 = R(x) = r_0$, $\forall\, x \in \mathbb{K}$. Άρα το πολυώνυμο $R(t)$ είναι το μηδενικό και τότε $P(t) = (t^q - t)Q(t) \in (t^q - t)$, δηλαδή $\mathsf{Ker}(\Phi) \subseteq (t^q - t)$. Επομένως $\mathsf{Ker}(\Phi) = (t^q - t)$. ■

Τα παραπάνω απότελέσματα γενικεύονται και, κατάλληλα τροποποιημένα, ισχύουν για πολυωνυμικούς δακτυλίους πολλών μεταβλητών με συντελεστές από ένα σώμα.

9.4 Το Σώμα Κλασμάτων μιας Ακέραιας Περιοχής

Έστω $\mathbb{K}$ ένα σώμα. Τότε προφανώς κάθε υποδακτύλιος του $\mathbb{K}$ είναι ακέραια περιοχή. Στην παρούσα ενότητα θα αποδείξουμε ότι, αντίστροφα, κάθε μεταθετική ακέραια περιοχή R είναι υποδακτύλιος ενός κατάλληλου σώματος $Q(R)$ και μάλιστα με βέλτιστο τρόπο, με την έννοια ότι, αν η ακέραια περιοχή R είναι επίσης υποδακτύλιος ενός σώματος $\mathbb{K}$, τότε υπάρχει μονομορφισμός σωμάτων $Q(R) \longrightarrow \mathbb{K}$. Επομένως το σώμα $Q(R)$ είναι, μέχρι ισομορφία, το μικρότερο δυνατό σώμα το οποίο περιέχει ως υποδακτύλιο την ακέραια περιοχή R. Η μέθοδος κατασκευής του σώματος $Q(R)$ από την ακέραια περιοχή R είναι παρόμοια με την μέθοδο κατασκευής του σώματος $\mathbb{Q}$ των ρητών αριθμών από τον δακτύλιο $\mathbb{Z}$ των ακεραίων.

Από τώρα και στο εξής θεωρούμε μια μεταθετική ακέραια περιοχή R, και όλοι οι εμπλεκόμενοι δακτύλιοι είναι μεταθετικοί. Ως συνήθως συμβολίζουμε με R^* το σύνολο των μη μηδενικών στοιχείων του R (προφανώς $R^* \neq \emptyset$, διότι $1_R \in R^*$). Στο σύνολο $R \times R^*$ ορίζουμε μια σχέση «$\sim$» ως εξής:

$$\forall (a,b),(c,d) \in R \times R^* : \quad (a,b) \sim (c,d) \iff ad = bc \tag{†}$$

Λήμμα 9.4.1. *Η σχέση «$\sim$» είναι μια σχέση ισοδυναμίας επί του συνόλου $R \times R^*$.*

Απόδειξη. Έστω $(a,b),(c,d),(e,f) \in R \times R^*$.

1. Θα έχουμε $(a,b) \sim (a,b)$, διότι $ab = ba$ επειδή ο δακτύλιος R είναι μεταθετικός. Άρα η σχέση «$\sim$» είναι ανακλαστική.

2. Έστω $(a,b) \sim (c,d)$. Τότε $ad = bc$ και επομένως λόγω μεταθετικότητας θα έχουμε $da = cb$, το οποίο σημαίνει ότι $(c,d) \sim (a,b)$. Άρα η σχέση «$\sim$» είναι συμμετρική.

3. Έστω ότι $(a,b) \sim (c,d)$ και $(c,d) \sim (e,f)$. Τότε θα έχουμε $ad = bc$ και $cf = de$, και επομένως $adf = bcf$, δηλαδή $adf = bde$ ή ισοδύναμα λόγω μεταθετικότητας $afd = bed$. Επειδή $d \in R^*$, δηλαδή $d \neq 0$, και επειδή ο δακτύλιος R είναι ακέραια περιοχή, θα έχουμε $af = be$, το οποίο σημαίνει ότι $(a,b) \sim (e,f)$. Άρα η σχέση «$\sim$» είναι μεταβατική.

Συνοψίζοντας, δείξαμε ότι η σχέση «$\sim$» είναι μια σχέση ισοδυναμίας επί του συνόλου $R \times R^*$. ■

Η κλάση ισοδυναμίας $[(a,b)]_\sim$ του στοιχείου (a,b) θα συμβολίζεται με

$$\frac{a}{b} = [(a,b)]_\sim = \{(c,d) \in R \times R^* \mid (a,b) \sim (c,d)\} = \{(c,d) \in R \times R^* \mid ad = bc\}$$

και καλείται το **κλάσμα** του στοιχείου a ως προς το μη μηδενικό στοιχείο b του R. Το σύνολο πηλίκο $(R \times R^*)/\sim$ των κλάσεων ισοδυναμίας επί του $R \times R^*$ ως προς τη σχέση ισοδυναμίας «$\sim$» θα συμβολίζεται με

$$Q(R) = \left\{ \frac{a}{b} \subseteq R \times R^* \mid (a,b) \in R \times R^* \right\}$$

Σημειώνουμε ότι για δύο κλάσματα $\frac{a}{b}$ και $\frac{c}{d}$, έχουμε:

$$\frac{a}{b} = \frac{c}{d} \iff ad = bc$$

Σκοπός μας είναι να ορίσουμε πράξεις πρόσθεσης «$+$» και πολλαπλασιασμού «$\cdot$» επί του συνόλου πηλίκου $Q(R)$ έτσι ώστε η τριάδα $(Q(R),+,\cdot)$ να είναι σώμα. Πράγματι ορίζουμε:

$$+ : Q(R) \times Q(R) \longrightarrow Q(R), \quad \left(\frac{a}{b},\frac{c}{d}\right) \longmapsto \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\cdot : Q(R) \times Q(R) \longrightarrow Q(R), \quad \left(\frac{a}{b},\frac{c}{d}\right) \longmapsto \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Δείχνουμε ότι οι παραπάνω απεικονίσεις, οι οποίες έχουν οριστεί επί κλάσεων ισοδυναμίας στοιχείων του $R \times R^*$, είναι καλά ορισμένες πράξεις επί του $Q(R)$. Χρησιμοποιούμε πάντα ότι, επειδή ο δακτύλιος R είναι ακέραια περιοχή, το σύνολο R^* είναι κλειστό στον πολλαπλασιασμό του R.

Θεωρούμε τυχόντα στοιχεία $(a,b),(c,d),(a',b')(c',d') \in R \times R^*$. Τότε ορίζονται τα κλάσματα $\frac{a}{b}$, $\frac{a'}{b'}$, $\frac{c}{d}$, και $\frac{c'}{d'}$. Επειδή τα στοιχεία $b,d,b',d' \in R^*$ είναι μη μηδενικά και το σύνολο R^* είναι κλειστό στον πολλαπλασιασμό του R, έπεται ότι τα στοιχεία bd και $b'd'$ είναι μη μηδενικά: $bd, b'd' \in R^*$. Επομένως ορίζονται τα κλάσματα $\frac{ad+bc}{bd}$, $\frac{a'd'+b'c'}{b'd'}$, $\frac{ac}{bd}$, και $\frac{a'c'}{b'd'}$.

1. Θα δείξουμε ότι:

$$\frac{a}{b}=\frac{a'}{b'} \quad \text{και} \quad \frac{c}{d}=\frac{c'}{d'} \quad \Longrightarrow \quad \frac{a}{b}+\frac{c}{d}=\frac{a'}{b'}+\frac{c'}{d'}, \quad \text{δηλαδή:} \quad \frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$$

Θα έχουμε:

$$ab'=ba' \quad \text{και} \quad cd'=dc' \quad \Longrightarrow \quad ab'dd'=ba'dd' \quad \text{και} \quad cd'bb'=dc'bb' \quad \Longrightarrow$$

$$\Longrightarrow \quad ab'dd'+cd'bb'=ba'dd'+dc'bb' \quad \Longrightarrow \quad (ad+bc)b'd'=(a'd'+b'c')bd$$

Η τελευταία ισότητα δείχνει ότι $\frac{ad+bc}{bd}=\frac{a'd'+b'c'}{b'd'}$, και επομένως η πράξη «+» είναι καλά ορισμένη.

2. Θα δείξουμε ότι:

$$\frac{a}{b}=\frac{a'}{b'} \quad \text{και} \quad \frac{c}{d}=\frac{c'}{d'} \quad \Longrightarrow \quad \frac{a}{b}\cdot\frac{c}{d}=\frac{a'}{b'}\cdot\frac{c'}{d'}, \quad \text{δηλαδή:} \quad \frac{ac}{bd}=\frac{a'c'}{b'd'}$$

Θα έχουμε:

$$ab'=ba' \quad \text{και} \quad cd'=dc' \quad \Longrightarrow \quad ab'cd'=ba'cd' \quad \Longrightarrow \quad ab'cd'=ba'dc' \quad \Longrightarrow$$

$$\Longrightarrow \quad acb'd'=a'c'bd \quad \Longrightarrow \quad (ac)b'd'=(a'c')bd$$

Η τελευταία ισότητα δείχνει ότι $\frac{ac}{bd}=\frac{a'c'}{b'd'}$, και επομένως η πράξη «·» είναι καλά ορισμένη.

Επομένως το σύνολο $Q(R)$ είναι εφοδιασμένο με τις πράξεις «+» (πρόσθεση κλασμάτων) και «·» (πολλαπλασιασμός κλασμάτων).

Παρατήρηση 9.4.2. Παρατηρούμε ότι

$$\frac{a}{b}+\frac{c}{b}=\frac{ab+bc}{b^2}=\frac{b(a+c)}{b^2}=\frac{a+c}{b}$$

όπου η τελευταία σχέση προέκυψε διότι, χρησιμοποιώντας ότι ο δακτύλιος R είναι μεταθετικός, έχουμε: $(a+c)b^2=b(a+c)b=b^2(a+c)$.

Επίσης, αν $c \in R^*$, τότε για κάθε $\frac{a}{b} \in Q(R)$, θα έχουμε:

$$\frac{ac}{bc}=\frac{a}{b}$$

διότι, χρησιμοποιώντας ότι ο δακτύλιος R είναι μεταθετικός, έχουμε: $acb=bca$. ▲

Το παρακάτω βασικό αποτέλεσμα δείχνει ότι κάθε ακέραια περιοχή μπορεί να «εμφυτευθεί» σε ένα σώμα με βέλτιστο τρόπο.

Θεώρημα 9.4.3. *Αν R είναι μια ακέραια περιοχή, τότε με τους παραπάνω συμβολισμούς:*

1. *Η τριάδα $Q(R)=(Q(R),+,\cdot)$ είναι ένα σώμα, και η απεικόνιση*

$$\varphi\colon R \longrightarrow Q(R), \quad \varphi(a)=\frac{a}{1_R}$$

είναι ένας μονομορφισμός δακτυλίων.

2. *Αν $\mathbb{K}$ είναι ένα σώμα και $g\colon R \longrightarrow \mathbb{K}$ είναι ένας μονομορφισμός δακτυλίων, τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων $g^*\colon Q(R) \longrightarrow \mathbb{K}$, ο οποίος είναι μονομορφισμός σωμάτων, έτσι ώστε: $g^* \circ \varphi = g$.*

3. *Αν $\mathbb{F}$ είναι ένα σώμα και $\psi\colon R \longrightarrow \mathbb{F}$ είναι ένας μονομορφισμός δακτυλίων, έτσι ώστε για κάθε άλλο σώμα $\mathbb{K}$ και μονομορφισμό δακτυλίων $f\colon R \longrightarrow \mathbb{K}$ υπάρχει μοναδικός ομομορφισμός δακτυλίων $f^*\colon \mathbb{F} \longrightarrow \mathbb{K}$, ο οποίος είναι μονομορφισμός σωμάτων, έτσι ώστε: $f^* \circ \psi = f$, τότε υπάρχει μοναδικός ισομορφισμός σωμάτων*

$$\omega\colon Q(R) \xrightarrow{\cong} \mathbb{F}, \quad \text{έτσι ώστε:} \quad \omega \circ \varphi = \psi$$

Απόδειξη. 1. Θα δείξουμε ότι η τριάδα $(Q(R), +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα, κάθε μη μηδενικό στοιχείο του οποίου είναι αντιστρέψιμο.

(α΄) Έστω $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(R)$. Τότε:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{(ad+bc)f + (bd)e}{bdf} = \frac{adf + bcf + bde}{bdf}$$

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{(adf + b(cf+de)}{bdf} = \frac{adf + bcf + bde}{bdf}$$

Λαμβάνοντας υπόψη την μεταθετικότητα του δακτυλίου R, θα έχουμε:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right)$$

και άρα η πράξη της πρόσθεσης «+» είναι προσεταιριστική.

(β΄) Έστω $\frac{a}{b}, \frac{c}{d} \in Q(R)$. Τότε:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$$

και άρα η πράξη της πρόσθεσης «+» είναι μεταθετική.

(γ΄) Για το στοιχείο $\frac{0}{1}$, το οποίο προφανώς ανήκει στο σύνολο $Q(R)$, θα έχουμε $\forall \frac{a}{b} \in Q(R)$:

$$\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1 + b\cdot 0}{b\cdot 1} = \frac{a}{b}$$

Επειδή η πράξη πρόσθεσης «+» είναι μεταθετική, έπεται ότι το στοιχείο $\frac{0}{1}$ είναι ουδέτερο στοιχείο για την πράξη «+» της πρόσθεσης.

(δ΄) Για κάθε στοιχείο $\frac{a}{b} \in Q(R)$, το στοιχείο $\frac{-a}{b} \in Q(R)$ και θα έχουμε:

$$\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b\cdot b} = \frac{0}{b^2} = \frac{0}{1}$$

όπου η τελευταία σχέση προέκυψε διότι $0 \cdot 1 = b^2 \cdot 0$. Επειδή η πράξη πρόσθεσης «+» είναι μεταθετική, έπεται ότι το στοιχείο $\frac{-a}{b}$ είναι το αντίθετο στοιχείο του $\frac{a}{b}$ ως προς την πράξη «+» της πρόσθεσης.

(ε΄) Έστω $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(R)$. Τότε, χρησιμοποιώντας την προσεταιριστικότητα του πολλαπλασιασμού του R, θα έχουμε:

$$\left(\frac{a}{b} \cdot \frac{c}{d}\right) \cdot \frac{e}{f} = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{(ac)e}{(bd)f}$$

$$\frac{a}{b} \cdot \left(\frac{c}{d} \cdot \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{ce}{df} = \frac{a(ce)}{b(df)} = \frac{(ac)e}{(bd)f}$$

Άρα η πράξη του πολλαπλασιασμού «·» είναι προσεταιριστική.

(ϛ΄) Έστω $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(R)$. Τότε, χρησιμοποιώντας τη μεταθετικότητα του πολλαπλασιασμού του R, θα έχουμε:

$$\frac{a}{b}\cdot\frac{c}{d} = \frac{ac}{bd} = \frac{ca}{db} = \frac{c}{d}\cdot\frac{a}{b}$$

Άρα η πράξη «$\cdot$» του πολλαπλασιασμού είναι μεταθετική.

(ζ΄) Έστω $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in Q(R)$.

$$\Big(\frac{a}{b}+\frac{c}{d}\Big)\cdot\frac{e}{f} = \frac{ad+bc}{bd}\cdot\frac{e}{f} = \frac{(ad+bc)e}{bdf} = \frac{ade+bce}{bdf}$$

$$\frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f} = \frac{ae}{bf}+\frac{ce}{df} = \frac{aedf+bfce}{bdf^2} = \frac{f(aed+bce)}{f(bdf)} = \frac{aed+bce}{bdf}$$

Άρα $\big(\frac{a}{b}+\frac{c}{d}\big)\cdot\frac{e}{f} = \frac{a}{b}\cdot\frac{e}{f}+\frac{c}{d}\cdot\frac{e}{f}$, και παρόμοια δείχνουμε ότι:

$$\frac{a}{b}\cdot\Big(\frac{c}{d}+\frac{e}{f}\Big) = \frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}$$

Επομένως ισχύει η επιμεριστική ιδιότητα του πολλαπλασιασμού «$\cdot$» ως προς την πρόσθεση «$+$».

(η΄) Θεωρούμε το στοιχείο $\frac{1}{1}$, το οποίο προφανώς ανήκει στο σύνολο $Q(R)$. Τότε για κάθε στοιχείο $\frac{a}{b} \in Q(R)$, θα έχουμε:

$$\frac{a}{b}\cdot\frac{1}{1} = \frac{a\cdot 1}{b\cdot 1} = \frac{a}{b}$$

Επειδή η πράξη πολλαπλασιασμού «$\cdot$» είναι μεταθετική, έπεται ότι το στοιχείο $\frac{1}{1}$ είναι ουδέτερο στοιχείο για την πράξη «$\cdot$» του πολλαπλασιασμού.

Τα παραπάνω δείχνουν ότι η τριάδα $(Q(R),+,\cdot)$ είναι ένας μεταθετικός δακτύλιος με μονάδα το κλάσμα $\frac{1}{1}$ και μηδενικό στοιχείο το κλάσμα $\frac{0}{1}$.

Έστω $\frac{a}{b}$ ένα μη μηδενικό στοιχείο του $Q(R)$. Σημειώνουμε ότι το στοιχείο $\frac{a}{b}$ είναι μηδενικό στοιχείο, δηλαδή $\frac{a}{b} = \frac{0}{1}$, αν και μόνο αν $a\cdot 1 = b\cdot 0$, δηλαδή αν και μόνο αν $a = 0$. Άρα, αν το κλάσμα $\frac{a}{b}$ είναι μη μηδενικό, θα έχουμε ότι $a \neq 0$, δηλαδή $a \in R^*$, και επομένως ορίζεται το κλάσμα $\frac{b}{a} \in Q(R)$. Τότε θα έχουμε:

$$\frac{a}{b}\cdot\frac{b}{a} = \frac{ab}{ab} = \frac{1}{1}, \quad \text{διότι:} \quad (ab)\cdot 1 = (ab)\cdot 1$$

Επειδή η πράξη πολλαπλασιασμού «$\cdot$» είναι μεταθετική, έπεται ότι το στοιχείο $\frac{b}{a}$ είναι το αντίστροφο του μη μηδενικού στοιχείου $\frac{a}{b}$. Έτσι δείξαμε ότι κάθε μη μηδενικό στοιχείο του $Q(R)$ είναι αντιστρέψιμο, και επομένως ο μεταθετικός δακτύλιος $Q(R)$ είναι σώμα.

Θεωρούμε την απεικόνιση

$$\varphi\colon R \longrightarrow Q(R), \quad \varphi(a) = \frac{a}{1_R}$$

Τότε $\varphi(1) = \frac{1}{1} = 1_{Q(R)}$. Επιπλέον, $\forall a, c \in R$:

$$\varphi(a+c) = \frac{a+c}{1} = \frac{a}{1}+\frac{c}{1} = \varphi(a)+\varphi(c) \qquad \text{και} \qquad \varphi(ac) = \frac{ac}{1} = \frac{a}{1}\cdot\frac{c}{1} = \varphi(a)\cdot\varphi(c)$$

Άρα η απεικόνιση φ είναι ομομορφισμός δακτυλίων. Τέλος:

$$\mathsf{Ker}(\varphi) = \big\{a \in R \mid \varphi(a) = 0_{Q(R)}\big\} = \Big\{a \in R \mid \frac{a}{1} = \frac{0}{1}\Big\} = \big\{a \in R \mid a\cdot 1 = 1\cdot 0\big\} = \big\{a \in R \mid a = 0\big\} = \{0\}$$

Επομένως, ο ομομορφισμός φ είναι μονομορφισμός δακτυλίων.

2. Έστω ότι $\mathbb{K}$ είναι ένα σώμα και $g\colon R \longrightarrow \mathbb{K}$ είναι ένας μονομορφισμός δακτυλίων. Αν $b \in R^*$, δηλαδή $b \neq 0$, τότε, επειδή η απεικόνιση g είναι μονομορφισμός, θα έχουμε $\mathbb{K} \ni g(b) \neq 0$. Επειδή το $\mathbb{K}$ είναι σώμα, έπεται ότι υπάρχει το στοιχείο $g(b)^{-1} \in \mathbb{K}$. Μπορούμε τώρα να ορίσουμε απεικόνιση

$$g^*\colon Q(R) \longrightarrow \mathbb{K}, \quad g^*\big(\frac{a}{b}\big) = g(a)g(b)^{-1}$$

Η παραπάνω απεικόνιση είναι καλά ορισμένη διότι, αν $\frac{a}{b}, \frac{c}{d} \in Q(R)$, τότε:

$$\frac{a}{b} = \frac{c}{d} \implies ad = bc \implies g(ad) = g(bc) \implies g(a)g(d) = g(b)g(c) \implies$$

$$\implies g(a)g(b)^{-1} = g(c)g(d)^{-1} \implies g^*\big(\frac{a}{b}\big) = g^*\big(\frac{c}{d}\big)$$

Δείχνουμε ότι η απεικόνιση g^* είναι ομομορφισμός δακτυλίων.

(α΄) Θα έχουμε: $g^*\big(\frac{1_R}{1_R}\big) = g(1_R)g(1_R)^{-1} = 1_{\mathbb{K}}1_{\mathbb{K}}^{-1} = 1_{\mathbb{K}}$.

(β΄) Θα έχουμε:

$$g^*\big(\frac{a}{b} + \frac{c}{d}\big) = g^*\big(\frac{ad+bc}{bd}\big) = g(ad+bc)g(bd)^{-1} = \big(g(a)g(d) + g(b)g(c)\big)g(b)^{-1}g(d)^{-1} =$$

$$= g(a)g(b)^{-1}g(d)g(d)^{-1} + g(c)g(d)^{-1}g(b)g(b)^{-1} = g(a)g(b)^{-1} + g(c)g(d)^{-1} = g^*\big(\frac{a}{b}\big) + g^*\big(\frac{c}{d}\big)$$

(γ΄) Θα έχουμε:

$$g^*\big(\frac{a}{b}\cdot\frac{c}{d}\big) = g^*\big(\frac{ac}{bd}\big) = g(ac)g(bd)^{-1} = g(a)g(c)g(b)^{-1}g(d)^{-1} = g(a)g(b)^{-1}g(c)g(d)^{-1} = g^*\big(\frac{a}{b}\big)\cdot g^*\big(\frac{c}{d}\big)$$

Οι παραπάνω σχέσεις δείχνουν ότι η απεικόνιση g^* είναι ένας ομομορφισμός μεταξύ σωμάτων. Επομένως η g^* είναι μονομορφισμός, διότι κάθε μη μηδενικός ομομορφισμός ο οποίος ξεκινάει από ένα σώμα είναι μονομορφισμός. Διαφορετικά: αν $g^*(\frac{a}{b}) = 0$, τότε $g(a)g(b)^{-1} = 0$, και τότε προφανώς $g(a) = 0$. Επειδή ο ομομορφισμός g είναι μονομορφισμός, έπεται ότι $a = 0$ και τότε $\frac{a}{b} = \frac{0}{1} = 0_{Q(R)}$, και άρα ο g^* είναι μονομορφισμός. Επίσης θα έχουμε, $\forall\, a \in R$:

$$(g^* \circ \varphi)(a) = g^*(\varphi)(a)) = g^*(\big(\frac{a}{1}\big) = g(a)g(1)^{-1} = g(a)1^{-1} = g(a) \implies g^* \circ \varphi = g$$

Τέλος, αν $h\colon Q(R) \longrightarrow \mathbb{K}$ είναι ένας μονομορφισμός έτσι ώστε: $h \circ \varphi = g$, τότε $h(\varphi(a)) = h\big(\frac{a}{1}\big) = g(a)$, $\forall\, a \in R$. Έστω $\frac{a}{b} \in Q(R)$. Τότε το στοιχείο $\frac{b}{1}$ του $Q(R)$ είναι αντιστρέψιμο με αντίστροφο το στοιχείο $\frac{1}{b}$. Επειδή η απεικόνιση h είναι ομομορφισμός, η h στέλνει αντιστρέψιμα στοιχεία σε αντιστρέψιμα στοιχεία και ιδιαίτερα θα έχουμε $h\big(\frac{b}{1})^{-1}\big) = h\big(\frac{1}{b}\big)$. Χρησιμοποιώντας αυτή τη σχέση, θα έχουμε:

$$g^*\big(\frac{a}{b}\big) = g(a)g(b)^{-1} = h(\varphi(a))h(\varphi(b))^{-1} = h\big(\frac{a}{1}\big)h\big(\frac{b}{1}\big)^{-1} = h\big(\frac{a}{1}\big)h\big(\frac{1}{b}\big) = h\big(\frac{a}{1}\cdot\frac{1}{b}\big) = h\big(\frac{a}{b}\big)$$

Η παραπάνω σχέση δείχνει ότι $g^* = h$, και επομένως ο μονομορφισμός g^* είναι ο μοναδικός μονομορφισμός σωμάτων $h\colon Q(R) \longrightarrow \mathbb{K}$, έτσι ώστε $h \circ \varphi = g$.

3. Έστω ότι $\mathbb{F}$ είναι ένα σώμα και $\psi\colon R \longrightarrow \mathbb{F}$ είναι ένας μονομορφισμός δακτυλίων, έτσι ώστε για κάθε άλλο σώμα $\mathbb{K}$ και μονομορφισμό δακτυλίων $f\colon R \longrightarrow \mathbb{K}$ υπάρχει μοναδικός ομομορφισμός δακτυλίων $f^*\colon \mathbb{F} \longrightarrow \mathbb{K}$, ο οποίος είναι μονομορφισμός σωμάτων, έτσι ώστε: $f^* \circ \psi = f$. Επιλέγοντας, όπως στο μέρος 2., $\mathbb{K} = Q(R)$ και $f = \phi\colon R \longrightarrow Q(R)$, $\phi(r) = \frac{r}{1}$, έπεται ότι υπάρχει μοναδικός μονομορφισμός δακτυλίων $\phi^*\colon \mathbb{F} \longrightarrow Q(R)$, έτσι ώστε $\phi^* \circ \psi = \phi$. Από την άλλη πλευρά, όπως αποδείξαμε στο μέρος 2., έπεται ότι υπάρχει μοναδικός μονομορφισμός δακτυλίων $\psi^*\colon Q(R) \longrightarrow \mathbb{F}$, έτσι ώστε $\psi^* \circ \phi = \psi$. Τότε θα έχουμε

$$\psi^* \circ \phi = \psi \implies \psi^* \circ \phi^* \circ \psi = \psi \quad \text{και} \quad \phi^* \circ \psi = \phi \implies \phi^* \circ \psi^* \circ \phi = \phi$$

Έτσι έχουμε δύο μονομορφισμούς δακτυλίων $\psi^* \circ \phi^*$, $\mathrm{Id}_{\mathbb{F}} : \mathbb{F} \longrightarrow \mathbb{F}$, έτσι ώστε $\psi^* \circ \phi^* \circ \psi = \psi = \mathrm{Id}_{\mathbb{F}} \circ \psi$, και επομένως από τη μοναδικότητα της υπόθεσης του μέρους 3., θα έχουμε $\psi^* \circ \phi^* = \mathrm{Id}_{\mathbb{F}}$. Παρόμοια έχουμε δύο μονομορφισμούς $\phi^* \circ \psi^*$, $\mathrm{Id}_{Q(R)} : Q(R) \longrightarrow Q(R)$, έτσι ώστε $\phi^* \circ \psi^* \circ \phi = \phi = \mathrm{Id}_{Q(R)} \circ \phi$, και επομένως από το μέρος 2. θα έχουμε $\phi^* \circ \psi^* = \mathrm{Id}_{Q(R)}$. Άρα ο μονομορφισμός δακτυλίων $\phi^* : Q(R) \longrightarrow \mathbb{F}$ είναι ισομορφισμός με αντίστροφο τον ισομορφισμό δακτυλίων $\psi^* : \mathbb{F} \longrightarrow Q(R)$. ■

Ορισμός 9.4.4. *Αν R είναι μια ακέραια περιοχή, τότε το μονοσήμαντο ορισμένο, με ακρίβεια ισομορφισμού σωμάτων, σώμα $Q(R)$ καλείται το* **σώμα κλασμάτων** *της ακέραιας περιοχής R.*

Παρατηρούμε ότι το σώμα κλασμάτων μιας ακέραιας περιοχής R είναι το μικρότερο σώμα το οποίο περιέχει ως υπόσωμα την ακέραια περιοχή R:

Πόρισμα 9.4.5. *Έστω $\mathbb{F}$ ένα σώμα το οποίο περιέχει ως υποδακτύλιο μια ακέραια περιοχή R. Τότε το σώμα $\mathbb{F}$ περιέχει ως υπόσωμα ένα ισόμορφο αντίγραφο του σώματος κλασμάτων $Q(R)$ της ακέραιας περιοχής R.*

Απόδειξη. Έστω $\phi : R \longrightarrow Q(R)$, $\phi(a) = \frac{a}{1}$ ο κανονικός μονομορφισμός δακτυλίων, και έστω $\iota : R \longrightarrow \mathbb{F}$ η κανονική έγκλειση. Τότε από το Θεώρημα 9.4.3 έπεται ότι υπάρχει μοναδικός μονομορφισμός σωμάτων $\iota^* : Q(R) \longrightarrow \mathbb{F}$ έτσι ώστε $\iota^* \circ \phi = \iota$. Από το Πρώτο Θεώρημα Ισομορφισμών Δακτυλίων έπεται ότι το σώμα κλασμάτων $Q(R)$ της R είναι ισόμορφο με ένα υπόσωμα του σώματος $\mathbb{F}$: $Q(R) \cong \iota^*(Q(R)) \subseteq \mathbb{F}$. ■

Η ακόλουθη συνέπεια αποτελεί ένα χρήσιμο κριτήριο αναγνώρισης του σώματος κλασμάτων μιας ακέραιας περιοχής.

Πόρισμα 9.4.6. *Έστω R μια ακέραια περιοχή και υποθέτουμε ότι $\iota : R \longrightarrow \mathbb{K}$ είναι ένας μονομορφισμός δακτυλίων, όπου $\mathbb{K}$ είναι ένα σώμα. Αν κάθε στοιχείο x του $\mathbb{K}$ είναι της μορφής $x = \iota(a)\iota(b)^{-1}$, όπου $a, b \in R$ και $b \neq 0$, τότε το σώμα $\mathbb{K}$ είναι ισόμορφο με το σώμα κλασμάτων $Q(R)$ της ακέραιας περιοχής R.*

Απόδειξη. Θεωρούμε τον κανονικό μονομορφισμό $\phi : R \longrightarrow Q(R)$, $\phi(a) = \frac{a}{1}$ της ακέραιας περιοχής R στο σώμα κλασμάτων της $Q(R)$. Από το Θεώρημα 9.4.3 έπεται ότι υπάρχει μοναδικός μονομορφισμός δακτυλίων $\iota^* : Q(R) \longrightarrow \mathbb{K}$, έτσι ώστε $\iota^* \circ \phi = \iota$, και τότε $\iota^*(\frac{a}{b}) = \iota(a)\iota)b)^{-1}$, $\forall \frac{a}{b} \in Q(R)$. Επειδή από την υπόθεση, κάθε στοιχείο του σώματος $\mathbb{K}$ είναι της μορφής $\iota(a)\iota)b)^{-1} = \iota^*(\frac{a}{b})$, όπου $\frac{a}{b} \in Q(R)$, έπεται ότι η απεικόνιση ι^* είναι επιμορφισμός και άρα ισομορφισμός σωμάτων. ■

Παράδειγμα 9.4.7.

1. Αν $\mathbb{K}$ είναι ένα σώμα, τότε η ταυτοτική απεικόνιση $\mathrm{Id}_{\mathbb{K}} : \mathbb{K} \longrightarrow \mathbb{K}$, $\mathrm{Id}_{\mathbb{K}}(k) = k$, είναι μονομορφισμός δακτυλίων και κάθε στοιχείο $k \in \mathbb{K}$ είναι της μορφής $k = k1^{-1} = \mathrm{Id}_{\mathbb{K}}(k)\mathrm{Id}_{\mathbb{K}}(1)^{-1}$. Επομένως από το Πόρισμα 9.4.6 έπεται ότι θα έχουμε έναν ισομορφισμό σωμάτων.

$$Q(\mathbb{K}) \cong \mathbb{K}$$

2. Το σώμα κλασμάτων $Q(\mathbb{Z})$ της ακέραιας περιοχής των ακεραίων $\mathbb{Z}$ συμπίπτει προφανώς με το σώμα $\mathbb{Q}$ των ρητών αριθμών, όπως προκύπτει αμέσως από τον ορισμό του σώματος κλασμάτων μιας ακέραιας περιοχής, ή, διαφορετικά, με χρήση του Πορίσματος 9.4.6. Επομένως:

$$Q(\mathbb{Z}) = \mathbb{Q}$$

3. Θεωρούμε το σύνολο των ρητών του Gauss:

$$\mathbb{Q}(i) = \{x + yi \in \mathbb{C} \mid x, y \in \mathbb{Q}\}$$

Εύκολα βλέπουμε ότι το σύνολο $\mathbb{Q}(i)$ είναι ένας υποδακτύλιος του σώματος $\mathbb{C}$ και μάλιστα είναι ένα υπόσωμα του $\mathbb{C}$ διότι, αν $0 \neq x + yi \in \mathbb{Q}(i)$, τότε το αντίστροφό του $(x+yi)^{-1} = \frac{x}{x^2+y^2} + \frac{-y}{x^2+y^2} i$ στο σώμα $\mathbb{C}$ συμπίπτει με τον αντίστροφο του $x + yi$ στον δακτύλιο $\mathbb{Q}(i)$ διότι $\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2} \in \mathbb{Q}$, αν $x, y \in \mathbb{Q}$. Επομένως το σύνολο $\mathbb{Q}(i)$ είναι σώμα ως υπόσωμα του $\mathbb{C}$.

Θεωρούμε την απεικόνιση

$$\iota\colon \mathbb{Z}[i] \longrightarrow \mathbb{Q}(i), \quad \iota(n+mi) = n+mi$$

η οποία προφανώς είναι μονομορφισμός δακτυλίων. Έστω $x+yi \in \mathbb{Q}(i)$. Τότε $x, y \in \mathbb{Q}$ και μπορούμε να γράψουμε $x = \frac{a}{b}$ και $y = \frac{c}{d}$, όπου $a, b, c, d \in \mathbb{Z}$ και $b, d \in \mathbb{Z} \setminus \{0\}$. Τότε θα έχουμε:

$$x+yi = \frac{a}{b} + \frac{c}{d}i = \frac{ad+bci}{bd} = (ad+bci)(bd)^{-1} = \iota(ad+bci)\iota(bd)^{-1}$$

Άρα κάθε στοιχείο $x+yi$ του $\mathbb{Q}(i)$ είναι της μορφής $x+yi = \iota(ad+bci)\iota(bd)^{-1}$, όπου $ad+bci, bd \in \mathbb{Z}[i]$ και $b, d \neq 0$. Τότε από το Πόρισμα 9.4.6 έπεται ότι ο μοναδικός μονομορφισμός σωμάτων $\iota^*\colon Q(\mathbb{Z}[i]) \longrightarrow \mathbb{Q}(i)$ είναι ισομορφισμός. Επομένως

$$Q\big(\mathbb{Z}[i]\big) \cong \mathbb{Q}(i)$$

4. Θεωρούμε το υποσύνολο

$$\mathbb{Z}[\sqrt{2}] = \big\{a+b\sqrt{2} \in \mathbb{R} \mid a, b \in \mathbb{Z}\big\}$$

Τότε $1 = 0+1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Αν $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, τότε:

$$(a+b\sqrt{2})+(c+d\sqrt{2}) = (a+c)+(b+d)\sqrt{2}) \qquad \text{και} \qquad (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$$

Οι παραπάνω σχέσεις δείχνουν ότι το σύνολο $\mathbb{Z}[\sqrt{2}]$ είναι υποδακτύλιος του σώματος $\mathbb{R}$ των πραγματικών αριθμών, και ιδιαίτερα είναι ακέραια περιοχή. Θεωρούμε το υποσύνολο

$$\mathbb{Q}(\sqrt{2}) = \big\{x+y\sqrt{2} \in \mathbb{R} \mid x, y \in \mathbb{Q}\big\}$$

Όπως και παραπάνω, εύκολα βλέπουμε ότι το υποσύνολο $\mathbb{Q}(\sqrt{2})$ είναι ένας υποδακτύλιος του $\mathbb{R}$, ο οποίος προφανώς περιέχει τον υποδακτύλιο $\mathbb{Z}[\sqrt{2}]$. Επιπρόσθετα, αν $x+y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, είναι ένα μη μηδενικό στοιχείο, τότε $(x, y) \neq (0, 0)$, και επειδή $\sqrt{2} \notin \mathbb{Q}$, έπεται ότι $2y^2 - x^2 \neq 0$. Εύκολα υπολογίζουμε ότι

$$(x+y\sqrt{2})^{-1} = \frac{-x}{2y^2-x^2} + \frac{y}{2y^2-x^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

Επομένως κάθε μη μηδενικό στοιχείο $x+y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ είναι αντιστρέψιμο με αντίστροφο το αντίστροφό του στο σώμα $\mathbb{R}$. Αυτό σημαίνει ότι το υποσύνολο $\mathbb{Q}(\sqrt{2})$ είναι ένα υπόσωμα του $\mathbb{R}$ το οποίο περιέχει την ακέραια περιοχή $\mathbb{Z}[\sqrt{2}]$.

Θεωρούμε την απεικόνιση

$$\iota\colon \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{Q}(\sqrt{2}), \quad \iota(m+n\sqrt{2}) = m+n\sqrt{2}$$

η οποία προφανώς είναι μονομορφισμός δακτυλίων. Έστω $x+y\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Τότε $x, y \in \mathbb{Q}$ και μπορούμε να γράψουμε $x = \frac{a}{b}$ και $y = \frac{c}{d}$, όπου $a, b, c, d \in \mathbb{Z}$ και $b, d \in \mathbb{Z} \setminus \{0\}$. Τότε θα έχουμε:

$$x+y\sqrt{2} = \frac{a}{b} + \frac{c}{d}\sqrt{2} = \frac{ad+bc\sqrt{2}}{bd} = (ad+bc\sqrt{2})(bd)^{-1} = \iota(ad+bc\sqrt{2})\iota(bd)^{-1}$$

Άρα κάθε στοιχείο $x+y\sqrt{2}$ του $\mathbb{Q}(\sqrt{2})$ είναι της μορφής $x+y\sqrt{2} = \iota(ad+bc\sqrt{2})\iota(bd)^{-1}$, όπου $ad+bc\sqrt{2}, bd \in \mathbb{Z}[\sqrt{2}]$ και $b, d \neq 0$. Τότε από το Πόρισμα 9.4.6 έπεται ότι ο μοναδικός μονομορφισμός σωμάτων $\iota^*\colon Q(\mathbb{Z}[\sqrt{2}]) \longrightarrow \mathbb{Q}(\sqrt{2})$ είναι ισομορφισμός. Επομένως

$$Q\big(\mathbb{Z}[\sqrt{2}]\big) \cong \mathbb{Q}(\sqrt{2}) \quad \surd$$

Παρατήρηση 9.4.8. Όπως είδαμε, κάθε (μεταθετική) ακέραια περιοχή R μπορεί να εμφυτευθεί σε ένα σώμα $\mathbb{K}$, δηλαδή υπάρχει μονομορφισμός $R \longrightarrow \mathbb{K}$, όπου $\mathbb{K}$ είναι ένα σώμα, και μάλιστα με βέλτιστο τρόπο. Τι συμβαίνει αν παραλείψουμε τη μεταθετικότητα του δακτυλίου R και θεωρήσουμε μια περιοχή R, δηλαδή έναν, όχι απαραίτητα μεταθετικό, δακτύλιο χωρίς διαιρέτες του μηδενός; Το παραπάνω πρόβλημα έθεσαν οι

Kolmogorov[2] και van der Waerden[3], και η απάντηση, η οποία ήταν αρνητική, δόθηκε από τον A. Malcev[4] το 1937. Αναλυτικότερα, ο Malcev έδειξε ότι υπάρχουν μη μεταθετικοί δακτύλιοι χωρίς διαιρέτες του μηδενός, οι οποίοι δεν μπορούν να εμφυτευθούν σε έναν, κατ' ανάγκην μη μεταθετικό δακτύλιο διαίρεσης. ▲

9.5 Το Σώμα των Ρητών Συναρτήσεων

Έστω R μια ακέραια περιοχή. Από την Πρόταση 9.1.2 γνωρίζουμε ότι ο δακτύλιος πολυωνύμων $R[t_1, t_2, \cdots, t_n]$, $n \geq 1$, είναι επίσης μια ακέραια περιοχή. Επομένως ορίζεται το σώμα κλασμάτων της $Q(R[t_1, t_2, \cdots, t_n])$.

Ορισμός 9.5.1. *Αν R είναι μια ακέραια περιοχή, τότε το σώμα κλασμάτων του δακτυλίου πολυωνύμων $R[t_1, t_2, \cdots, t_n]$ συμβολίζεται με*

$$R(t_1, t_2, \cdots, t_n) = Q(R[t_1, t_2, \cdots, t_n])$$

και καλείται το **σώμα των ρητών συναρτήσεων στις n μεταβλητές** *υπεράνω της ακέραιας περιοχής R.*

Σύμφωνα με την ενότητα 9.4, τα στοιχεία του σώματος κλασμάτων $R(t_1, t_2, \cdots, t_n)$ μιας ακέραιας περιοχής R είναι κλάσματα της μορφής

$$\frac{P(t_1, t_2, \cdots, t_n)}{Q(t_1, t_2, \cdots, t_n)}, \qquad P(t_1, t_2, \cdots, t_n),\ Q(t_1, t_2, \cdots, t_n) \in R[t_1, t_2, \cdots, t_n], \quad Q(t_1, t_2, \cdots, t_n) \neq 0$$

Για παράδειγμα, το κλάσμα $\frac{t^4+3t^3-2t^2+1}{2t^3-3t^2+5t-1}$ είναι μια ρητή συνάρτηση μιας μεταβλητής υπεράνω του σώματος $\mathbb{Q}$ των ρητών, και το κλάσμα $\frac{t_1^3-2t_1^2t_2+4t_1t_2^5-5t_2^2+1}{6t_1^2t_2+\sqrt{2}t_1t_2+4t_2-1}$ είναι μια ρητή συνάρτηση δύο μεταβλητών υπεράνω του σώματος $\mathbb{R}$ των πραγματικών αριθμών.

Ο όρος ρητή συνάρτηση νοείται ως ενιαίος και όχι ως σύνθεση των όρων «ρητή» και «συνάρτηση», καθώς μια ρητή συνάρτηση δεν είναι απαραίτητα συνάρτηση. Για παράδειγμα, θεωρούμε τις ρητές συναρτήσεις

$$\frac{(t^2-4)(t+3)}{t(t-2)}, \ \frac{(t+2)(t+3)}{t} \in \mathbb{Q}(t)$$

Τα κλάσματα αυτά ορίζονται διότι τα πολυώνυμα $t(t-2)$ και t δεν είναι τα μηδενικά πολυώνυμα και στον δακτύλιο πολυωνύμων $\mathbb{Q}[t]$ ισχύει ότι: $(t^2-4)(t+3)t = (t+2)(t+3)t(t-2)$, επομένως τα κλάσματα αυτά είναι ίσα ως στοιχεία του $Q(t)$: $\frac{(t^2-4)(t+3)}{t(t-2)} = \frac{(t+2)(t+3)}{t}$. Σημειώνουμε ότι τα παραπάνω κλάσματα, αν και ονομάζονται ρητές συναρτήσεις, δεν είναι συναρτήσεις με την κλασική έννοια του όρου, π.χ. με πεδίο ορισμού το $\mathbb{Q}$, διότι η πρώτη δεν ορίζεται στα σημεία $0, 2$, και η δεύτερη στο σημείο 0.

Κλείνουμε την παρούσα ενότητα δείχνοντας ότι μια ακέραια περιοχή και το σώμα κλασμάτων της μοιράζονται το ίδιο σώμα ρητών συναρτήσεων.

Έστω $f : R \longrightarrow S$ ένας ομομορφισμός μεταξύ δακτυλίων R και S. Τότε υπάρχει το ακόλουθο μεταθετικό διάγραμμα

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & S \\ {\scriptstyle \iota_R}\downarrow & & \downarrow{\scriptstyle \iota_S} \\ R[t] & \xrightarrow{\ f^*\ } & S[t] \end{array} \tag{9.2}$$

[2]Andrey Nikolaevich Kolmogorov (25 Απριλίου 1903 - 20 Οκτωβρίου 1987) [https://en.wikipedia.org/wiki/Andrey_Kolmogorov]: Επιφανής Ρώσος μαθηματικός, με θεμελιώδη συμβολή σε ένα ευρύ φάσμα ερευνητικών περιοχών: στη Θεωρία Πιθανοτήτων, στην Ανάλυση και στην Τοπολογία, στη Λογική, στην Κλασική Μηχανική, στη Θεωρία της Πληροφορίας και Πολυπλοκότητας κλπ.

[3]Bartel Leendert van der Waerden (2 Φεβρουαρίου 1903 - 12 Ιανουαρίου 1996) [https://en.wikipedia.org/wiki/Bartel_Leendert_van_der_Waerden]: Ολλανδός μαθηματικός και ιστορικός, γνωστός κυρίως για το δίτομο έργο του *Modern Algebra* (1930, 1931) το οποίο άσκησε καθοριστική επίδραση στην εξάπλωση των ιδεών της Emmy Noether, του Emil Artin και άλλων. Είναι επίσης γνωστός για τα βιβλία ιστορίας Μαθηματικών τα οποία συνέγραψε.

[4]Anatoly Ivanovich Malcev (27 Νοεμβρίου 1909 - 7 Ιουνίου 1967) [https://en.wikipedia.org/wiki/Anatoly_Maltsev]: Ρώσος μαθηματικός, με συμβολή στην Άλγεβρα και στη Μαθηματική Λογική. Γνωστός κυρίως για την συμβολή του στην αποφασισιμότητα θεωριών διάφορων αλγεβρικών συστημάτων.

όπου f^* είναι ο μοναδικός ομομορφισμός δακτυλίων, έτσι ώστε $f^*(\mathsf{r}) = \mathsf{f}(\mathsf{r})$, $\forall r \in R$, όπου r και $\mathsf{f}(\mathsf{r})$ είναι τα σταθερά πολυώνυμα r και $f(r)$ αντίστοιχα, και $f^*(t) = t$. Προφανώς $f^*(\sum_{k=0}^n a_k t^k) = \sum_{k=0}^n f(a_k) t^k$.

Υποθέτουμε ότι ο ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$ είναι μονομορφισμός. Αν $P(t) = \sum_{k=0}^n a_k t^k \in R[t]$ είναι ένα πολυώνυμο τέτοιο ώστε $f^*(P(t)) = 0$, τότε $\sum_{k=0}^n f(a_k) t^k = 0$. Τότε εξ ορισμού του μηδενικού πολυωνύμου θα έχουμε $f(a_k) = 0$, $0 \le k \le n$. Επειδή ο ομομορφισμός f είναι μονομορφισμός, θα έχουμε $a_k = 0$, $0 \le k \le n$, δηλαδή το πολυώνυμο $P(t) = 0$. Έτσι $\mathsf{Ker}(f^*) = \{0\}$ και επομένως ο ομομορφισμός f^* είναι μονομορφισμός. Έτσι αποδείξαμε την ακόλουθη βοηθητική Πρόταση:

Λήμμα 9.5.2. *Κάθε ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$, επεκτείνεται σε έναν ομομορφισμό δακτυλίων $f^*\colon R[t] \longrightarrow S[t]$, έτσι ώστε το διάγραμμα ομομορφισμών δακτυλίων (9.2) είναι μεταθετικό. Επιπρόσθετα, αν ο ομομορφσιμός f είναι μονομορφισμός, τότε ο ομομορφισμός f^* είναι μονομορφισμός.*

Υποθέτουμε τώρα ότι οι δακτύλιοι R και S είναι ακέραιες περιοχές, και ο ομομορφισμός δακτυλίων $f\colon R \longrightarrow S$ είναι μονομορφισμός.

Θεωρούμε τα σώματα κλασμάτων $Q(R[t]) = R(t)$ και $Q(S[t]) = S(t)$ των ακέραιων περιοχών R και S αντίστοιχα, και έστω $\phi_R\colon R[t] \longrightarrow R(t)$, $\phi_R(P(t)) = \frac{P(t)}{1}$ και $\phi_S\colon S[t] \longrightarrow S(t)$, $\phi_S(P(t)) = \frac{P(t)}{1}$, οι κανονικοί μονομορφισμοί. Η σύνθεση $\phi_S \circ f^*\colon R[t] \longrightarrow S(t)$ είναι τότε μονομορφισμός δακτυλίων, και άρα από το Θεώρημα 9.4.3, έπεται ότι ο μονομορφισμός δακτυλίων $\phi_S \circ f^*\colon R[t] \longrightarrow S(t)$ επεκτείνεται μοναδικά σε έναν μονομορφισμό σωμάτων $\widetilde{f}\colon Q(R[t]) = R(t) \longrightarrow Q(S[t]) = S(t)$, έτσι ώστε το ακόλουθο διάγραμμα να είναι μεταθετικό:

$$\begin{array}{ccc} R[t] & \xrightarrow{\quad f^* \quad} & S[t] \\ {\scriptstyle \phi_R}\downarrow & & \downarrow{\scriptstyle \phi_S} \\ R(t) & \xrightarrow{\quad \widetilde{f} \quad} & S(t) \end{array} \tag{9.3}$$

Η επόμενη Πρόταση δείχνει ότι για κάθε ακέραια περιοχή R ισχύει ότι: $Q(R)(t) \cong Q(R[t]) = R(t)$.

Πρόταση 9.5.3. *Έστω R μια ακέραια περιοχή, και $Q(R)$ το σώμα κλασμάτων της. Τότε υπάρχει μοναδικός ισομορφισμός σωμάτων*

$$\widetilde{\iota}\colon\ R(t) \xrightarrow{\ \cong\ } Q(R)(t)$$

έτσι ώστε το ακόλουθο διάγραμμα μονομορφισμών δακτυλίων να είναι μεταθετικό:

$$\begin{array}{ccc} R[t] & \xrightarrow{\quad \iota^* \quad} & Q(R)[t] \\ {\scriptstyle \phi_R}\downarrow & & \downarrow{\scriptstyle \phi_{Q(R)}} \\ R(t) & \xrightarrow[\quad \widetilde{\iota} \quad]{\ \cong\ } & Q(R)(t) \end{array} \tag{9.4}$$

Απόδειξη. Θέτοντας στο Λήμμα 9.5.2, $f = \iota\colon R \longrightarrow Q(R) = S$, έπεται ότι υπάρχει μοναδικός μονομορφισμός σωμάτων $\iota^*\colon R(t) \longrightarrow Q(R)(t)$, έτσι ώστε το αντίστοιχο του διαγράμματος (9.2) να είναι μεταθετικό. Θεωρώντας τον μονομορφισμό $\phi_{Q(R)} \circ \iota^*\colon R[t] \longrightarrow Q(R)(t)$, από το Θεώρημα 9.4.3 έπεται ότι υπάρχει μοναδικός μονομορφισμός δακτυλίων $\widetilde{\iota}\colon R(t) \longrightarrow Q(R)(t)$, έτσι ώστε το διάγραμμα μονομορφισμών δακτυλίων (9.4) να είναι μεταθετικό. Αρκεί να δείξουμε ότι ο μονομορφισμός $\widetilde{\iota}$ είναι επιμορφισμός. Από το Θεώρημα 9.4.3 έπεται ότι

$$\widetilde{\iota}\Big(\frac{P(t)}{Q(t)}\Big) = (\phi^*_{Q(R)} \circ \iota)(P(t))((\phi^*_{Q(R)} \circ \iota)(Q(t)))^{-1} = \frac{\iota(P(t))}{1}\big(\frac{\iota(Q(t))}{1}\big)^{-1} = \frac{\frac{P(t)}{1}}{1}\Big(\frac{\frac{Q(t)}{1}}{1}\Big)^{-1} = \frac{P(t)}{Q(t)} = P(t)Q(t)^{-1}$$

Έστω $\frac{A(t)}{B(t)} \in Q(R)(t)$, όπου $A(t), B(t) \in Q(R)[t]$, $B(t) \neq 0$. Τότε

$$A(t) = \frac{\frac{a_0}{b_0} + \frac{a_1}{b_1}t + \cdots + \frac{a_n}{b_n}t^n}{\frac{c_0}{d_0} + \frac{c_1}{d_1}t + \cdots + \frac{c_m}{d_m}t^m} \qquad \text{και} \qquad B(t) = \frac{\frac{r_0}{s_0} + \frac{r_1}{s_1}t + \cdots + \frac{r_k}{s_k}t^k}{\frac{x_0}{y_0} + \frac{x_1}{y_1}t + \cdots + \frac{x_l}{y_l}t^l}$$

όπου τα στοιχεία $a_i, b_i, c_i, d_i, r_i, s_i, x_i, y_i$ ανήκουν στην ακέραια περιοχή R και τα στοιχεία b_i, d_i, s_i, y_i είναι μη μηδενικά. Επειδή ο δακτύλιος R είναι ακέραια περιοχή, έπεται ότι τα στοιχεία $\beta = b_0 \cdot b_1 \cdots b_n$, $\delta = d_0 \cdot d_1 \cdots d_m$, $\sigma = s_0 \cdot s_1 \cdots s_k$, και $\psi = y_0 \cdot y_1 \cdots y_l$ είναι επίσης μη μηδενικά. Τότε μπορούμε να γράψουμε :

$$A(t) = \frac{\frac{a_0\beta_0 + a_1\beta_1 t + \cdots + a_n\beta_n t^n}{\beta}}{\frac{d_0\delta_0 + d_1\delta_1 t + \cdots + d_m\delta_m t^m}{\delta}} = \frac{\delta a_0\beta_0 + \delta a_1\beta_1 t + \cdots + \delta a_n\beta_n t^n}{\beta d_0\delta_0 + \beta d_1\delta_1 t + \cdots + \beta d_m\delta_m t^m} = \frac{C(t)}{D(t)} \in R(t)$$

$$B(t) = \frac{\frac{r_0\sigma_0 + r_1\sigma_1 t + \cdots + r_k\sigma_k t^k}{\sigma}}{\frac{x_0\psi_0 + x_1\psi_1 t + \cdots + x_l\psi_l t^l}{\psi}} = \frac{\psi r_0\sigma_0 + \psi r_1\sigma_1 t + \cdots + \psi r_k\sigma_k t^k}{\sigma x_0\psi_0 + \sigma x_1\psi_1 t + \cdots + \sigma x_l\psi_l t^l} = \frac{E(t)}{F(t)} \in R(t)$$

όπου $\beta_i, \delta_i, \sigma_i, \psi_i$ συμβολίζουν τα γινόμενα $\beta, \delta, \sigma, \psi$, έχοντας παραλείψει τους παράγοντες b_i, d_i, s_i, y_i, αντίστοιχα. Επομένως θα έχουμε

$$Q(R)(t) \ni \frac{A(t)}{B(t)} = \frac{\frac{C(t)}{D(t)}}{\frac{E(t)}{F(t)}} = \frac{C(t)F(t)}{D(t)E(t)} = P(t)Q(t)^{-1} = \widetilde{\iota}\Big(\frac{P(t)}{Q(t)}\Big)$$

όπου θέσαμε $P(t) = C(t)F(t)$ και $Q(t) = D(t)E(t)$. Η παραπάνω σχέση δείχνει ότι ο μονομορφισμός $\widetilde{\iota}\colon R(t) \longrightarrow Q(R)(t)$ είναι επιμορφισμός και άρα είναι ισομορφισμός σωμάτων. ■

Για παράδειγμα, επειδή $\mathbb{Q} = Q(\mathbb{Z})$, έπεται ότι τα σώματα κλασμάτων $\mathbb{Z}(t)$ και $\mathbb{Q}(t)$ είναι ισόμορφα.

Τυπικές Δυναμοσειρές Laurent

Θα προσδιορίσουμε το σώμα κλασμάτων της ακέραιας περιοχής $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω ενός σώματος $\mathbb{K}$.

Λήμμα 9.5.4. *Έστω R μια ακέραια περιοχή. Τότε ο δακτύλιος $R[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του R είναι ακέραια περιοχή.*

Απόδειξη. Έστω $P(t) = \sum_{k=0}^{\infty} a_k t^k$ και $Q(t) = \sum_{k=0}^{\infty} b_k t^k$ δύο τυπικές δυναμοσειρές, και έστω ότι $P(t)Q(t) = 0$. Υποθέτοντας ότι $P(t) \neq 0$, θα δείξουμε ότι $Q(t) = 0$. Υπενθυμίζουμε ότι

$$P(t)Q(t) = \sum_{k=0}^{\infty} c_k t^k, \qquad c_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad k \geq 0$$

Επομένως από την υπόθεση θα έχουμε:

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = 0, \quad \forall k \geq 0$$

Επειδή $P(t) \neq 0$, κάποιος από τους συντελεστές $a_i \neq 0$. Έστω k ο μικρότερος ακέραιος ≥ 0 έτσι ώστε $a_k \neq 0$. Τότε $a_i = 0$, $0 \leq i \leq k-1$. Επειδή $c_k = \sum_{i=1}^{k} a_i b_{k-i} = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = 0$, θα έχουμε $a_k b_0 = 0$. Επειδή ο δακτύλιος R είναι ακέραια περιοχή και $a_k \neq 0$, έπεται ότι $b_0 = 0$.

Επαγωγική Υπόθεση: Υποθέτουμε ότι $b_i = 0$, όπου $0 \leq i \leq l$ και $l \geq 1$. Θα δείξουμε ότι $b_{l+1} = 0$.

Επειδή $c_{k+l+1} = \sum_{i=0}^{k+l+1} a_i b_{k-i} = a_0 b_{k+l+1} + a_1 b_{k+l} + \cdots + a_{k-1} b_{l+2} + a_k b_{l+1} = 0$, και επειδή $a_i = 0$, $0 \leq i \leq k-1$ και $b_i = 0$, $0 \leq i \leq l$, έπεται ότι θα έχουμε $a_k b_{l+1} = 0$. Επειδή $a_k \neq 0$ και ο δακτύλιος R είναι ακέραια περιοχή, έπεται ότι $b_{l+1} = 0$.

Επομένως από την Αρχή Μαθηματικής Επαγωγής έπεται ότι $b_i = 0$, $\forall i \geq 0$ και επομένως $Q(t) = \sum_{k=0}^{\infty} b_k t^k = 0$.

Άρα ο δακτύλιος $R[\![t]\!]$ είναι μια ακέραια περιοχή. ■

Επομένως, για κάθε ακέραια περιοχή R, ο δακτύλιος των τυπικών δυναμοσειρών $R[\![t]\!]$ είναι μια ακέραια περιοχή, και ως τέτοια διαθέτει ένα σώμα κλασμάτων:

Ορισμός 9.5.5. *Για κάθε ακέραια περιοχή R, το σώμα κλασμάτων της ακέραιας περιοχής $R[\![t]\!]$ συμβολίζεται με*

$$Q(R[\![t]\!]) = R((t))$$

και καλείται το **σώμα των τυπικών δυναμοσειρών Laurent**[5] *υπεράνω του R.*

Θα δείξουμε ότι, αν $\mathbb{K}$ είναι ένα σώμα, τότε καθε στοιχείο $P(t)$ του σώματος $R((t))$ είναι της μορφής

$$P(t) = \sum_{k=-n}^{\infty} a_k t^k, \quad \text{για κάποιο} \quad n \geq 0$$

Έστω το σύνολο

$$\mathscr{U} = \{P(t) = \sum_{k=-n}^{\infty} a_k t^k \quad \text{για κάποιο} \quad n = n_{P(t)} \geq 0\}$$

το οποίο είναι εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» τυπικών δυναμοσειρών.

Πρόταση 9.5.6. *Έστω $\mathbb{K}$ ένα σώμα. Τότε η τριάδα $(\mathscr{U}, +, \cdot)$ είναι σώμα το οποίο είναι ισόμορφο με το σώμα $\mathbb{K}((t))$ των τυπικών δυναμοσειρών Laurent υπεράνω του $\mathbb{K}$.*

Απόδειξη. Εύκολα βλέπουμε ότι το σύνολο $\mathscr{U}$, εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» τυπικών δυναμοσειρών, είναι σώμα με μονάδα την τυπική δυναμοσειρά $1 = 1+0+0+\cdots$. Δείχνουμε μόνο ότι κάθε μη μηδενικό στοιχείο του $\mathscr{U}$ είναι αντιστρέψιμο. Έστω $0 \neq P(t) = \sum_{k \geq n_{P(t)}}^{\infty} a_k t^k$ ένα στοιχείο του $\mathscr{U}$, όπου $n_{P(t)} \in \mathbb{Z}$. Προφανώς μπορούμε να διαλεξουμε το $n_{P(t)}$ να είναι ο μικρότερος ακέραιος με την ιδιότητα $a_{n_{P(t)}} \neq 0$. Επειδή το $\mathbb{K}$ είναι σώμα, υπάρχει το αντίστροφο $a_{n_{P(t)}}^{-1} \in \mathbb{K}$. Ορίζουμε ένα στοιχείο του συνόλου $\mathscr{U}$, ως εξής: $Q(t) = \sum_{k \geq -n_{P(t)}}^{\infty} b_k t^k$, όπου τα στοιχεία b_k, $\forall k \geq -n_{P(t)}$, ορίζονται επαγωγικά ως εξής:

$$b_{-n_{P(t)}} = a_{n_{P(t)}}^{-1}, \qquad b_{k+1} = -a_{n_{P(t)}}^{-1} \sum_{l=k}^{k+n_{P(t)}+1} a_{k+n_{P(t)}+1-l} b_l, \quad \forall k \geq -n_{P(t)}$$

Τότε εύκολα βλέπουμε ότι $P(t)Q(t) = 1 = 1+0+0+\cdots$ και άρα $P(t)^{-1} = Q(t)$ στο σώμα $\mathscr{U}$. Για το μη μηδενικό στοιχείο $P(t)$ όπως παραπάνω παρατηρούμε ότι, αν $n_{P(t)} \geq 0$, τότε $P(t) \in \mathbb{K}[\![t]\!]$. Έστω ότι $n_{P(t)} < 0$. Τότε από τον υπολογισμό του αντίστροφου στοιχείου $P(t)^{-1}$ έπεται ότι θα έχουμε $P(t)^{-1} \in \mathbb{K}[\![t]\!]$.

Προφανώς η κανονική έγκλειση $\iota \colon \mathbb{K}[\![t]\!] \longrightarrow \mathscr{U}$, $\iota(P(t)) = P(t)$, όπου η τυπική δυναμοσειρά $P(t)$ θεωρείται ως στοιχείο του $\mathscr{U}$, είναι ένας μονομορφισμός δακτυλίων. Από το Θεώρημα 9.4.3, έπεται ότι υπάρχει μοναδικός μονομορφισμός σωμάτων

$$\iota^* \colon Q(\mathbb{K}[\![t]\!]) = \mathbb{K}((t)) \longrightarrow \mathscr{U}, \quad \iota^*\Big(\frac{P(t)}{Q(t)}\Big) = P(t)Q(t)^{-1}$$

Έστω $P(t) \in \mathscr{U}$. Αν $n_{P(t)} \geq 0$, τότε $P(t) \in \mathbb{K}[\![t]\!]$, και τότε $\iota^*(P(t)) = \iota^*(\frac{P(t)}{1}) = P(t)$. Αν $n_{P(t)} < 0$, τότε όπως είδαμε παραπάνω $P(t)^{-1} \in \mathbb{K}[\![t]\!]$, και άρα $\frac{1}{P(t)^{-1}} \in \mathbb{K}((t))$. Τότε θα έχουμε $\iota^*(\frac{1}{P(t)^{-1}}) = 1(P(t)^{-1})^{-1} = 1P(t) = P(t)$. Επομένως ο μονομορφισμός σωμάτων ι^* είναι επιμορφισμός και άρα είναι ισομορφισμός. ■

Παρατήρηση 9.5.7. Τα παραπάνω αποτελέσματα γενικεύονται εύκολα, με χρήση της Αρχής Μαθηματικής Επαγωγής, και για σώματα ρητών συναρτήσεων $R(t_1, t_2, \cdots, t_n)$ πολλών μεταβλητών, υπεράνω μιας ακέραιας περιοχής R. Η διατύπωση και περαιτέρω ανάλυσή τους αφήνεται στον αναγνώστη.

Σημειώνουμε ότι σώματα ρητών συναρτήσεων της μορφής $\mathbb{K}(t_1, t_2, \cdots, t_n)$, όπου $\mathbb{K}$ είναι ένα σώμα, διαδραματίζουν σημαντικό ρόλο στην Αλγεβρική Γεωμετρία. ▲

[5] Pierre Alphonse Laurent (18 Ιουλίου 1813 - 2 Σεπτεμβρίου 1854) [https://en.wikipedia.org/wiki/Pierre_Alphonse_Laurent]: Γάλλος μαθηματικός, γνωστός κυρίως για την ανακάλυψη των σειρών που φέρουν το όνομά του.

9.6 Ασκήσεις

Άσκηση 9.6.1. *Να εξεταστεί αν ο δακτύλιος πηλίκο $\mathbb{C}[t]/(t^2+2)$ είναι ακέραια περιοχή.*

Άσκηση 9.6.2. *Θεωρούμε του δακτύλιο πολυωνύμων $\mathbb{Q}[t]$ και το κύριο ιδεώδες $(P(t))$ το οποίο παράγεται από το πολυώνυμο $P(t)=t^3+3t-2$. Να δειχθεί ότι ο δακτύλιος πηλίκο $\mathbb{R}[t]/(P(t))$ είναι σώμα.*

Άσκηση 9.6.3. *Να δειχθεί ότι:*

1. *το πολυώνυμο $P(t)=t^2+t+1\in\mathbb{Z}_2[t]$ είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_2$.*
2. *το πολυώνυμο $P(t)=t^2+1\in\mathbb{Z}_7[t]$ είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_7$.*
3. *το πολυώνυμο $P(t)=t^3-9\in\mathbb{Z}_{31}[t]$ είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_{31}$.*
4. *το πολυώνυμο $P(t)=t^3-9\in\mathbb{Z}_{11}[t]$ δεν είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_{11}$.*

Άσκηση 9.6.4. *Να δειχθεί ότι το πολυώνυμο $P(t)=t^3+t^2+1\in\mathbb{Z}_3[t]$ είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_3$ και ακολούθως να δειχθεί ότι ο δακτύλιος πηλίκο $\mathbb{Z}_3[t]/(P(t))$ είναι ένα σώμα με 8 στοιχεία.*

Άσκηση 9.6.5. *Έστω R ένας μεταθετικός δακτύλιος ο οποίος δεν περιέχει μη μηδενικά μηδενοδύναμα στοιχεία. Να δειχθεί ότι[6] ένα στοιχείο $P(t)\in R[t]$ είναι διαιρέτης του μηδενός αν και μόνο αν υπάρχει $0\neq a\in R$: $aP(t)=0$.*

Άσκηση 9.6.6. *Στον δακτύλιο πολυωνύμων $\mathbb{Z}[t]$ να δειχθεί ότι $(2)\cap(t)=(2t)$. Ισχύει ότι $(p)\cap(t)=(pt)$ (όπου p: πρώτος); Ισχύει ότι $(n)\cap(t)=(nt)$ (όπου $n\in\mathbb{N}$);*

Άσκηση 9.6.7. *Έστω ότι $\mathbb{K}$ είναι ένα σώμα και $a,b\in\mathbb{K}$, όπου $a\neq 0$. Να δειχθεί ότι ένα πολυώνυμο $P(t)\in\mathbb{K}[t]$ είναι ανάγωγο αν και μόνο αν το πολυώνυμο $P(at+b)$ είναι ανάγωγο.*

Άσκηση 9.6.8.

1. *Να εξεταστεί αν τα ακόλουθα πολυώνυμα είναι ανάγωγα*

$$t^2+1\in\mathbb{Z}_3[t] \quad \text{και} \quad Q(t)=t^3+t+2\in\mathbb{Z}_5[t]$$

2. *Να δειχθεί ότι για κάθε $a\in\mathbb{Z}_5$, το πολυώνυμο $P(t)=t^4+at+1\in\mathbb{Z}_5[t]$ δεν είναι ανάγωγο υπεράνω του σώματος $\mathbb{Z}_5$.*
3. *Να δειχθεί ότι τα ακόλουθα πολυώνυμα του $\mathbb{Z}_3[t]$*

$$P(t)=t^5+t^3+t \quad \text{και} \quad Q(t)=t^5+2t$$

ορίζουν την ίδια πολυωνυμική συνάρτηση υπεράνω του $\mathbb{Z}_3$.

Άσκηση 9.6.9. *Έστω ότι R είναι ένας μεταθετικός δακτύλιος και ότι I είναι ένα ιδεώδες του R. Να δειχθεί ότι το σύνολο*

$$I^*=\left\{\sum_{k=0}^{n}a_kt^k\in R[t]\mid a_0\in I\right\}$$

είναι ένα ιδεώδες του $R[t]$ και να προσδιοριστεί ο δακτύλιος πηλίκο $R[t]/I^*$.

[6] Το αποτέλεσμα της Άσκησης ισχύει για κάθε μεταθετικό δακτύλιο.

Άσκηση 9.6.10. *Αν R και S είναι δύο μεταθετικοί δακτύλιοι, να δειχθεί ότι:*[7]

$$R \cong S \quad \Longrightarrow \quad R[t] \cong S[t] \quad \Longrightarrow \quad R(t) \cong S(t)$$

Άσκηση 9.6.11. *Έστω $\mathbb{F}$ ένα σώμα. Να δειχθεί ότι οι δακτύλιοι $\mathbb{F}[t]/(t^2)$ και $\mathbb{F}[t]/(t^2-1)$ είναι ισόμορφοι αν και μόνο αν $\mathsf{char}(\mathbb{F}) = 2$.*

Άσκηση 9.6.12. *Να δειχθεί ότι:*

$$Q(\mathbb{Z}[i]) \xrightarrow{\cong} \mathbb{Q}[i]$$

Άσκηση 9.6.13 (Κριτήριο του Eisenstein)**.** [8] *Έστω $P(t) \in \mathbb{Z}[t]$ ένα πολυώνυμο με ακέραιους συντελεστές, όπου $P(t) = a_0 + a_1 t + \cdots + a^n t^n$. Υποθέτουμε ότι υπάρχει ένας πρώτος αριθμός p έτσι ώστε:*

$$p \nmid a_n, \quad p \mid a_0, \quad p \mid a_1, \quad \cdots, \quad p \mid a_{n-1}, \quad p^2 \nmid a_0$$

Να δειχθεί ότι το πολυώνυμο $P(t)$ είναι ανάγωγο υπεράνω του σώματος $\mathbb{Q}$ των ρητών.

Άσκηση 9.6.14. *Αν p είναι ένας πρώτος αριθμός, να δειχθεί ότι το πολυώνυμο $P(t) = t^n - p \in \mathbb{Z}[t]$, $n \geq 2$, είναι ανάγωγο υπεράνω του σώματος των ρητών.*

Άσκηση 9.6.15. *Έστω ότι ο ρητός αριθμός $\frac{m}{n} \in \mathbb{Q}$, όπου $(m,n) = 1$, είναι ρίζα ενός πολυωνύμου $P(t) == a_0 + a_1 t + \cdots + a_k t^k \in \mathbb{Z}[t]$. Να δειχθεί ότι: $m \mid a_0$ και $n \mid a_k$.*

Άσκηση 9.6.16. *Έστω ότι ο ρητός αριθμός $q \in \mathbb{Q}$, είναι ρίζα ενός μονικού πολυωνύμου $P(t) \in \mathbb{Z}[t]$. Να δειχθεί ότι ο ρητός αριθμός q είναι ακέραιος.*

Άσκηση 9.6.17. *Να δειχθεί ότι το σώμα κλασμάτων της ακέραιας περιοχής $\mathbb{Q}^{(p)}$ της Άσκησης 8.5.66 συμπίπτει με το σώμα $\mathbb{Q}$ των ρητών.*

Παρατηρούμε ότι $Q(\mathbb{Q}^{(p)}) \cong \mathbb{Q} \cong Q(\mathbb{Z})$, αλλά $\mathbb{Z} \ncong \mathbb{Q}^{(p)}$, δηλαδή υπάρχουν μη ισόμορφες ακέραιες περιοχές με ισόμορφα σώματα κλασμάτων.

Άσκηση 9.6.18. *Έστω R ένας μεταθετικός δακτύλιος και $a \in R$. Θεωρούμε του δακτύλιο*

$$\overline{R} = R[t]/(at-1)$$

Να δειχθεί ότι το στοιχείο $a + (at-1)$ είναι αντιστρέψιμο στον δακτύλιο $\overline{R}$ και αν

$$f\colon R \longrightarrow \overline{R}, \quad f(r) = r + (at-1)$$

να δειχθεί ότι

$$\mathsf{Ker}(f) = \left\{ r \in R \mid \exists n \in \mathbb{N}\colon\ a^n r = 0 \right\}$$

Με ποιον δακτύλιο συμπίπτει ο δακτύλιος $\overline{R}$ αν το στοιχείο a είναι μηδενοδύναμο;

---

[7] Υπάρχουν παραδείγματα μη ισόμορφων μεταθετικών δακτυλίων R και S, έτσι ώστε $R[t] \cong S[t]$, βλέπε το άρθρο του M. Hochster, *Nonuniqueness of coefficient rings in a polynomial ring*, Proc. Amer. Math. Soc. **34** (1972), 81–82.

Σύμφωνα με την Άσκηση 9.6.17, υπάρχουν παραδείγματα μη ισόμορφων μεταθετικών δακτυλίων R και S, έτσι ώστε $R(t) \cong S(t)$. Έτσι οι συνεπαγωγές της παρούσας Άσκησης δεν είναι αναστρέψιμες.

[8] Ferdinand Gotthold Max Eisenstein (16 Απριλίου 1823 - 11 Οκτωβρίου 1852) [https://en.wikipedia.org/wiki/Gotthold_Eisenstein]: Γερμανός μαθηματικός με συμβολή στη Θεωρία Αριθμών και στην Ανάλυση. Γνωστός κυρίως για το παρόν κριτήριο που φέρει το όνομά του, καθώς και για τις ομώνυμες σειρές.

Άσκηση 9.6.19. *Στην Άσκηση 9.6.18 θέτουμε $R = \mathbb{F}[t]$, όπου $\mathbb{F}$ είναι ένα σώμα, και $a = t$. Τότε ο δακτύλιος $\overline{R} = \mathbb{F}[t,x]/(xt-1)$ είναι ισόμορφος με τον δακτύλιο $\mathbb{F}[t,t^{-1}]$ των* **πολυωνύμων Laurent** *τα στοιχεία του οποίου είναι πολυώνυμα στις μεταβλητές t και t^{-1}, δηλαδή της μορφής*

$$P(t) = \sum_{k=-n}^{n} a_k t^k$$

Άσκηση 9.6.20. *Ποιο είναι το σώμα κλασμάτων ενός σώματος;*

Η επόμενη άσκηση έχει ως στόχο την κατασκευή του δακτυλίου τοπικοποίησης $R[S^{-1}]$ ενός μεταθετικού δακτυλίου R ως προς ένα πολλαπλασιαστικό σύνολο S μη μηδενικών στοιχείων του R το οποίο είναι κλειστό στον πολλαπλασιασμό του R. Η κατασκευή αυτή γενικεύει την κατασκευή του σώματος κλασμάτων μιας ακέραιας περιοχής.

Ένα υποσύνολο $S \subseteq R^* = R \setminus \{0\}$ καλείται **πολλαπλασιαστικό σύνολο** αν:

$$1_R \in S \quad \text{και} \quad \forall a,b \in S: \quad ab \in S$$

Άσκηση 9.6.21. *Έστω R ένας μεταθετικός δακτύλιος και $S \subseteq R^*$ ένα πολλαπλασιαστικό υποσύνολο του R. Στο σύνολο $R \times S$ ορίζουμε μια σχέση «$\sim$» ως εξής, $\forall (a,s),(b,t) \in R \times S$:*

$$(a,s) \sim (b,t) \iff \exists\, u \in S: \ u(at-bs) = 0$$

1. *Να δειχθεί ότι η σχέση «$\sim$» είναι μια σχέση ισοδυναμίας επί του συνόλου $R \times S$.*

   Συμβολίζουμε με $a/s = [(a,s)]_\sim$ την κλάση ισοδυναμίας του στοιχείου (a,s) και με $R[S^{-1}]$ το σύνολο πηλίκο $(R \times S)/\sim$, δηλαδή

$$a/s = \{(b,t) \in R \times S \mid (a,s) \sim (b,t)\} = \{(b,t) \in R \times S \mid \exists u \in S: \ u(at-bs) = 0\}$$

$$R[S^{-1}] = \{a/s \subseteq R \times S \mid a \in R,\ s \in S\}$$

2. *Ορίζοντας πράξεις πρόσθεσης και πολλαπλασιασμού στο σύνολο πηλίκο $R[S^{-1}]$ ως εξής, $\forall a/s, b/t \in R[S^{-1}]$:*

$$a/s + b/t = (at+bs)/st \quad \text{και} \quad a/s \cdot b/t = ab/st$$

   να δειχθεί ότι η τριάδα $(R[S^{-1}], +, \cdot)$ είναι ένας μεταθετικός δακτύλιος με μηδενικό στοιχείο $0_{R[S^{-1}]} = 0_R/1_R$ και μονάδα $1_{R[S^{-1}]} = 1_R/1_R$.

3. *Να δειχθεί ότι η απεικόνιση*

$$\phi\colon R \longrightarrow R[S^{-1}], \quad \phi(a) = a/1_R$$

   είναι ένας ομομορφισμός δακτυλίων.

4. *Ο ομομορφισμός δακτυλίων ϕ είναι μονομορφισμός αν και μόνο αν κανένα στοιχείο του S δεν είναι διαιρέτης του μηδενός.*

5. *Να δειχθεί ότι κάθε στοιχείο της μορφής $s/1_R$, $s \in S$, είναι αντιστρέψιμο στοιχείο του $R[S^{-1}]$.*

Ο δακτύλιος $R[S^{-1}]$ καλείται ο **δακτύλιος τοπικοποίησης** του μεταθετικού δακτυλίου R ως προς το πολλαπλασιαστικό σύνολο $S \subseteq R$. Για παράδειγμα, αν $R = \mathbb{Z}$ και $S = \mathbb{Z} \setminus \{0\}$, τότε $\mathbb{Z}[(\mathbb{Z} \setminus \{0\})^{-1}] = \mathbb{Q}$.

Άσκηση 9.6.22. *Αν R είναι μια ακέραια περιοχή και $S = R^*$, να δειχθεί ότι ο δακτύλιος τοπικοποποίησης $R[S^{-1}]$ συμπίπτει με το σώμα κλασμάτων της R.*

Άσκηση 9.6.23. *Έστω R ένας μεταθετικός δακτύλιος και S είναι το σύνολο όλων των στοιχείων του R τα οποία δεν είναι διαιρέτες του μηδενός.*

1. *Να δειχθεί ότι το S είναι πολλαπλασιαστικό υποσύνολο του R.*
2. *Ο δακτύλιος τοπικοποίησης $R[S^{-1}]$ του R ως προς το S καλείται ο* **ολικός δακτύλιος κλασμάτων** *του R και συμβολίζεται με $Q(R)$.*
3. *Ο ολικός δακτύλιος κλασμάτων $Q(R)$ είναι σώμα αν και μόνο αν ο δακτύλιος R είναι ακέραια περιοχή.*

Άσκηση 9.6.24. *Έστω R ένας μεταθετικός δακτύλιος και a ένα στοιχείο του R το οποίο δεν είναι διαιρέτης του μηδενός. Έστω $S = \{1, a, a^2, \cdots, a^n, \cdots, \}$. Να δειχθεί ότι το S είναι ένα πολλαπλασιαστικό σύνολο και υπάρχει ένας ισομορφισμός δακτυλίων*

$$R[S^{-1}] \xrightarrow{\cong} R[t]/(at-1)$$

Άσκηση 9.6.25. *Έστω R ένας μεταθετικός δακτύλιος και S είναι ένα πολλαπλασιαστικό σύνολο του R έτσι ώστε $0 \notin S.$, Να δειχθεί ότι, αν ο δακτύλιος R είναι περιοχή κυρίων ιδεωδών, τότε και ο δακτύλιος τοπικοποίησης $R[S^{-1}]$ είναι περιοχή κυρίων ιδεωδών.*

Κεφάλαιο 10

Πρώτα και Μεγιστοτικά Ιδεώδη

Στο παρόν Κεφάλαιο θα μελετήσουμε ειδικούς τύπους ιδεωδών σε έναν δακτύλιο και την επίδραση που έχουν οι επιπλέον ιδιότητες τις οποίες ικανοποιούν τα ιδεώδη αυτά στους επαγόμενους δακτύλιους πηλίκα. Θα επικεντρωθούμε στην ανάλυση των βασικών ιδιοτήτων δύο σημαντικών κλάσεων ιδεωδών, των *πρώτων* και των *μεγιστοτικών* ιδεωδών ενός δακτυλίου, και θα προσδιορίσουμε τα πρώτα και μεγιστοτικά ιδεώδη σε διάφορες κλάσεις δακτυλίων. Γενικά η δομή των πρώτων ή/και των μεγιστοτικών ιδεωδών είναι πολύ πιο πλούσια στην περίπτωση των μεταθετικών δακτυλίων, έτσι θα επικεντρώσουμε τη μελέτη μας στο πλαίσιο των μεταθετικών δακτυλίων.

Θεωρούμε τον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων του Gauss, και έστω τα κύρια ιδεώδη του

$$(2+i) \quad \text{και} \quad (1+5i) \quad \text{και} \quad (0)$$

τα οποια παράγονται από τα στοιχεία του $2+i$, $1+5i$, και 0. Στο παράδειγμα 8.4.6 είδαμε ότι:

$$\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5 \quad \text{και} \quad \mathbb{Z}[i]/(1+5i) \cong \mathbb{Z}_{26} \quad \text{και} \quad \mathbb{Z}[i]/(0) \cong \mathbb{Z}[i]$$

Ας δούμε κάποιες διαφορές στα παραπάνω ιδεώδη οι οποίες αντανακλώνται στους επαγόμενους δακτυλίους πηλίκα.

1. Ο δακτύλιος $\mathbb{Z}_5$ είναι σώμα διότι ο 5 είναι πρώτος αριθμός. Επομένως τα μόνα ιδεώδη του είναι τα: το μηδενικό ιδεώδες $(2+i)$ και όλος ο δακτύλιος $\mathbb{Z}[i]/(2+i)$, και άρα από την περιγραφή των ιδεωδών ενός δακτυλίου πηλίκου, βλέπε το Πόρισμα 8.3.12, *δεν υπάρχει* ιδέωδες J διαφορετικό από τα $(2+i)$ και $\mathbb{Z}[i]$, έτσι ώστε $(2+i) \subseteq J \subseteq \mathbb{Z}[i]$.

   Παρατηρούμε ότι, αν $x, y \in \mathbb{Z}[i]$ και $x \cdot y \in (2+i)$, τότε είτε $x \in (2+i)$ είτε $y \in (2+i)$. Πράγματι τότε στον δακτύλιο πηλίκο $\mathbb{Z}[i]/(2+i)$ θα έχουμε $(x+(2+i)) \cdot (y+(2+i)) = (2+i)$, και άρα, επειδή ένα σώμα δεν έχει διαιρέτες του μηδενός, θα έχουμε $x+(2+i) = (2+i)$ ή $y+(2+i) = (2+i)$, δηλαδή $x \in (2+i)$ ή $y \in (2+i)$.

2. Ο δακτύλιος $\mathbb{Z}_{26}$ δεν είναι σώμα διότι ο 26 είναι σύνθετος, και δεν είναι ούτε ακέραια περιοχή διότι, για παράδειγμα, $[2]_{26} \cdot [13]_{26} = [0]_{26}$.

   Από την άλλη πλευρά, σύμφωνα με το Πόρισμα 8.3.12, τα ιδεώδη του $\mathbb{Z}[i]/(1+5i)$ είναι της μορφής $I/(1+5i)$, όπου I είναι ένα ιδεώδες του $\mathbb{Z}[i]$ έτσι ώστε: $(1+5i) \subseteq I \subseteq \mathbb{Z}[i]$, παράδειγμα τέτοιου ιδεώδους είναι το $I = (-24+10i) = (1+5i)^2$ και βλέπουμε εύκολα ότι $(1+5i) \neq J \neq \mathbb{Z}[i]$. Παρατηρούμε ότι υπάρχουν στοιχεία $x, y \in \mathbb{Z}[i]$ έτσι ώστε $x \cdot y \in (1+5i)$, αλλά $x \notin (1+5i)$ και $y \in (1+5i)$. Πράγματι, για τα στοιχεία $x = 2$ και $y = 13$ του $\mathbb{Z}[i]$ έχουμε $2 \cdot 13 = 26 = (1-5i) \cdot (1+5i) \in (1+5i)$. Τότε $2 \notin (1+5i)$ και $13 \notin (1+5i)$. Πράγματι, εύκολα βλέπουμε ότι, αν $2 \in (1+5i)$, τότε $26a = 2$, και αν $13 \notin (1+5i)$, τότε $26b = 13$, για κάποια $a, b \in \mathbb{Z}$. Και οι δύο περιπτώσεις μάς οδηγούν σε αντίφαση.

3. Ο δακτύλιος $\mathbb{Z}[i]$ είναι ακέραια περιοχή ως υποδακτύλιος του $\mathbb{C}$. Υπάρχουν άπειρα ιδεώδη I του $\mathbb{Z}[i]$ έτσι ώστε $(0) \subsetneq I \subsetneq \mathbb{Z}[i]$. Παρατηρούμε ότι *δεν υπάρχουν* στοιχεία $x, y \in \mathbb{Z}[i]$ έτσι ώστε $x \cdot y \in (0)$, και $x \notin (0)$ και $y \notin (0)$, διότι ο δακτύλιος $\mathbb{Z}[i]$ είναι ακέραια περιοχή.

Έτσι η διαφορετική συμπεριφορά των ιδεωδών $I \in \{(2+i),(1+5i),(0)\}$ του δακτυλίου $\mathbb{Z}[i]$ εντοπίζεται: (α) σε ιδιότητες του επαγόμενου δακτυλίου πηλίκου $\mathbb{Z}[i]/I$, (β) στην δυνατότητα να παρεμβάλλουμε γνήσια $I \subsetneqq J \subsetneqq \mathbb{Z}[i]$ ένα ιδεώδες J ανάμεσα στο I και στον δακτύλιο $\mathbb{Z}[i]$, και (γ) στη δυνατότητα το γινόμενο δύο στοιχείων του $\mathbb{Z}[i]$ να ανήκει στο I χωρίς κανένα από τα στοιχεία να ανήκει στο I.

Σκοπός μας είναι να τυποποιήσουμε τις παραπάνω διαφορές στην γενική περίπτωση ιδεωδών τυχόντος δακτυλίου και να μελετήσουμε τη δομή των κλάσεων ιδεωδών που θα προκύψουν.

10.1 Μεγιστοτικά Ιδεώδη

Ιδεώδη τα οποία συμπεριφέρονται ανάλογα με το ιδεώδες $(2+i)$ του $\mathbb{Z}[i]$ καλούνται μεγιστοτικά ιδεώδη, με την έννοια του ακόλουθου ορισμού.

Έστω $R = (R, +, \cdot)$ ένας δακτύλιος.

Ορισμός 10.1.1. *Ένα ιδεώδες $I \subseteq R$ καλείται* **μεγιστοτικό ιδεώδες** *του R, αν:*

1. $I \neq R$.
2. *Αν J είναι ένα ιδεώδες του R έτσι ώστε $I \subseteq J \subseteq R$, τότε: είτε $I = J$ είτε $J = R$.*

Το σύνολο όλων των μεγιστοτικών ιδεωδών του δακτυλίου R συμβολίζεται με $\mathsf{Max}(R)$.

Δηλαδή τα μεγιστοτικά ιδεώδη σε έναν δακτύλιο είναι εκείνα τα γνήσια ιδεώδη του R τα οποία δεν περιέχονται γνήσια σε άλλο γνήσιο ιδεώδες του R.

Παρατήρηση 10.1.2.

1. Προς το παρόν δεν γνωρίζουμε αν το σύνολο $\mathsf{Max}(R)$ όλων των μεγιστοτικών ιδεωδών ενός δακτυλίου R είναι κενό ή περιέχει τουλάχιστον ένα μεγιστοτικό ιδεώδες. Αργότερα θα δούμε ότι, τουλάχιστον για δακτυλίους με μονάδα, έχουμε πάντα $\mathsf{Max}(R) \neq \emptyset$.
2. Κατ' αναλογία μπορούμε να ορίσουμε την έννοια του αριστερού ή δεξιού μεγιστοτικού ιδεώδους ενός δακτυλίου R. Έτσι ένα αριστερό, αντίστοιχα, δεξιό ιδεώδες $I \subseteq R$ καλείται *μεγιστοτικό αριστερό ιδεώδες*, αντίστοιχα *μεγιστοτικό δεξιό ιδεώδες*, αν $I \neq R$ και, αν J είναι ένα αριστερό, αντίστοιχα δεξιό, ιδεώδες του R έτσι ώστε $I \subseteq J \subseteq R$, τότε: είτε $I = J$ είτε $J = R$. Αν και οι έννοιες αυτές είναι ενδιαφέρουσες, δεν θα μας απασχολήσουν ιδιαίτερα στη συνέχεια στο πλαίσιο αυτών των σημειώσεων. ▲

Ας δούμε κάποια στοιχειώδη παραδείγματα μεγιστοτικών ιδεωδών.

Παράδειγμα 10.1.3.

1. Έστω $\mathbb{K}$ ένα σώμα. Τότε τα μόνα ιδεώδη του R είναι τα τετριμμένα (0) και $\mathbb{K}$, και προφανώς $(0) \neq \mathbb{K}$. Αυτό σημαίνει ότι το μηδενικό ιδεώδες (0) είναι μεγιστοτικό.
2. Παρόμοια, το μηδενικό ιδεώδες (0) ενός δακτυλίου διαίρεσης είναι μεγιστοτικό, καθώς τα μόνα ιδέωδη ενός δακτυλίου διαίρεσης R είναι τα (0) και R, και $(0) \neq R$.
3. Έχουμε δείξει, βλέπε την Πρόταση 8.1.19, ότι ο δακτύλιος πινάκων $\mathsf{M}_n(R)$ υπεράνω ενός δακτυλίου διαίρεσης είναι απλός, και άρα τα μόνα του ιδεώδη είναι τα τετριμμένα: (0) και $\mathsf{M}_n(R)$. Όπως και παραπάνω, αυτό σημαίνει ότι το μηδενικό ιδεώδες (0) είναι μεγιστοτικό ιδεώδες του $\mathsf{M}_n(R)$.
4. Το μηδενικό ιδεώδες (0) του δακτυλίου $\mathbb{Z}$ δεν είναι μεγιστοτικό διότι περιέχεται γνήσια σε κάθε κύριο γνήσιο ιδεώδες (n) του $\mathbb{Z}$, όπου $n \neq 0, \pm 1$.
5. Το ιδεώδες $n\mathbb{Z}$ του $\mathbb{Z}$ δεν είναι μεγιστοτικό αν ο n είναι σύνθετος, έστω $n = mk$, όπου $1 < k, m < n$. Πράγματι θα έχουμε $n\mathbb{Z} \subseteq k\mathbb{Z} \subseteq \mathbb{Z}$ και προφανώς $n\mathbb{Z} \subsetneqq k\mathbb{Z} \subsetneqq \mathbb{Z}$.
6. Το ιδεώδες (t) στον δακτύλιο πολυωνύμων $\mathbb{Z}[t]$ δεν είναι μεγιστοτικό διότι: $(t) \subseteq (2,t) \subseteq \mathbb{Z}[t]$ και προφανώς $(t) \subsetneqq (2,t) \subsetneqq \mathbb{Z}[t]$. Το ιδεώδες (t), αντιστοιχα το $(2,t)$, αποτελείται από όλα τα πολυώνυμα $P(t) \in \mathbb{Z}[t]$ με μηδενικό σταθερό όρο, αντίστοιχα με άρτιο σταθερό όρο.

7. Αντιθετα, αν $\mathbb{K}$ είναι ένα σώμα, τότε το ιδεώδες (t) του $\mathbb{K}[t]$ είναι μεγιστοτικό. Πράγματι, έστω I ένα ιδεώδες του $\mathbb{K}[t]$ έτσι ώστε $(t) \subsetneq I \subseteq \mathbb{K}[t]$. Θα δείξουμε ότι $I = \mathbb{K}[t]$. Επειδή $(t) \subsetneq I$ υπάρχει πολυώνυμο $P(t) = a_0 + a_1 t + \cdots + a_b t^n \in I$, όπου $a_0 \neq 0$. Τότε το πολυώνυμο $P(t) - a_0$ έχει μηδενικό σταθερό όρο, και άρα ανήκει στο ιδεώδες (t), άρα και στο I, επειδή $(t) \subseteq I$. Τοτε το I περιέχει και τη διαφορά $P(t) - (P(t) - a_0) = a_0$, δηλαδή περιέχει ένα μη μηδενικό σταθερό πολυώνυμο. Επειδή το $\mathbb{K}$ είναι σώμα, υπάρχει το αντίστροφο στοιχείο $a_0^{-1} \in \mathbb{K}$. Τότε όμως για κάθε πολυώνυμο $Q(t) \in \mathbb{K}[t]$, θα έχουμε $Q(t) = a_0(a_0^{-1}Q(t)) \in I$, και άρα $I = \mathbb{K}[t]$.

8. Το ιδεώδες $(2+i)$ του δακτυλίου $\mathbb{Z}[i]$ είναι μεγιστοτικό, όπως είδαμε στην αρχή του Κεφαλαίου. $\surd$

Επειδή ο έλεγχος για το αν ένα ιδεώδες ενός δακτυλίου είναι μεγιστοτικό ή όχι, με χρήση του ορισμού, είναι σε κάποιες περιπτώσεις επίπονος, θα αποδείξουμε το ακόλουθο χρήσιμο κριτήριο διαμέσου του οποίου θα μπορούμε να ελέγχουμε αν ένα ιδεώδες ενός δακτυλίου είναι μεγιστοτικό ή όχι. Πρώτα θα χρειαστούμε μια μικρή υπενθύμιση.

Αν $I \subseteq R$ είναι ένα ιδεώδες του R και $a \in R$, τότε υπενθυμίζουμε ότι το ιδεώδες (I, a) του R είναι το ιδεώδες του R το οποίο παράγεται από το σύνολο $I \cup \{a\}$. Ως γνωστόν, θα έχουμε $(I, a) = I + RaR$, όπου RaR είναι το κύριο ιδεώδες το οποίο παράγεται από το a. Επομένως τα στοιχεία του (I, a) θα είναι της μορφής

$$I + RaR = \left\{ x + \sum_{k=1}^{n} r_k a s_k \in R \mid x \in I,\ r_k, s_k \in R,\ n \geq 1 \right\}$$

Πράγματι, προφανώς το ιδέωδες $I + RaR$ είναι το ιδεώδες του οποίο παράγεται από το σύνολο $I \cup RaR$, και άρα $(I, a) \subseteq (I \cup RaR) = I + RaR$. Τότε θα έχουμε ισότητα $(I, a) = (I \cup RaR) = I + RaR$ διότι κάθε ιδεώδες του R το οποίο περιέχει το I και το a θα περιέχει προφανώς και καθε στοιχείο του $I + RaR$.

Αν ο δακτύλιος R είναι μεταθετικός, τότε προφανώς θα έχουμε:

$$(I, a) = I + Ra = \{ x + ra \in R \mid r \in R, x \in I \}$$

Θεώρημα 10.1.4. *Για ένα ιδεώδες I ενός δακτυλίου R, τα ακόλουθα είναι ισοδύναμα:*

1. *Το ιδεώδες I είναι μεγιστοτικό.*
2. *Ο δακτύλιος πηλίκο R/I είναι απλός.*
3. *Το ιδεώδες I είναι γνήσιο και για κάθε $a \in R \setminus I$: $(I, a) = R$.*

Ιδαίτερα, αν ο δακτύλιος R είναι μεταθετικός, τότε: το I είναι μεγιστοτικό $\iff$ ο δακτύλιος πηλίκο R/I είναι σώμα.

Απόδειξη. Η απόδειξη συνίσταται σε μια άμεση εφαρμογή της Πρότασης 8.1.19.

1. «1. $\implies$ 2.» Υποθέτουμε ότι το ιδεώδες I του R είναι μεγιστοτικό. Τότε το I είναι ιδιαίτερα γνήσιο ιδεώδες του R: $I \neq R$. Έστω $K \subseteq R/I$ ένα ιδεώδες του δακτυλίου πηλίκου R/I. Από την Πρόταση 8.1.19, έπεται ότι το K είναι της μορφής $K = J/I$, όπου J είναι ένα ιδεώδες του R έτσι ώστε $I \subseteq J \subseteq R$. Επειδή το I είναι μεγιστοτικό, έπεται ότι είτε $I = J$ είτε $J = R$. Αν $I = J$, τότε το $K = J/I = I$ είναι το μηδενικό ιδεώδες του R/I, και αν $J = R$, τότε το $K = R/I$ είναι όλος ο δακτύλιος πηλίκο. Έτσι δείξαμε ότι ο δακτύλιος R/I έχει μόνο δύο ιδεώδη, τα τετριμμένα, και άρα είναι απλός.

2. «2. $\implies$ 1.» Αντίστροφα, έστω ότι ο δακτύλιος πηλίκο R/I είναι απλός. Τότε τα μόνα ιδεώδη του είναι δύο: τα I και R/I. Ιδιαίτερα έπεται ότι το I είναι γνήσιο. Αν J είναι ένα ιδεώδες του R έτσι ώστε $I \subseteq J \subseteq R$, τότε θα έχουμε το ιδεώδες J/I του R/I, και άρα είτε $J/I = I$ είτε $J/I = R/I$, ισοδύναμα είτε $I = J$ είτε $R = J$. Επομένως το I είναι μεγιστοτικό.

3. «1. $\implies$ 3.» Έστω ότι το I είναι μεγιστοτικό ιδεώδες του R και $a \in R \setminus I$. Τότε το ιδεώδες $(I, a) = I + RaR$ είναι ένα ιδεώδες του R το οποίο περιέχει το I, δηλαδή $I \subseteq I + RaR \subseteq R$. Προφανώς $I \neq I + RaR$, διότι διαφορετικά θα είχαμε $a \in RaR \subseteq I + RaR = I$, το οποίο είναι άτοπο. Επειδή $(I, a) \neq I$ και το I είναι μεγιστοτικό, έπεται ότι θα έχουμε το ζητούμενο $(I, a) = I + RaR = R$.

4. «3. $\Longrightarrow$ 1.» Υποθέτουμε ότι το ιδεώδες I είναι γνήσιο και έστω ότι $a \in R \setminus I$: $(I, a) = R$. Έστω J ένα ιδεώδες του R έτσι ώστε $I \subseteq J \subseteq R$. Αν $I \neq J$, τότε υπάρχει $a \in J \setminus I$. Θεωρούμε τότε το ιδεώδες (I, a), για το οποίο από την υπόθεση θα έχουμε $(I, a) = R$. Όμως επειδή $I \subseteq J$ και $a \in J$, θα έχουμε $R = (I, a) \subseteq J$ και επομένως $J = R$. Αυτό δείχνει ότι το ιδεώδες I είναι μεγιστοτικό.

Αν ο δακτύλιος R είναι μεταθετικός, τότε το συμπέρασμα προκύπτει από το γεγονός ότι ένας μεταθετικός δακτύλιος είναι απλός αν και μόνο αν είναι σώμα, βλέπε την Πρόταση 8.1.17. ■

Η παραπάνω συνέπεια του Θεωρήματος 10.1.4 δείχνει ότι τα μεγιστοτικά ιδώδη ενός δακτυλίου R είναι σε αμφιμονοσήμαντη αντιστοιχία με τους επιμορφισμούς δακτυλίων $R \longrightarrow F$, όπου F είναι ένα σώμα.

Πόρισμα 10.1.5. *Αν R είναι ένας δακτύλιος, τότε η απεικόνιση*

$$M \quad \longmapsto \quad \pi_M \colon R \longrightarrow R/M, \;\; \pi_M(r) = r + M$$

ορίζει μια «1-1» και «επί» αντιστοιχία μεταξύ του συνόλου των μεγιστοτικών ιδεωδών M του δακτυλίου R και του συνόλου των επιμορφισμών δακτυλίων $f \colon R \longrightarrow F$, όπου F είναι ένα σώμα. Η αντίστροφη αντιστοιχία ορίζεται ως εξής:

$$f \colon R \longrightarrow F, \quad \longmapsto \quad \mathsf{Ker}(f)$$

Απόδειξη. Αν M είναι ένα μεγιστοτικό ιδεώδες του R, τότε ο δακτύλιος πηλίκο R/M είναι σώμα και η απεικόνιση π_M είναι επιμορφισμός δακτυλίων με πυρήνα το μεγιστοτικό ιδεώδες M. Αντίστροφα, αν $f \colon R \longrightarrow F$ είναι ένας επιμορφισμός δακτυλίων, όπου F είναι σώμα, τότε από το Θεώρημα 10.1.4, έπεται ότι ο πυρήνας $\mathsf{Ker}(f)$ είναι ένα μεγιστοτικό ιδώδες του R διότι για τον δακτύλιο πηλίκο θα έχουμε $R/\mathsf{Ker}(f) \cong F$. ■

Πόρισμα 10.1.6. *Το μηδενικό ιδεώδες (0) σε έναν δακτύλιο R είναι μεγιστοτικό αν και μονον αν ο δακτύλιος R είναι απλός. Αν ο δακτύλιος R είναι μεταθετικός, τότε το μηδενικό ιδεώδες (0) του R είναι μεγιστοτικό αν και μόνο αν ο δακτύλιος R είναι σώμα.*

Ο ακόλουθος χαρακτηρισμός μεγιστοτικών ιδεωδών βασίζεται στη συμπεριφορά στοιχείων του δακτυλίου.

Πόρισμα 10.1.7. *Αν R είναι ένας μεταθετικός δακτύλιος, τότε ένα γνήσιο ιδεώδες I του R είναι μεγιστοτικό αν και μόνο αν*

$$\forall r \in R \setminus I, \quad \exists s \in R \colon \quad 1 - rs \in I$$

Απόδειξη. Αν το ιδεώδες I είναι μεγιστοτικό, τότε ο δακτύλιος πηλίκο R/I είναι σώμα. Επομένως, αν $r \in R \setminus I$, τότε το $r + I$ είναι ένα μη μηδενικό στοιχείο του σώματος R/I και επομένως είναι αντιστρέψιμο, δηλαδή υπάρχει $s + I \in R/I$ έτσι ώστε

$$(r + I) \cdot (s + I) = 1 + I \quad \Longrightarrow \quad r \cdot s + I = 1 + I \quad \Longrightarrow \quad 1 - r \cdot s + I = I \quad \Longrightarrow \quad 1 - r \cdot s \in I$$

Αντίστροφα, αν $\forall r \in R \setminus I$, υπάρχει $s \in R$: $1 - rs \in I$, τότε όπως παραπάνω θα έχουμε ότι κάθε μη μηδενικό στοιχείο του δακτυλίου πηλίκου R/I είναι αντιστρέψιμο, και άρα ο μεταθετικός δακτύλιος R/I είναι σώμα. Τότε όμως από το Θεώρημα 10.1.4 έπεται ότι το ιδεώδες I είναι μεγιστοτικό. ■

Παράδειγμα 10.1.8.

1. Έστω $\mathbb{K}$ ένα σώμα. Τότε το μηδενικό ιδεώδες (0) είναι μεγιστοτικό.
2. Παρόμοια το μηδενικό ιδεώδες (0) ενός δακτυλίου διαίρεσης είναι μεγιστοτικό.
3. Επειδή ο δακτύλιος πινάκων $\mathsf{M}_n(R)$ υπεράνω ενός δακτυλίου διαίρεσης R είναι απλός, έπεται ότι το μηδενικό του ιδεώδες (0) είναι μεγιστοτικό.
4. Το μηδενικό ιδεώδες (0) του δακτυλίου $\mathbb{Z}$ δεν είναι μεγιστοτικό διότι ο δακτύλιος πηλίκο $\mathbb{Z}/(0) \cong \mathbb{Z}$ δεν είναι σώμα.

5. Το ιδεώδες $n\mathbb{Z}$ του $\mathbb{Z}$ είναι μεγιστοτικό αν και μόνο αν ο n είναι πρώτος. Αυτό προκύπτει από το γεγονός ότι ο δακτύλιος πηλίκο $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$ είναι σώμα αν και μονο αν ο n είναι πρώτος.

6. Το ιδεώδες (t) στον δακτύλιο πολυωνύμων $\mathbb{Z}[t]$ δεν είναι μεγιστοτικό διότι ο δακτύλιος $\mathbb{Z}[t]/(t) \cong \mathbb{Z}$ δεν είναι σώμα.

   Αντίθετα θα δείξουμε ότι το ιδεώδες $(2,t) \subseteq \mathbb{Z}[t]$ είναι μεγιστοτικό. Ορίζουμε απεικόνιση

   $$f : \mathbb{Z}[t] \longrightarrow \mathbb{Z}_2, \quad f(P(t)) = [P(0)]_2$$

   Η απεικόνιση f προκύπτει από τον φυσικό επιμορφισμό $\mathbb{Z} \longrightarrow \mathbb{Z}[2]$ και το στοιχείο $u = [0]_2 \in \mathbb{Z}_2$, με χρήση της Πρότασης 8.2.22. Ιδιαίτερα έπεται ότι η απεικόνιση f είναι ομομορφισμός δακτυλίων. Η απεικόνιση f είναι επιμορφισμός, διότι για κάθε $[k]_2 \in \mathbb{Z}_2$, έχουμε $f(P(t)) = [k]_2$, όπου $P(t) = k$ είναι το σταθερό πολυώνυμο ίσο με $k = 0$ ή 1.

   $$\mathsf{Ker}(f) = \{P(t) \in \mathbb{Z}[t] \mid P(t) = 0_{\mathbb{Z}_2}\} = \{P(t) \in \mathbb{Z}[t] \mid [P(0)]_2 = [0]_2\} = \{P(t) \in \mathbb{Z}[t] \mid 2 \mid P(0)\} = (2,t)$$

   Από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε ότι ο f επάγει έναν ισομορφισμό δακτυλίων:

   $$\widetilde{f} : \mathbb{Z}[t]/(2,t) \xrightarrow{\cong} \mathbb{Z}_2$$

   Επειδή ο δακτύλιος $\mathbb{Z}_2$ είναι σώμα, έπεται ότι το ιδεώδες $(2,t)$ είναι μεγιστοτικό.

7. Αν $\mathbb{K}$ είναι ένα σώμα, τότε το ιδεώδες (t) του $\mathbb{K}[t]$ είναι μεγιστοτικό, διότι $\mathbb{K}[t]/(t) \cong \mathbb{K}$ είναι σώμα.

8. Γενικότερα, αν $\mathbb{K}$ είναι ένα σώμα και $a \in \mathbb{K}$, τότε το υποσύνολο $I = \{P(t) \in \mathbb{K}[t] \mid P(a) = 0\}$ είναι ένα μεγιστοτικό ιδεώδες του $\mathbb{K}[t]$. Αυτό προκύπτει από το γεγονός ότι $I = \mathsf{Ker}(\Phi_a)$, όπου Φ_a είναι ο ομομορφισμός εκτίμησης $\Phi_a : \mathbb{K}[t] \longrightarrow \mathbb{K}$ ο οποίος είναι επιμορφισμός και επάγει έναν ισομορφισμό δακτυλίων $\mathbb{K}[t]/I \cong \mathbb{K}$.

9. Θεωρούμε τον υποδακτύλιο $\mathscr{C}([0,1],\mathbb{R}) \subseteq \mathscr{F}([0,1],\mathbb{R})$ των συνεχών πραγματικών συναρτήσεων ορισμένων επί του κλειστού διαστήματος $[0,1]$. Τότε για κάθε $r \in [0,1]$, έχουμε τον ομομορφισμό εκτίμησης

   $$\Phi_r : \mathscr{C}([0,1],\mathbb{R}) \longrightarrow \mathbb{R}, \quad \Phi_r(f) = f(r)$$

   ο οποίος είναι ένας επιμορφισμός δακτυλίων. Προφανώς $\mathsf{Ker}(\Phi_r) = \{f \in \mathscr{C}([0,1],\mathbb{R}) \mid f(r) = 0\} := M_r$ είναι τότε ένα μεγιστοτικό του $\mathscr{C}([0,1])$ διότι έχουμε έναν ισομορφισμό δακτυλίων

   $$\mathscr{C}([0,1])/M_r \xrightarrow{\cong} \mathbb{R}$$

   Παρατηρούμε ότι, αν $r,s \in [0,1]$, τότε: $r \neq s \Longrightarrow M_r \neq M_s$. Πράγματι, αν είχαμε $M_r = M_s$, τότε η συνεχής συνάρτηση $f : [0,1] \longrightarrow \mathbb{R}$, $f(x) = x - r$ θα ανήκει στο ιδεώδες M_s διότι ανήκει προφανώς στο M_r. Έτσι θα έχουμε $f(s) = 0$, δηλαδή $s - r = 0$, και άρα $s = r$ το οποίο είναι άτοπο.

   Άρα το πλήθος των μεγιστοτικών ιδεωδών του δακτυλίου $\mathscr{C}([0,1])$ είναι τουλάχιστον όσο το πλήθος των στοιχείων του $[0,1]$, δηλαδή μη αριθμήσιμο. Αργότερα θα δείξουμε ότι η «1-1» απεικόνιση $[0,1] \longrightarrow \mathsf{Max}(\mathscr{C}([0,1]))$, $r \longmapsto M_r$ είναι και «επί», βλέπε το Παράρτημα Α΄.

10. Θεωρούμε τον δακτύλιο ευθύ γινόμενο $\mathbb{Z} \times \mathbb{Z}$, έστω p ένας πρώτος αριθμός, και έστω το υποσύνολο

    $$I = \{(n, pm) \in \mathbb{Z} \times \mathbb{Z} \mid n, m \in \mathbb{Z}\}$$

    Δηλαδή $I = \mathbb{Z} \times p\mathbb{Z}$.

    Θεωρούμε απεικόνιση

    $$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}_p, \quad f(n,m) = [m]_p$$

    Εύκολα βλέπουμε ότι η απεικόνιση f είναι ομομορφισμός δακτυλίων, και είναι προφανώς «επί». Από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε έναν ισομορφισμό δακτυλίων

    $$\widetilde{f} : (\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times p\mathbb{Z}) \xrightarrow{\cong} \mathbb{Z}_p$$

    και επομένως, επειδή ο δακτύλιος $\mathbb{Z}_p$ είναι σώμα, αφού το p είναι πρώτος, έπεται ότι το ιδεώδες I του $\mathbb{Z} \times \mathbb{Z}$ είναι μεγιστοτικό.

11. Το ιδεώδες $(2+i)$ του δακτυλίου $\mathbb{Z}[i]$ είναι μεγιστοτικό, διότι ο δακτύλιος πηλίκο $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}_5$ είναι σώμα. $\surd$

Παράδειγμα 10.1.9. Στον δακτύλιο $\mathsf{AT}_2(\mathbb{K})$ των 2×2 άνω τριγωνικών πινάκων με στοιχεία από ένα σώμα $\mathbb{K}$, θεωρούμε τα υποσύνολα

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in \mathsf{AT}_2 \mid a,b \in \mathbb{K} \right\} \quad \text{και} \quad J = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \in \mathsf{AT}_2 \mid b,c \in \mathbb{K} \right\} \quad \text{και} \quad K = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \in \mathsf{AT}_2 \mid b \in \mathbb{K} \right\}$$

Θα δείξουμε ότι τα I και J είναι μεγιστοτικά ιδεώδη, και το $K = I \cap J$ δεν είναι μεγιστοτικό ιδεώδες. Κατασκευάζουμε απεικονίσεις

$$f : \mathsf{AT}_2(\mathbb{K}) \longrightarrow \mathbb{K}, \qquad f\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = c$$

$$g : \mathsf{AT}_2(\mathbb{K}) \longrightarrow \mathbb{K}, \qquad f\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = a$$

$$h : \mathsf{AT}_2(\mathbb{K}) \longrightarrow \mathbb{K}\times\mathbb{K}, \qquad f\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a,c)$$

Εύκολα βλέπουμε ότι οι απεικονίσεις f, g, και h είναι ομομορφισμοί δακτυλίων και είναι προφανώς «επί». Επιπλέον

$$\mathsf{Ker}(f) = I \quad \text{και} \quad \mathsf{Ker}(g) = J \quad \text{και} \quad \mathsf{Ker}(h) = K$$

Από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε τότε ισομορφισμούς δακτυλίων

$$\mathsf{T}_2(\mathbb{K})/I \xrightarrow{\cong} \mathbb{K} \quad \text{και} \quad \mathsf{T}_2(\mathbb{K})/J \xrightarrow{\cong} \mathbb{K} \quad \text{και} \quad \mathsf{T}_2(\mathbb{K})/K \xrightarrow{\cong} \mathbb{K}\times\mathbb{K}$$

Από το Θεώρημα 10.1.4, έπεται ότι τα ιδεώδη I και J είναι μεγιστοτικά (διότι το $\mathbb{K}$ είναι σώμα), αλλά το ιδεώδες K δεν είναι μεγιστοτικό (διότι το $\mathbb{K}\times\mathbb{K}$ δεν είναι σώμα). $\surd$

10.1.1 Ύπαρξη Μεγιστοτικών Ιδεωδών

Είδαμε ότι τα μεγιστοτικά ιδεώδη σε έναν δακτύλιο έχουν ευχάριστες ιδιότητες. Δεν γνωρίζουμε όμως αν υπάρχουν μεγιστοτικά ιδεώδη σε έναν τυχόντα δακτύλιο. Στην παρούσα υποενότητα θα δούμε ένα σημαντικό αποτέλεσμα, γνωστό ως Θεώρημα του Krull, το οποίο μας εξασφαλίζει ότι, πράγματι σε κάθε δακτύλιο με μονάδα, υπάρχουν μεγιστοτικά ιδεώδη. Στην απόδειξη, η οποία είναι υπαρξιακού χαρακτήρα, χρησιμοποιείται δραστικά ένα σπουδαίο συνολοθεωρητικό αποτέλεσμα, γνωστό ως Λήμμα του Zorn.

Υπενθυμίζουμε ότι ένα *μερικώς διατεταγμένο σύνολο* είναι ένα ζεύγος $(X, \preccurlyeq)$ όπου το X είναι ένα μη κενό σύνολο και «$\preccurlyeq$» είναι μια σχέση μερικής διάταξης επί του X, δηλαδή η σχέση «$\preccurlyeq$» ικανοποιεί (α) την ανακλαστική ιδιότητα: $x \preccurlyeq x$, $\forall x \in X$, (β) την αντισυμμετρική ιδιότητα: $x \preccurlyeq y$ και $y \preccurlyeq x \Longrightarrow x = y$, και ($\gamma$) την μεταβατική ιδιότητα: $x \preccurlyeq y$ και $y \preccurlyeq z \Longrightarrow x \preccurlyeq z$. Άν $S \subseteq X$ είναι ένα μη κενό υποσύνολο του μερικώς διατεταγμένου συνόλου $(X, \preccurlyeq)$, τότε ένα *άνω φράγμα* για το S είναι ένα στοιχείο $x \in X$ έτσι ώστε: $s \preccurlyeq x$, $\forall s \in S$. Ένα *μεγιστοτικό στοιχείο* για το X είναι ένα στοιχείο $w \in X$ έτσι ώστε $w \preccurlyeq x \Longrightarrow w = x$. Ένα *ολικώς διατεταγμένο σύνολο* είναι ένα μερικώς διατεταγμένο σύνολο $(X, \preccurlyeq)$ έτσι ώστε: $\forall x, y \in X$: είτε $x \preccurlyeq y$ είτε $y \preccurlyeq x$.

Λήμμα 10.1.10 (Λήμμα του Zorn)**.** [1] *Έστω $(\mathcal{T}, \preccurlyeq)$ ένα μερικώς διατεταγμένο σύνολο, το οποίο ικανοποιεί την ιδιότητα ότι κάθε ολικά διατεταγμένο υποσύνολο του έχει άνω φράγμα στο $\mathcal{T}$. Τότε το $\mathcal{T}$ έχει μεγιστοτικό στοιχείο.*

[1] Max Zorn (6 Ιουνίου 1906 - 9 Μαρτίου 1993) [https://en.wikipedia.org/wiki/Max_August_Zorn]: Γερμανός μαθηματικός, με συμβολή στην Άλγεβρα, στη Θεωρία Ομάδων και στην Αριθμητική Ανάλυση. Είναι περισσότερο γνωστός για το παρόν Λήμμα που φέρει το όνομά του.

Το Λήμμα του Zorn είναι αποτέλεσμα υπαρξιακού χαρακτήρα και δεν «κατασκευάζει» το μεγιστοτικό στοιχείο.

Θεώρημα 10.1.11 (Θεώρημα του Krull)**.** [2] *Έστω R ένας δακτύλιος με μονάδα. Τότε κάθε γνήσιο ιδεώδες του R περιέχεται σε ένα μεγιστοτικό ιδεώδες.*

Απόδειξη. Έστω I ένα γνήσιο ιδεώδες του R. Θεωρούμε τη συλλογή όλων των γνήσιων ιδεωδών του R τα οποία περιέχουν το I:

$$\mathcal{T} = \{J \subseteq R \mid J: \text{ γνήσιο ιδεώδες του } R \text{ και } I \subseteq J\}$$

Η συλλογή υποσυνόλων $\mathcal{T}$ είναι μη-κενή διότι $I \in R$. Εφοδιασμένο με την σχέση «$\subseteq$» του περιέχεσθαι η συλλογή υποσυνόλων $\mathcal{T}$ είναι ένα μερικώς διατεταγμένο σύνολο $(\mathcal{T}, \subseteq)$. Έστω $\mathcal{S}$ ένα ολικά διατεταγμένο υποσύνολο του $\mathcal{T}$. Θα δείξουμε ότι το σύνολο

$$K = \bigcup_{S \in \mathcal{S}} S$$

είναι ένα άνω φράγμα του $\mathcal{S}$ στο $\mathcal{T}$. Επειδη προφανώς $L \subseteq K$ για κάθε ιδεώδες της συλλογής $\mathcal{S}$, αρκεί να δείξουμε ότι το K είναι ένα γνήσιο ιδεώδες του R το οποίο περιέχει του I, δηλαδή το K ανήκει στη συλλογή $\mathcal{T}$. Έστω $a, b \in K$, και $r \in R$. Τότε υπάρχουν ιδέωδη $S_1, S_2 \in \mathcal{S}$ έτσι ώστε $a \in \mathcal{S}_1$ και $b \in \mathcal{S}_2$. Επειδή η συλλογή $\mathcal{S}$ είναι ολικά διατεταγμένη, έπεται ότι είτε $S_1 \subseteq S_2$ είτε $S_2 \subseteq S_1$. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $S_1 \subseteq S_2$ (αν $S_2 \subseteq S_1$, εργαζόμαστε ανάλογα). Τότε $a, b \in S_2$ και επομένως, επειδή το S_2 είναι ιδεώδες του R, θα έχουμε ότι $0 \in S_2$ και $a - b \in S_2$. Επίσης $r \cdot a, a \cdot r \in S_2$. Αυτό σημαίνει ότι $0, a - b, r \cdot a, a \cdot r \in K$, και επομένως το υποσύνολο K είναι ένα ιδεώδες του R. Το ιδεώδες K είναι γνήσιο, διότι διαφορετικά, αν $K = R$, θα είχαμε $1_R \in K$ και επομένως $1_R \in S$ για κάποιο ιδεώδες S της συλλογής $\mathcal{S}$. Τότε προφανώς $S = R$ και αυτό είναι άτοπο διότι η συλλογή $\mathcal{S}$ αποτελείται από γνήσια ιδεώδη. Επειδή κάθε ιδεώδες της συλλογής $\mathcal{S}$ περιέχει το I, έπεται ότι $I \subseteq K$. Άρα $K \in \mathcal{T}$.

Επομένως δείξαμε ότι κάθε ολικά διατεταγμένο υποσύνολο $\mathcal{S}$ του $\mathcal{T}$ έχει ένα άνω φράγμα στο $\mathcal{T}$. Από το Λήμμα του Zorn 10.1.10 έπεται ότι η συλλογή $\mathcal{T}$ έχει μεγιστοτικό στοιχείο M. Δηλαδή το M είναι ένα γνήσιο ιδεώδες του R το οποίο περιέχει το I, και αν J είναι ένα γνήσιο ιδεώδες του R το οποίο περιέχει το I και $M \subseteq J$, τότε $M = J$. Θα δείξουμε ότι το ιδεώδες M είναι μεγιστοτικό. Πράγματι, αν L είναι ένα ιδεώδες του R έτσι ώστε $M \subseteq L \subseteq R$ και $L \neq R$, τότε το L είναι ένα γνήσιο ιδεώδες του R το οποίο περιέχει το I, διότι $I \subseteq M \subseteq L$, και άρα το L είναι στοιχείο του μερικώς διατεταγμένου συνόλου $\mathcal{T}$. Επειδή το ιδεώδες M είναι μεγιστοτικό στοιχείο του $\mathcal{T}$ και $M \subseteq L$, έπεται ότι $M = L$. Επομένως το M είναι ένα μεγιστοτικό ιδεώδες του R το οποίο περιέχει το ιδεώδες I. ■

Υπενθυμίζουμε ότι στις παρούσες σημειώσεις με τον όρο «δακτύλιος» εννοούμε έναν μη-μηδενικό δακτύλιο με μονάδα και $1_R \neq 0_R$.

Πόρισμα 10.1.12. *Κάθε δακτύλιος R περιέχει μεγιστοτικά ιδεώδη.*

Απόδειξη. Επειδή $\{0_R\} \neq R$, το μηδενικό ιδεώδες του R είναι γνήσιο και επομένως από το Θεώρημα 10.1.14 έπεται ότι περιέχεται σε ένα μεγιστοτικό ιδεώδες του R. ■

Πόρισμα 10.1.13. *Έστω R ένας δακτύλιος. Τότε υπάρχει ένας μη τετριμμένος επιμορφισμός δακτυλίων $R \longrightarrow S$, όπου ο δακτύλιος S είναι απλός. Αν ο δακτύλιος R είναι μεταθετικός, τότε υπάρχει ένας μη τετριμμένος επιμορφισμός $R \longrightarrow S$, όπου ο δακτύλιος S είναι σώμα.*

Απόδειξη. Από το Πόρισμα 10.1.12, ο δακτύλιος R διαθέτει ένα μεγιστοτικό ιδεώδες M, και τότε ο δακτύλιος πηλίκο R/M είναι απλός. Ο φυσικός επιμορφισμός $\pi_M \colon R \longrightarrow R/M$, $\pi_M(x) = x + M$ είναι τότε ο ζητούμενος επιμορφισμός δακτυλίων. Ο τελευταίος ισχυρισμός προκύπτει από το γεγονός ότι ένας μεταθετικός δακτύλιος είναι απλός αν και μόνο αν είναι σώμα. ■

[2] Wolfgang Krull (26 Αυγούστου 1899 - 12 Απριλίου 1971) [https://en.wikipedia.org/wiki/Wolfgang_Krull]: Σημαντικός Γερμανός μαθηματικός, με θεμελιώδη συμβολή στη Μεταθετική Άλγεβρα.

Παρατήρηση 10.1.14. Αν στο Θεώρημα του Krull θεωρήσουμε γνήσια αριστερά (ή δεξιά) ιδεώδη, με την έννοια της Παρατήρησης 10.1.2, τότε η απόδειξη δείχνει ότι:

«*Κάθε γνήσιο αριστερό, αντίστοιχα δεξιό, ιδεώδες ενός δακτυλίου R περιέχεται σε ένα μεγιστοτικό αριστερό, αντίστοιχα δεξιό, ιδεώδες του R*». ▲

Πόρισμα 10.1.15. *Αν R είναι ένας μεταθετικός δακτύλιος, και $r \in R$ είναι ένα στοιχείο του, τότε το r είναι αντιστρέψιμο αν και μόνο αν το r δεν ανήκει σε κανένα μεγιστοτικό ιδώδες του R.*

Απόδειξη. Έστω ότι το στοιχείο r είναι αντιστρέψιμο. Τότε προφανώς το r δεν ανήκει σε κανένα γνήσιο ιδεώδες του R. Πράγματι, αν $r \in I$ όπου I είναι ένα γνήσιο ιδεώδες του R, τότε, επειδή το r είναι αντιστρέψιμο θα έχουμε $sr = 1_R$ για κάποιο $s \in R$ και τότε $1_R \in I$. Αυτό σημαίνει ότι $\forall t \in R : t = t \cdot 1_R \in I$ και άρα $I = R$ το οποίο είναι άτοπο. Άρα $r \notin I$ για κάθε γνήσιο ιδεώδες I του R και επομένως ιδιαίτερα το r δεν ανήκει σε κανένα μεγιστοτικό ιδεώδες του R. Αντίστροφα, αν το στοιχείο r δεν ανήκει σε κανένα μεγιστοτικό ιδώδες του R, τότε το κύριο ιδεώδες Rr το οποίο παράγεται από το r δεν περιέχεται σε κανένα μεγιστοτικό ιδεώδες του R. Σύμφωνα με το Θεώρημα 10.1.14, αυτό μπορεί να συμβεί μόνο αν το ιδεώδες Rr δεν είναι γνήσιο, δηλαδή αν $Rr = R$. Τότε όμως θα έχουμε $s \cdot r = 1$ για κάποιο $s \in R$ και επειδή ο δακτύλιος R είναι μεταθετικός, αυτό σημαίνει ότι το r είναι αντιστρέψιμο. ■

Ένας Δακτύλιος χωρίς Μονάδα και χωρίς Μεγιστοτικά Ιδεώδη

Είδαμε ότι κάθε δακτύλιος με μονάδα έχει μεγιστοτικά ιδεώδη. Θα δούμε τώρα έναν δακτύλιο χωρίς μονάδα ο οποίος δεν έχει κανένα μεγιστοτικό ιδεώδες.

Θεωρούμε την προσθετική ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών. Θέτοντας $x \circ y = 0$, $\forall x, y \in Q$, εύκολα βλέπουμε ότι η τριάδα $(\mathbb{Q}, +, \circ)$ είναι ένας μεταθετικός δακτύλιος χωρίς μονάδα.

Πρόταση 10.1.16. *Ο δακτύλιος χωρίς μονάδα $R = (\mathbb{Q}, +, \circ)$ δεν περιέχει κανένα μεγιστοτικό ιδεώδες.*

Απόδειξη. Λόγω του τετριμμένου πολλαπλασιασμού, τα ιδεώδη του δακτυλίου χωρίς μονάδα R συμπίπτουν με τις υποομάδες της προσθετικής ομάδας $(\mathbb{Q}, +)$. Έστω $M \subseteq \mathbb{Q}$ ένα μεγιστοτικό ιδεώδες του R, δηλαδή M είναι μια γνήσια υποομάδα της προσθετικής ομάδας $(\mathbb{Q}, +)$, και αν $M \subseteq N \subseteq \mathbb{Q}$, όπου N είναι υποομάδα της $\mathbb{Q}$, τότε είτε $M = N$ είτε $N = \mathbb{Q}$. Αυτό σημαίνει ότι η ομάδα πηλίκο $\mathbb{Q}/M$ είναι μη τετριμμένη και οι μόνες υποομάδες της είναι οι τετριμμένες υποομάδες, με άλλα λόγια η ομάδα πηλίκο $\mathbb{Q}/M$ είναι απλή αβελιανή ομάδα. Γνωρίζουμε ότι μια απλή αβελιοανή ομάδα είναι ισόμορφη με μια κυκλική πμάδα πρώτης τάξης, και άρα θα έχουμε $\mathbb{Q}/M \cong \mathbb{Z}_p$, όπου p είναι ένας πρώτος αριθμός. Έστω $x \in \mathbb{Q} \setminus M$, αυτή η επιλογή είναι εφικτή διότι $\mathbb{Q} \neq M$. Τότε επίσης $\frac{x}{p} \in \mathbb{Q} \setminus M$. Πράγματι, αν $\frac{x}{p} \in M$, τότε $x = p \cdot \frac{x}{p} = \frac{x}{p} + \frac{x}{p} + \cdots + \frac{x}{p} \in M$ (p-παράγοντες), και αυτό είναι άτοπο. Τότε στην ομάδα πηλίκο $\mathbb{Q}/M$ η οποία είναι τάξης p θα έχουμε:

$$p\left(\frac{x}{p} + M\right) = M \implies p\frac{x}{p} + M = M \implies x + M = M \implies x \in M$$

και αυτό είναι άτοπο, διότι $x \notin M$. Άρα η προσθετική ομάδα $(\mathbb{Q}, +)$ δεν περιέχει γνήσιες υποομάδες M έτσι ώστε, αν $M \subseteq N \subseteq \mathbb{Q}$, όπου N είναι υποομάδα της $\mathbb{Q}$, τότε είτε $M = N$ είτε $N = \mathbb{Q}$. Αυτό σημαίνει ότι ο δακτύλιος $(\mathbb{Q}, +, \circ)$ δεν περιέχει κανένα μεγιστοτικό ιδεώδες. ■

Τοπικοί Δακτύλιοι

Είδαμε ότι κάθε δακτύλιος περιέχει μεγιστοτικά ιδεώδη. Το μηδενικό ιδεώδες ενός σώματος είναι μεγιστοτικό, και είναι προφανώς το μοναδικό μεγιστοτικό ιδεώδες. Από την άλλη πλευρά, ο δακτύλιος των ακεραίων περιέχει άπειρα σε πλήθος μεγιστοτικά ιδεώδη.

Έτσι προκύπτει εύλογα το ερώτημα: *ποιοί δακτύλιοι περιέχουν ακριβώς ένα μεγιστοτικό ιδεώδες;*

Πρόταση 10.1.17. *Έστω R ένας μεταθετικός δακτύλιος. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Ο R έχει ακριβώς ένα μεγιστοτικό ιδεώδες.*
2. *Για κάθε $r \in R$: είτε το r είναι αντιστρέψιμο είτε το $1_R - r$ είναι αντιστρέψιμο.*
3. *Το σύνολο $R \setminus \mathsf{U}(R)$ των μη αντιστρέψιμων στοιχείων του R είναι ένα ιδεώδες του R.*

Αν ο R έχει ακριβώς ένα μεγιστοτικό ιδεώδες M, τότε $M = R \setminus \mathsf{U}(R)$.

Απόδειξη. 1. 1. «$\Longrightarrow$» 2. Έστω ότι ο R περιέχει ακριβώς ένα μεγιστοτικό ιδώδες M. Αν $r \in R$, τότε θεωρούμε τα κύρια ιδεώδη (r) και $(1-r)$ του R τα οποία παράγονται από τα στοιχεία r και $1-r$. Αν το στοιχείο r δεν είναι αντιστρέψιμο, τότε το ιδεώδες (r) είναι γνήσιο και επομένως από το Θεώρημα 10.1.14 θα έχουμε ότι το (r) περιέχεται σε ένα μεγιστοτικό ιδεώδες του R. Επειδή ο R έχει ακριβώς ένα μεγιστοτικό ιδεώδες, το M, έπεται ότι $(r) \subseteq M$. Θα δείξουμε ότι το στοιχείο $1-r$ είναι αντιστρέψιμο. Πράγματι διαφορετικά όπως παραπάνω θα είχαμε ότι $(1-r) \subseteq M$, και τότε $r, 1-r \in M$. Επειδή το M είναι ιδεώδες του R έπεται ότι $1_R = r + 1_R - r \in M$ και αυτό είναι άτοπο διότι το M, ως μεγιστοτικό ιδεώδες, είναι γνήσιο. Άρα, αν το r δεν είναι αντιστρέψιμο, έπεται ότι το $1_R - r$ είναι αντιστρέψιμο. Παρόμοια εργαζόμενοι, δείχνουμε ότι, αν το $1_R - r$ δεν είναι αντιστρέψιμο, έπεται ότι το r είναι αντιστρέψιμο.

2. 2. «$\Longrightarrow$» 1. Υποθέτουμε ότι για κάθε $r \in R$: είτε το r είναι αντιστρέψιμο είτε το $1_R - r$ είναι αντιστρέψιμο, και έστω M και N δύο μεγιστοτικά ιδεώδη του R και υποθέτουμε ότι $N \neq M$ (τουλάχιστον ένα μεγιστοτικό ιδεώδες υπάρχει από το Πόρισμα 10.1.12). Τότε υπάρχει $r \in N$ και $r \notin M$. Από το Θεώρημα 10.1.4 έπεται ότι θα έχουμε $(r) + M = R$ και επειδή $(r) \subseteq N$ θα έχουμε $R = (r) + M \subseteq N + M$, δηλαδή $R = N + M$. Τότε $1_R = x + y$, όπου $x \in N$ και $y \in M$. Από την υπόθεση είτε το x είναι αντιστρέψιμο (και αυτό είναι άτοπο διότι το x είναι στοιχείο του μεγιστοτικού, και άρα γνήσιου, ιδεώδους N), είτε το $1_R - x = y$ είναι αντιστρέψιμο (και αυτό είναι επίσης άτοπο διότι το y είναι στοιχείο του μεγιστοτικού, και άρα γνήσιου, ιδεώδους M). Στο άτοπο οδηγηθήκαμε υποθέτοντας ότι υπάρχουν τουλάχιστον δύο μεγιστοτικά ιδεώδη. Άρα ο δακτύλιος R έχει ακριβώς ένα μεγιστοτικό ιδώδες.

   1. «$\Longrightarrow$» 3. Έστω ότι ο R έχει ακριβώς ένα μεγιστοτικό ιδεώδες, το M. Αν $r \in R \setminus M$, τότε το r είναι αντιστρέψιμο. Πράγματι, όπως και στην απόδειξη της κετεύθυνσης «1. $\Longrightarrow$ 2.», αν το r δεν είναι αντιστρέψιμο, θα έχουμε $r \in (r) \subseteq M$, το οποίο είναι άτοπο. Άρα $R \setminus M \subseteq \mathsf{U}(R)$. Αντίστροφα, αν το r είναι αντιστρέψιμο, τότε προφανώς $r \notin M$ διότι το M, ως μεγιστοτικό ιδεώδες, είναι γνήσιο. Άρα $r \in R \setminus M$ και επομένως $R \setminus M = \mathsf{U}(R)$ ή ισοδύναμα $R \setminus \mathsf{U}(R) = M$, δηλαδή το μοναδικό μεγιστοτικό ιδεώδες M συμπίπτει με το σύνολο των μη αντιστρέψιμων στοιχείων του R, ιδιαίτερα το τελευταίο είναι ιδεώδες του R.

   3. «$\Longrightarrow$» 1. Έστω ότι το σύνολο $R \setminus \mathsf{U}(R)$ των μη αντιστρέψιμων στοιχείων του R είναι ένα ιδεώδες του R. Αν I είναι ένα γνήσιο ιδεώδες του R, τότε το I δεν περιέχει κανένα αντιστρέψιμο στοιχείο και άρα $I \subseteq R \setminus \mathsf{U}(R)$. Άρα κάθε γνήσιο ιδεώδες του R περιέχεται στο ιδεώδες $R \setminus \mathsf{U}(R)$ και αυτό ιδιαίτερα σημαίνει ότι το σύνολο $R \setminus \mathsf{U}(R)$ είναι το μοναδικό μεγιστοτικό ιδεώδες του R. ■

(Μεταθετικοί) δακτύλιοι οι οποίοι ικανοποιούν μία από τις δύο ισοδύναμες συνθήκες της Πρότασης 10.1.17 καλούνται τοπικοί και διαδραματίζουν σημαντικό ρόλο στην Άλγεβρα, στη Γεωμετρία και στην Ανάλυση. Έτσι ένας μεταθετικός δακτύλιος R καλείται **τοπικός** αν διαθέτει ακριβώς ένα μεγιστοτικό ιδεώδες, και τότε το μοναδικό μεγιστοτικό ιδεώδες του R αποτελείται από το σύνολο όλων των μη-αντιστρέψιμων στοιχείων του.

Τετριμμένα παραδείγματα τοπικών δακτυλίων αποτελούν τα σώματα. Τα ακόλουθα είναι κάποια μη-τετριμμένα παραδείγματα τοπικών δακτυλίων.

Παράδειγμα 10.1.18. Θεωρούμε έναν πρώτο αριθμό p, έναν θετικό ακέραιο $n \geq 1$, και έστω ο μεταθετικός δακτύλιος $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$. Από το Πόρισμα 8.3.12, έπεται ότι τα ιδεώδη του $\mathbb{Z}_{p^n}$ είναι της μορφής

$$k\mathbb{Z}/p^n\mathbb{Z}, \quad \text{όπου} \quad p^n\mathbb{Z} \subseteq k\mathbb{Z}$$

Για ένα τέτοιο ιδεώδες θα έχουμε $p^n \in k\mathbb{Z}$ και άρα $p^n = k \cdot l$ και επομένως k είναι ένας διαιρέτης του p^n. Επειδή $k\mathbb{Z} = (-k)\mathbb{Z}$, προφανώς μπορούμε να περιοριστούμε σε μη αρνητικούς ακεραίους και επομένως

τα ιδεώδη του $\mathbb{Z}_{p^n}$ είναι της μορφής $k\mathbb{Z}/p^n\mathbb{Z}$, όπου k είναι ένας θετικός διαιρέτης του p^n, δηλαδή $k = 1, p, p^2, p^3, \cdots, p^n$. Επομένως τα ιδεώδη του $\mathbb{Z}/p^n\mathbb{Z}$ είναι τα $\mathbb{Z}/p^n\mathbb{Z}$, $p\mathbb{Z}/p^n\mathbb{Z}$, $p^2\mathbb{Z}/p^n\mathbb{Z}$, $\cdots$, $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$, $p^n\mathbb{Z}/p^n\mathbb{Z}$, για τα οποία έχουμε τις ακόλουθες σχέσεις έγκλεισης

$$p^n\mathbb{Z}/p^n\mathbb{Z} \subseteq p^{n-1}\mathbb{Z}/p^n\mathbb{Z} \subseteq \cdots \subseteq p^2\mathbb{Z}/p^n\mathbb{Z} \subseteq p\mathbb{Z}/p^n\mathbb{Z} \subseteq \mathbb{Z}/p^n\mathbb{Z}$$

Είναι φανερό ότι το μοναδικό μεγιστοτικό ιδεώδες του $\mathbb{Z}/p^n\mathbb{Z}$ είναι το $p\mathbb{Z}/p^n\mathbb{Z}$, και άρα ο δακτύλιος $\mathbb{Z}/p^n\mathbb{Z}$ είναι τοπικός. Τέλος, για τον επαγόμενο δακτύλιο πηλίκο θα έχουμε $\mathbb{Z}/p^n\mathbb{Z}\big/p\mathbb{Z}/p^n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$. $\surd$

Παράδειγμα 10.1.19. Θεωρούμε το ακόλουθο υποσύνολο των ρητών

$$\mathbb{Z}_{(2)} = \Big\{ \frac{a}{b} \in \mathbb{Q} \mid a \in \mathbb{Z},\ \ 2 \nmid b \Big\}$$

το οποίο αποτελείται από όλους τους ρητούς με περιττό παρονομαστή. Το σύνολο $\mathbb{Z}_{(2)}$ είναι προφανώς ένας υποδακτύλιος του $\mathbb{Q}$, διότι περιέχει τη μονάδα του $\mathbb{Q}$, και είναι κλειστό στην διαφορά και στο γινόμενο ρητών αριθμών με περιττό παρονομαστή. Ένα μη μηδενικό στοιχείο $\frac{a}{b}$ του $\mathbb{Z}_{(2)}$ είναι αντιστρέψιμο, ως στοιχείο του υποδακτυλίου $\mathbb{Z}_{(2)}$, αν και μόνο αν ο αριθμητής a είναι περιττός (διότι τότε το κλάσμα $\frac{b}{a} \in \mathbb{Z}_{(2)}$). Αυτό σημαίνει ότι το σύνολο των μη αντιστρέψιμων στοιχείων του $\mathbb{Z}_{(2)}$ είναι

$$\mathbb{Z}_{(2)} \setminus \mathsf{U}(\mathbb{Z}_{(2)}) = \Big\{ \frac{a}{b} \in \mathbb{Q} \ \Big|\ 2 \mid a \ \text{ και } \ 2 \nmid b \Big\}$$

Από την περιγραφή των στοιχείων του βλέπουμε αμέσως ότι το σύνολο $\mathbb{Z}_{(2)} \setminus \mathsf{U}(\mathbb{Z}_{(2)})$ είναι ιδεώδες του $\mathbb{Z}_{(2)}$, και άρα, σύμφωνα με την Πρόταση 10.1.17, ο δακτύλιος $\mathbb{Z}_{(2)}$ είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες $M := \mathbb{Z}_{(2)} \setminus \mathsf{U}(\mathbb{Z}_{(2)})$.

Θα προσδιορίσουμε τον δακτύλιο πηλίκο $\mathbb{Z}_{(2)}/M$. Ορίσουμε απεικόνιση

$$f \colon \mathbb{Z}_{(2)} \longrightarrow \mathbb{Z}_2, \quad f\big(\frac{a}{b}\big) = [a]_2$$

Τότε $f(1) = [1]_2 = 1_{\mathbb{Z}_2}$, και

$$f\big(\frac{a}{b} + \frac{c}{d}\big) = f\big(\frac{ad+bc}{bd}\big) = [ad+bc]_2 = [ad]_2 + [bc]_2 = [a]_2[d]_2 + [b]_2[c]_2 = [a]_2 + [c]_2 = f\big(\frac{a}{b}\big) + f\big(\frac{c}{d}\big)$$

όπου η προτελευταία ισότητα προέκυψε διότι, επειδή οι παρονομαστές b και d είναι περιττοί, θα έχουμε $[b]_2 = [1]_2 = [d]_2$. Παρόμοια

$$f\big(\frac{a}{b} \cdot \frac{c}{d}\big) = f\big(\frac{ac}{bd}\big) = [ac]_2 = [a]_2 \cdot [c]_2 = f\big(\frac{a}{b}\big) \cdot f\big(\big(\frac{c}{d}\big)$$

Άρα η απεικόνιση f είναι ομομορφισμός δακτυλίων, και μάλιστα είναι επιμορφισμός, διότι $f\big(\frac{0}{1}\big) = [0]_2$ και $f\big(\frac{1}{1}\big) = [1]_2$. Για τον πυρήνα του f θα έχουμε:

$$\mathsf{Ker}(f) = \Big\{ \frac{a}{b} \in \mathbb{Z}_{(2)} \ \Big|\ f\big(\frac{a}{b}\big) = [0]_2 \Big\} = \Big\{ \frac{a}{b} \in \mathbb{Z}_{(2)} \ \Big|\ [a]_2 = [0]_2 \Big\} = \Big\{ \frac{a}{b} \in \mathbb{Z}_{(2)} \ \Big|\ 2 \mid a \Big\} = M$$

Από το πρώτο Θεώρημα Ισομορφισμών έπεται ότι $\mathbb{Z}_{(2)}/M \cong \mathbb{Z}_2$. $\surd$

Παράδειγμα 10.1.20. Έστω $\mathbb{K}$ ένα σώμα. Στον δακτύλιο πολυωνύμων $\mathbb{K}[t]$ θεωρούμε το ιδεώδες (t^n), $\forall n \geq 1$, το οποίο παράγεται από το πολυώνυμο t^n. Ισχυριζόμαστε ότι ο δακτύλιος πηλίκο $\mathbb{K}[t]/(t^n)$ είναι τοπικός.

Πράγματι θεωρούμε το ιδεώδες $(t)/(t^n)$ του δακτυλίου $\mathbb{K}[t]/(t^n)$, το οποίο είναι μεγιστοτικό διότι για τον αντίστοιχο δακτύλιο πηλίκο θα έχουμε

$$\mathbb{K}[t]/(t^n)\big/(t)/(t^n) \ \cong\ \mathbb{K}[t]/(t) \ \cong\ \mathbb{K}$$

Αν K είναι ένα ιδεώδες του $\mathbb{K}[t]/(t^n)$, τότε το K θα είναι της μορφής $I/(t^n)$ για κάποιο ιδεώδες I του $\mathbb{K}[t]$ το οποίο περιέχει το (t^n). Από το Θεώρημα 9.2.1, κάθε ιδεώδες του $\mathbb{K}[t]$ είναι κύριο και άρα $I=(P(t))$ για κάποιο πολυώνυμο $P(t)$. Έτσι $(t^n)\subseteq(P(t))$, δηλαδή $t^n\in(P(t))$ και άρα υπάρχει πολυώνυμο $Q(t)$ έτσι ώστε $t^n=P(t)\cdot Q(t)$. Με άλλα λόγια, το πολυώνυμο $P(t)$ είναι διαιρέτης του t^n, και άρα το $P(t)$ είναι ένα εκ των $1,\ t,\ t^2,\ \cdots,\ t^n$. Αυτό σημαίνει ότι το ιδεώδες $I/(t^n)$ είναι ένα εκ των $(1)/(t^n)=\mathbb{K}[t]/(t^n)$, $(t)/(t^n)$, $t^2/(t^n)$, $\cdots$, $t^n/(t^n)$. Περιοριζόμενοι στα γνήσια ιδεώδη, έχουμε τις ακόλουθες σχέσεις έγκλεισης

$$\left\{0_{\mathbb{K}[t]/(t^n)}\right\}=(t^n)/(t^n)\ \subseteq\ (t^{n-1})/(t^n)\ \subseteq\ (t^{n-2})/(t^n)\ \subseteq\ \cdots\ \subseteq\ (t^2)/(t^n)\ \subseteq\ (t)/(t^n)$$

Είναι φανερό ότι το μοναδικό μεγιστοτικό ιδεώδες του $\mathbb{K}[t]/(t^n)$ είναι το $(t)/(t^n)$, και άρα ο δακτύλιος $\mathbb{K}[t]/(t^n)$ είναι τοπικός. Τέλος, για τον επαγόμενο δακτύλιο πηλίκο θα έχουμε $\mathbb{K}[t]/(t^n)\big/(t)/(t^n)\cong\mathbb{K}$. $\surd$

10.1.2 Μεγιστοτικά Ιδεώδη Ειδικού τύπου Δακτυλίων

Στην παρούσα υποενότητα θα μελετήσουμε μεγιστοτικά ιδεώδη σε ειδικές κλάσεις δακτυλίων.

Μεγιστοτικά Ιδεώδη Ευθέων Γινομένων Δακτυλίων

Έστω $R_i=(R_i,+,\cdot)$, $1\le i\le n$, μια πεπερασμένη ακολουθία δακτυλίων (χρησιμοποιποιούμε πάντα τα ίδια σύμβολα για τις πράξεις πρόσθεσης και πολλαπλασιασμού, για τα μηδενικά στοιχεία, και τις μονάδες των δακτυλίων R_i, $1\le i\le n$), και θεωρούμε τον δακτύλιο ευθύ γινόμενο

$$R:=\prod_{i=1}^{n}R_i=\left\{(r_1,r_2,\cdots,r_n)\mid r_i\in R_i,\ 1\le i\le n\right\}$$

όπου οι πράξεις πρόσθεσης και πολλαπλασιασμού επί του $\prod_{i=1}^{n}R_i$ ορίζονται, «κατά συνιστώσα», ως εξής:

$$+:\ \prod_{i=1}^{n}R_i\times\prod_{i=1}^{n}R_i\ \longrightarrow\ \prod_{i=1}^{n}R_i,\qquad (r_1,r_2,\cdots,r_n)+(r_1',r_2',\cdots,r_n')=(r_1+r_1',r_2+r_2',\cdots,r_n+r_n')$$

$$\cdot:\ \prod_{i=1}^{n}R_i\times\prod_{i=1}^{n}R_i\ \longrightarrow\ \prod_{i=1}^{n}R_i,\qquad (r_1,r_2,\cdots,r_n)\cdot(r_1',r_2',\cdots,r_n')=(r_1\cdot r_1',r_2\cdot r_2',\cdots,r_n\cdot r_n')$$

και το μηδενικό στοιχείο του δακτυλίου $\prod_{i=1}^{n}R_i$ είναι η n-άδα $0=(0,0,\cdots,0)$ και η μονάδα του είναι η n-άδα $1=(1,1,\cdots,1)$.

Σκοπός στην παρούσα υποενότητα είναι να προσδιορίσουμε τα ιδεώδη του δακτυλίου ευθέος γινομένου $R=\prod_{k=1}^{n}R_k$ και ακολούθως να περιγράψουμε τα μεγιστοτικά ιδεώδη του R.

Υπενθυμίζουμε ότι ορίζονται οι επιμορφισμοί δακτυλίων, $1\le k\le n$:

$$\pi_k\colon R\longrightarrow R_k,\quad \pi_k(r_1,r_2,\cdots,r_n)=r_k$$

Με βάση τους παραπάνω ομομορφισμούς θα έχουμε :

$$\forall \mathsf{r}=(r_1,r_2,\cdots,r_n)\in R\colon\quad \mathsf{r}=\left((\pi_1(\mathsf{r}),\pi_2(\mathsf{r}),\cdots,\pi_n(\mathsf{r})\right)$$

Πρόταση 10.1.21. *Αν $I_k\subseteq R_k$ είναι ιδεώδη των δακτυλίων R_k αντίστοιχα, $1\le k\le n$, τότε το υποσύνολο*

$$I=I_1\times I_2\times\cdots\times I_n=\left\{(r_1,r_2,\cdots,r_n)\in\prod_{k=1}^{n}R_k\mid r_k\in I_k,\ 1\le k\le n\right\}$$

είναι ένα ιδεώδες του $R=\prod_{k=1}^{n}R_k$.

Αντίστροφα, κάθε ιδεώδες I του δακτυλίου ευθέος γινομένου $\prod_{k=1}^{n}R_k$ είναι της μορφής $I_1\times I_2\times\cdots\times I_n$, όπου $I_k\subseteq R_k$ είναι ιδεώδες του δακτυλίου R_k αντίστοιχα, $1\le k\le n$.

Απόδειξη. Προφανώς $0 = (0,0,\cdots,0) \in I$. Αν $x = (x_1, x_2, \cdots, x_n) \in I$, $y = (y_1, y_2, \cdots, y_n) \in I$ και $r = (r_1, r_2, \cdots, r_n) \in R$, τότε, επειδή $x_k - y_k \in I_k$ και $r_k x_k$, $x_k r_k \in I_k$, $1 \leq k \leq n$, θα έχουμε:

$$x - y = (x_1, x_2, \cdots, x_n) - (y_1, y_2, \cdots, y_n) = (x_1 - y_1, x_2 - y_2, \cdots, x_n - y_n) \ \in \ I$$

$$r \cdot x = (r_1, r_2, \cdots, r_n) \cdot (x_1, x_2, \cdots, x_n) = (r_1 x_1, r_2 x_2, \cdots, r_n x_n) \ \in \ I$$

$$x \cdot r = (x_1, x_2, \cdots, x_n) \cdot (r_1, r_2, \cdots, r_n) = (x_1 r_1, x_2 r_2, \cdots, x_n r_n) \ \in \ I$$

Επομένως το υποσύνολο I είναι ιδεώδες του R.

Αντίστροφα, έστω $K \subseteq R$ ένα ιδεώδες του R. Θεωρούμε τους κανονικούς επιμορφισμούς δακτυλίων

$$\pi_k : R = \prod_{k=1}^{n} R_k \longrightarrow R_k, \quad \pi_k(r_1, r_2, \cdots, r_n) = r_k, \quad 1 \leq k \leq n$$

και θέτουμε

$$I_k = \pi_k(K) = \big\{ r_k \in R_k \mid (r_1, r_2, \cdots, r_n) \in K \big\}, \quad 1 \leq k \leq n$$

Επειδή οι απεικονίσεις π_k, $1 \leq k \leq n$, είναι επιμορφισμοί δακτυλίων, από την Πρόταση 8.2.10, έπεται ότι το σύνολο I_k, $1 \leq k \leq n$, είναι ιδεώδες του R_k. Θα δείξουμε ότι $K = I_1 \times I_2 \times \cdots \times I_n$.

Αν $(r_1, r_2, \cdots, r_n) \in K$, τότε εκ κατασκευής γνωρίζουμε ότι $r_k \in I_k$, $1 \leq k \leq n$, και επομένως $(r_1, r_2, \cdots, r_n) \in I_1 \times I_2 \times \cdots \times I_n$. Άρα $K \subseteq I_1 \times I_2 \times \cdots \times I_n$.

Αντίστροφα, αν $r = (r_1, r_2, \cdots, r_n) \in I_1 \times I_2 \times \cdots \times I_n$, τότε υπάρχουν στοιχεία $s_1, s_2, \cdots, s_n \in K$, έτσι ώστε $\pi_k(s_k) = r_k$, $1 \leq k \leq n$. Επειδή για κάθε $k = 1, 2, \cdots, n$, έχουμε $s_k = (\pi_1(s_k), \pi_2(s_k), \cdots, \pi_n(s_k)) \in K$ και το K είναι ιδεώδες του R, θα έχουμε $(0, \cdots, 0, 1, 0, \cdots, 0) \cdot s_k = (0, \cdots, 0, \pi_k(s_k), 0, \cdots, 0) \in K$, $1 \leq k \leq n$, όπου η μονάδα είναι στην k-θέση. Επειδή το K είναι ιδεώδες του R, θα έχουμε

$$(\pi_1(s_1), 0, \cdots, 0) + (0, \pi_2(s_2), 0 \cdots, 0) + \cdots + (0, \cdots, 0, \pi_n(s_n)) = (\pi_1(s_1), \pi_2(s_2), \cdots, \pi_n(s_n)) = (r_1, r_2, \cdots, r_n) \in K$$

Αυτό σημαίνει ότι $I_1 \times I_2 \times \cdots \times I_n \subseteq K$, και άρα $K = I_1 \times I_2 \times \cdots \times I_n$. ■

Έχοντας προσδιορίσει τα ιδεώδη του $R_1 \times R_2 \times \cdots \times R_n$, προχωρούμε στην εύρεση όλων των μεγιστοτικών ιδεωδών του δακτυλίου $R_1 \times R_2 \times \cdots \times R_n$.

Θεώρημα 10.1.22. *Έστω $R = \prod_{k=1}^{n} R_k$ ο δακτύλιος ευθύ γινόμενο των δακτυλίων $R_1, R_2, \cdots, R_n$. Για ένα ιδεώδες M του R, τα ακόλουθα είναι ισοδύναμα:*

1. *Το M είναι μεγιστοτικό ιδεώδες του R.*
2. *Υπάρχει $k = 1, 2, \cdots, n$, και ένα μεγιστοτικό ιδεώδες M_k του δακτυλίου R_k, έτσι ώστε:*

$$M = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n$$

Απόδειξη. 2. «$\Longrightarrow$» 1. Υποθέτουμε ότι $M = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n$, όπου M_k είναι ένα μεγιστοτικό ιδεώδες του R_k. Ορίζουμε απεικόνιση

$$f_k : R \longrightarrow R_k / M_k, \quad f_k(r_1, r_2, \cdots, r_n) = r_k + M_k$$

Η απεικόνιση f_k είναι επιμορφισμός δακτυλίων διότι είναι σύνθεση $f_k = \pi_{M_k} \circ \pi_k$ των κανονικών επιμορφισμών $\pi_{M_k} : R_k \longrightarrow R_k / M_k$, $\pi_{M_k}(r_k) = r_k + M_k$, και $\pi_k : \prod_{k=1}^{n} R_k \longrightarrow R_k$, $\pi_k(r_1, r_2, \cdots, r_n) = r_k$.

Για τον πυρήνα του επιμορφισμού f_k, θα έχουμε:

$$\mathsf{Ker}(f_k) = \big\{ (r_1, r_2, \cdots, r_n) \in R \mid f_k(r_1, r_2, \cdots, r_n) = 0_{R_k/M_k} \big\} = \big\{ (r_1, r_2, \cdots, r_n) \in R \mid r_k + M_k = M_k \big\} =$$

$$= \big\{ (r_1, r_2, \cdots, r_n) \in R \mid r_k \in M_k \big\} = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n = M$$

Επομένως από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε έναν ισομορφισμό δακτυλίων

$$(R_1 \times \cdots R_{k-1} \times R_k \times R_{k+1} \times \cdots \times R_n) \big/ (R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n) \ \cong \ R_k / M_k$$

Επειδή το ιδεώδες M_k του R_k είναι μεγιστοτικό, έπεται ότι ο δακτύλιος R_k / M_k είναι απλός, και επομένως και ο δακτύλιος $(R_1 \times \cdots R_{k-1} \times R_k \times R_{k+1} \times \cdots \times R_n) \big/ (R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n)$ είναι απλός. Αυτό σημαίνει ότι το ιδεώδες $R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n$ του R είναι μεγιστοτικό.

1. «$\Longrightarrow$» 2. Θεωρούμε ένα μεγιστοτικό ιδεώδες M του $R_1 \times R_2 \times \cdots \times R_n$. Τότε από την Πρόταση 10.1.21 έπεται ότι $M = M_1 \times M_2 \times \cdots \times M_n$, όπου κάθε $M_l \subseteq R_l$ είναι ένα ιδεώδες του R_l, $1 \leq l \leq n$. Ορίζουμε απεικόνιση

$$f\colon R_1 \times R_2 \times \cdots \times R_n \longrightarrow R_1/M_1 \times R_2/M_2 \times \cdots \times R_n/M_n, \quad f(r_1, r_2, \cdots, r_n) = (r_1 + M_1, r_2 + M_2, \cdots, r_n + M_n)$$

Δηλαδή η f είναι το ευθύ γινόμενο των κανονικών επιμορφισμών δακτυλίων $\pi_k\colon R_k \longrightarrow R_k/M_k$, $\pi_k(r_k) = r_k + M_k$. Εύκολα βλέπουμε ότι η f είναι ένας επιμορφισμός δακτυλίων και επομένως από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε: $R_1 \times R_2 \times \cdots \times R_n)/\mathsf{Ker}(f) \cong R_1/M_1 \times R_2/M_2 \times \cdots \times R_n/M_n$. Επειδή προφανώς $\mathsf{Ker}(f) = M_1 \times M_2 \times \cdots \times M_n = M$, θα έχουμε έναν ισομορφισμό δακτυλίων

$$R/M \cong R_1/M_1 \times R_2/M_2 \times \cdots \times R_n/M_n$$

Επειδή, το ιδεώδες M είναι μεγιστοτικό, έπεται ότι ο δακτύλιος πηλίκο R/M είναι απλός, ή ισοδύναμα ο δακτύλιος ευθύ γινόμενο $R_1/M_1 \times R_2/M_2 \times \cdots \times R_n/M_n$ είναι απλός. Όμως, αν μεταξύ των ιδεωδών $M_1, M_2, \cdots, M_n$ υπάρχουν τουλάχιστον δύο ιδεώδη τα οποία είναι γνήσια, χωρίς βλάβη της γενικότητας, έστω τα M_k και M_l, όπου $k < l$, τότε ο δακτύλιος ευθύ γινόμενο $R_1/M_1 \times R_2/M_2 \times \cdots \times R_n/M_n$ δεν μπορεί να είναι απλός διότι περιέχει ως γνήσιο μη μηδενικό ιδεώδες το $M_1 \times \cdots \times R_k/M_k \times \cdots \times R_l/M_l \times \cdots \times M_n$. Επομένως όλα τα ιδεώδη $M_1, M_2, \cdots, M_n$ είναι μη γνήσια, εκτός από ένα, έστω το ιδεώδες M_k, και επομένως

$$M = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n$$

Το ιδεώδες M_k είναι μεγιστοτικό ιδεώδες του R_k διότι διαφορετικά θα είχαμε είτε ότι $M_k = R_k$ (το οποίο είναι άτοπο διότι διαφορετικά το M θα ήταν μη γνήσιο) είτε ότι υπάρχει ιδεώδες I του R_k έτσι ώστε $M_k \subseteq I$ (το οποίο είναι άτοπο διότι διαφορετικά θα είχαμε μια γνήσια έγκλειση ιδεωδών $M = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n \subseteq R_1 \times \cdots \times R_{k-1} \times I \times R_{k+1} \times \cdots \times R_n$, και αυτό μας οδηγεί σε αντίφαση διότι το M είναι μεγιστοτικό). Άρα καταλήγουμε ότι $M = R_1 \times \cdots \times R_{k-1} \times M_k \times R_{k+1} \times \cdots \times R_n$, όπου M_k είναι ένα μεγιστοτικό ιδεώδες του R_k για κάποιο $k = 1, 2, \cdots, n$. ■

Πόρισμα 10.1.23. *Έστω $R_1, R_2, \cdots, R_n$ μια πεπερασμένη οικογένεια απλών δακτυλίων, για παράδειγμα σωμάτων. Τότε ο δακτύλιος ευθύ γινόμενο $R_1 \times R_2 \times \cdots \times R_n$ περιέχει ακριβώς 2^n ιδεώδη και ακριβώς n μεγιστοτικά ιδεώδη.*

Απόδειξη. Επειδή κάθε δακτύλιος R_k είναι απλός, έπεται ότι περιέχει ακριβώς 2 ιδεώδη, τα τετριμμένα. Από την Πρόταση 10.1.21 έπεται τότε ότι ο δακτύλιος ευθέος γινομένου περιέχει ακριβώς 2^n ιδεώδη, τα εξής:

$$I_1 \times I_2 \times \cdots \times I_n, \quad \text{όπου} \quad I_k = \{0\} \ \text{ή} \ I_k = R_k, \quad 1 \leq k \leq n$$

Για τα μεγιστοτικά ιδεώδη, επειδή το μοναδικό μεγιστοτικό ιδεώδες του απλού δακτυλίου R_k είναι το μηδενικό ιδεώδες, έπεται ότι τα μεγιστοτικά ιδεώδη του δακτυλίου ευθύ γινόμενο $R_1 \times R_2 \times \cdots \times R_n$ είναι σε πλήθος ακριβώς n, τα εξής:

$$\{0\} \times R_2 \times \cdots \times R_n, \ \ R_1 \times \{0\} \times \cdots \times R_n, \ \cdots, \ R_1 \times R_2 \times \cdots \times \{0\}$$ ■

Παράδειγμα 10.1.24. Θεωρούμε τον δακτύλιο ευθύ γινόμενο $R = \mathbb{R} \times \mathbb{C} \times \mathbb{Z}$. Τότε τα μεγιστοτικά ιδεώδη του R είναι τα εξής:

$$\{0\} \times \mathbb{C} \times \mathbb{Z}, \quad \mathbb{R} \times \{0\} \times \mathbb{Z}, \quad \mathbb{R} \times \mathbb{C} \times p\mathbb{Z} \quad (p\colon \text{πρώτος})$$

με αντίστοιχους δακτυλίους πηλίκα, τα σώματα: $\mathbb{R}$, $\mathbb{C}$, και $\mathbb{Z}/p\mathbb{Z}$. $\surd$

Μεγιστοτικά Ιδεώδη σε Δακτυλίους Τυπικών Δυναμοσειρών

Έστω $\mathbb{K}[\![t]\!]$ ο δακτύλιος των τυπικών δυναμοσειρών με στοιχεία από ένα σώμα $\mathbb{K}$. Στην παρούσα υποενότητα θα προσδιορίσουμε τα μεγιστοτικά και τα πρώτα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$.

Θεωρούμε το υποσύνολο

$$M = \left\{ P(t) = \sum_{n=0}^{\infty} a_n t^n \in \mathbb{K}[\![t]\!] \mid a_0 = 0 \right\}$$

Τότε $M = (t)$ είναι το κύριο ιδεώδες του $\mathbb{K}[\![t]\!]$ το οποίο παράγεται από το πολυώνυμο t. Πράγματι, προφανώς θα έχουμε $M \subseteq (t)$. Αντίστροφα, αν $P(t) \in (t)$, τότε $P(t) = Q(t)t$, όπου $Q(t) \in \mathbb{K}[\![t]\!]$. Αν $Q(t) = \sum_{k=0}^{\infty} b_k t^k$, τότε $P(t) = Q(t)t = \sum_{k=0}^{\infty} b_k t^{k+1}$ και προφανώς $P(t) \in M$, διότι ο σταθερός όρος της τυπικής δυναμοσειράς είναι ίσος με 0.

Θεωρούμε απεικόνιση

$$f : \mathbb{K}[\![t]\!] \longrightarrow \mathbb{K}, \quad f\Big(\sum_{k=0}^{\infty} a_k t^k\Big) = a_0$$

Από τον ορισμό των πράξεων πρόσθεσης και πολλαπλασιασμού τυπικών δυναμοσειρών, έπεται άμεσα ότι η απεικόνιση f είναι ομομορφισμός δακτυλίων, ο οποίος προφανώς είναι επιμορφισμός. Για τον πυρήνα του f έχουμε $\mathsf{Ker}(f) = M$, και επομένως από το Πρώτο Θεώρημα Ισομορφισμών δακτυλίων, θα έχουμε έναν ισομορφισμό δακτυλίων:

$$\mathbb{K}[\![t]\!]/M \cong \mathbb{K}$$

Άρα το M είναι μεγιστοτικό ιδεώδες του $\mathbb{K}[\![t]\!]$.

Θα δείξουμε ότι το M είναι το μοναδικό μεγιστοτικό ιδεώδες του $\mathbb{K}[\![t]\!]$, δηλαδή ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι τοπικός. Σύμφωνα με την Πρόταση 10.1.17, αρκεί να δείξουμε ότι για κάθε τυπική δυναμοσειρά $P(t) = \sum_{k=0}^{\infty} a_k t^k$, είτε η $P(t)$ είναι αντιστρέψιμη είτε η $1 - P(t)$ είναι αντιστρέψιμη.

Θα αναλύσουμε το πρόβλημα σε γενικότερο πλαίσιο, προσδιορίζοντας πρώτα τα αντιστρέψιμα στοιχεία του δακτυλίου $R[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω τυχόντος μεταθετικού δακτυλίου R.

Λήμμα 10.1.25. *Έστω R ένας μεταθετικός δακτύλιος. Μια τυπική δυναμοσειρά $P(t) = \sum_{k=0}^{\infty} a_k t^k$ είναι αντιστρέψιμο στοιχείο του δακτυλίου $R[\![t]\!]$ αν και μόνο αν ο σταθερός όρος της a_0 είναι αντιστρέψιμο στοιχείο του R:*

$$\mathsf{U}\big(\mathbb{K}[\![t]\!]\big) = \left\{ \sum_{n=0}^{\infty} a_n t^n \in \mathbb{K}[\![t]\!] \;\Big|\; a_0 \in \mathsf{U}(R) \right\}$$

Απόδειξη. Αν η τυπική δυναμοσειρά $P(t)$ είναι αντιστρέψιμη, τότε υπάρχει τυπική δυναμοσειρά $Q(t) = \sum_{k=0}^{\infty} b_k t^k$, έτσι ώστε $P(t)Q(t) = 1$, δηλαδή $a_0 b_0 + (a_0 b_1 + a_1 b_0)t + (a_0 b_2 + a_1 b_1 + a_2 b_0)t^2 + \cdots = 1 + 0 + 0 + \cdots$, από όπου έπεται ότι $a_0 b_0 = 1$ και επομένως το στοιχείο a_0 είναι αντιστρέψιμο στοιχείο του R.

Αντίστροφα, αν το στοιχείο a_0 είναι αντιστρέψιμο στοιχείο του R, έστω $b_0 = a_0^{-1}$ το αντίστροφό του στον δακτύλιο R. Ορίζουμε στοιχεία του R επαγωγικά ως εξής:

$$b_k = -a_0^{-1} \sum_{i=1}^{k} a_i b_{k-i}, \quad k \geq 1$$

Έτσι για παράδειγμα: $b_1 = -a_0^{-1} a_1 b_0$, $b_2 = -a_0^{-1}(a_1 b_1 + a_2 b_0)$, κλπ. Θεωρούμε την τυπική δυναμοσειρά $Q(t) = \sum_{k=0}^{\infty} b_k t^k$. Από τον ορισμό των πράξεων πρόσθεσης και πολλαπλασιασμού τυπικών δυναμοσειρών έπεται άμεσα ότι $P(t)Q(t) = 1$ και επομένως η τυπική δυναμοσειρά $P(t)$ είναι αντιστρέψιμο στοιχείο του $R[\![t]\!]$. ■

Ιδιαίτερα αν $\mathbb{K}$ είναι ένα σώμα, η τυπική δυναμοσειρά $P(t) = \sum_{k=0}^{\infty} a_k t^k$ είναι αντιστρέψιμο στοιχείο του δακτυλίου $\mathbb{K}[\![t]\!]$ αν και μόνο αν ο σταθερός όρος $a_0 \neq 0$.

Παράδειγμα 10.1.26. Θεωρούμε τις τυπικές δυναμοσειρές (πολυώνυμα) $1 + t$ και $1 - t$, οι οποίες, σύμφωνα με το Λήμμα 10.1.25, είναι αντιστρέψιμα στοιχεία του $\mathbb{K}[\![t]\!]$, όπου $\mathbb{K}$ είναι ένα σώμα. Λαμβάνοντας υπόψη την

κατασκευή της αντίστροφης μιας αντιστρέψιμης τυπικής δυναμοσειράς στο Λήμμα 10.1.25, υπολογίζουμε εύκολα ότι:

$$(1-t)^{-1} = \sum_{k=0}^{\infty} t^k = 1 + t + t^2 + \cdots + t^n + \cdots \qquad \text{και} \qquad (1+t)^{-1} = \sum_{k=0}^{\infty} (-1)^k t^k = 1 - t + t^2 - \cdots + (-1)^n t^n + \cdots \quad \surd$$

Έστω τώρα η τυπική δυναμοσειρά $P(t) = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{K}[\![t]\!]$, όπου $\mathbb{K}$ είναι ένα σώμα. Αν $a_0 \neq 0$, τότε η $P(t)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$. Αν $a_0 = 0$, τότε ο σταθερός όρος της δυναμοσειράς $1 - P(t)$ είναι $1 - a_0 = 1 \neq 0$ και η $1 - P(t)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$.

Γενικότερα, αν R είναι ένας τοπικός (μεταθετικός) δακτύλιος, και $P(t) = \sum_{k=0}^{\infty} a_k t^k \in R[\![t]\!]$, τότε για τον σταθερό όρο θα έχουμε ότι είτε το a_0 είναι αντιστρέψιμο στοιχείο του R είτε το $1 - a_0$ είναι αντιστρέψιμο στοιχείο του R. Αυτό σημαίνει ότι είτε η δυναμοσειρά $P(t)$ είναι αντιστρέψιμο στοιχείο του $R[\![t]\!]$ είτε η δυναμοσειρά $1 - P(t)$ είναι αντιστρέψιμο στοιχείο του $R[\![t]\!]$. Επομένως από την Πρόταση 10.1.17 έπεται ότι ο δακτύλιος $R[\![t]\!]$ είναι τοπικός. Ιδιαίτερα ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες το M. Παρόμοια το μοναδικό μεγιστοτικό ιδεώδες του δακτυλίου $R[\![t]\!]$, όπου R είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες το $\mathfrak{n} = R \setminus \mathsf{U}(R)$, είναι το ιδεώδες

$$\mathfrak{m} = \left\{ P(t) = \sum_{n=0}^{\infty} a_n t^n \ \in \ \mathbb{K}[\![t]\!] \mid a_0 \in R \setminus \mathsf{U}(R) = \mathfrak{N} \right\}$$

Πράγματι, θεωρούμε την απεικόνιση

$$f \colon R[\![t]\!] \longrightarrow R/\mathfrak{n}, \quad f\big(\sum_{k=0}^{\infty} a_k t^k\big) = a_0 + \mathfrak{n}$$

Η απεικόνιση f είναι επιμορφισμός δακτυλίων ως σύνθεση των επιμορφισμών $R[\![t]\!] \longrightarrow R$, $\sum_{k=0}^{\infty} a_k t^k \longmapsto a_0$ και $R \longrightarrow R/\mathfrak{n}$, $r \longmapsto r + \mathfrak{n}$. Για τον πυρήνα της f θα έχουμε

$$\mathsf{Ker}(f) = \big\{ \sum_{k=0}^{\infty} a_k t^k \in R[\![t]\!] \mid f\big(\sum_{k=0}^{\infty} a_k t^k\big) = 0_{R/\mathfrak{n}} \big\} = \big\{ \sum_{k=0}^{\infty} a_k t^k \in R[\![t]\!] \mid a_0 + \mathfrak{n} = \mathfrak{n} \big\} = \big\{ \sum_{k=0}^{\infty} a_k t^k \in R[\![t]\!] \mid a_0 \in \mathfrak{n} \big\} = \mathfrak{m}$$

Επομένως θα έχουμε ένα ισομορφισμό δακτυλίων

$$R[\![t]\!]/\mathfrak{m} \ \cong \ R/\mathfrak{n}$$

Επειδή το $\mathfrak{n}$ είναι μεγιστοτικό ιδεώδες του R, ο δακτύλιος $R/\mathfrak{n}$, ισοδύναμα ο δακτύλιος $R[\![t]\!]/\mathfrak{m}$, είναι σώμα, και επομένως το ιδεώδες $\mathfrak{m}$ του $R[\![t]\!]$ είναι μεγιστοτικό, και άρα είναι το μοναδικό μεγιστοτικό ιδεώδες του τοπικού δακτυλίου $R[\![t]\!]$.

Συνοψίζοντας, θα έχουμε την ακόλουθη Πρόταση:

Πρόταση 10.1.27. *Έστω R ένας μεταθετικός τοπικός δακτύλιος με μοναδικό μεγιστοτικό ιδεώδες $\mathfrak{n}$. Τότε ο δακτύλιος $R[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του R είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες το*

$$\mathfrak{m} = \left\{ \sum_{k=0}^{\infty} a_k t^k \in R[\![t]\!] \mid a_0 \in \mathfrak{n} \right\}$$

Ιδιαίτερα ο δακτύλιος $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω ενός σώματος $\mathbb{K}$ είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες το κύριο ιδεώδες (t), δηλαδή το σύνολο όλων των τυπικών δυναμοσειρών υπεράνω του $\mathbb{K}$ με μηδενικό σταθερό όρο.

10.2 Πρώτα Ιδέωδη

Ορισμός 10.2.1. *Ένα ιδεώδες $I \subseteq R$ καλείται* **πρώτο ιδεώδες** *του R, αν:*

1. $I \neq R$.
2. *Αν I και J είναι ιδεώδη του R, τότε:*

$$I \cdot J \subseteq P \implies I \subseteq P \quad J \subseteq P$$

Το σύνολο όλων των πρώτων ιδεωδών του δακτυλίου R συμβολίζεται με $\mathsf{Spec}(R)$.

Ορισμός 10.2.2. *Ένας δακτύλιος R καλείται* **πρώτος δακτύλιος** *αν και μονον αν το μηδενικό ιδεώδες του είναι πρώτο, δηλαδή, αν I και J είναι ιδεώδη του R, τότε:*

$$I \cdot J = 0 \implies I = 0 \quad J = 0$$

Η έννοια του πρώτου δακτυλίου, όπως αυτή ορίστηκε παραπάνω, δεν έχει σχέση με την έννοια του πρωτοδακτυλίου ενός δακτυλίου R, όπως αυτή μελετήθηκε στην υποενότητα 7.3.1, δηλαδή του υποδακτυλίου του R ο οποίος παράγεται από την μονάδα 1_R του R.

Παράδειγμα 10.2.3. Έστω R ένας απλός δακτύλιος. Τότε το μηδενικό ιδεώδες $\{0\}$ του R είναι πρώτο. Πράγματι, επειδή τα μόνα ιδεώδη του R είναι τα τετριμμένα $\{0\}$ και R, αν I, J είναι ιδεώδη του R έτσι ώστε $I \cdot J = \{0\}$, τότε προφανώς είτε $I = \{0\}$ ή $J = \{0\}$. $\surd$

Θα επικεντρώσουμε την προσοχή μας στη μελέτη των πρώτων ιδεωδών στο πλαίσιο μεταθετικών δακτυλίων. Σ' αυτή την κατεύθυνση, έχουμε τους ακόλουθους βασικούς χαρακτηρισμούς πρώτων ιδεωδών.

Θεώρημα 10.2.4. *Αν R είναι ένας μεταθετικός δακτύλιος, τότε για ένα γνήσιο ιδεώδες P του R τα ακόλουθα είναι ισοδύναμα:*

1. *Το ιδεώδες P είναι πρώτο.*
2. *Αν $r, s \in R$, τότε: $r \cdot s \in P \implies r \in P$ ή $s \in P$.*
3. *Ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή.*

Απόδειξη. «1. $\implies$ 2.» Υποθέτουμε ότι το ιδεώδες P είναι πρώτο, και έστω $r, s \in R$ δύο στοιχεία του R έτσι ώστε $rs \in P$. Θεωρούμε τα κύρια ιδεώδη (r) και (s) τα οποία παράγονται από τα στοιχεία r, s. Επειδή ο δακτύλιος R είναι μεταθετικός, θα έχουμε $(r) = \{ar \in R \mid a \in R\}$ και ανάλογα $(s) = \{as \in R \mid a \in R\}$. Ένα τυπικό στοιχείο του ιδεώδους γινόμενο $(r) \cdot (s)$ είναι ένα πεπερασμένο άθροισμα γινομένων της μορφής $arbs = abrs$ και επομένως, επειδή $rs \in P$, έπεται άμεσα ότι κάθε στοιχείο του γινομένου $(r) \cdot (s)$ ανήκει στο P, δηλαδή: $(r) \cdot (s) \subseteq P$. Επειδή το ιδεώδες P είναι πρώτο, έπεται ότι $(r) \subseteq P$ ή $(s) \subseteq P$. Αυτό σημαίνει ιδιαίτερα ότι $r \in P$ ή $s \in P$.

«2. $\implies$ 3.» Υποθέτουμε ότι αν $r, s \in R$, και $r \cdot s \in P$, τότε είτε $r \in P$ είτε $s \in P$. Έστω $a + P$, $b + P$ δύο στοιχεία του δακτυλίου πηλίκου R/P. Τότε, χρησιμοποιώντας την υπόθεση, θα έχουμε:

$$(a+P) \cdot (b+P) = P \implies a \cdot b + P = P \implies a \cdot b \in P \implies a \in P \text{ ή } b \in P \implies a + P = P \text{ ή } b + P = P$$

Άρα ο μεταθετικός δακτύλιος R/P δεν έχει διαιρέτες του μηδενός και επομένως είναι ακέραια περιοχή.

«3. $\implies$ 1.» Υποθέτουμε ότι ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή και έστω I και J δύο ιδεώδη του R έτσι ώστε $I \cdot J \subseteq P$. Έστω ότι $I \nsubseteq P$. Τότε υπάρχει στοιχείο $a \in I$ και $a \notin P$. Για κάθε στοιχείο $b \in J$, θεωρούμε το στοιχείο ab. Προφανώς το στοιχείο $ab \in I \cdot J$ και άρα $ab \in P$. Επειδή ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή, θα έχουμε

$$ab \in P \implies ab + P = P \implies (a+P) \cdot (b+P) = P \implies a \in P \text{ ή } b \in P$$

Επειδή $a \notin P$, έπεται ότι $b \in P$. Έτσι δείξαμε ότι κάθε στοιχείο b του J ανήκει στο P και άρα $J \subseteq P$. Παρόμοια δείχνουμε ότι αν $J \nsubseteq P$, τότε $I \subseteq P$. Άρα το ιδεώδες P είναι πρώτο. ■

Από το παραπανω Θεώρημα έπεται ότι, αν ο δακτύλιος R είναι μεταθετικός, τότε ένα ιδεώδες $P \subseteq R$ είναι πρώτο αν και μόνο το σύνολο $R \setminus P$ είναι κλειστό στον πολλαπλασιασμό και περιέχει την μονάδα, δηλαδή το ιδεώδες P είναι πρώτο αν και μονον αν το σύνολο $R \setminus P$ είναι ένα υπομονοειδές του πολλαπλασιαστικού μονοειδούς $(R, \cdot)$.

Παράδειγμα 10.2.5. Αν ο δακτύλιος R δεν είναι μεταθετικός, τότε το Θεώρημα 10.2.4 δεν ισχύει. Πράγματι έστω ο δακτύλιος $R = \mathsf{M}_n(\mathbb{K})$ των $n \times n$ πινάκων με στοιχεία από ένα σώμα $\mathbb{K}$. Γνωρίζουμε ότι ο δακτύλιος R είναι απλός, και άρα, σύμφωνα με το Παράδειγμα 10.2.3, το μηδενικό ιδεώδες του $\{0\}$ είναι πρώτο. Όμως $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\cdot\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right) = 0$, αλλά $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right),\ \left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right) \notin \left\{\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)\right\}$. $\surd$

Πόρισμα 10.2.6. *Σε έναν μεταθετικό δακτύλιο R κάθε μεγιστοτικό ιδεώδες είναι πρώτο.*

Απόδειξη. Έστω R ένας μεταθετικός δακτύλιος και έστω P ένα μεγιστοτικό ιδεώδες του R. Τότε, σύμφωνα με το Θεώρημα 10.1.4, ο δακτύλιος πηλίκο R/P είναι σώμα. Επειδή, όπως γνωρίζουμε, κάθε σώμα είναι ακέραια περιοχή, έπεται ότι ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή. Τότε από το Θεώρημα 10.2.4 έπεται ότι το ιδεώδες P είναι πρώτο. ■

Παράδειγμα 10.2.7. Το συμπέρασμα του παραπάνω Πορίσματος δεν ισχύει αν ο μεταθετικός δακτύλιος R δεν έχει μονάδα. Πράγματι το σύνολο $2\mathbb{Z}$ των άρτιων ακεραίων είναι ένας μεταθετικός δακτύλιος χωρίς μονάδα. Η προσθετική υποομάδα $4\mathbb{Z} \subseteq 2\mathbb{Z}$ είναι προφανώς ένα ιδεώδες του $\mathbb{Z}$ το οποίο είναι μεγιστοτικό. Πράγματι το $4\mathbb{Z}$ είναι γνήσιο ιδεώδες του $2\mathbb{Z}$. Έστω I ένα ιδεώδες του $2\mathbb{Z}$ έτσι ώστε $4\mathbb{Z} \subseteq I \subseteq 2\mathbb{Z}$ και $4\mathbb{Z} \neq I$. Αν $I \neq 2\mathbb{Z}$, τότε υπάρχει $x \in I \setminus 2\mathbb{Z}$, και άρα $x = 2k$, όπου $k \in \mathbb{Z}$. Αν $k = 2m$ για κάποιον ακέραιο $m \in \mathbb{Z}$, τότε $x = 4m \in 4\mathbb{Z}$, το οποίο είναι άτοπο. Άρα $k = 2m+1$, όπου $m \in \mathbb{Z}$, και τότε $x = 4m+2 \in I$. Επειδή $4m \in 4\mathbb{Z} \subseteq I$, θα έχουμε $2 = x - 4m \in I$ και τότε προφανώς $I = \mathbb{Z}$, το οποίο είναι άτοπο. Άρα $I = 2\mathbb{Z}$ και επομένως το $4\mathbb{Z}$ είναι μεγιστοτικό ιδεώδες του $2\mathbb{Z}$, το οποίο όμως δεν είναι πρώτο διότι $4 = 2 \cdot 2 \in 4\mathbb{Z}$ αλλά $2 \notin 4\mathbb{Z}$. $\surd$

Πόρισμα 10.2.8. *Αν ο δακτύλιος R είναι μεταθετικός, τότε το μηδενικό ιδεώδες (0) του R είναι πρώτο αν και μόνο αν ο δακτύλιος R είναι ακέραια περιοχή.*

Απόδειξη. Επειδή το μηδενικό ιδεώδες είναι γνήσιο και $R/(0) \cong R$, από το Θεώρημα 10.2.4, έπεται ότι ο δακτύλιος R είναι ακέραια περιοχή αν και μόνο αν το μηδενικό ιδεώδες (0) είναι πρώτο. ■

Το ακόλουθο παράδειγμα δείχνει ότι υπάρχουν πρώτα ιδεώδη τα οποία δεν είναι μεγιστοτικά.

Παράδειγμα 10.2.9.

1. Επειδή ο δακτύλιος των ακεραίων $\mathbb{Z}$ είναι ακέραια περιοχή, το μηδενικό ιδέωδες (0) του $\mathbb{Z}$ είναι πρώτο. Όμως, επειδή ο δακτύλιος $\mathbb{Z}$ δεν είναι σώμα, από το Πόρισμα 10.1.6 έπεται ότι το μηδενικό ιδεώδες (0) δεν είναι μεγιστοτικό.

2. Αν εξαιρέσουμε το μηδενικό ιδεώδες του $\mathbb{Z}$, τότε κάθε μη μηδενικό πρώτο ιδεώδες του $\mathbb{Z}$ είναι μεγιστοτικό. Πράγματι, αυτό προκύπτει άμεσα από την Πρόταση 7.4.16.

3. Θεωρούμε τον δακτύλιο πολυωνύμων $\mathbb{Z}[t]$. Τότε το κύριο ιδεώδες (t), το οποίο αποτελείται από όλα τα πολυώνυμα με μηδενικό σταθερό όρο, είναι ένα πρώτο ιδεώδες το οποίο δεν είναι μεγιστοτικό διότι ο δακτύλιος πηλίκο $\mathbb{Z}[t]/(t)$ είναι ισόμορφος με τον δακτύλιο $\mathbb{Z}$ των ακεραίων ο οποίος είναι ακέραια περιοχή αλλά όχι σώμα. $\surd$

P: πρώτο ιδεώδες $\Longrightarrow$ P: μεγιστοτικό ιδεώδες

Γνωρίζουμε ότι κάθε μεγιστοτικό ιδεώδες σε έναν δακτύλιο είναι πρώτο, αλλά γενικά ένα πρώτο ιδεώδες σε έναν δακτύλιο δεν είναι μεγιστοτικό. Στην παρούσα υποενότητα, θα δούμε κάποιες κλάσεις δακτυλίων στις οποίες κάθε πρώτο (μη μηδενικό) ιδεώδες είναι μεγιστοτικό.

Παράδειγμα 10.2.10. Θα προσδιορίσουμε τα πρώτα και τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{Z}_n$, $n \geq 2$.

Από το Θεώρημα αντιστοιχίας, έπεται ότι τα γνήσια ιδεώδη του $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ είναι της μορφής $k\mathbb{Z}/n\mathbb{Z}$, όπου $n\mathbb{Z} \subseteq k\mathbb{Z}$. Η τελευταία σχέση έγκλεισης είναι προφανώς ισοδύναμη με το ότι $n \in k\mathbb{Z}$, δηλαδή $n = k \cdot l$ ή ισοδύναμα $k \mid n$. Δηλαδή τα γνήσια ιδεώδη του $\mathbb{Z}_n$ είναι της μορφής $k\mathbb{Z}/n\mathbb{Z}$, όπου k είναι ένας θετικός διαιρέτης του n. Για τους επαγόμενους δακτύλιους πηλίκα, θα έχουμε:

$$\mathbb{Z}/n\mathbb{Z}\big/k\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/k\mathbb{Z}$$

και επομένως το ιδεώδες $k\mathbb{Z}/n\mathbb{Z}$ είναι μεγιστοτικό αν και μόνο αν ο δακτύλιος $\mathbb{Z}/k\mathbb{Z}$ είναι σώμα, και το ιδεώδες $k\mathbb{Z}/n\mathbb{Z}$ είναι πρώτο αν και μόνο αν ο δακτύλιος $\mathbb{Z}/k\mathbb{Z}$ είναι ακέραια περιοχή. Χρησιμοποιώντας την Πρόταση 7.4.16, έπεται τότε ότι το ιδεώδες $k\mathbb{Z}/n\mathbb{Z}$ του δακτυλίου $\mathbb{Z}/n\mathbb{Z}$ είναι μεγιστοτικό αν και μόνο αν είναι πρώτο αν και μόνο αν ο k είναι ένας πρώτος διαιρέτης του n. $\surd$

Το παραπάνω παράδειγμα, το οποίο ιδιαίτερα δείχνει ότι στον πεπερασμένο δακτύλιο $\mathbb{Z}_n$, ένα ιδεώδες είναι μεγιστοτικό αν και μόνο αν είναι πρώτο, είναι ειδική περίπτωση του ακόλουθου γενικότερου αποτελέσματος.

Πρόταση 10.2.11. *Έστω R ένας μεταθετικός δακτύλιος με πεπερασμένο πλήθος στοιχείων. Τότε ένα ιδεώδες του R είναι πρώτο αν και μόνο αν είναι μεγιστοτικό.*

Απόδειξη. Γνωρίζουμε ότι σε έναν μεταθετικό δακτύλιο κάθε μεγιστοτικό ιδεώδες είναι πρώτο. Έστω P ένα πρώτο ιδεώδες του δακτυλίου R ο οποίος υποθέτουμε ότι έχει πεπερασμένο πλήθος στοιχείων. Γνωρίζουμε τότε ότι: (α) ότι ο δακτύλιος πηλίκο R/P είναι μια ακέραια περιοχή (διότι το ιδεώδες P είναι πρώτο), και (β) ο δακτύλιος R/P έχει πεπερασμένο πλήθος στοιχείων (διότι $|R| < \infty$). Επειδή κάθε πεπερασμένη ακέραια περιοχή είναι σώμα, έπεται ότι ο δακτύλιος R/P είναι σώμα, και αυτό είναι ισοδύναμο με το ότι το ιδεώδες P είναι μεγιστοτικό. ■

Μεγιστοτικά-Πρώτα Ιδεώδη σε Δακτυλίους του Boole

Θα δούμε μια ενδιαφέρουσα κλάση δακτυλίων στην οποία κάθε πρώτο ιδεώδες είναι μεγιστοτικό.

Ένας δακτύλιος R καλείται **δακτύλιος του Boole**, αν κάθε στοιχείο του είναι ταυτοδύναμο: $r^2 = r$, $\forall r \in R$. Η ακόλουθη Πρόταση περιγράφει τις βασικές ιδιότητες ενός δακτυλίου του Boole.

Πρόταση 10.2.12. *Έστω R ένας δακτύλιος του Boole.*

1. *Ο δακτύλιος R είναι μεταθετικός με χαρακτηριστική* $\mathsf{char}(R) = 2$.
2. *Κάθε υποδακτύλιος και κάθε δακτύλιος πηλίκο του R είναι δακτύλιος του Boole.*
3. *Ο R είναι σώμα $\iff$ ο R είναι ακέραια περιοχή $\iff$ ο R ισόμορφος με το σώμα $\mathbb{Z}_2$.*

Απόδειξη. 1. Αν $x, y \in R$, τότε θα έχουμε:

$$(x+y)^2 = x+y \implies (x+y)\cdot(x+y) = x+y \implies x^2+xy+yx+y^2 = x+y \implies x+xy+yx+y = x+y \implies$$

$$\implies xy+yx = 0 \implies xy = -yx \qquad (*)$$

Θέτοντας στην παραπάνω σχέση $x = y = r \in R$, βλέπουμε ότι $r \cdot r = -r \cdot r$, δηλαδή $r^2 = -r^2$ ή ισοδύναμα $r = -r$, $\forall r \in R$. Έτσι η σχέση $(*)$ γράφεται $xy = yx$, $\forall x, y \in R$, δηλαδή ο δακτύλιος R είναι μεταθετικός. Τέλος, επειδή $r = -r$, $\forall r \in R$, θα έχουμε $2r = 0$, από όπου άμεσα έπεται ότι $\mathsf{char}(R) = 2$.

2. Προφανώς κάθε υποδακτύλιος του R είναι δακτύλιος του Boole. Έστω $I \subseteq R$ ένα ιδεώδες του R, τότε για το τυχόν στοιχείο $x + I \in R/I$, θα έχουμε

$$(x+I)^2 = (x+I)\cdot(x+I) = x^2 + I = x + I$$

και επομένως ο δακτύλιος πηλίκο R/I είναι δακτύλιος του Boole.

3. Αν ο δακτύλιος R είναι σώμα, τότε είναι ακέραια περιοχή. Αν ο δακτύλιος του Boole R είναι ακέραια περιοχή, τότε για κάθε στοιχείο $r \in R$, θα έχουμε $r^2 = r$, δηλαδή $r \cdot (1_R - r) = 0$, από όπου επειδή ο R δεν έχει διαιρέτες του μηδενός, έπεται ότι $r = 0$ ή $r = 1_R$. Αυτό σημαίνει ότι $R = \{0, 1_R\}$ και τότε η απεικόνιση
$$f : R \longrightarrow \mathbb{Z}_2, \quad f(0) = [0]_2 \quad \text{και} \quad f(1_R) = [1]_2$$
είναι ένας ισομορφισμός δακτυλίων διότι: f στέλνει τη μονάδα του R στη μονάδα του $\mathbb{Z}_2$, και για την μόνη μη τετριμμένη πράξη μεταξύ των στοιχείων του R, δηλαδή διαφορετική των $0 + 1_R, 1_R + 0, 0 + 0$, και $0 \cdot 1_R, 1_R \cdot 0, 0 \cdot 0, 1_R \cdot 1_R$, θα έχουμε: $f(1_R + 1_R) = f(0) = [0]_2 = [2]_2 = [1]_2 + [1]_2 = f(1_R) + f(1_R)$, διότι $\mathsf{char}(R) = 2$. Τέλος, προφανώς ο R είναι σώμα, αν είναι ισόμορφος με το σώμα $\mathbb{Z}_2$. ■

Πόρισμα 10.2.13. *Σε έναν δακτύλιο του Boole, ένα ιδεώδες είναι μεγιστοτικό αν και μόνο αν είναι πρώτο.*

Απόδειξη. Έστω R ένας δακτύλιος του Boole και P ένα πρώτο ιδεώδες του R. Τότε ο δακτύλιος πηλίκο R/P είναι ακέραια περιοχή, και επίσης, σύμφωνα με την Πρόταση 10.2.12, είναι δακτύλιος του Boole. Τότε πάλι από την Πρόταση 10.2.12 ο δακτύλιος πηλίκο R/P είναι σώμα (ισόμορφος με το σώμα $\mathbb{Z}_2$), και άρα το ιδεώδες P είναι μεγιστοτικό. ■

Μεγιστοτικά-Πρώτα Ιδεώδη σε Δακτυλίους Πολυωνύμων

Υπενθυμίζουμε ότι ένα πολυώνυμο $P(t) \in \mathbb{K}[t]$ με συντελεστές από ένα σώμα $\mathbb{K}$ καλείται *ανάγωγο πολυώνυμο*, αν το $P(t)$ δεν είναι σταθερό πολυώνυμο και δεν μπορεί να γραφεί ως γινόμενο $P(t) = P_1(t) \cdot P_2(t)$ δύο μη σταθερών πολυωνύμων $P_1(t), P_2(t) \in \mathbb{K}[t]$. Στην απόδειξη του ακόλουθου αποτελέσματος, θα χρησιμοποιήσουμε το Θεώρημα 9.2.1 το οποίο πιστοποιεί ότι κάθε ιδεώδες του δακτυλίου πολυωνύμων $\mathbb{K}[t]$, όπου $\mathbb{K}$ είναι ένα σώμα, είναι κύριο ιδεώδες.

Πρώτα σημειώνουμε ότι το μηδενικό ιδεώδες του δακτυλίου $\mathbb{K}[t]$ είναι πρώτο, διότι ο δακτύλιος $\mathbb{K}[t]$ είναι ακέραια περιοχή, και δεν είναι μεγιστοτικό διότι ο δακτύλιος $\mathbb{K}[t]$ δεν είναι σώμα. Επίσης ένα κύριο ιδεώδες $I = (P(t))$ όπου το πολυώνυμο $P(t)$ είναι σταθερό μη μηδενικό πολυώνυμο, δεν είναι ποτέ πρώτο ή μεγιστοτικό διότι, αν $P(t) = a \in \mathbb{K} \setminus \{0\}$, τότε το $P(t)$ είναι προφανώς αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$ και άρα $I = (P(t)) = \mathbb{K}[t]$.

Πρόταση 10.2.14. *Έστω $\mathbb{K}$ ένα σώμα και $\mathbb{K}[t]$ ο δακτύλιος πολυωνύμων υπεράνω του $\mathbb{K}$. Αν I είναι ένα μη μηδενικό γνήσιο ιδεώδες του $\mathbb{K}[t]$, τότε τα ακόλουθα είναι ισοδύναμα*

1. *Το ιδεώδες I είναι μεγιστοτικό.*
2. *Το ιδεώδες I είναι πρώτο.*
3. *$I = (P(t))$ είναι το κύριο ιδεώδες του $\mathbb{K}[t]$ το οποίο παράγεται από ένα ανάγωγο πολυώνυμο $P(t) \in \mathbb{K}[t]$.*

Απόδειξη. 1. «$\Longrightarrow$» 2. Προφανώς κάθε μεγιστοτικό ιδεώδες είναι πρώτο.

2. «$\Longrightarrow$» 3. Επειδή κάθε ιδεώδες του $\mathbb{K}[t]$ είναι κύριο, θα έχουμε $I = (P(t))$, για ένα πολυώνυμο $P(t) \in \mathbb{K}[t]$. Έστω ότι το ιδεώδες I είναι πρώτο, οπότε ο δακτύλιος πηλίκο $\mathbb{K}[t]/I$ είναι ακέραια περιοχή. Έστω $P(t) = P_1(t) \cdot P_2(t)$, για κάποια πολυώνυμα $P_1(t), P_2(t) \in \mathbb{K}[t]$. Τότε στον δακτύλιο πηλίκο $\mathbb{K}[t]/I$, θα έχουμε:
$$(P_1(t) + I) \cdot (P_2(t) + I) = P_1(t) \cdot P_2(t) + I = P(t) + I = P(t) + (P(t))$$
και επομένως, επειδή ο δακτύλιος πηλίκο $\mathbb{K}[t]/I$ δεν έχει διαιρέτες του μηδενός, θα έχουμε $P_1(t) \in I$ ή $P_2(t) \in I$, δηλαδή $P_1(t) = P(t) \cdot Q(t)$ ή $P_2(t) = P(t) \cdot R(t)$. Επειδή $\deg P_i(t) \leq \deg P(t)$, $i = 1, 2$, έπεται ότι είτε το πολυώνυμο $Q(t) = c \in \mathbb{K} \setminus \{0\}$ είναι σταθερό μη μηδενικό πολυώνυμο ή το πολυώνυμο $R(t) = d \in \mathbb{K} \setminus \{0\}$ είναι σταθερό μη μηδενικό πολυώνυμο. Αυτό σημαίνει αντίστοιχα ότι είτε $P(t) = c^{-1} P_1(t)$ ή $P(t) = d^{-1} P_2(t)$, δηλαδή το $P(t)$ είναι ανάγωγο.

3. «$\Longrightarrow$» 1. Έστω ότι το πολυώνυμο $P(t)$ είναι ανάγωγο, και έστω $I = (P(t)) \subseteq J \subseteq \mathbb{K}[t]$, όπου J είναι ένα ιδεώδες του $\mathbb{K}[t]$, και επομένως $J = (Q(t))$, όπου $Q(t) \in \mathbb{K}[t]$. Τότε προφανώς θα έχουμε $P(t) \in I \subseteq J$ και άρα $P(t) = Q(t) \cdot A(t)$, για ένα πολυώνυμο $A(t) \in \mathbb{K}[t]$. Επειδή το $P(t)$ είναι ανάγωγο, έπεται ότι είτε το πολυώνυμο $Q(t)$ είναι σταθερό μη μηδενικό πολυώνυμο (αν $Q(t) = 0$, τότε $P(t) = 0$ το οποίο είναι άτοπο διότι $I \neq 0$), είτε το πολυώνυμο $A(t)$ είναι σταθερό μη μηδενικό πολυώνυμο (αν $A(t) = 0$, τότε $P(t) = 0$ το οποίο είναι άτοπο διότι $I \neq 0$). Στην πρώτη περίπτωση θα έχουμε $Q(t) = c \in \mathbb{K} \setminus \{0\}$, και τότε το σταθερό μη μηδενικό πολυώνυμο $Q(t)$ είναι αντιστρέψιμο. Επομένως $J = (Q(t)) = \mathbb{K}[t]$. Στην δεύτερη περίπτωση θα έχουμε $A(t) = d \in \mathbb{K} \setminus \{0\}$, δηλαδή το σταθερό μη μηδενικό πολυώνυμο $A(t) = d$ είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$, και τότε $Q(t) = d^{-1}P(t) \in (P(t)) = I$. Η τελευταία σχέση δείχνει ότι $J = (Q(t)) \subseteq (P(t)) = I$ και επομένως $I = J$. Επομένως το ιδεώδες I είναι μεγιστοτικό. ■

Σε επόμενο Κεφάλαιο θα δούμε μια γενίκευση του παραπάνω αποτελέσματος.

Έχοντας προσδιορίσει στην Πρόταση 10.2.14 τα πρώτα και μεγιστοτικά ιδεώδη του δακτυλίου πολυωνύμων $\mathbb{K}[t]$ υπεράνω ενός σώματος $\mathbb{K}$, και στην Πρόταση 10.1.27 τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του $\mathbb{K}$, στην επόμενη Πρόταση προσδιορίζουμε τα πρώτα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$. Ιδιαίτερα προκύπτει ότι κάθε μη μηδενικό πρώτο ιδεώδες του $\mathbb{K}[\![t]\!]$ είναι μεγιστοτικό.

Πρόταση 10.2.15. *Έστω $\mathbb{K}$ ένα σώμα. Τότε τα πρώτα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του $\mathbb{K}$, είναι το μηδενικό ιδεώδες $\{0\}$ και το κύριο (και μεγιστοτικό) ιδεώδες (t).*

Απόδειξη. Το μηδενικό ιδεώδες $\{0\}$ του $\mathbb{K}[\![t]\!]$ είναι πρώτο διότι, σύμφωνα με το Λήμμα 9.5.4, ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι ακέραια περιοχή. Έστω P ένα μη μηδενικό πρώτο ιδεώδες του $\mathbb{K}[\![t]\!]$. Επειδή το P είναι πρώτο, εξ ορισμού το P είναι γνήσιο. Θεωρούμε το ιδεώδες $(t) + P \subseteq \mathbb{K}[\![t]\!]$. Επειδή $(t) \subseteq (t) + P$ και το ιδεώδες (t), συμφωνα με την Πρόταση 10.1.27, είναι μεγιστοτικό, θα έχουμε ότι είτε $(t) = (t) + P$ είτε $\mathbb{K}[\![t]\!] = (t) + P$. Στην τελευταία περίπτωση μπορούμε να γράψουμε $1 = P(t) + Q(t)$, όπου $P(t) \in (t)$ και $Q(t) \in P$. Επειδή ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι τοπικός, από την Πρόταση 10.1.17, έπεται ότι είτε το στοιχείο $Q(t) \in P$ είναι αντιστρέψιμο είτε το στοιχείο $1 - Q(t) = P(t) \in (t)$ είναι αντιστρέψιμο. Και οι δύο περιπτώσεις μάς οδηγούν σε αντίφαση, διότι τα ιδεώδη (t) και P, ως γνήσια, δεν περιέχουν αντιστρέψιμα στοιχεία. Άρα $(t) = (t) + P$ το οποίο σημαίνει ότι $P \subseteq (t)$. Υποθέτουμε ότι $P \neq (t)$ και επομένως $t \notin P$. Επειδή το ιδεώδες P είναι μη μηδενικό, έπεται ότι περιέχει ένα μη μηδενικό στοιχείο $P(t) = \sum_{k=0}^{\infty} a_k t^k$. Τότε $a_0 = 0$ διότι $P(t) \in P \subseteq (t)$, και άρα $P(t) = tP_1(t)$, όπου $P_1(t) = \sum_{k=1}^{\infty} a_k t^{k-1}$. Επειδή το ιδεώδες P είναι πρώτο και $t \notin P$, έπεται ότι $P_1(t) \in P$. Όπως και προηγουμένως, επειδή $P(t) \in (t)$, θα έχουμε ότι ο σταθερός όρος a_1 του $P_1(t)$ θα είναι ίσος με $a_1 = 0$. Συνεχίζοντας αυτή τη διαδικασία, προκύπτει εύκολα με χρήση της Αρχής Μαθηματικής Επαγωγής ότι $a_n = 0$, $\forall n \geq 0$, και επομένως $P(t) = 0$, το οποίο είναι άτοπο διότι $P(t) \neq 0$. Στο άτοπο καταλήξαμε υποθέτοντας ότι $P \neq (t)$. Άρα $P = (t)$. ■

Μεγιστοτικά-Πρώτα Ιδεώδη και Ομομορφισμοί Δακτυλίων

Κλείνουμε την παρούσα ενότητα με την ακόλουθη Πρόταση η οποία υπογραμμίζει μια σημαντική διαφορά στη συμπεριφορά των πρώτων και των μεγιστοτικών ιδεωδών ως προς τους ομομορφισμούς δακτυλίων. Αυτή η διαφοροποίηση επέδρασε σημαντικά στη θεμελίωση της σύγχρονης Αλγεβρικής Γεωμετρίας η οποία βασίζεται αποφασιστικά στην έννοια του πρώτου ιδεώδους.

Πρόταση 10.2.16. *Έστω $f : R \longrightarrow S$ ένας ομομορφισμός μεταθετικών δακτυλίων.*

1. *Αν P είναι ένα πρώτο ιδεώδες του S, τότε το $f^{-1}(P)$ είναι ένα πρώτο ιδεώδες του R.*
2. *Αν M είναι ένα μεγιστοτικό ιδεώδες του S, τότε γενικά το $f^{-1}(M)$ δεν είναι μεγιστοτικό ιδεώδες του R,*
3. *Αν ο ομομορφισμός f είναι επιμορφισμός, τότε για κάθε μεγιστοτικό ιδεώδες M του S, το $f^{-1}(M)$ είναι μεγιστοτικό ιδεώδες του R.*

Απόδειξη. 1. Έστω P ένα πρώτο ιδεώδες του S και έστω $Q = f^{-1}(P) \subseteq R$. Από την Πρόταση 8.2.10, έπεται ότι το Q είναι ιδεώδες του R. Έστω r_1, r_2 στοιχεία του R, και έστω $r_1 \cdot r_2 \in Q$. Τότε $f(r_1 \cdot r_2) = f(r_1) \cdot f(r_2) \in f(Q) = f(f^{-1}(P))$. Επειδή πάντα έχουμε $f(f^{-1}(P)) \subseteq P$, έπεται ότι $f(r_1) \cdot f(r_2) \in P$. Επειδή το ιδεώδες P είναι πρώτο, έπεται ότι $f(r_1) \in P$ ή $f(r_2) \in P$. Δηλαδή $r_1 \in f^{-1}(P)$ ή $r_2 \in f^{-1}(P)$ και άρα το ιδεώδες $f^{-1}(P)$ είναι πρώτο.

2. Θεωρούμε την κανονική έγκλειση $\iota \colon \mathbb{Z} \longrightarrow \mathbb{Q}$, $\iota(z) = z$, η οποία είναι μονομορφισμός αλλά όχι επιμορφισμός δακτυλίων. Επειδή ο δακτύλιος $\mathbb{Q}$ είναι σώμα, το μηδενικό ιδεώδες 0 είναι μεγιστοτικό ιδεώδες του $\mathbb{Q}$, και επειδή η ι είναι μονομορφισμός, θα έχουμε $\iota^{-1}(0) = 0$ το οποίο είναι πρώτο αλλά όχι μεγιστοτικό ιδεώδες του $\mathbb{Z}$, διότι ο τελευταίος δακτύλιος είναι ακέραια περιοχή αλλά όχι σώμα.

3. Υποθέτουμε ότι ο ομομορφισμός f είναι επιμορφισμός. Θεωρούμε απεικόνιση

$$\widetilde{f} \colon R \longrightarrow S/M, \quad \widetilde{f}(r) = f(r) + M$$

Η απεικόνιση $\widetilde{f}$ είναι επιμορφισμός δακτυλίων ως σύνθεση $\widetilde{f} = \pi_M \circ f$ των επιμορφισμών δακτυλίων $\pi_M \colon S \longrightarrow S/M$, $\pi_M(s) = s + M$, και $f \colon R \longrightarrow S$. Θα προσδιορίσουμε τον πυρήνα του $\widetilde{f}$:

$$\mathsf{Ker}(\widetilde{f}) = \{r \in R \mid \widetilde{f}(r) = 0_{S/M}\} = \{r \in R \mid f(r) + M = M\} = \{r \in R \mid f(r) \in M\} = f^{-1}(M)$$

Από το Πρώτο Θεώρημα Ισομορφισμών, έπεται ότι ο επιμορφισμός $\widetilde{f}$ επάγει έναν ισομορφισμό δακτυλίων

$$R/f^{-1}(M) \cong S/M$$

Επειδή το ιδεώδες M είναι μεγιστοτικό, έπεται ότι ο δακτύλιος πηλίκο S/M είναι σώμα. Τότε και ο δακτύλιος πηλίκο $R/f^{-1}(M)$ είναι σώμα, δηλαδή το ιδεώδες $f^{-1}(M)$ είναι μεγιστοτικό. ■

10.3 Ασκήσεις

Άσκηση 10.3.1. *1. Βρείτε όλα τα πρώτα ιδεώδη και όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{Z}_{12}$.*

2. Βρείτε όλα τα πρώτα ιδεώδη και όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{Z}_2 \times \mathbb{Z}_2$.

3. Βρείτε ένα μεγιστοτικό ιδεώδες του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$.

4. Βρείτε ένα πρώτο ιδεώδες του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$ το οποίο να μην είναι μεγιστοτικό.

5. Βρείτε ένα πρώτο ιδεώδες του δακτυλίου $\mathbb{Z}[t]$ το οποίο να μην είναι μεγιστοτικό.

6. Βρείτε ένα μη μηδενικό γνήσιο ιδεώδες του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$ το οποίο να μην είναι πρώτο.

Άσκηση 10.3.2. *Να βρεθούν όλα τα πρώτα (μεγιστοτικά) ιδεώδη του δακτυλίου $\mathbb{Z}_n$.*

Άσκηση 10.3.3. *Να βρεθούν όλα τα πρώτα και όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{Z} \times \mathbb{Z}$.*

Άσκηση 10.3.4. *Να δείξετε ότι κάθε ακέραια περιοχή με πεπερασμένο πλήθος (κύριων) ιδεωδών είναι σώμα.*

Άσκηση 10.3.5. *Γνωρίζουμε ότι σε έναν δακτύλιο (με μονάδα) κάθε μεγιστοτικό ιδεώδες είναι πρώτο. Να δοθεί παράδειγμα δακτυλίου χωρίς μονάδα ο οποίος περιέχει μεγιστοτικά ιδεώδη τα οποία δεν είναι πρώτα.*

Άσκηση 10.3.6. *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Δείξτε ότι κάθε πρώτο ιδεώδες του R είναι μεγιστοτικό ιδεώδες, αν ισχύει μια από τις ακόλουθες συνθήκες:*

1. *Ο δακτύλιος R έχει πεπερασμένο πλήθος στοιχείων.*
2. *Ο δακτύλιος R έχει πεπερασμένο πλήθος ιδεωδών.*

Άσκηση 10.3.7. *Δείξτε ότι το N είναι μεγιστοτικό ιδεώδες ενός δακτυλίου R αν και μόνο αν ο R/N είναι απλός δακτύλιος, δηλαδή δεν έχει γνήσια μη μηδενικά ιδεώδη.*

Άσκηση 10.3.8. *Έστω R ένας μεταθετικός δακτύλιος με μονάδα, και υποθέτουμε ότι κάθε ιδεώδες του R είναι πρώτο ιδέωδες. Να δείξετε ότι ο R είναι σώμα.*

Άσκηση 10.3.9. *Να βρεθούν όλα τα πρώτα και όλα τα μεγιστοτικά ιδεώδη του δακτυλίου*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b, c \in \mathbb{R} \right\}$$

Άσκηση 10.3.10. *Έστω R ένας δακτύλιος του Boole, και έστω P ένα γνήσιο ιδεώδες του R. Αποδείξτε ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Το ιδεώδες P είναι πρώτο.*
2. *$\forall x, y \in R$: είτε $x \in P$ ή $y \in P$ ή $x + y \in P$.*
3. *Το ιδεώδες P είναι μεγιστοτικό.*
4. *Ο δακτύλιος πηλίκο R/P είναι ισόμορφος με το σώμα $\mathbb{Z}_2$.*

Άσκηση 10.3.11. *Έστω R ένας μεταθετικός δακτύλιος με μονάδα, και P ένα πρώτο ιδεώδες του R. Υποθέτουμε ότι το P δεν περιέχει διαιρέτες του μηδενός. Να δείξετε οτι ο δακτύλιος R είναι ακέραια περιοχή.*

Άσκηση 10.3.12. *Αν $R = \mathbb{Z}$ ή ο $R = S[t]$, όπου S είναι μια μεταθετική ακέραια περιοχή, να δειχθεί ότι η τομή όλων των μεγιστοτικών ιδεωδών του R είναι το μηδενικό ιδεώδες.*

Άσκηση 10.3.13. *Έστω R ένας μεταθετικός δακτύλιος με μονάδα. Υποθέτουμε ότι:*

$$\forall x \in R, \ \exists\, n \geq 2 : \quad x^n = x$$

Να δείξετε ότι κάθε πρώτο ιδεώδες του R είναι μεγιστοτικό.

Άσκηση 10.3.14. *Έστω R μια περιοχή κυρίων ιδεωδών, δηλαδή ο μεταθετικός δακτύλιος με μονάδα R είναι ακέραια περιοχή, και κάθε ιδεώδες του R είναι κύριο.*

Να δείξετε οτι κάθε μη μηδενικό πρώτο ιδεώδες του R είναι μεγιστοτικό.

Άσκηση 10.3.15.

1. *Να δείξετε ότι το κύριο ιδεώδες (t) το οποίο παράγεται από το πολυώνυμο t του δακτυλίου πολυωνύμων $\mathbb{F}[t]$, όπου $\mathbb{F}$ είναι σώμα, είναι μεγιστοτικό.*
2. *Να δείξετε ότι το κύριο ιδεώδες (t) το οποίο παράγεται από το πολυώνυμο t του δακτυλίου πολυωνύμων $\mathbb{Z}[t]$, είναι πρώτο αλλά όχι μεγιστοτικό.*
3. *Να δείξετε ότι ο δακτύλιος $\mathbb{Z}[t]$ δεν είναι περιοχή κυρίων ιδεωδών, δείχνοντας ότι το ιδεώδες*

$$(2, t) := \left\{ 2P(t) + tQ(t) \in \mathbb{Z}[t] \mid P(t), Q(t) \in \mathbb{Z}[t] \right\}$$

δεν είναι κύριο.

4. *Να δείξετε ότι το ιδεώδες $(2,t)$ του δακτυλίου $\mathbb{Z}[t]$ είναι μεγιστοτικό.*

Άσκηση 10.3.16. *Να προσδιοριστούν τα μεγιστοτικά ιδεώδη του δακτυλίου πολυωνύμων $\mathbb{C}[t]$.*

Άσκηση 10.3.17. *Έστω ότι $f\colon R \longrightarrow S$ είναι ένας ομομορφισμός δακτυλίων, και I είναι ένα ιδεώδες του R.*

1. *Αν το I είναι πρώτο ιδεώδες του R, είναι το $f(I)$ πρώτο ιδεώδες του S;*
2. *Αν το I είναι μεγιστοτικό ιδεώδες του R, είναι το $f(I)$ μεγιστοτικό ιδεώδες του S;*

Αν η απάντηση στα παραπάνω ερωτήματα είναι αρνητική, να βρεθούν κατάλληλες συνθήκες οι οποίες να εξασφαλίζουν θετική απάντηση.

Άσκηση 10.3.18.
1. *Βρείτε όλα τα πρώτα ιδεώδη και όλα τα μεγιστοτικά ιδεώδη του $\mathbb{Z}_6$.*
2. *Βρείτε όλα τα πρώτα ιδεώδη και όλα τα μεγιστοτικά ιδεώδη του $\mathbb{Z}_2 \times \mathbb{Z}_4$.*
3. *Βρείτε όλα τα πρώτα ιδεώδη και όλα τα μεγιστοτικά ιδεώδη του $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.*

Σε κάθε περίπτωση να περιγραφούν οι αντίστοιχοι δακτύλιοι πηλίκα.

Άσκηση 10.3.19.
1. *Να εξεταστεί, αν το σύνολο $I = \{(2x,3x) \mid x \in \mathbb{Z}_6\}$ είναι ιδεώδες του δακτυλίου $\mathbb{Z}_6 \times \mathbb{Z}_6$.*
2. *Να δειχθεί ότι το $\mathbb{Z} \times \{0\}$ είναι ένα ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$.*
3. *Να δειχθεί ότι το $\mathbb{Z} \times 2\mathbb{Z}$ είναι ένα ιδεώδες του $\mathbb{Z} \times \mathbb{Z}$.*

Είναι κάποιο από τα παραπάνω ιδεώδη πρώτο ή μεγιστοτικό;

Άσκηση 10.3.20. *Έστω $n = p_1 p_2 \cdots p_k$, όπου $p_1, p_2, \cdots, p_k$ διακεκριμένοι πρώτοι αριθμοί.*

1. *Να βρεθούν όλα τα πρώτα και μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{Z}_n$.*
2. *Να δείξετε ότι υπάρχουν ακριβώς 2^k ταυτοδύναμα[3] στοιχεία στον δακτύλιο $\mathbb{Z}_n$.*
3. *Να βρεθεί το πλήθος των μηδενοδύναμων[4] στοιχείων του δακτύλιου $\mathbb{Z}_n$.*
4. *Να δείξετε ότι το σύνολο όλων των μηδενοδύναμων στοιχείων του $\mathbb{Z}_n$ είναι ένα ιδεώδες το οποίο είναι ίσο με την τομή όλων των πρώτων ιδεωδών του $\mathbb{Z}_n$.*

Άσκηση 10.3.21. *Έστω X ένα μη κενό σύνολο. Θεωρούμε του μεταθετικό δακτύλιο $\mathscr{P}(X)$ όλων των υποσυνόλων του X, ο οποίος είναι δακτύλιος του Boole. Αν $|X| = 2,3,4$, να βρεθούν τα πρώτα (μεγιστοτικά) ιδεώδη του δακτυλίου $\mathscr{P}(X)$.*

Άσκηση 10.3.22. *Στον δακτύλιο $\mathbb{Z}[i] = \{a+bi \in \mathbb{C} \mid a,b \in \mathbb{Z}\}$ των ακεραίων του Gauss, θεωρούμε το υποσύνολο*

$$I = \{a+bi \in \mathbb{Z}[i] \mid 3 \mid a \text{ και } 3 \mid b\} \quad \text{και} \quad J = \{a+bi \in \mathbb{Z}[i] \mid 5 \mid a \text{ και } 5 \mid b\}$$

Να δειχθεί ότι το I είναι ένα μεγιστοτικό, και άρα πρώτο, ιδεώδες του $\mathbb{Z}[i]$, και το J δεν είναι πρώτο, και άρα ούτε μεγιστοτικό, ιδεώδες του $\mathbb{Z}[i]$.

---

[3] Υπενθυμίζουμε ότι ένα στοιχείο r σε έναν δακτύλιο R καλείται ταυτοδύναμο αν: $r^2 = r$.

[4] Υπενθυμίζουμε ότι ένα στοιχείο r σε έναν δακτύλιο R καλείται μηδενοδύναμο αν: $r^m = 0$, για κάποιο $m \geq 1$.

Άσκηση 10.3.23. *Έστω ο δακτύλιος*

$$\mathsf{AT}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b, c \in \mathbb{R} \right\}$$

των 2×2 άνω τριγωνικών πινάκων με στοιχεία πραγματικούς αριθμούς, και έστω τα υποσύνολα του $\mathsf{AT}_2(\mathbb{R})$:

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\} \quad \text{και} \quad J = \left\{ \begin{pmatrix} 0 & b \\ 0 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid b, c \in \mathbb{R} \right\}$$

1. *Να δείξετε ότι τα σύνολα I, J και $K = I \cap J$ είναι ιδεώδη του δακτυλίου $\mathsf{AT}_2(\mathbb{R})$.*
2. *Να εξετάσετε αν τα σύνολα I, J και K είναι ιδεώδη του δακτυλίου $\mathsf{M}_2(\mathbb{R})$.*
3. *Να προσδιοριστούν ο δακτύλιοι πηλίκα $\mathsf{AT}_2(\mathbb{R})/I$, $\mathsf{AT}_2(\mathbb{R})/J$ και $\mathsf{AT}_2(\mathbb{R})/K$.*
4. *Να εξεταστεί αν τα ιδεώδη I, J και K είναι πρώτα ή (μεγιστοτικά).*
5. *Να δείξετε ότι η ομάδα πηλίκο I/K είναι ιδεώδες του δακτυλίου $\mathsf{AT}_2(\mathbb{R})/K$ και να εξεταστεί αν το ιδεώδες I/K είναι πρώτο ή μεγιστοτικό.*

Άσκηση 10.3.24. *Να βρεθούν:*

1. *όλα τα πρώτα ιδεώδη του δακτυλίου $\mathbb{Z}_n \times \mathbb{Z}_m$, όπου $n, m \geq 1$,*
2. *όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{C} \times \mathbb{Z}_n \times \mathbb{R}[t]/(t^2)$,*
3. *όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \in \mathsf{M}_2(\mathbb{R}) \mid a, b \in \mathbb{R} \right\}$.*

Άσκηση 10.3.25. *Να βρεθεί ένα γνήσιο πρώτο ιδεώδες του δακτυλίου πολυωνύμων $\mathbb{Q}[t_1, t_2]$ το οποίο δεν είναι μεγιστοτικό.*

Άσκηση 10.3.26. *Να βρεθούν τα μεγιστοτικά ιδώδη των δακτυλίων*

$$\mathbb{R}[t]/(t^2 - 3t + 2) \quad \text{και} \quad \mathbb{R}[t]/(t^2 + t + 1)$$

Άσκηση 10.3.27.
1. *Να δείξετε ότι το κύριο ιδεώδες $(t^2 + t + 1)$ του δακτυλίου πολυωνύμων $\mathbb{Z}_2[t]$ είναι πρώτο.*
2. *Να δείξετε ότι το κύριο ιδεώδες $(t^4 + 4)$ του δακτυλίου πολυωνύμων $\mathbb{Q}[t]$ δεν είναι πρώτο.*
3. *Να δείξετε ότι το κύριο ιδεώδες $(t^3 - t - 1)$ του δακτυλίου πολυωνύμων $\mathbb{Z}_3[t]$ είναι μεγιστοτικό.*

Άσκηση 10.3.28. *Στον δακτύλιο πολυωνύμων $\mathbb{Q}[t]$ θεωρούμε το κύριο ιδεώδες (t) το οποίο παράγεται από το πολυώνυμο t.*

1. *Να δειχθεί ότι, με τις συνηθισμένες πράξεις πρόσθεσης και πολλαπλασιασμού πολυωνύμων, το ιδεώδες (t) είναι ένας δακτύλιος χωρίς μονάδα.*
2. *Να δειχθεί ότι ο δακτύλιος χωρίς μονάδα (t) δεν έχει μεγιστοτικά ιδεώδη.*

Άσκηση 10.3.29. *Έστω R ένας μεταθετικός δακτύλιος με πεπερασμένο πλήθος (κύριων) ιδεωδών. Να δειχθεί ότι ένα ιδεώδες του R είναι πρώτο αν και μόνο αν είναι μεγιστοτικό.*

Άσκηση 10.3.30. *Για κάθε πρώτο αριθμό p, θεωρούμε το ακόλουθο υποσύνολο του σώματος των ρητών αριθμών*

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\}$$

Να δειχθεί ότι το σύνολο $\mathbb{Z}_{(p)}$ είναι ένας υποδακτύλιος του $\mathbb{Q}$, και να εξεταστεί αν ο δακτύλιος $\mathbb{Z}_{(p)}$ είναι τοπικός.

Άσκηση 10.3.31. *Έστω ότι I είναι ένα ιδεώδες ενός δακτυλίου R και M είναι ένα ιδεώδες του R έτσι ώστε $I \subseteq M$. Θεωρούμε το ιδεώδες $N = M/I$ του δακτυλίου πηλίκου R/I. Να δειχθεί ότι το ιδεώδες M του R είναι μεγιστοτικό αν και μόνο αν το ιδεώδες N του R/I είναι μεγιστοτικό.*

Άσκηση 10.3.32. *Θεωρούμε το ακόλουθο υποσύνολο του δακτυλίου $\mathsf{M}_3(\mathbb{R})$ των 3×3 πινάκων υπεράνω του $\mathbb{R}$:*

$$R = \left\{ \begin{pmatrix} a & 0 & b \\ 0 & a & c \\ 0 & 0 & a \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \mid a, b, c \in \mathbb{R} \right\}$$

και τα υποσύνολα του

$$I = \left\{ \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \mid b, c \in \mathbb{R} \right\} \quad \text{και} \quad J = \left\{ \begin{pmatrix} 0 & 0 & b \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \mid b \in \mathbb{R} \right\} \quad \text{και} \quad K = \left\{ \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \mid c \in \mathbb{R} \right\}$$

1. *Να δείξετε ότι το σύνολο R είναι ένας μεταθετικός υποδακτύλιος του δακτυλίου $\mathsf{M}_3(\mathbb{R})$.*
2. *Να δείξετε ότι το υποσύνολο I είναι ένα μεγιστοτικό ιδεώδες του R και να προσδιοριστεί με ποιον γνωστό σας δακτύλιο είναι ισόμορφος ο δακτύλιος πηλίκο R/I.*
3. *Να δείξετε ότι τα υποσύνολα J και K είναι ιδεώδη του R και να εξεταστεί αν είναι πρώτα ή μεγιστοτικά.*
4. *Έστω $\mathsf{U}(R)$ η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου R. Να προσδιορίσετε υποομάδα H της $\mathsf{U}(R)$ και έναν ισομορφισμό ομάδων $\mathsf{U}(R)/H \cong \mathbb{R}^*$.*

Άσκηση 10.3.33. *Να βρεθούν όλα τα μεγιστοτικά ιδεώδη του δακτυλίου $\mathbb{K}[t]/(t^n)$, όπου $\mathbb{K}$ είναι ένα σώμα και $n \geq 1$.*

Άσκηση 10.3.34. *Να βρεθούν όλα τα πρώτα και μεγιστοτικά ιδώδη του δακτυλίου $\mathsf{AT}_2(\mathbb{K})$ των 2×2 άνω τριγωνικών πινάκων υπεράνω ενός σώματος $\mathbb{K}$.*

Άσκηση 10.3.35. *Έστω ότι R είναι ένας μεταθετικός δακτύλιος και ότι M είναι ένα ιδεώδες του R. Αν $R \setminus M \subseteq \mathsf{U}(R)$, δηλαδή αν κάθε στοιχείο του R το οποίο δεν ανήκει στο ιδεώδες M είναι αντιστρέψιμο, να δειχθεί ότι το ιδεώδες M είναι μεγιστοτικό και μάλιστα είναι το μοναδικό μεγιστοτικό ιδεώδες του R (δηλαδή ο δακτύλιος R είναι τοπικός).*

Άσκηση 10.3.36. *Για τον δακτύλιο $\mathbb{Z}_{(p)}$, όπου p είναι πρώτος, της Άσκησης 10.3.30, και για κάθε θετικό ακέραιο n, να προσδιοριστεί ο δακτύλιος πηλίκο*

$$\mathbb{Z}_{(p)}/(p^n)$$

όπου (p^n) είναι το κύριο ιδεώδες του $\mathbb{Z}_{(p)}$ το οποίο παράγεται από το στοιχείο p^n.

Άσκηση 10.3.37. *Να δειχθεί ότι στον δακτύλιο των ακεραίων του Gauss, το κύριο ιδεώδες (p), όπου p είναι ένας πρώτος αριθμός, είναι πρώτο αν και μόνο αν δεν υπάρχουν ακέραιοι a, b έτσι ώστε $p = a^2 + b^2$.*

Άσκηση 10.3.38. *Να δειχθεί ότι στον δακτύλιο των ακεραίων του Gauss, τα κύρια ιδεώδη* (3), $(1+i)$, *είναι πρώτα, αλλά το κύριο ιδεώδες* (2) *δεν είναι πρώτο ιδεώδες.*

Άσκηση 10.3.39. *Έστω ότι* R *είναι ένας μεταθετικός δακτύλιος και ότι* $\mathfrak{m}$ *είναι ένα μεγιστοτικό ιδεώδες του* R *έτσι ώστε το στοιχείο* $1+m$ *είναι αντιστρέψιμο, για κάθε στοιχείο* $m \in \mathfrak{m}$. *Να δειχθεί ότι το* $\mathfrak{m}$ *είναι το μοναδικό μεγιστοτικό ιδεώδες του* R *και άρα ο δακτύλιος* R *είναι τοπικός.*

Άσκηση 10.3.40. *Έστω ότι* R *είναι ένας μεταθετικός δακτύλιος και ότι* $\mathfrak{m}$ *είναι ένα μεγιστοτικό ιδεώδες του* R. *Να δειχθεί ότι για κάθε θετικό ακέραιο* n, *ο δακτύλιος πηλίκο* $R/\mathfrak{m}^n$ *είναι τοπικός.*

Άσκηση 10.3.41. *Να δειχθεί ότι το ιδεώδες* (n,t) *του δακτυλίου πολυωνύμων* $\mathbb{Z}[t]$ *το οποίο παράγεται από του θετικό ακέραιο* n *και το πολυώνυμο* t, *είναι μεγιστοτικό αν και μόνο αν ο θετικός ακέραιος* n *είναι πρώτος.*

Άσκηση 10.3.42. *Για κάθε πρώτο αριθμό* p, *θεωρούμε τον δακτύλιο*

$$\mathbb{Q}^{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid (p,b) = 1 \right\}$$

της Άσκησης 8.5.66. Να δειχθεί ότι ο δακτύλιος $\mathbb{Q}^{(p)}$ *είναι τοπικός.*

Άσκηση 10.3.43. *Στον δακτύλιο* $\mathbb{Q}[t_1,t_2]$ *να δειχθεί ότι:*

1. *Το ιδεώδες* (t_1^2) *δεν είναι πρώτο.*
2. *Το ιδεώδες* (t_1-2, t_2-3) *είναι μεγιστοτικό.*
3. *Το ιδεώδες* (t_2-3) *είναι πρώτο αλλά όχι μεγιστοτικό.*

Άσκηση 10.3.44. *Θεωρούμε το ακόλουθο σύνολο* 3×3 *πινάκων με στοιχεία πραγματικούς αριθμούς*

$$R = \left\{ \begin{pmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{pmatrix} \in \mathsf{M}_3(\mathbb{R}) \;\middle|\; a,b,c \in \mathbb{R} \right\}$$

1. *Να δειχθεί ότι το σύνολο* R *είναι ένας μεταθετικός υποδακτύλιος του δακτυλίου* $\mathsf{M}_3(\mathbb{R})$.

2. *Να βρεθεί ένα μεγιστοτικό ιδεώδες του* R.

3. *Να δειχθεί ότι υπάρχει ένας ισομορφισμός δακτυλίων* $\mathbb{R}[t]/(t^3) \cong R$, *όπου* (t^3) *είναι το κύριο ιδεώδες του δακτυλίου πολυωνύμων* $\mathbb{R}[t]$ *το οποίο παράγεται από το πολυώνυμο* t^3.

Άσκηση 10.3.45. *Θεωρούμε το σώμα* $\mathbb{C}$ *των μιγαδικών αριθμών, και τους δακτυλίους* $R = (\mathbb{R}^2, +, \circ)$ *και* $S = (\mathbb{R}^2, +, *)$, *όπου «*$+$*» είναι η συνήθης πρόσθεση ζευγών πραγματικών αριθμών, και ο πολλαπλασιασμοί «*$\circ$*» και «*$*$*» ορίζονται αντίστοιχα ως εξής:*

$$(x_1,y_1)\circ(x_2,y_2) = (x_1x_2, x_1y_2+y_1x_2) \qquad \text{και} \qquad (x_1,y_1)*(x_2,y_2) = (x_1x_2-y_1y_2, x_1y_2+y_1x_2)$$

για κάθε $\forall\,(x_1,y_1),\ (x_2,y_2) \in \mathbb{R}^2$.

(a) *Να εξεταστεί αν, οι δακτύλιοι* $\mathbb{C}$, R *και* S *είναι ανά δύο ισόμορφοι.*

(b) *Να βρεθούν όλα τα πρώτα και μεγιστοτικά ιδεώδη του* R *και να προσδιοριστούν οι επαγόμενοι δακτύλιοι πηλίκο.*

(c) *Υπάρχει ιδεώδες* J *του* S *έτσι ώστε* $S/J \cong \mathbb{R}$;

Άσκηση 10.3.46. *Θεωρούμε το σύνολο*

$$R = \left\{ \frac{a}{b} \in \mathbb{Q} \mid a, b \in \mathbb{Z},\ b \neq 0,\ (a,b) = 1,\ \text{και } b : \text{περιττός} \right\}$$

1. *Να δειχθεί ότι το σύνολο R είναι ένας υποδακτύλιος του $\mathbb{Q}$.*
2. *Να προσδιοριστεί η ομάδα $\mathsf{U}(R)$ των αντιστρέψιμων στοιχείων του R.*
3. *Να δειχθεί ότι το σύνολο $I := R \setminus \mathsf{U}(R)$ των μη αντιστρέψιμων στοιχείων του R είναι ιδεώδες του R.*
4. *Να προσδιοριστεί ο δακτύλιος πηλίκο R/I.*

Άσκηση 10.3.47. *Θεωρούμε το σύνολο*

$$R = \left\{ (a_n)_{n\geq 0} \in \mathsf{A}(\mathbb{R}) \mid \exists k \geq 0 :\ a_k = a_{k+1} = \cdots \right\}$$

όλων των ακολουθιών πραγματικών αριθμών οι οποίες είναι τελικά σταθερές. Στο σύνολο R ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού ως εξής:

$$(a_n)_{n\geq 0} + (b_n)_{n\geq 0} = (a_n + b_n)_{n\geq 0} \qquad \text{και} \qquad (a_n)_{n\geq 0} \cdot (b_n)_{n\geq 0} = (a_n b_n)_{n\geq 0}$$

1. *Να δειχθεί ότι η τριάδα $R = (R, +, \cdot)$ είναι ένας μεταθετικός δακτύλιος.*
2. *Να βρεθούν τα μεγιστοτικά ιδεώδη του R.*

Άσκηση 10.3.48. [5] *Έστω $\mathscr{C}([0,1])$ ο δακτύλιος των συνεχών συναρτήσεων $f : [0,1] \longrightarrow \mathbb{R}$. Για ένα υποσύνολο $M \subseteq \mathscr{C}([0,1])$, να δείξετε ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Το M είναι μεγιστοτικό ιδεώδες του δακτυλίου $\mathscr{C}([0,1])$.*
2. *Υπάρχει $r \in [0,1]$:*
$$M = M_r := \left\{ f \in \mathscr{C}([0,1]) \mid f(r) = 0 \right\}$$

Επιπλέον να δείξετε ότι η απεικόνιση

$$[0,1] \longrightarrow \left\{ \text{μεγιστοτικά ιδεώδη του } \mathscr{C}([0,1]) \right\},\quad r \longmapsto M_r$$

είναι «1-1» και «επί».

[5] Άσκηση αυξημένης δυσκολίας. Βλέπε το Παράρτημα Α΄.

Κεφάλαιο 11

Δακτύλιοι Κυρίων Ιδεωδών και Περιοχές Μονοσήμαντης Ανάλυσης

Στο παρόν Κεφάλαιο θα μελετήσουμε διεξοδικά δύο βασικές κλάσεις μεταθετικών δακτυλίων: τις περιοχές κυρίων ιδεωδών και τις περιοχές μονοσήμαντης ανάλυσης. Οι δύο αυτές κλάσεις δακτυλίων αποτελούν φυσική γενίκευση του δακτυλίου των ακεραίων, και διαδραματίζουν σημαντικό ρόλο στην Άλγεβρα και στη Θεωρία Αριθμών.

11.1 Περιοχές Κυρίων Ιδεωδών

Στην παρούσα ενότητα, $R = (R, +, \cdot)$ συμβολίζει έναν μεταθετικό δακτύλιο, όπως πάντα με μονάδα $1_R \neq 0_R$.

Ενδιαφερόμαστε για το πότε ο δακτύλιος έχει απλή αλλά μη τετριμμένη δομή ιδεωδών, όπου στην παρούσα περίπτωση με «απλή δομή» εννοούμε ότι τα ιδεώδη του παράγονται από το λιγότερο δυνατό πλήθος στοιχείων. Έτσι σ' αυτό το πλαίσιο, λαμβάνοντας υπόψη ότι ένα ιδεώδες του R έχει απλή δομή αν είναι κύριο, δηλαδή, αν παράγεται από ένα στοιχείο του δακτυλίου, προκύπτει φυσικά ο ακόλουθος ορισμός.

Ορισμός 11.1.1. *Ένας μεταθετικός δακτύλιος καλείται* **δακτύλιος κυρίων ιδεωδών**, *αν κάθε ιδεώδες του είναι κύριο. Μια ακέραια περιοχή η οποία είναι δακτύλιος κυρίων ιδεωδών, καλείται* **περιοχή κυρίων ιδεωδών**.

Προφανώς το μηδενικό ιδεώδες $0 = \{0\} = (0)$ και ο δακτύλιος $R = (1_R)$ είναι κύρια ιδεώδη. Επειδή ο δακτύλιος R είναι μεταθετικός, ένα κύριο ιδεώδες $I = (r)$ του R θα είναι της μορφής:

$$I = (r) = \{rx \in R \mid x \in R\} = \{xr \in R \mid x \in R\}$$

Παράδειγμα 11.1.2.

1. Κάθε σώμα είναι περιοχή κυρίων ιδεωδών. Αυτό προκύπτει από το γεγονός ότι τα μόνα ιδεώδη ενός σώματος R είναι τα τετριμμένα, $\{0\} = (0)$ και $R = (1)$, τα οποία είναι κύρια.

2. Θεωρούμε τον δακτύλιο $\mathbb{Z}$ των ακεραίων. Σύμφωνα με την Πρόταση 8.1.4, τα ιδεώδη του δακτυλίου $\mathbb{Z}$ των ακεραίων, συμπίπτουν με τις υποομάδες της προσθετικής ομάδας $(\mathbb{Z}, +)$ και άρα είναι τα εξης:

$$n\mathbb{Z} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\}, \quad n = 0, 1, 2, 3, \cdots$$

Με άλλα λόγια, τα ιδεώδη του $\mathbb{Z}$ είναι τα εξής: (n), όπου $n = 0, 1, 2, 3, \cdots$, δηλαδή είναι όλα κύρια. Επομένως ο δακτύλιος $\mathbb{Z}$ είναι περιοχή κυρίων ιδεωδών. $\surd$

Ένα σημαντικό παράδειγμα περιοχής κυρίων ιδεωδών αποτελεί ο δακτύλιος πολυωνύμων μιας μεταβλητής υπεράνω ενός σώματος. Πράγματι από το Θεώρημα 9.2.1 προκύπτει το ακόλουθο αποτέλεσμα.

Πρόταση 11.1.3. *Έστω $\mathbb{K}$ ένα σώμα. Τότε ο δακτύλιος $\mathbb{K}[t]$ είναι περιοχή κυρίων ιδεωδών.*

Παρατήρηση 11.1.4. Οι δακτύλιοι πολυωνύμων $\mathbb{K}[t_1, t_2, \cdots, t_n]$, $n \geq 2$, όπου $\mathbb{K}$ είναι σώμα, δεν είναι περιοχές κυρίων ιδεωδών, όπως προκύπτει από το Παράδειγμα 9.2.2. Από το ίδιο παράδειγμα προκύπτει ότι ο δακτύλιος πολυωνύμων $R[t]$ δεν είναι γενικά περιοχή κυρίων ιδεωδών, αν η ακέραια περιοχή R δεν είναι σώμα (π.χ. αν $R = \mathbb{Z}$). ▲

Έχοντας αποδείξει ότι κάθε ιδεώδες του δακτυλίου πολυωνύμων $\mathbb{K}[t]$, όπου $\mathbb{K}$ είναι σώμα, είναι κύριο, στη συνέχεια δείχνουμε ότι το ίδιο συμβαίνει και για τα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του $\mathbb{K}$.

Πρόταση 11.1.5. *Έστω $\mathbb{K}$ ένα σώμα. Τότε ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Σύμφωνα με την Πρόταση 10.1.27, ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι τοπικός με μοναδικό μεγιστοτικό ιδεώδες το κύριο ιδεώδες (t), και σύμφωνα με την Πρόταση 9.5.4, ο δακτύλιος $\mathbb{K}[\![t]\!]$ είναι ακέραια περιοχή.

Αν I είναι ένα γνήσιο ιδεώδες του $\mathbb{K}[\![t]\!]$, τότε από το Θεώρημα του Krull 10.1.14, έπεται ότι το I περιέχεται σε ένα μεγιστοτικό ιδεώδες, και άρα το I περιέχεται στο μοναδικό μεγιστοτικό ιδεώδες (t) του $\mathbb{K}[\![t]\!]$. Ισχυριζόμαστε ότι το I είναι ένα από τα κύρια ιδεώδη (t^n), $n \neq 1$. Έστω ότι $I \neq \{0\}$, και άρα το I περιέχει μια μη-μηδενική τυπική δυναμοσειρά $P(t) = \sum_{k=0}^{\infty} a_k t^k$. Τότε $a_0 = 0$ διότι $P(t) \in I \subseteq (t)$, και άρα $P(t) = tP_1(t)$, για κάποια τυπική δυναμοσειρά $P_1(t)$. Αν η δυναμοσειρά $P_1(t)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$, τότε προφανώς θα έχουμε ότι $t = P_1(t)^{-1}P(t) \in I$. Τότε θα έχουμε $(t) \subseteq I$, και επομένως $I = (t)$. Αν η δυναμοσειρά $P_1(t)$ δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$, τότε, σύμφωνα με το Λήμμα 10.1.25, ο σταθερός της όρος θα είναι ίσος με μηδέν και άρα $P_1(t) \in (t)$, δηλαδή $P_1(t) = tP_2(t)$, για κάποια τυπική δυναμοσειρά $P_2(t) \in \mathbb{K}[\![t]\!]$. Τότε $P(t) = t^2P_2(t) \in (t^2)$. Αν η δυναμοσειρά $P_2(t)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$, τότε προφανώς $t^2 \in I$ και επομένως, όπως παραπάνω, $I = (t^2)$. Αν η δυναμοσειρά $P_2(t)$ δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[\![t]\!]$, τότε, όπως πριν, ο σταθερός της όρος θα είναι ίσος με μηδέν και άρα $P_2(t) \in (t)$, δηλαδή $P_2(t) = tP_3(t)$, και τότε $P(t) = t^3P_3(t)$, για μια δυναμοσειρά $P_3(t)$. Αν η τυπική δυναμοσειρά $P_3(t)$ είναι αντιστρέψιμη, τότε όπως παραπάνω θα έχουμε $I = (t^3)$. Διαφορετικά, συνεχίζοντας την παραπάνω διαδικασία, προκύπτει εύκολα, με χρήση της Αρχής Μαθηματικής Επαγωγής, ότι το ιδεώδες I είναι ένα εκ των κύριων ιδεωδών (t^n), $n \geq 1$. ■

Όπως προκύπτει από την απόδειξη της Πρόταση 11.1.5, τα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$ μπορούν να τοποθετηθούν σε μια αλυσίδα:

Πόρισμα 11.1.6. *Τα ιδεώδη του δακτυλίου $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω ενός σώματος $\mathbb{K}$ είναι τα $\{(t^n) \subseteq \mathbb{K}[\![t]\!] \mid n \in \mathbb{N}_0\}$ και ικανοποιούν τις ακόλουθες σχέσεις:*

$$\{0\} \subseteq \cdots \subseteq (t^n) \subseteq (t^{n-1}) \subseteq \cdots \subseteq (t^2) \subseteq (t) \subseteq (1) = \mathbb{K}[\![t]\!]$$

Η επόμενη Πρόταση πιστοποιεί ότι δακτύλιοι κυρίων ιδεωδών ικανοποιούν μια σημαντική ιδιότητα περατότητας. Πρώτα θα χρειαστούμε έναν ορισμό:

Ορισμός 11.1.7. *Ένας (μεταθετικός) δακτύλιος R καλείται* **δακτύλιος της Noether**,[1] *αν ο R ικανοποιεί την* **συνθήκη αύξουσας αλυσίδας** *για κάθε αλυσίδα ιδεωδών του R:*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

υπάρχει θετικός ακέραιος k έτσι ώστε $I_k = I_n$, $\forall\, n \geq k$.

[1] Emmy Noether (23 Μαρτίου 1882 - 14 Απριλίου 1935) [https://en.wikipedia.org/wiki/Emmy_Noether]: Σημαντική Γερμανίδα μαθηματικός, με θεμελιώδη συμβολή στην Άλγεβρα, και ιδιαίτερα στη Θεωρία Δακτυλίων, Αλγεβρών και Σωμάτων, και στη Θεωρία Αναπαραστάσεων. Οι ιδέες της αποτελούν τη βάση της σύγχρονης Άλγεβρας.

Παρατήρηση 11.1.8. Γνωρίζουμε ότι, γενικά, η ένωση ιδεωδών ενός δακτυλίου δεν είναι ιδεώδες. Όμως, αν μια οικογένεια ιδεωδών $\{I_n\}_{n=1}^{\infty}$ ενός δακτυλίου R σχηματίζει μια αλυσίδα, όπως στον ορισμό 11.1.7:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

τότε η ένωση $I := \bigcup_{n=1}^{\infty} I_n$ είναι ιδεώδες του R.

Πράγματι, προφανώς $0 \in I$. Αν $x, y \in I$, τότε υπάρχουν θετικοί ακέραιοι n, m έτσι ώστε $x \in I_n$ και $y \in I_m$. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι $n \leq m$. Τότε $I_n \subseteq I_m$ και επομένως $x, y \in I_m$. Επειδή το σύνολο είναι ιδεώδες του R, έπεται ότι $x - y \in I_m$ και rx, $xr \in I_m$, $\forall in R$. Τότε όμως $x - y$, rx, $xr \in I$. Επομένως το σύνολο I είναι ιδεώδες.

Η παραπάνω απόδειξη δείχνει ότι η ένωση μιας αλυσίδας δεξιών ή αριστερών ιδεωδών σε έναν όχι απαραίτητα μεταθετικό δακτύλιο είναι δεξιό ή αριστερό ιδεώδες αντίστοιχα. ▲

Πρόταση 11.1.9. *Κάθε μεταθετικός δακτύλιος κυρίων ιδεωδών R είναι δακτύλιος της Noether.*

Απόδειξη. Θεωρούμε μια αλυσίδα ιδεωδών του R:

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_n \subseteq I_{n+1} \subseteq \cdots$$

Από την Παρατήρηση 11.1.8, έπεται ότι η ένωση $I := \bigcup_{n=1}^{\infty} I_n$ είναι ιδεώδες του R. Επειδή ο δακτύλιος R είναι δακτύλιος κυρίων ιδεωδών, έπεται ότι $I = (r)$ για κάποιο $r \in R$. Επειδή $r \in I$, προφανώς θα έχουμε ότι $r \in I_k$ για κάποιο $k \geq 1$. Τότε $I = (r) \subseteq I_k$ και επειδή προφανώς $I_n \subseteq I$, $\forall n \geq 1$, έπεται ότι $I = I_k$. Τότε, $\forall l \geq 1$, θα έχουμε $I_{k+l} \subseteq I = I_k \subseteq I_{k+l}$, και επομένως $I_k = I_{k+l}$, $\forall l \geq 1$. Αυτό σημαίνει ότι ο δακτύλιος R είναι δακτύλιος της Noether. ■

Παρατήρηση 11.1.10. Από την Πρόταση 11.1.9 έπεται ότι οι δακτύλιοι $\mathbb{Z}$, $\mathbb{K}$, $\mathbb{K}[t]$, $\mathbb{K}[\![t]\!]$ είναι δακτύλιοι της Noether, ως δακτύλιοι κυρίων ιδεώδων. Υπάρχουν όμως και δακτύλιο της Noether οι οποίοι δεν είναι δακτύλιοι κυρίων ιδεώδων. Για παράδειγμα αποδεικνύεται[2] ότι, αν και οι δακτύλιοι πολυωνύμων $\mathbb{K}[t_1, t_2, \cdots, t_n]$, $n \geq 2$, δεν είναι δακτύλιοι κυρίων ιδεωδών, είναι δακτύλιοι της Noether. ▲

11.2 Διαιρετότητα σε Περιοχές Κυρίων Ιδεωδών

Στην παρούσα ενότητα θα αναπτύξουμε τη βασική θεωρία διαιρετότητας στο πλαίσιο των περιοχών κυρίων ιδεωδών, γενικεύοντας την αντίστοιχη οικεία θεωρία διαιρετότητας στον δακτύλιο των ακεραίων και στον δακτύλιο πολυωνύμων μιας μεταβλητής υπεράνω ενός σώματος.

Από τώρα και στο εξής σταθεροποιούμε έναν μεταθετικό δακτύλιο R, ο οποίος αργότερα θα υποθέσουμε ότι είναι περιοχή κυρίων ιδεωδών.

Ορισμός 11.2.1. *Αν a, b είναι στοιχεία του R, όπου $b \neq 0$, τότε ορίζουμε ότι* **το στοιχείο b διαιρεί το στοιχείο a**, *αν: υπάρχει στοιχείο $c \in R$ έτσι ώστε $a = bc$, και τότε θα γράφουμε $b \mid a$:*

$$\forall a, b \in R, a \neq 0: \quad b \mid a \quad \Longleftrightarrow \quad \exists c \in R: \quad a = bc$$

Σ΄ αυτή την περίπτωση επίσης θα λέμε ότι **το b είναι διαιρέτης του a** *ή* **το a είναι πολλαπλάσιο του b.**

Όταν το στοιχείο b δεν διαιρεί το στοιχείο a, θα γράφουμε: $b \nmid a$.

[2] Θεώρημα Βάσης του Hilbert: «*Αν ο δακτύλιος R είναι δακτύλιος της Noether, για παράδειγμα, αν ο R είναι σώμα, τότε ο δακτύλιος πολυωνύμων $R[t_1, t_2, \cdots, t_n]$ είναι δακτύλιος της Noether*». Για μια απόδειξη βλέπε το βιβλίο [24].

- David Hilbert (23 Ιανουαρίου 1862 - 14 Φεβρουαρίου 1943) [https://en.wikipedia.org/wiki/David_Hilbert]: Επιφανής Γερμανός μαθηματικός, ένας εκ των μεγαλύτερων μαθηματικών του 19ου και του 20ου αιώνα, με θεμελιώδη συμβολή σε ένα ευρύ φάσμα ερευνητικών περιοχών: στην Άλγεβρα, στη Συναρτησιακή Ανάλυση, στη Μαθηματική Λογική, στη Μαθηματική Φυσική, στη Γεωμετρία κλπ. Οι ιδέες του επηρέασαν πολλές γενιές Μαθηματικών.

Παράδειγμα 11.2.2. 1. Στον δακτύλιο $\mathbb{Z}$ των ακεραίων έχουμε $4 \mid 8$.

2. Στον δακτύλιο των πολυωνύμων $\mathbb{R}[t]$ έχουμε $t-2 \mid t^2-4$.

3. Στον δακτύλιο $\mathbb{Z}[i]$ των ακεραίων του Gauss έχουμε $(3+i) \mid (11+17i)$ (διότι $11+17i = (3+i)(5+4i)$).

4. Στον δακτύλιο $\mathbb{Z}[\sqrt{2}]$ έχουμε $(1+\sqrt{2}) \mid (7+5\sqrt{2})$ (διότι $7+5\sqrt{2} = (1+\sqrt{2})(3+2\sqrt{2})$). $\surd$

Η επόμενη Παρατήρηση καταγράφει κάποιες χρήσιμες συνέπειες του Ορισμού 11.2.1.

Παρατήρηση 11.2.3. 1. Η μονάδα 1 του δακτυλίου R διαιρεί κάθε στοιχείο r του δακτυλίου R, διότι $r = 1 \cdot r$.

2. Κάθε αντιστρέψιμο στοιχείο r του δακτυλίου R διαιρεί κάθε στοιχείο s του δακτυλίου R, διότι $s = r \cdot r^{-1} \cdot s$.

3. Αν ο δακτύλιος R είναι σώμα, τότε κάθε μη μηδενικό στοιχείο του R διαιρεί κάθε στοιχείο του R, όπως προκύπτει από το μέρος 2.

4. Αν S είναι ένας υποδακτύλιος του R, τότε μπορεί ένα στοιχείο $s \in S$ να διαιρείται από ένα στοιχείο $s' \in S$, όπου τα στοιχεία s, s' θεωρούνται ως στοιχεία του R, αλλά το s να μη διαιρείται από το στοιχείο s', όταν τα στοιχεία s, s' θεωρούνται ως στοιχεία του S.

   Για παράδειγμα θεωρούμε τον δακτύλιο $\mathbb{Z}$ των ακεραίων ως υποδακτύλιο του σώματος $\mathbb{Q}$ των ρητών: $\mathbb{Z} \subseteq \mathbb{Q}$. Τότε $3 \mid 5$ στο σώμα $\mathbb{Q}$, διότι $5 = \frac{5}{3}3$, αλλά προφανώς $3 \nmid 5$ στον δακτύλιο $\mathbb{Z}$. ▲

Έστω όπως πριν R ένας μεταθετικός δακτύλιος, και $a, b \in R$, όπου $b \neq 0$. Τότε:

$$b \mid a \quad \Longleftrightarrow \quad (a) \subseteq (b) \tag{11.1}$$

Πράγματι, αν $b \mid a$, τότε υπάρχει $c \in R$ έτσι ώστε $a = bc \in (b)$, και τότε προφανώς θα έχουμε $(a) \subseteq (b)$. Αντίστροφα, αν $(a) \subseteq (b)$, τότε $a \in (a) \subseteq (b) = \{bx \in R \mid x \in R\}$, και άρα $a = bc$, για κάποιο $c \in R$. Επομένως $b \mid a$.

Η σχέση διαιρετότητας στο σύνολο R^* των (μη μηδενικών) στοιχείων ενός μεταθετικού δακτυλίου R προφανώς ικανοποιεί την ανακλαστική ιδιότητα, διότι $a \mid a$, $\forall a \in R^*$, ικανοποιεί τη μεταβατική ιδιότητα, διότι, αν $a \mid b$ και $b \mid c$, όπου $a, b, c \in R^*$, τότε θα έχουμε $b = ad_1$ και $c = bd_2$, για κάποια στοιχεία $d_1, d_2 \in R$, και επομένως θα έχουμε $c = ad_1d_2$, δηλαδή $a \mid c$. Όμως η σχέση διαιρετότητας δεν ικανοποιεί γενικά τη συμμετρική ιδιότητα, δηλαδή γενικά δεν ισχύει ότι, αν $a \mid b$, τότε έπεται ότι $b \mid a$. Πράγματι, αν για παράδειγμα στον δακτύλιο $\mathbb{Z}$ των ακεραίων ισχύει ότι $n \mid m$ και $m \mid n$, όπου n, m είναι μη μηδενικοί ακέραιοι, τότε γνωρίζουμε (και συνάγεται εύκολα) ότι $n = \pm m$. Παρόμοια, η σχέση διαιρετότητας δεν ικανοποιεί την αντισυμμετρική ιδιότητα, δηλαδή γενικά δεν ισχύει ότι αν $a \mid b$ και $b \mid a$, τότε $a = b$. Επομένως η σχέση διαιρετότητας σε έναν (μεταθετικό) δακτύλιο δεν είναι σχέση ισοδυναμίας ούτε σχέση μερικής διάταξης. Όπως θα δούμε σε λίγο, η αιτία για την οποία συμβαίνει αυτό είναι ότι τα αντιστρέψιμα στοιχεία σε ένα δακτύλιο R είναι γενικά περισσότερα της μονάδας του δακτυλίου R, για παράδειγμα στον δακτύλιο $\mathbb{Z}$ τα αντιστρέψιμα στοιχεία είναι τα $1, -1$. Τι συμβαίνει γενικά σε έναν μεταθετικό δακτύλιο;

Ορισμός 11.2.4. *Έστω a, b δύο μη-μηδενικά στοιχεία ενός μεταθετικού δακτυλίου R. Τα στοιχεία a, b καλούνται* **συντροφικά** *αν: $a \mid b$ και $b \mid a$.*

Για παράδειγμα, κάθε μη μηδενικό στοιχείο a του R είναι συντροφικό με τον εαυτό του, και επίσης με το αντίθετό του $-a$, διότι $-a = (-1)a$ και $a = (-1)(-a)$. Για να χαρακτηρίσουμε τα συντροφικά στοιχεία ενός δακτυλίου R, χρειάζεται να υποθέσουμε ότι οι δακτύλιος R είναι ακέραια περιοχή.

Πρόταση 11.2.5. *Έστω a, b δύο μη-μηδενικά στοιχεία μιας μεταθετικής ακέραιας περιοχής R. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. Τα στοιχεία a, b είναι συντροφικά.

2. *Τα κύρια ιδεώδη τα οποία παράγονται από τα a, b συμπίπτουν:* $(a) = (b)$.

3. *Υπάρχει αντιστρέψιμο στοιχείο $u \in R$:* $a = ub$.

Ιδιαίτερα, ένα στοιχείο r του R είναι αντιστρέψιμο αν και μόνο αν το r είναι συντροφικό με την μονάδα 1 του R αν και μόνο αν $(r) = (1) = R$.

Απόδειξη. 1. «$\Longleftrightarrow$» 2. Προκύπτει άμεσα από την σχέση (11.1).

1. «$\Longrightarrow$» 3. Επειδή $a \mid b$ και $b \mid a$, υπάρχουν στοιχεία $r, s \in R$, έτσι ώστε: $b = va$ και $a = ub$. Τότε, χρησιμοποιώντας ότι ο δακτύλιος R είναι ακέραια περιοχή, και τα στοιχεία a, b είναι μη μηδενικά, θα έχουμε:

$$b = va = vub \quad \Longrightarrow \quad (1 - vu)b = 0 \quad \Longrightarrow \quad 1 - vu = 0 \quad \Longrightarrow \quad vu = 1$$

και παρόμοια $uv = 1$. Άρα $a = ub$, όπου το u είναι αντιστρέψιμο (και $b = va$, όπου το $v = u^{-1}$ είναι αντιστρέψιμο).

3. «$\Longrightarrow$» 1. Αν $a = ub$ για ένα αντιστρέψιμο στοιχείο u του R, τότε προφανώς $b \mid a$. Επειδή $b = u^{-1}a$, θα έχουμε και $a \mid b$ και επομένως τα στοιχεία a, b είναι συντροφικά.

Το τελευταίο μέρος είναι άμεση συνέπεια των παραπάνω. ■

Αν και, όπως είδαμε, η σχέση διαιρετότητας στο σύνολο των (μη μηδενικών) στοιχείων ενός μεταθετικού δακτυλίου δεν είναι σχέση ισοδυναμίας, η σχέση ότι δύο αντιστρέψιμα στοιχεία μιας ακέραιας περιοχής R είναι συντροφικά είναι μια σχέση ισοδυναμίας στο σύνολο των αντιστρέψιμων στοιχείων της.

Ορίζουμε μια σχέση «$\sim$» στο σύνολο R^* των μη μηδενικών στοιχείων μιας ακέραιας περιοχής R, ως εξής:

$$\forall a, b \in R^*: \quad a \sim b \quad \Longleftrightarrow \quad \text{τα στοιχεία } a, b \text{ είναι συντροφικά, δηλαδή ισοδύναμα, αν: } (a) = b)$$

Λήμμα 11.2.6. *Έστω R μια ακέραια περιοχή. Τότε η σχέση συντροφικότητας «$\sim$» είναι μια σχέση ισοδυναμίας επί του συνόλου R^*, και για κάθε $a \in R^*$, η κλάση ισοδυναμίας $[a]_\sim$ του a είναι το σύνολο:*

$$[a]_\sim = \{ua \in R \mid u \in \mathsf{U}(R)\} = \mathsf{U}(R)a$$

Απόδειξη. Προφανώς $a \sim a$, διότι $(a) = (a)$, $\forall a \in R^*$. Αν $a, b \in R^*$ και $a \sim b$, τότε $(a) = (b)$ και επομένως θα έχουμε και $b \sim a$. Τέλος, αν $a, b, c \in R^*$ και $a \sim b$ και $b \sim c$, τότε θα έχουμε $(a) = (b)$ και $(b) = (c)$. Επομένως θα έχουμε $(a) = (c)$, δηλαδή $a \sim c$. Έτσι η σχέση συντροφικότητας είναι μια σχέση ισοδυναμίας επί του συνόλου R^*.

Έστω $a \in R^*$. Τότε

$$[a]_\sim = \{b \in R \mid b \sim a\} = \{b \in R \mid \exists u \in \mathsf{U}(R): \ b = ua\} = \{ua \in R \mid u \in \mathsf{U}(R)\} = \mathsf{U}(R)a$$ ■

Έχοντας ορίσει την έννοια διαιρετότητας σε έναν μεταθετικό δακτύλιο, μπορούμε να ορίσουμε τώρα την έννοια ενός μέγιστου κοινού διαιρέτη ή την έννοια ενός ελάχιστου κοινού πολλαπλασίου, έννοιες οι οποίες γενικεύουν τις αντίστοιχες οικείες έννοιες από τη Θεωρία Αριθμών ή τη Θεωρία Πολυωνύμων.

Ορισμός 11.2.7. *Έστω $a_1, a_2, \cdots, a_n$ μη μηδενικά στοιχεία ενός μεταθετικού δακτυλίου R.*

1. *Ένας* **κοινός διαιρέτης** *των στοιχείων $a_1, a_2, \cdots, a_n$ είναι ένα στοιχείο $d \in R$, το οποίο είναι διαιρέτης του a_k, δηλαδή $d \mid a_k$, $\forall k = 1, 2, \cdots, n$.*

   Ένας κοινός διαιρέτης $d \in R$ των $a_1, a_2, \cdots, a_n$ είναι ένας **μέγιστος κοινός διαιρέτης**, *συντομογραφικά* **ΜΚΔ**, *των $a_1, a_2, \cdots, a_n$, αν κάθε άλλος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$ είναι επίσης διαιρέτης του d.*

2. *Ένα* **κοινό πολλαπλάσιο** *των στοιχείων $a_1, a_2, \cdots, a_n$ είναι ένα στοιχείο $e \in R$, το οποίο είναι πολλαπλάσιο του a_k, δηλαδή $a_k \mid e$, $\forall k = 1, 2, \cdots, n$.*

   Ένα κοινό πολλαπλάσιο $e \in R$ των $a_1, a_2, \cdots, a_n$ είναι ένα **ελάχιστο κοινό πολλαπλάσιο**, *συντομογραφικά* **ΕΚΠ**, *των $a_1, a_2, \cdots, a_n$, αν κάθε άλλο κοινό πολλαπλάσιο των $a_1, a_2, \cdots, a_n$ είναι επίσης πολλαπλάσιο του e.*

Από τον παραπάνω ορισμό προκύπτει ότι η έννοια ενός μέγιστου κοινού διαιρέτη ή ενός ελάχιστου κοινού πολλαπλασίου δεν ορίζεται μοναδικά. Η επόμενη Παρατήρηση περιγράφει το σύνολο όλων των μέγιστων κοινών διαιρετών ή των ελάχιστων κοινών πολλαπλασίων ενός πεπερασμένου συνόλου μη μηδενικών στοιχείων ενός δακτυλίου.

Παρατήρηση 11.2.8. [Μοναδικότητα ΜΚΔ και ΕΚΠ]

1. Αν d είναι ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \cdots, a_n$, και $u \in \mathsf{U}(R)$ είναι ένα αντιστρέψιμο στοιχείο του R, τότε το στοιχείο ud είναι επίσης ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \cdots, a_n$. Πράγματι, επειδή $d \mid a_k$, έπεται ότι $a_k = dr_k$, $1 \leq k \leq n$, και τότε $a_k = duu^{-1}r_k$ και άρα το στοιχείο du είναι κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$. Αν d' είναι ένας άλλος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$, τότε $d' \mid d$ και άρα $d = d's$, για κάποιο $s \in R$, διότι το d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$. Τότε θα έχουμε $du = d'su$, δηλαδή $d' \mid du$. Επομένως το στοιχείο du είναι επίσης ενας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$. Άρα κάθε συντροφικό στοιχείο ενός μέγιστου κοινού διαιρέτη είναι επίσης μέγιστος κοινός διαρέτης. Αντίστροφα, αν d, d' είναι μέγιστοι κοινοί διαιρέτες των $a_1, a_2, \cdots, a_n$, τότε εξ ορισμού θα έχουμε $d \mid d'$ και $d' \mid d$, και επομένως τα στοιχεία d, d' είναι συντροφικά.

   Επομένως, η έννοια ενός μέγιστου κοινού διαιρέτη των μη μηδενικών στοιχείων $a_1, a_2, \cdots, a_n$ του R δεν ορίζεται μοναδικά. Όμως δύο μέγιστοι κοινοί διαιρέτες d, d' των $a_1, a_2, \cdots, a_n$ είναι συντροφικά στοιχεία ή ισοδύναμα παράγουν το ίδιο κύριο ιδεώδες. Έτσι θα λέμε ότι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$, ορίζεται με ακρίβεια συντροφικού στοιχείου, και συνήθως θα συμβολίζεται με

$$d = \left(a_1, a_2, \cdots, a_n\right)$$

   λαμβάνοντας υπόψη ότι αυτός ο συμβολισμός υπονοεί έναν μέγιστο κοινό διαιρέτη των $a_1, a_2, \cdots, a_n$, κάθε άλλος μέγιστος κοινός διαιρέτης είναι της μορφής du, $u \in \mathsf{U}(R)$.

2. Παρόμοια, το σύνολο των ελάχιστων κοινών πολλαπλασίων των στοιχείων $a_1, a_2, \cdots, a_n$, είναι της μορφής eu, όπου e είναι ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \cdots, a_n$, και $e \in \mathsf{U}(R)$, και άρα δύο ελάχιστα κοινά πολλαπλάσια των $a_1, a_2, \cdots, a_n$, παράγουν το ίδιο κύριο ιδεώδες, δηλαδή διαφέρουν κατά συντροφικό στοιχείο του R. Ένα ελάχιστο κοινό πολλαπλάσιο των $a_1, a_2, \cdots, a_n$ θα συμβολίζεται

$$e = \left[a_1, a_2, \cdots, a_n\right] \quad \blacktriangle$$

Σημειώνουμε ότι δύο συντροφικά στοιχεία έχουν ακριβώς τους ίδιους διαιρέτες.

Ένας Δακτύλιος χωρίς ΜΚΔ

Υπάρχουν ακέραιες περιοχές οι οποίες περιέχουν στοιχεία για τα οποία δεν υπάρχει μέγιστος κοινός διαιρέτης ή ελάχιστο κοινό πολλαπλάσιο. Στην παρούσα υποενότητα θα δώσουμε ένα τέτοιο παράδειγμα.

Έστω $d < -1$ ένα αρνητικός ακέραιος και θεωρούμε το σύνολο

$$\mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \in \mathbb{C} \mid a, b \in \mathbb{Z}\right\}$$

Αν $a = x + y\sqrt{d}$ και $b = z + w\sqrt{d}$ είναι δύο στοιχεία του $\mathbb{Z}[\sqrt{d}]$, τότε $a = b$ αν και μόνο αν $x = z$ και $y = w$. Πράγματι, αν $y \neq w$, τότε μπορούμε να γράψουμε $\sqrt{d} = \frac{z-x}{y-w}$, και άρα $(\frac{z-x}{y-w})^2 = d < -1$, το οποίο είναι άτοπο.

Προφανώς $1 \in \mathbb{Z}[\sqrt{d}]$. Αν $k + l\sqrt{d}, m + n\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, τότε:

$$(k + l\sqrt{d}) + (m + n\sqrt{d}) = (k + m) + (l + n)\sqrt{d} \qquad \text{και} \qquad (k + l\sqrt{d})(m + n\sqrt{d}) = (km + dln) + (kn + lm)\sqrt{d}$$

Επομένως το σύνολο $\mathbb{Z}[\sqrt{d}]$ είναι ένας υποδακτύλιος του $\mathbb{C}$, και ιδιαίτερα είναι ακέραια περιοχή. Ποια είναι τα αντιστρέψιμα στοιχεία του; Για να τα προσδιορίσουμε θα χρειαστούμε την απεικόνιση

$$N\colon \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}, \quad N(x + y\sqrt{d}) = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2$$

Παρατηρούμε ότι $N(x+y\sqrt{d}) = x^2 - dy^2 \geq 0$, διότι $d < -1$ και άρα $-d = \delta > 1$. Έτσι $N(x+y\sqrt{d}) = x^2 + \delta y^2$, όπου $\delta > 1$.

Η σημαντικότερη ιδιότητα της συνάρτησης N συνίσταται στο ότι είναι πολλαπλασιαστική με την έννοια ότι $N(ab) = Na)N(b)$. Με βάση αυτή την ιδιότητα θα περιγράψουμε τα αντιστρέψιμα στοιχεία της ακέραιας περιοχής $\mathbb{Z}[\sqrt{d}]$.

Λήμμα 11.2.9. *Θεωρούμε την ακέραια περιοχή $\mathbb{Z}[\sqrt{d}]$, όπου $\mathbb{Z} \ni d < -1$.*

1. $\forall a, b\colon\ N(ab) = Na)N(b)$.
2. $\mathsf{U}(\mathbb{Z}[\sqrt{d}]) = \{a \in \mathbb{Z}[\sqrt{d}] \mid N(a) = 1\} = \{1, -1\}$.

Απόδειξη. 1. Έστω $a = x + y\sqrt{d}$ και $b = z + w\sqrt{d}$ δύο στοιχεία του $\mathbb{Z}[\sqrt{d}]$. Τότε $ab = (xz + dyw) + (xw + yz)\sqrt{d}$, και θα έχουμε:

$$N(ab) = (xz+dyw)^2 - d(xw+yz)^2 = x^2w^2 + d^2y^2w^2 + 2dxzyw - dx^2w^2 - dy^2z^2 - 2dxwyz =$$
$$= x^2(z^2 - dw^2) - dy^2(z^2 - dw^2) = (x^2 - dy^2)(z^2 - dw^2) = N(a)N(b)$$

2. Έστω ότι $a = x + y\sqrt{d} \in \mathsf{U}(\mathbb{Z}[\sqrt{d}])$. Τότε υπάρχει στοιχείο $b = z + w\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$, έτσι ώστε: $ab = 1$. Χρησιμοποιώντας ότι η συνάρτηση N είναι πολλαπλασιαστική και προφανώς $N(1) = 1$, θα έχουμε:

$$ab = 1 \implies N(ab) = N(1) \implies N(a)N(b) = 1 \implies (x^2 - dy^2)(z^2 - dw^2) = 1$$

Επειδή $d < -1$, έπεται ότι $N(a), N(b) \geq 0$ και προφανώς $N(a) = 0$ μόνο αν $a = 0$. Έτσι επειδή $a, b \neq 0$, θα έχουμε $N(a), N(b) \geq 1$, από όπου η παραπάνω σχέση δίνει άμεσα ότι $N(a) = 1$. Αντίστροφα, αν $N(a) = 1$, τότε θεωρούμε το στοιχείο $b = x - y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Τότε προφανώς θα έχουμε $ab = 1$, και άρα $a \in \mathsf{U}(\mathbb{Z}[\sqrt{d}])$.

Έστω $N(a) = 1$, όπου $a = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Τότε $x^2 - dy^2 = 1$. Αν $y = 0$, τότε προφανώς $x = \pm 1$. Αν $y \neq 0$, τότε προφανώς $y^2 \geq 1$ και άρα, επειδή $-d > 1$, έπεται ότι $-dy^2 \geq 2$ και άρα $N(a) = x^2 - dy^2 \geq 2$, το οποίο είναι άτοπο. Άρα $y = 0$ και $a = \pm 1$. Επομένως $\mathsf{U}(\mathbb{Z}[\sqrt{d}] = \{1, -1\}$. ■

Αν $d = -1$, τότε το συμπέρασμα του μέρους 2. του Λήμματος 11.2.9 δεν ισχύει διότι $\mathbb{Z}[\sqrt{-1}] = \mathbb{Z}[i] = \{1, -1, i, -i\}$.

Λήμμα 11.2.10. *Θεωρούμε την ακέραια περιοχή $\mathbb{Z}[\sqrt{d}]$, όπου $\mathbb{Z} \ni d < -1$. Αν a, b είναι δύο μη-μηδενικά στοιχεία του $\mathbb{Z}[\sqrt{d}]$, έτσι ώστε: $(a) \subseteq (b)$ ή ισοδύναμα $b \mid a$, τότε:*

$$(a) \subsetneqq (b) \iff N(b) < N(a)$$

Απόδειξη. Επειδή $b \mid a$, θα έχουμε $a = bc$, για κάποιο $c \in \mathbb{Z}[\sqrt{d}]$. Τότε από το Λήμμα 11.2.9, θα έχουμε $N(a) = N(b)N(c)$, και επειδή η απεικόνιση έχει τιμές στους μη αρνητικούς ακεραίους, έπεται ότι $N(b) \leq N(a)$.

Έστω $(a) \subsetneqq (b)$, και υποθέτουμε ότι $N(b) = N(a) = N(b)N(c)$. Επειδή $a, b, c \neq 0$, θα έχουμε τότε $N(a), N(b), N(c) \neq 0$ και επομένως $N(c) = 1$. Από το Λήμμα 11.2.9, έπεται ότι το στοιχείο c είναι αντιστρέψιμο και τότε $b = ac^{-1} \in (a)$, δηλαδή $(b) \subseteq (a)$ το οποίο είναι άτοπο διότι $(a) \subsetneqq (b)$. Άρα $N(b) < N(a)$. Αν $N(b) < N(a)$ και $(a) = (b)$, τότε τα στοιχεία a, b είναι συντροφικά και επομένως $b = ua$, για ένα αντιστρέψιμο στοιχείο u του $\mathbb{Z}[\sqrt{d}]$. Από το Λήμμα 11.2.9, θα έχουμε $N(u) = 1$ και άρα $N(b) = N(u)N(a) = N(a)$ το οποίο είναι άτοπο διότι $N(b) < N(a)$. ■

Παράδειγμα 11.2.11. Θέτουμε $d = -3$ και θεωρούμε την ακέραια περιοχή $\mathbb{Z}[\sqrt{-3}]$.

Υποθέτουμε ότι τα στοιχεία 4 και $2(1+\sqrt{-3})$ έχουν έναν μέγιστο κοινό διαιρέτη $\delta = x + y\sqrt{-3}$ στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-3}]$, όπου $x, y \in \mathbb{Z}$, ιδιαίτερα θα έχουμε $\delta \mid 4$. Προφανώς $\delta \neq 0$ και επομένως $N(\delta) = x^2 + 3y^2 \neq 0$, και αν $a \mid b$ στον δακτύλιο $\mathbb{Z}[\sqrt{-3}]$, τότε $N(a) \mid N(b)$ στον δακτύλιο $\mathbb{Z}$. Επομένως $N(\delta) \mid N(4) = 16$ και επειδή $N(a) \geq 1$, έπεται ότι $N(\delta) \in \{1, 2, 4, 8, 16\}$. Για το στοιχείο $4 \in \mathbb{Z}[\sqrt{-3}]$, θα έχουμε:

$$2 \mid 4 \quad \text{διότι} \quad 4 = 2 \cdot 2 \qquad \text{και} \qquad 1 + \sqrt{-3} \mid 4 \quad \text{διότι} \quad 4 = (1+\sqrt{-3}) \cdot (1-\sqrt{-3})$$

Επομένως τα στοιχεία $2, 1 + \sqrt{-3}$ είναι κοινοί διαιρέτες των στοιχείων 4 και $2(1+\sqrt{-3})$ και άρα $2 \mid \delta$ και $(1+\sqrt{-3}) \mid \delta$. Ιδιαίτερα θα έχουμε $N(2) = 4 \mid N(\delta)$. Έτσι $N(\delta) = \{4, 8, 16\}$.

1. Έστω $x^2+3y^2=4$. Αν $y=0$, τότε προφανώς $x=\pm 2$. Επομένως

$$\delta \in \{2,\ -2\}$$

Αν $\delta=\pm 2$, τότε επειδή $(1+\sqrt{-3}) \mid 4, 2(1+\sqrt{-3}$, έπεται ότι $1+\sqrt{-3} \mid \pm 2$ και επομένως θα έχουμε $\pm 2=(1+\sqrt{-3})(k+l\sqrt{-3})=(k-3l)+(k+l)\sqrt{-3}$, για κάποιο $k+l\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$. Τότε $k-3l=\pm 2$ και $k+l=0$, δηλαδή $4k=\pm 2$, απ' όπου $2k=\pm 1$ και αυτό είναι άτοπο διότι $k \in \mathbb{Z}$.

– Άρα αυτή η περίπτωση δεν εμφανίζεται.

Αν $y \neq 0$, τότε $y^2 \geq 1$ και άρα $3y^2 \geq 3$, οπότε $4=x^2+3y^2 \geq 4$ και αυτό μπορεί να συμβαίνει μόνο αν $x=\pm 1$. Άρα σ' αυτή την περίπτωση

$$\delta \in \{1+\sqrt{-3},\ 1-\sqrt{-3},\ -1+\sqrt{-3},\ -1-\sqrt{-3}\}$$

Όπως και παραπάνω, επειδή $2 \mid 4, 2(1+\sqrt{-3}$, έπεται ότι $2 \mid \delta=(\pm 1)+(\pm)\sqrt{-3}$. Επομένως θα έχουμε $(\pm 1)+(\pm 1)\sqrt{-3}=2(k+l\sqrt{-3})$, για κάποιο $k+l\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$. Τότε όμως θα έχουμε $2k=\pm 1$ και αυτό είναι άτοπο διότι $k \in \mathbb{Z}$.

– Άρα αυτή η περίπτωση δεν εμφανίζεται.

2. Έστω $x^2+3y^2=8$. Αν $x=0$, τότε $3y^2=8$ και αυτό είναι άτοπο. Άρα $x \geq 1$. Αν $y=0$, τότε $x^2=8$ και αυτό είναι άτοπο. Άρα $y \neq 1$ και επομένως $y \geq 1$. Τότε $8=x^2+3y^2 \geq 4$. Αν $y=2$, τότε $8=x^2+3y^2 \geq x^2+12$ το οποίο είναι άτοπο.

– Άρα αυτή η περίπτωση δεν εμφανίζεται.

3. Έστω $x^2+3y^2=16$. Αν $x=0$, τότε $3y^2=16$ και αυτό είναι άτοπο. Άρα $x \geq 1$. Αν $y=0$, τότε $x^2=16$ και αυτό σημαίνει ότι $\delta=x=\pm 4$, και άρα

$$\delta \in \{4,\ -4\}$$

Επειδή $\delta=\pm 4 \mid 2(1+\sqrt{-3})$, θα έχουμε $2(1+\sqrt{-3})=\pm 4(k+l\sqrt{-3})$, από όπου προκύπτει ότι $1+\sqrt{-3}=(\pm 2)k+(\pm 2)l\sqrt{-3}$, δηλαδή $2k=\pm 1$ και αυτό είναι άτοπο διότι $k \in \mathbb{Z}$.

– Άρα αυτή η περίπτωση δεν εμφανίζεται.

Αν $y \neq 0$, τότε $y \geq 1$, και για να ισχύει x^2+3y^2, θα πρέπει προφανώς $x=\pm 2$ και $y=\pm 2$. Άρα σ' αυτή την περίπτωση

$$\delta \in \{2+2\sqrt{-3},\ 2-2\sqrt{-3},\ -2+2\sqrt{-3},\ -2-2\sqrt{-3}\}$$

Επειδή $\delta \mid 4$, θα έχουμε $4=\delta(k+l\sqrt{-3})$. Αν $\delta=2+2\sqrt{-3}$, τότε $4=(2+2\sqrt{-3})(k+l\sqrt{-3})$, από όπου $2=(1+\sqrt{-3})(k+l(\sqrt{-3})=(k-3l)+(k+l)\sqrt{-3}$. Η τελευταία σχέση δίνει $k-3l=2$ και $k=-l$, από όπου έπεται ότι $4k=2$ το οποίο είναι άτοπο διότι $k \in \mathbb{Z}$. Αν $\delta=-2+2\sqrt{-3}$, τότε $4=(-2+2\sqrt{-3})(k+l\sqrt{-3})$, απ' όπου $2=(-1+\sqrt{-3})(k+l(\sqrt{-3})=(-k-3l)+(k-l)\sqrt{-3}$. Η τελευταία σχέση δίνει $-k-3l=2$ και $k=l$, από όπου έπεται ότι $-4k=2$ το οποίο είναι άτοπο διότι $k \in \mathbb{Z}$. Αν $\delta=2-2\sqrt{-3}$, τότε $4=(2-2\sqrt{-3})(k+l\sqrt{-3})$, από όπου $2=(1-\sqrt{-3})(k+l(\sqrt{-3})=(k+3l)+(-k+l)\sqrt{-3}$. Η τελευταία σχέση δίνει $k+3l=2$ και $k=l$, από όπου έπεται ότι $4k=2$ το οποπιο είναι άτοπο διότι $k \in \mathbb{Z}$. Αν $\delta=-2-2\sqrt{-3}$, τότε $4=(-2-2\sqrt{-3})(k+l\sqrt{-3})$, από όπου $2=(-1-\sqrt{-3})(k+l(\sqrt{-3})=(-k+3l)+(-k-l)\sqrt{-3}$. Η τελευταία σχέση δίνει $-k+3l=2$ και $k=-l$, από όπου έπεται ότι $-4k=2$ το οποίο είναι άτοπο διότι $k \in \mathbb{Z}$.

– Άρα αυτή η περίπτωση δεν εμφανίζεται.

Επομένως, υποθέτοντας ότι υπάρχει ένας μέγιστος κοινός διαιρέτης των στοιχείων 4 και $2(1+\sqrt{-3})$, καταλήξαμε σε άτοπο. Άρα στον δακτύλιο $\mathbb{Z}[\sqrt{-3}]$ υπάρχουν στοιχεία για τα οποία δεν υπάρχει μέγιστος κοινός διαιρέτης.

Τέλος, παρατηρούμε ότι τα στοιχεία 4, $2(1+\sqrt{-3})$ δεν είναι συντροφικά. Πράγματι, επειδή $\mathsf{U}(\mathbb{Z}[\sqrt{-3}])=\{1,-1\}$, αν τα στοιχεία ήταν συντροφικά, θα είχαμε $4=(\pm 1)2(1+\sqrt{-3})=(\pm 2)+(\pm 2)\sqrt{-3}$, από όπου $2=(\pm 1)+(\pm 1)\sqrt{-3}$), και ιδιαίτερα $2=\pm 1$ το οποίο είναι άτοπο. Άρα τα στοιχεία 4, $2(1+\sqrt{-3})$ δεν είναι συντροφικά. Έτσι για το στοιχείο $4 \in \mathbb{Z}[\sqrt{-3}]$ έχουμε δύο παραγοντοποίησεις

$$4=2\cdot 2=(1+\sqrt{-3})\cdot(1-\sqrt{-3})$$

και οι παράγοντες 2 και $1+\sqrt{-3}$, και 2 και $1-\sqrt{-3}$, δεν είναι συντροφικά στοιχεία της ακέραιας περιοχής $\mathbb{Z}[\sqrt{-3}]$. $\surd$

Το ακόλουθο Θεώρημα δείχνει ότι, αν περιοριστούμε σε περιοχές κυρίων ιδεωδών, τότε υπάρχει μέγιστος κοινός διαιρέτης και ελάχιστο κοινό πολλαπλάσιο κάθε πεπερασμένου συνόλου στοιχείων.

Θεώρημα 11.2.12. *Έστω R μια περιοχή κυρίων ιδεωδών, και $a_1, a_2, \cdots, a_n$ μη μηδενικά στοιχεία της.*

1. *(α') Υπάρχει ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \cdots, a_n$.*

   (β') Αν d είναι ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \cdots, a_n$, τότε υπάρχουν στοιχεία $r_1, r_2, \cdots, r_n$, έτσι ώστε:
   $$d = a_1 r_1 + a_2 r_2 + \cdots + a_n r_n$$

   (γ') Το στοιχείο d είναι ένας μέγιστος κοινός διαιρέτης των στοιχείων $a_1, a_2, \cdots, a_n$ αν και μόνο αν
   $$(d) = (a_1) + (a_2) + \cdots + (a_n)$$

2. *(α') Υπάρχει ένα ελάχιστο κοινό πολλαπλάσιο των στοιχείων $a_1, a_2, \cdots, a_n$.*

   (β') Το στοιχείο e είναι ένα ελάχιστο κοινό πολλαπλάσιο των στοιχείων $a_1, a_2, \cdots, a_n$ αν και μόνο αν
   $$(e) = (a_1) \cap (a_2) \cap \cdots \cap (a_n)$$

Απόδειξη. 1. Θεωρούμε τα κύρια ιδεώδη $(a_k) = \{ra_k \in R \mid r \in R\}$ του R, $1 \le k \le n$. Επειδή κάθε ιδεώδες του R είναι κύριο, για το άθροισμα ιδεωδών $(a_1) + (a_2) + \cdots + (a_n)$ υπάρχει στοιχείο $d \in R$, έτσι ώστε:
$$(d) = (a_1) + (a_2) + \cdots + (a_n)$$
Επειδή $a_k \in (a_1) + (a_2) + \cdots + (a_n) = (d)$, $1 \le k \le n$, έπεται ότι υπάρχουν στοιχεία $x_1, x_2, \cdots, x_n$, έτσι ώστε: $a_k = x_k d$, και επομένως $d \mid a_k$, $1 \le k \le n$. Επίσης από την παραπάνω ισότητα ιδεωδών, έπεται ότι υπάρχουν στοιχεία $y_k = r_k a_k \in (a_k)$, έτσι ώστε
$$d = y_1 + y_2 + \cdots + y_n = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$$
Αν δ είναι ένας κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$, δηλαδή $a_k = \delta s_k$, $1 \le k \le n$, τότε θα έχουμε
$$d = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k = r_1 s_1 \delta + r_2 s_2 \delta + \cdots + r_k s_k \delta = (r_1 s_1 + r_2 s_2 + \cdots + r_k s_k)\delta \implies \delta \mid d$$
Επομένως το στοιχείο d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$.

Αν δ είναι ένας άλλος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$, τότε από την Παρατήρηση 11.2.8 γνωρίζουμε ότι τα στοιχεία d, δ είναι συντροφικά, και άρα $\delta = du$, όπου $u \in \mathsf{U}(R)$. Τότε, χρησιμοποιώντας ότι $d = r_1 a_1 + r_2 a_2 + \cdots + r_k a_k$, θα έχουμε
$$\delta = ud = (ur_1)a_1 + (ur_2)a_2 + \cdots + (ur_k)a_k$$
και άρα ο τυχόν μέγιστος κοινός διαιρέτης δ των $a_1, a_2, \cdots, a_n$ έχει την επιθυμητή μορφή.

Αν $(d) = (a_1) + (a_2) + \cdots + (a_n)$, τότε δείξαμε παραπάνω ότι το στοιχείο d είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$. Αντίστροφα, αν δ είναι ένας μέγιστος κοινός διαιρέτης των $a_1, a_2, \cdots, a_n$, τότε, όπως παραπάνω, θέτοντας $(d) = (a_1) + (a_2) + \cdots + (a_n)$, θα έχουμε ότι οι μέγιστοι κοινοί διαιρέτες d, δ είναι συντροφικά στοιχεία του R και επομένως $\delta = ud$, όπου $u \in \mathsf{U}(R)$. Προφανώς τότε $\delta \in (d)$ και άρα $(\delta) \subseteq (d)$. Επειδή $d = u^{-1}\delta$, θα έχουμε $d \in (\delta)$ και άρα $(d) \subseteq (\delta)$. Επομένως $(\delta) = (d) = (a_1) + (a_2) + \cdots + (a_n)$.

2. Θεωρούμε την τομή $(a_1)\cap(a_2)\cap\cdots\cap(a_n)$ των ιδεωδών (a_k), $1\le k\le n$. Επειδή κάθε ιδεώδες του R είναι κύριο, έπεται ότι υπάρχει στοιχείο $e\in R$, έτσι ώστε:

$$(e)=(a_1)\cap(a_2)\cap\cdots\cap(a_n)$$

Τότε προφανώς $e\in(a_k)$, και άρα $e=x_ka_k$, για κάποιο στοιχείο $x_k\in R$, δηλαδή το στοιχείο e είναι πολλαπλάσιο του στοιχείου a_k, $\forall k=1,2,\cdots,n$. Αν f είναι ένα κοινό πολλαπλάσιο των $a_1,a_2,\cdots,a_n$, τότε θα έχουμε $f=y_ka_k\in(a_k)$, $1\le k\le n$, και άρα $f\in(a_1)\cap(a_2)\cap\cdots\cap(a_n)$. Επομένως $f\in(f)\subseteq(a_1)\cap(a_2)\cap\cdots\cap(a_n)=(e)$, και άρα $f=ez$, για κάποιο $z\in R$, δηλαδή το f είναι πολλαπλάσιο του e. Έτσι δείξαμε ότι το e είναι ένα ελάχιστο κοινό πολλαπλάσιο των στοιχείων $a_1,a_2,\cdots,a_n$, και για κάθε άλλο κοινό πολλαπλάσιο f των $a_1,a_2,\cdots,a_n$, έχουμε $(f)\subseteq(e)$. Αν το f είναι επίσης ελάχιστο κοινό πολλαπλάσιο των $a_1,a_2,\cdots,a_n$, τότε από την Παρατήρηση 11.2.8 γνωρίζουμε ότι τα στοιχεία e,f είναι συντροφικά, και άρα $e=uf$, όπου $u\in\mathsf{U}(R)$. Τότε $e\in(f)$ και άρα $(e)\subseteq(f)$. Επομένως $(f)=(e)=(a_1)\cap(a_2)\cap\cdots\cap(a_n)$. ■

Παράδειγμα 11.2.13. Από το Παράδειγμα 11.2.11, έπεται ότι στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-3}]$ υπάρχουν στοιχεία τα οποία δεν διαθέτουν μέγιστο κοινό διαιρέτη. Επομένως, από το Θεώρημα 11.2.12 έπεται ότι ο δακτύλιος $\mathbb{Z}[\sqrt{-3}]$ δεν είναι περιοχή κυρίων ιδεωδών. Για παράδειγμα, το ιδεώδες $I=(4,2(1+\sqrt{-3})$ το οποίο παράγεται από τα στοιχεία 4 και $2(1+\sqrt{-3})$ δεν είναι κύριο διότι, αν ήταν κύριο με γεννήτορα το στοιχείο d, τότε το d θα ήταν ένας μέγιστος κοινός διαιρέτης των 4 και $2(1+\sqrt{-3})$, και αυτό είναι άτοπο διότι, σύμφωνα με το Παράδειγμα 11.2.11, τα στοιχεία αυτά δεν έχουν μέγιστο κοινό διαιρέτη. √

Ιδιαίτερο ενδιαφέρον παρουσιάζει η περίπτωση κατά την οποία ένας μέγιστος κοινός διαιρέτης των μη μηδενικών στοιχείων $a_1,a_2,\cdots,a_n$ είναι η μονάδα του δακτυλίου.

Ορισμός 11.2.14. *Τα μη μηδενικά στοιχεία $a_1,a_2,\cdots,a_n$ του δακτυλίου R καλούνται* **σχετικώς πρώτα** *αν:*

$$\big(a_1,a_2,\cdots,a_n\big)=1$$

Ισοδύναμα, ένας μέγιστος κοινός διαιρέτης τους είναι αντιστρέψιμο στοιχείο του R.

Τα μη μηδενικά στοιχεία $a_1,a_2,\cdots,a_n$ του δακτυλίου R καλούνται **πρώτα μεταξύ τους ανά δύο** *αν:*

$$1\le i\ne j\le n\quad\Longrightarrow\quad\big(a_i,a_j\big)=1$$

Ισοδύναμα, ανά δύο, τα στοιχεία αυτά έχουν μέγιστο κοινό διαιρέτη ένα αντιστρέψιμο στοιχείο του R.

Παρατήρηση 11.2.15. Έστω R μια περιοχή κυρίων ιδεωδών, και έστω τα μη μηδενικά στοιχεία $a_1,a_2,\cdots,a_n$ του R. Αν τα $a_1,a_2,\cdots,a_n$ είναι πρώτα μεταξύ τους ανά δύο, τότε είναι και σχετικώς πρώτα.

Πράγματι, αν $d=(a_1,a_2,\cdots,a_n)$ είναι ένας μέγιστος κοινός διαιρέτης τους, τότε για κάθε $1\le i\ne j\le n$, θα έχουμε ότι $d\mid a_i$ και $d\mid a_j$ και επομένως $d\mid 1=(a_i,a_j)$. Τότε $1=dr$, για κάποιο $r\in R$ και επομένως το στοιχείο d είναι αντιστρέψιμο. Αυτό σημαίνει ότι τα $a_1,a_2,\cdots,a_n$ είναι σχετικώς πρώτα.

Υπάρχουν περιοχές κυρίων ιδεωδών, οι οποίοι περιέχουν σχετικώς πρώτα αλλά όχι πρώτα μεταξύ τους ανά δύο στοιχεία (αναγκαστικά το πλήθος τους θα πρέπει να είναι ≥ 3).

Πράγματι, στην ακέραια περιοχή $\mathbb{Z}$ των ακεραίων, θεωρούμε τα στοιχεία $6,15,49$, τα οποία είναι ανά δύο δεν είναι πρώτα μεταξύ τους, διότι $(6,15)=3$ και το 3 δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}$. Από την άλλη πλευρά, τα στοιχεία $6,15,49$ δεν έχουν κοινό διαιρέτη και επομένως $(6,15,49)=1$, δηλαδή τα στοιχεία $6,15,49$ είναι σχετικώς πρώτα. ▲

Η ακόλουθη συνέπεια προκύπτει άμεσα από το Θεώρημα 11.2.12.

Πόρισμα 11.2.16 (Ταυτότητα του Bezout)**.** [3] *Έστω R μια περιοχή κυρίων ιδεωδών, και έστω τα μη μηδενικά στοιχεία $a_1,a_2,\cdots,a_n$ του R. Τότε:*

$$\text{Τα στοιχεία}\quad a_1,a_2,\cdots,a_n\quad\text{είναι σχετικώς πρώτα}\quad\Longleftrightarrow\quad\exists\, r_1,r_2,\cdots,r_n\in R:\quad r_1a_1+r_2a_2+\cdots+r_na_n=1$$

[3] Étienne Bézout (31 Μαρτίου 1730 - 27 Σεπτεμβρίου 1783) [https://en.wikipedia.org/wiki/Etienne_Bezout]: Γάλλος μαθηματικός, γνωστός κυρίως για την παρούσα ταυτότητα η οποία φέρει το όνομά του.

Από τη στοιχεώδη Θεωρία Αριθμών, γνωρίζουμε ότι, αν n, m είναι θετικοί ακέραιοι, τότε $(n,m)[n,m] = nm$. Η ακόλουθη Πρόταση περιγράφει το συμβαίνει σε μια τυχούσα περιοχή κυρίων ιδεωδών.

Πρόταση 11.2.17. *Έστω ότι a, b είναι μη μηδενικά στοιχεία σε μια περιοχή κυρίων ιδεωδών R. Αν (a,b) είναι ένας μέγιστος κοινός διαιρέτης των a, b και $[a,b]$ είναι ένα ελάχιστο κοινό πολλαπλάσιο των a, b, τότε υπάρχει αντιστρέψιμο στοιχείο $u \in \mathsf{U}(R)$, έτσι ώστε:*

$$(a,b)[a,b] = uab$$

δηλαδή τα στοιχεία $(a,b)[a,b]$ και ab είναι συντροφικά.

Απόδειξη. Έστω $d = (a,b)$ και $e = [a,b]$. Αρκεί να δείξουμε ότι $ab \mid de$ και $de \mid ab$.

Επειδή $d \mid a$ και $d \mid b$, έπεται ότι θα έχουμε $a = dr$ και $b = ds$, για κάποια στοιχεία $r, s \in R$. Τότε $rds = as = br$ και άρα το στοιχείο rds είναι κοινό πολλαπλάσιο των στοιχείων a και b. Επομένως το στοιχείο rds θα είναι και πολλαπλάσιο κάθε ελάχιστου κοινού πολλαπλασίου, και άρα $rds = ec$. Τότε

$$ab = rdsd = dec \implies de \mid ab$$

Επειδή $d = (a,b)$, από το Θεώρημα 11.2.12 έπεται ότι υπάρχουν στοιχεία $x, y \in R$ έτσι ώστε $d = ax + by$. Από την άλλη πλευρά, επειδή $e = [a,b]$, θα έχουμε $e = ka = lb$, για κάποια στοιχεία $k, l \in R$. Τότε

$$de = eax + eby = lbax + kaby = ab(lx + ky) \implies ab \mid de$$

Από τις παραπάνω σχέσεις έπεται ότι τα στοιχεία $ab = (a,b)[a,b]$ και ab είναι συντροφικά. ■

Κλείνουμε την παρούσα υποενότητα με την ακόλουθη σημαντική συνέπεια της Πρότασης 11.2.17 η οποία μας είναι οικεία από την στοιχειώδη Θεωρία Αριθμών.

Πόρισμα 11.2.18. *Έστω R μια περιοχή κυρίων ιδεωδών και a, b δύο σχετικώς πρώτα στοιχεία της, δηλαδή $(a,b) = 1$. Αν $c \in R$, τότε:*

1. $a \mid bc \implies a \mid c$.
2. $a \mid c$ *και* $b \mid c \implies ab \mid c$.

Απόδειξη. Επειδή $(a,b) = 1$, από την Πρόταση 11.2.17, μπορούμε να γράψουμε $ax + by = 1$, για κάποια στοιχεία $x, y \in R$.

1. Επειδή $a \mid bc$, θα έχουμε $bc = ad$ για κάποιο στοιχείο $d \in R$. Τότε από τη σχέση $ax + by = 1$, θα έχουμε $acx + bcy = c$ και επομένως $acx + ady = c$, δηλαδή $a(cx + dy) = c$. Επομένως $a \mid c$.
2. Επειδή $a \mid c$ και $b \mid c$, θα έχουμε $c = ad_1$ και $c = bd_2$ για κάποια στοιχεία $d_1, d_2 \in R$. Τότε από τη σχέση $ax + by = 1$, θα έχουμε:

$$c = acx + bcy = bd_2ax + bad_1y = ab(xd_2 + yd_1) \implies ab \mid c$$ ■

11.3 Ευκλείδειες Περιοχές

Στην παρούσα ενότητα θα μελετήσουμε μια σπουδαία κλάση περιοχών κυρίων ιδεωδών, τις Ευκλείδειες περιοχές. Οι περισσότερες περιοχές κυρίων ιδεωδών τις οποίες έχουμε δει μέχρι τώρα διαθέτουν μια απεικόνιση, «*Ευκλείδεια στάθμη*», η οποία εισάγει ένα είδος μεγέθους στον δακτύλιο και συμπεριφέρεται καλά ως προς την Ευκλείδεια διαίρεση. Από την άλλη πλευρά, η ύπαρξη Ευκλείδειας στάθμης αποτέλεσε το κύριο εργαλείο με το οποίο αποδείξαμε ότι ακέραιες περιοχές, όπως ο δακτύλιος των ακεραίων και ο δακτύλιος πολυωνύμων, είναι περιοχές κυρίων ιδεωδών.

Ορισμός 11.3.1. *Αν R είναι μια ακέραια περιοχή, μια απεικόνιση*

$$\delta\colon R\setminus\{0\}\longrightarrow\mathbb{N}_0,\quad a\longmapsto\delta(a)$$

καλείται **Ευκλείδεια στάθμη** *επί της R, αν για τυχόντα στοιχεία $a,b\in R$, όπου $b\neq 0$, υπάρχουν στοιχεία $q,r\in R$ έτσι ώστε:*

$$a=bq+r,\qquad \text{όπου:}\quad \text{είτε}\quad r=0\quad \text{είτε}\quad \delta(r)<\delta(b)$$

Μια ακέραια περιοχή καλείται **Ευκλείδεια περιοχή** *αν είναι εφοδιασμένη με μια Ευκλείδεια στάθμη.*

Παράδειγμα 11.3.2.

1. Η ακέραια περιοχή $\mathbb{Z}$ των ακεραίων είναι Ευκλείδεια περιοχή με Ευκλείδεια στάθμη
$$\delta\colon R\setminus\{0\}\longrightarrow\mathbb{N}_0,\quad a\longmapsto\delta(a):=|a|$$
Αυτό προκύπτει από την Ευκλείδεια διαίρεση ακεραίων αριθμών.

2. Η ακέραια περιοχή $\mathbb{K}[t]$ των πολυωνύμων υπεράνω ενός σώματος $\mathbb{K}$ είναι Ευκλείδεια περιοχή με Ευκλείδεια στάθμη
$$\delta\colon \mathbb{K}[t]\setminus\{0\}\longrightarrow\mathbb{N}_0,\quad P(t)\longmapsto\delta(a):=\deg P(t)$$
Αυτό προκύπτει από την Ευκλείδεια διαίρεση πολυωνύμων όπως αποδείχθηκε στην Πρόταση 9.1.5.

3. Θα δείξουμε ότι η απεικόνιση
$$\delta\colon \mathbb{Z}[i]\setminus\{0\}\longrightarrow\mathbb{N}_0,\quad a=m+ni\longmapsto\delta(a):=a\overline{a}=m^2+n^2$$
είναι μια Ευκλείδεια στάθμη επί της ακέραιας περιοχής $\mathbb{Z}[i]$ των ακεραίων του Gauss.

   Προφανώς θα έχουμε $\delta(ab)=\delta(a)\delta(b)$. Έστω $a,b\in\mathbb{Z}[i]$, όπου $b\notin 0$. Έστω $b=k+li$, όπου $k,l\in\mathbb{Z}$. Επειδή $b\neq 0$, υπάρχει ο αντίστροφός του $b^{-1}=\frac{k}{k^2+l^2}+\frac{-l}{k^2+l^2}i$ στο σώμα $\mathbb{C}$, όπου $\frac{k}{k^2+l^2},\frac{-l}{k^2+l^2}\in\mathbb{Q}$. Τότε αν $a=m+ni$, θα έχουμε:
$$ab^{-1}=\frac{mk+nl}{k^2+l^2}+\frac{nk-ml}{k^2+l^2}i=x+yi$$
   Τότε υπάρχουν ακέραιοι t,s έτσι ώστε $|t-x|\leq\frac{1}{2}$ και $|s-y|\leq\frac{1}{2}$. Θέτουμε $z=x-t$ και $w=y-s$ και τότε οι αριθμοί z,w είναι ρητοί έτσι ώστε $|z|\leq\frac{1}{2}$ και $|w|\leq\frac{1}{2}$. Με τους παραπάνω συμβολισμούς:
$$ab^{-1}=x+yi=(z+t)+(w+s)i\quad\Longrightarrow\quad a=b\big((z+t)+(w+s)i\big)=bq+r$$
   όπου $q:=t+si\in\mathbb{Z}[i]$ διότι $t,s\in\mathbb{Z}$, και $r:=b(z+wi)\in\mathbb{Z}[i]$ διότι $r=a-bq$ και $a,b,q\in\mathbb{Z}[i]$. Τέλος, αν $r\neq 0$, θα έχουμε
$$\delta(r)=r\overline{r}=|r|^2=|b|^2|z+wi|=|b|^2(z^2+w^2)\leq|b|^2(\frac{1}{4}+\frac{1}{4})=\frac{1}{2}|b|^2=\frac{1}{2}\delta(b)<\delta(b)$$
   Επομένως, η απεικόνιση δ είναι μια Ευκλείδεια στάθμη στην ακέραια περιοχή $\mathbb{Z}[i]$ και επομένως ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι μια Ευκλείδεια περιοχή. $\surd$

Το ενδιαφέρον μας για τις Ευκλείδειες περιοχές προκύπτει από το ακόλουθο αποτέλεσμα.

Θεώρημα 11.3.3. *Κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών.*

Απόδειξη. Έστω R μια Ευκλείδεια περιοχή με Ευκλείδεια στάθμη δ, και I ένα ιδεώδες του R. Αν το I είναι το μηδενικό ιδεώδες, τότε το I είναι κύριο $I=(0)$. Έστω ότι $I\neq\{0\}$, και επομένως το I περιέχει μη μηδενικά στοιχεία. Από όλα τα μη μηδενικά στοιχεία του I μπορούμε προφανώς να επιλέξουμε[4] ένα μη μηδενικό στοιχείο $0\neq b\in I$, έτσι ώστε η τιμή $\delta(b)$ να είναι η μικρότερη από όλες τις τιμές $\delta(x)\in\mathbb{N}$, $0\neq x\in I$. Θα

[4] Το σύνολο $X=\{\delta(c)\in\mathbb{N}\mid 0\neq c\in I\}$ είναι ένα μη κενό σύνολο θετικών ακεραίων και άρα από την Αρχή Καλής Διάταξης έπεται ότι το X έχει ελάχιστο στοιχείο.

δείξουμε ότι $I=(b)$. Προφανώς $(b)\subseteq I$ διότι $b\in I$. Έστω $a\in I$. Επειδή η απεικόνιση δ είναι μια Ευκλείδεια στάθμη, έπεται ότι

$$a=bq+r, \qquad \text{όπου} \quad \text{είτε} \quad r=0 \quad \text{ή} \quad \delta(r)<\delta(b)$$

Αν $r=0$, τότε $a=bq\in(b)$ και επομένως $I\subseteq(b)$. Οπότε σ' αυτήν τη περίπτωση, θα έχουμε $I=(b)$. Αν $r\neq 0$, θα έχουμε $r=a-bq\in I$ διότι $a,b\in I$ και το I είναι ιδεώδες του R. Επειδή $\delta(r)<\delta(b)$, το r είναι ένα μη μηδενικό στοιχείο του I του οποίου η τιμή $\delta(r)$ είναι μικρότερη από την τιμή $\delta(b)$. Αυτό όμως είναι άτοπο από την επιλογή του b. Άρα η περίπτωση $r\neq 0$ δεν εμφανίζεται και επομένως $I=(b)$. Έτσι κάθε ιδεώδες του R είναι κύριο και η ακέραια περιοχή R είναι περιοχή κυρίων ιδεωδών. ■

Πόρισμα 11.3.4. *Ο δακτύλιος $\mathbb{Z}[i]$ των ακεραίων του Gauss είναι περιοχή κυρίων ιδεωδών.*

Παράδειγμα 11.3.5. Για κάθε πρώτο αριθμό p, θεωρούμε το ακόλουθο σύνολο

$$\mathbb{Z}_{(p)}=\left\{\frac{a}{b}\in\mathbb{Q}\mid p\nmid b\right\}$$

Εύκολα βλέπουμε ότι το σύνολο $\mathbb{Z}_{(p)}$ είναι ένας υποδακτύλιος του $\mathbb{Q}$ και επομένως είναι μια ακέραια περιοχή. Αν $\frac{c}{b}\in\mathbb{Z}_{(p)}$, τότε για τον αριθμητή c μπορούμε προφανώς να γράψουμε $c=p^t a$, όπου $t\in\mathbb{N}_0$ και $a\in\mathbb{Z}$ και $p\nmid a$. Έτσι, από τώρα και στο εξής, τα στοιχεία του $\mathbb{Z}_{(p)}$ μπορούν να γραφούν ως

$$\frac{p^t a}{b}, \quad t\in\mathbb{N}_0, \quad a,b\in\mathbb{Z}, \quad b\neq 0, \quad \text{και} \quad p\nmid a,\ p\nmid b$$

Ορίζουμε απεικόνιση

$$\delta\colon \mathbb{Z}_{(p)}\setminus\{0\}\longrightarrow\mathbb{N}_0, \quad \delta\big(\frac{p^t a}{b}\big)=t$$

Έστω $x=\frac{p^t a}{b}$ και $0\neq y=\frac{p^s c}{d}$ στοιχεία του $\mathbb{Z}_{(p)}$, όπου $a,b,c,d\in\mathbb{Z}$, $b,d\neq 0$ και ο p δεν διαιρεί κανέναν από τους a,b,c,d. Αν $t<s$, τότε θέτουμε $r=x$ και $q=0$, και θα έχουμε $x=qy+r$ και $\delta(x)=t<s=\delta(y)=s$. Αν $t\geq s$, μπορούμε να θεωρήσουμε τον ρητό αριθμό

$$q=\frac{x}{y}=\frac{\frac{p^t a}{b}}{\frac{p^s c}{d}}=\frac{p^t ad}{p^s bc}=\frac{p^{t-s}ad}{bc}$$

ο οποίος ανήκει στον δακτύλιο $\mathbb{Z}_{(p)}$ διότι $p\neq bc$, αφού ο p είναι πρώτος και $p\nmid b,c$. Έτσι $x=qy+r$, όπου $r=0$. Επομένως, η απεικόνιση δ είναι μια Ευκλείδεια στάθμη στην ακέραια περιοχή $\mathbb{Z}_{(p)}$ και επομένως ο δακτύλιος $\mathbb{Z}_{(p)}$ είναι μια Ευκλείδεια περιοχή, και επομένως είναι μια περιοχή κυρίων ιδεωδών. √

Παρατήρηση 11.3.6. Όπως είδαμε στο Θεώρημα 11.3.3, κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών. Το αντίστροφο δεν ισχύει: υπάρχουν περιοχές κυρίων ιδεωδών επί των οποίων δεν μπορεί να οριστεί Ευκλείδεια στάθμη. Ένα τέτοιο παράδειγμα αποτελεί ο δακτύλιος

$$R=\left\{a+b\frac{1+\sqrt{-19}}{2}\in\mathbb{C}\mid a,b\in\mathbb{Z}\right\}$$

Προκύπτει εύκολα ότι ο δακτύλιος R είναι υποδακτύλιος του $\mathbb{C}$ και επομένως είναι ακέραια περιοχή. Αποδεικνύεται[5] ότι ο δακτύλιος R είναι περιοχή κυρίων ιδεωδών, αλλά δεν είναι Ευκλείδεια περιοχή.

Χρησιμοποιώντας προχωρημένες μεθόδους, αποδεικνύεται επίσης ότι για κάθε μη μηδενικό ακέραιο d, ο δακτύλιος $\mathbb{Z}[\sqrt{d}]$ είναι Ευκλείδεια περιοχή αν και μόνο αν

$$d=-11,\ -7,\ -3,\ -2,\ -1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 11,\ 13,\ 17,\ 19,\ 21,\ 29,\ 33,\ 37,\ 41,\ 57,\ 73 \quad ▲$$

[5] Βλέπε T. Motzkin: "*The Euclidean Algorithm*", Bull. Amer. Math. Soc. **55** (1949), 1142–1146, και J. Wilson: "*A principal ideal ring that is not a Euclidean ring*", Mathematics Magazine, **46** (1973), 34–38.

Παρατήρηση 11.3.7. Έστω R μια Ευκλείδεια περιοχή με Ευκλείδεια στάθμη δ. Τότε, εξ ορισμού, για τυχόντα στοιχεία $a, b \in R$, όπου $b \neq 0$, υπάρχουν στοιχεία $q, r \in R$, έτσι ώστε $a = bq + r$ και είτε $r = 0$ είτε $\delta(r) < \delta(b)$. Αν απαιτήσουμε τα στοιχεία q, r να είναι μοναδικά, τότε αποδεικνύεται[6] ότι είτε ο δακτύλιος R είναι σώμα είτε είναι ο δακτύλιος πολυωνύμων υπεράνω ενός σώματος. ▲

11.4 Περιοχές Μονοσήμαντης Ανάλυσης

Όπως γνωρίζουμε από την στοιχειώδη Θεωρία Αριθμών, κάθε θετικός ακέραιος γράφεται κατά μοναδικό τρόπο ως γινόμενο δυνάμεων διακεκριμένων πρώτων αριθμών. Στην παρούσα ενότητα θα μελετήσουμε την ανάλογη ιδιότητα στο γενικότερο πλαίσιο των ακεραίων περιοχών, και θα αναπτύξουμε μια σειρά παραδειγμάτων στα οποία ισχύει η ύπαρξη και μοναδικότητα γραφής στοιχείων ως γινόμενο «πρώτων» στοιχείων.

11.4.1 Ανάγωγα και Πρώτα Στοιχεία

Από τώρα και στο εξής υποθέτουμε R είναι ένας μεταθετικός δακτύλιος και όλοι οι εμπλεκόμενοι δακτύλιοι είναι μεταθετικοί.

Τα στοιχεία ενός μεταθετικού δακτυλίου τα οποία διαδραματίζουν αντίστοιχο ρόλο με τους πρώτους αριθμούς στον δακτύλιο των ακεραίων ή τα ανάγωγα πολυώνυμα στον δακτύλιο των πολυωνύμων υπεράνω ενός σώματος.

Ορισμός 11.4.1. *Ένα μη μηδενικό στοιχείο a ενός μεταθετικού δακτυλίου R καλείται* **ανάγωγο** *αν δεν είναι αντιστρέψιμο, και οι μόνοι διαιρέτες του είναι αντιστρέψιμα στοιχεία του R ή τα συντροφικά του στοιχεία.*

Παράδειγμα 11.4.2.

1. Στον δακτύλιο $\mathbb{Z}$ των ακεραίων, το στοιχείο 3 είναι προφανώς ανάγωγο. Όμως, αν το 3 θεωρηθεί στο σώμα $\mathbb{Q}$ των ρητών, δεν είναι ανάγωγο διότι, για παράδειγμα, $3 = \frac{3}{2} \cdot 2$.

2. Αν ο δακτύλιος R είναι σώμα, τότε κανένα στοιχείο του δεν είναι ανάγωγο.

3. Θα προσδιορίσουμε τα ανάγωγα στοιχεία του δακτυλίου $\mathbb{Z}$. Έστω p ένας πρώτος αριθμός. Τότε προφανώς το p δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}$, και οι μόνοι διαιρέτες του p στον δακτύλιο $\mathbb{Z}$ είναι ο εαυτός του p, η μονάδα 1, και τα αντίθετά τους στοιχεία $-p$ και -1. Προφανώς το ίδιο ισχύει και για τον αριθμό $-p$, όπου ο p είναι πρώτος. Αντίστροφα, αν n είναι ένας ακέραιος με την ιδιότητα ότι είναι μη αντιστρέψιμο στοιχείο του $\mathbb{Z}$, δηλαδή $n \neq \pm 1$, και οι μόνοι διαιρέτες του είναι τα αντιστρέψιμα στοιχεία του $\mathbb{Z}$, δηλαδή τα $1, -1$, και οι αριθμοί $\pm n$, τότε προφανώς ο αριθμός $|p|$ είναι πρώτος. Επομένως τα μόνα ανάγωγα στοιχεία το $\mathbb{Z}$ είναι τα $\pm p$, όπου p είναι πρώτος.

4. Έστω $P(t)$ ένα ανάγωγο στοιχείο του δακτυλίου $\mathbb{K}[t]$, όπου ο δακτύλιος $\mathbb{K}$ είναι σώμα. Τότε το $P(t)$ δεν είναι αντιστρέψιμο στοιχείο του $\mathbb{K}[t]$ και άρα $\deg P(t) \geq 1$. Αν $Q(t) \mid P(t)$, τότε αναγκαστικά θα έχουμε ότι είτε $Q(t) = a$, όπου $0 \neq a \in \mathbb{K}$, είτε $Q(t) = aP(t)$, όπου $0 \neq a \in \mathbb{K}$. Αυτό όμως σημαίνει ότι το πολυώνυμο $P(t)$ είναι ανάγωγο. Αντίστροφα, όπου προκύπτει άμεσα από τον Ορισμό 9.1.8, κάθε ανάγωγο πολυώνυμο είναι ανάγωγο στοιχείο του $\mathbb{K}[t]$. √

Η έννοια του ανάγωγου στοιχείου σχετίζεται με την έννοια του *πρώτου στοιχείου* σε έναν μεταθετικό δακτύλιο:

Ορισμός 11.4.3. *Ένα μη μηδενικό στοιχείο $p \in R$ σε έναν μεταθετικό δακτύλιο R καλείται* **πρώτο στοιχείο**, *αν το p δεν είναι αντιστρέψιμο, και αν $a, b \in R$ είναι μη μηδενικά στοιχεία του R έτσι ώστε $p \mid ab$, τότε είτε $p \mid a$ είτε $p \mid b$.*

Το ακόλουθο Λήμμα γενικεύει την ιδιότητα με την οποία ορίζεται ένα πρώτο στοιχείο.

[6] Βλέπε N. Jacobson: "*A note on non-commutative polynonials*", Ann. of Math. **33** (1934), 209–210, και T.-S. Rhai: "*A characterization of polynomial domains over a field*", Amer. Math. Monthly, **69** (1962), 984–986.

Λήμμα 11.4.4. *Έστω p ένα πρώτο στοιχείο σε έναν μεταθετικό δακτύλιο R. Αν το στοιχείο p διαιρεί το γινόμενο $a_1a_2\cdots a_n$ στοιχείων $a_i \in R$, $1 \le i \le n$, τότε υπάρχει δείκτης $i = 1,2,\cdots,n$, έτσι ώστε ο p να διαιρεί το στοιχείο a_i.*

Απόδειξη. Εξ ορισμού ο ισχυρισμός είναι αληθής όταν $n = 2$. Υποθέτουμε ότι ο ισχυρισμός είναι αληθής για $n-1 > 1$ το πλήθος στοιχεία του R και έστω ότι $p \mid a_1a_2\cdots a_n$. Επειδή το στοιχείο p είναι πρώτο, θα έχουμε ότι είτε $p \mid a_1a_2\cdots a_{n-1}$ είτε $p \mid a_n$. Αν $p \nmid a_n$, τότε $p \mid a_1a_2\cdots a_{n-1}$ και από την επαγωγική υπόθεση θα έχουμε ότι $p \mid a_i$ για κάποιο $i = 1,2\cdots,n-1$. Άρα από την Αρχή Μαθηματικής Επαγωγής, ο ισχυρισμός είναι αληθής για κάθε θετικό ακέραιο n. ■

Η ακόλουθη Πρόταση δείχνει ότι σε μια ακέραια περιοχή, κάθε πρώτο στοιχείο είναι ανάγωγο, αλλά το αντίστροφο δεν ισχύει.

Πρόταση 11.4.5 (Πρώτο $\Longrightarrow$ ανάγωγο)**.**

1. *Σε μια ακέραια περιοχή R, κάθε πρώτο στοιχείο είναι ανάγωγο.*
2. *Στην ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$, το στοιχείο $2+\sqrt{-5}$ είναι ανάγωγο αλλά όχι πρώτο.*

Απόδειξη. 1. Έστω p ένα πρώτο στοιχείο στην ακέραια παριοχή R. Τότε εξ ορισμού το p δεν είναι αντιστρέψιμο. Έστω $a \mid p$ ένας διαιρέτης του p, οπότε μπορύμε να γράψουμε $p = ab$, για ένα στοιχείο $b \in R$. Επειδή το στοιχείο p είναι πρώτο, έπεται ότι είτε $p \mid a$ είτε $p \mid b$. Αν $p \mid a$, τότε τα στοιχεία p, a είναι συντροφικά. Αν $p \mid b$, τότε $b = pc$ για κάποιο στοιχείο $c \in R$, και επομένως $b = abc$, δηλαδή $b(1-ac) = 0$. Επειδή ο δακτύλιος R είναι ακέραια περιοχή, και επειδή προφανώς $b \neq 0$ (διότι διαφορετικά θα είχαμε $p = 0$ το οποίο είναι άτοπο), έπεται ότι $ab = 1$, δηλαδή το a είναι αντιστρέψιμο. Επομένως το στοιχείο p είναι ανάγωγο.

2. Θεωρούμε την απεικόνιση

$$N\colon \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}, \quad N(x+y\sqrt{-5}) = (x+y\sqrt{-5})(x-y\sqrt{d}) = x^2+5y^2$$

για την οποία, σύμφωνα με το Λήμμα 11.2.9, ισχύει ότι $N(ab) = N(a)N(b)$, και τα αντιστρέψιμα στοιχεία του $\mathbb{Z}[\sqrt{-5}]$ είναι ακριβώς τα στοιχεία a με την ιδιότητα $N(a) = 1$, και αυτά είναι τα $1, -1$. Το στοιχείο $2+\sqrt{-5}$ δεν είναι πρώτο. Πράγματι το $2+\sqrt{-5}$ δεν είναι αντιστρέψιμο και έχουμε $9 = (2+\sqrt{-5})(2-\sqrt{-5})$, δηλαδή $(2+\sqrt{-5}) \mid 3\cdot 3$ αλλά $(2+\sqrt{-5}) \nmid 3$, διότι διαφορετικά θα είχαμε $3 = (2+\sqrt{-5})(k+l\sqrt{-5})$ και τότε $9 = N(3) = N(2+\sqrt{-5})N(k+l\sqrt{-5}) = 9(k^2+5l^2)$. Αυτό σημαίνει ότι $N(k+l\sqrt{-5}) = 1$ και άρα το $k+l\sqrt{-5}$ είναι αντιστρέψιμο, δηλαδή $k+l\sqrt{-5} = \pm 1$. Έτσι $k = \pm 1$ και $l = 0$ από όπου $3 = (\pm 1)(2+\sqrt{-5})$, το οποίο προφανώς είναι άτοπο. Άρα το στοιχείο $2+\sqrt{-5}$ δεν είναι πρώτο.

Το στοιχείο $2+\sqrt{-5}$ είναι όμως ανάγωγο, διότι αν $2+\sqrt{-5} = ab$, όπου $a, b \in \mathbb{Z}[\sqrt{-5}]$ είναι μη αντιστρέψιμα στοιχεία, τότε θα έχουμε $9 = N(2+\sqrt{-5}) = N(a)N(b)$ και $N(a) \neq \pm 1 \neq N(b)$. Επομένως $N(a) = 3 = N(b)$, δηλαδή, αν $a = x+y\sqrt{-5}$, τότε θα έχουμε $N(a) = x^2+5y^2 = 3$, και αυτό είναι προφανώς άτοπο, διότι $x, y \in \mathbb{Z}$. Άρα το στοιχείο $2+\sqrt{-5}$ είναι ανάγωγο. ■

Το ακόλουθο Θεώρημα χαρακτηρίζει τα ανάγωγα στοιχεία σε μια περιοχή κυρίων ιδεωδών και ιδιαίτερα δείχνει ότι σε τέτοιους δακτυλίους, τα πρώτα και τα ανάγωγα στοιχεία συμπίπτουν.

Θεώρημα 11.4.6. *Έστω R μια περιοχή κυρίων ιδεωδών, και $p \in R$ ένα μη μηδενικό στοιχείο της. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Το στοιχείο p είναι ανάγωγο.*
2. *Το ιδεώδες (p) είναι μεγιστοτικό.*
3. *Το ιδεώδες (p) είναι πρώτο.*
4. *Το στοιχείο p είναι πρώτο.*

Ιδιαίτερα κάθε μη μηδενικό πρώτο ιδεώδες μιας περιοχής κυρίων ιδεωδών είναι μεγιστοτικό ιδεώδες.

Απόδειξη. (α) «1. $\Longrightarrow$ 2.» Έστω ότι το στοιχείο p είναι ανάγωγο, και θεωρουμε το κύριο ιδεώδες (p) του R. Επειδή το p είναι ανάγωγο, έπεται ότι το p δεν είναι αντιστρέψιμο, και επομένως το ιδεώδες (p) είναι γνήσιο. Επειδή κάθε γνήσιο ιδεώδες περιέχεται σε ένα μεγιστοτικό ιδεώδες και επειδή ο δακτύλιος R είναι περιοχή κυρίων ιδεωδών, έπεται ότι υπάρχει ένα στοιχείο $q \in R$ έτσι ώστε $(p) \subseteq (q) \subseteq R$ και το (q) είναι μεγιστοτικό ιδεώδες. Επειδή $p \in (p) \subseteq (q)$, έπεται ότι $p = qa$, για κάποιο στοιχείο $a \in R$. Επειδή το p είναι ανάγωγο, έπεται ότι είτε το q είναι αντιστρέψιμο είτε το q είναι συντροφικό στοιχείο του p. Επειδή το ιδεώδες (q), ως μεγιστοτικό, είναι γνήσιο, έπεται ότι το q δεν είναι αντιστρέψιμο και επομένως τα p, q είναι συντροφικά στοιχεία. Επειδή συντροφικά στοιχεία παράγουν το ίδιο κύριο ιδεώδες, θα έχουμε $(p) = (q)$ και άρα το (p) είναι μεγιστοτικό.

(β) «2. $\Longrightarrow$ 3.» Η απόδειξη είναι άμεση διότι κάθε μεγιστοτικό ιδεώδες σε έναν μεταθετικό δακτύλιο με μονάδα είναι πρώτο.

[(γ) «3. $\Longrightarrow$ 4.» Έστω ότι το κύριο ιδεώδες (p) είναι πρώτο. Τότε το (p) είναι γνήσιο και επομένως το στοιχείο p δεν είναι αντιστρέψιμο. Αν $a, b \in R$ είναι δύο μη μηδενικά στοιχεία του R, έτσι ώστε $p \mid ab$, τότε $ab = pc$, για κάποιο $c \in R$. Προφανώς τότε θα έχουμε $ab \in (p)$ και επειδή το (p) είναι πρώτο, έπεται ότι είτε $a \in (p)$ είτε $b \in (p)$. Ισοδύναμα, θα έχουμε ότι είτε $p \mid a$ είτε $p \mid b$. Επομένως το στοιχείο p είναι πρώτο.

(δ) «4. $\Longrightarrow$ 1.» Προκύπτει από την Πρόταση 11.4.5. ■

Παρατήρηση 11.4.7. Η ισοδυναμία

«Το στοιχείο $p \in R$ είναι πρώτο αν και μόνο αν το ιδεώδες (p) του R είναι πρώτο»

του Θεωρήματος 11.4.6 ισχύει σε κάθε ακέραια περιοχή, όχι κατ' ανάγκην περιοχή κυρίων ιδεωδών. Πράγματι, η απόδειξη ότι, αν το ιδεώδες (p) είναι πρώτο, τότε το στοιχείο p είναι πρώτο, ισχύει χωρίς καμία αλλαγή στο πλαίσιο των ακέραιων περιοχών. Αντίστροφα, αν το στοιχείο p είναι πρώτο και $ab \in (p)$, τότε $ab = pc$ για κάποιο $c \in R$. Τότε $p \mid ab$ και άρα, επειδή το p είναι πρώτο, θα έχουμε $p \mid a$ ή $p \mid b$, δηλαδή $a \in (p)$ ή $b \in (p)$. Άρα το ιδεώδες (p) είναι πρώτο. ▲

11.4.2 Περιοχές Μονοσήμαντης Ανάλυσης

Στον δακτύλιο $\mathbb{Z}$ των ακεραίων έχουμε τις ακόλουθες παραγοντοποιήσεις του αριθμού 10:

$$10 = 2 \cdot 5 = 5 \cdot 2 = (-2) \cdot (-5) = (-5)(-2)$$

Τα στοιχεία τα οποία εμφανίζονται στις παραπάνω παραγοντοποιήσεις είναι πρώτα και ανάγωγα στοιχεία του $\mathbb{Z}$, και, όπως βλέπουμε, αυτά διαφέρουν μόνο ως προς τη σειρά αναγραφής τους και ως προς τον πολλαπλασιασμό με αντιστρέψιμα στοιχεία του $\mathbb{Z}$. Με βάση αυτή την παρατήρηση, οι παραπάνω παραγοντοποιήσεις του 10 σε γινόμενο ανάγωγων στοιχείων δεν θεωρούνται διαφορετικές.

Από την άλλη πλευρά, στον δακτύλιο $\mathbb{Z}[\sqrt{-5}]$, έχουμε

$$9 = 3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{5})$$

και τα στοιχεία $3, 2 + \sqrt{-5}$ και $3, 2 - \sqrt{-5}$ δεν είναι αντιστρέψιμα, και δεν διαφέρουν κατά αντιστρέψιμο στοιχείο του $\mathbb{Z}[\sqrt{-5}]$ (τα αντιστρέψιμα στοιχεία του R είναι τα ± 1). Επιπλέον τα στοιχεία $3, 2 + \sqrt{-5}, 2 - \sqrt{-5}$ είναι ανάγωγα. Πράγματι, είδαμε στην Πρόταση 11.4.5 ότι το στοιχείο $2 + \sqrt{-5}$ είναι ανάγωγο, και παρόμοιο επιχείρημα δείχνει ότι το στοιχείο $2 - \sqrt{-5}$ είναι ανάγωγο. Το στοιχείο 3 δεν είναι αντιστρέψιμο, και, αν $3 = (x + y\sqrt{-5})(z + w\sqrt{-5})$, όπου τα στοιχεία $(x + y\sqrt{-5}), (z + w\sqrt{-5})$ δεν είναι αντιστρέψιμα, τότε θα έχουμε $9 = N(3) = N\big((x + y\sqrt{-5})(z + w\sqrt{-5})\big) = N(x + y\sqrt{-5})N(z + w\sqrt{-5}) = (x^2 + 5y^2)(z^2 + 5w^2)$, από όπου έπεται ότι $x^2 + 5y^2 = 3$ και αυτό είναι άτοπο διότι $x, y \in \mathbb{Z}$. Άρα το 3 είναι ανάγωγο στοιχείο στον δακτύλιο $\mathbb{Z}[\sqrt{-5}]$.

Επομένως οι παραπάνω παραγοντοποιήσεις του 9 είναι διαφορετικές με την έννοια ότι τα ανάγωγα στοιχεία τα οποία εμφανίζονται δεν είναι συντροφικά.

Η παραπάνω διαφοροποίηση μας οδηγεί στην εισαγωγή και μελέτη δακτυλίων στους οποίους η παραγοντοποίηση σε γινόμενο ανάγωγων στοιχείων είναι μοναδική, με την έννοια ότι η μόνη διαφοροποίηση εντοπίζεται στη σειρά εμφάνισης και σε γινόμενα των παραγόντων με αντιστρέψιμα στοιχεία.

Ορισμός 11.4.8. *Μια ακέραια περιοχή R καλείται* **περιοχή μονοσήμαντης ανάλυσης**, *αν:*

(ΠΜΑ1) Κάθε μη μηδενικό στοιχείο του R είναι είτε αντιστρέψιμο είτε (πεπερασμένο) γινόμενο ανάγωγων στοιχείων.

(ΠΜΑ2) Έστω $\{p_i\}_{i=1}^n$ και $\{q_j\}_{j=1}^m$ είναι δύο σύνολα ανάγωγων στοιχείων του R και ισχύει ότι:

$$a := p_1 p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$$

τότε $n = m$, υπάρχει μια μετάθεση $\sigma \in \mathsf{S}_n$ και αντιστρέψιμα στοιχεία u_i, $1 \le i \le n$, του R, έτσι ώστε: $q_{\sigma(i)} = u_i p_i$, $1 \le i \le n$.

Τότε θα λέμε ότι η ανάλυση ή παραγοντοποίηση του a σε γινόμενο ανάγωγων στοιχείων είναι μοναδική.

Οι ιδιότητες (ΠΜΑ1) και (ΠΜΑ2) διατυπώνονται ισοδύναμα ως εξής: κάθε μη μηδενικό στοιχείο $a \in R$ έχει **μοναδική ανάλυση ή μοναδική παραγοντοποίηση** σε γινόμενο ανάγωγων στοιχείων. Το πλήθος των ανάγωγων στοιχείων σε μια παραγοντοποίηση του a σε ανάγωγα στοιχεία εξαρτάται μόνο από το στοιχείο a και καλείται μήκος παραγοντοποίησης του a.

Με βάση την ανάλυση που προηγήθηκε, η ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι περιοχή μονοσήμαντης ανάλυσης. Αντίθετα, όπως προκύπτει από το Θεμελιώδες Θεώρημα της Αριθμητικής (και θα αποδείξουμε σε λίγο), ο δακτύλιος των ακεραίων είναι περιοχή μονοσήμαντης ανάλυσης.

Σκοπός μας στο υπόλοιπο αυτής της ενότητας είναι να αποδείξουμε κάποιους χαρακτηρισμούς περιοχών μονοσήμαντης ανάλυσης και να δείξουμε ότι κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μονοσήμαντης ανάλυσης. Ξεκινάμε δείχνοντας ότι σε μια περιοχή μονοσήμαντης ανάλυσης, τα πρώτα στοιχεία συμπίπτουν με τα ανάγωγα στοιχεία.

Πρόταση 11.4.9. *Σε μια περιοχή μονοσήμαντης ανάλυσης, ένα στοιχείο είναι πρώτο αν και μόνο αν είναι ανάγωγο.*

Απόδειξη. Από την Πρόταση 11.4.5 γνωρίζουμε ότι σε μια ακέραια περιοχή R κάθε πρώτο στοιχείο είναι ανάγωγο. Θα δείξουμε ότι, αν η περιοχή R είναι περιοχή μονοσήμαντης ανάλυσης, τότε κάθε ανάγωγο στοιχείο p της R είναι πρώτο. Έστω $a, b \in R \setminus \{0\}$, και υποθέτουμε ότι $p \mid ab$, δηλαδή $ab = pc$, για κάποιο $c \in R$ το οποίο είναι μη μηδενικό διότι, επειδή ο R είναι ακέραια περιοχή, θα έχουμε $ab \neq 0$. Αν το στοιχείο a είναι αντιστρέψιμο, τότε $pca^{-1} = b$ και άρα $p \mid b$. Παρόμοια, αν το b είναι αντιστρέψιμο, τότε $p \mid a$. Υποθέτουμε τώρα ότι τα στοιχεία a, b δεν είναι αντιστρέψιμα. Τότε από την ιδιότητα (ΠΜΑ1), έπεται ότι μπορούμε να γράψουμε $a = a_1 a_2 \cdots a_n$ και $b = b_1 b_2 \cdots b_m$, όπου τα στοιχεία a_i και b_j είναι ανάγωγα, $1 \le i \le n$ και $1 \le j \le m$. Έτσι θα έχουμε:

$$ab = pc = a_1 a_2 \cdots a_n \cdot b_1 b_2 \cdots b_m$$

Αν το στοιχείο c είναι αντιστρέψιμο, τότε το στοιχείο pc είναι προφανώς ανάγωγο και άρα, χρησιμοποιώντας την ιδιότητα (ΠΜΑ2), το στοιχείο pc ή ισοδύναμα το συντροφικό του p είναι συντροφικό με ένα εκ των $a_1, a_2, \cdots a_n, b_1, b_2, \cdots b_m$, δηλαδή είτε υπάρχει $i = 1, 2, \cdots, n$ και αντιστρέψιμο στοιχείο u έτσι ώστε $pu = a_i$ είτε υπάρχει $j = 1, 2, \cdots, m$ και αντιστρέψιμο στοιχείο v έτσι ώστε $pv = b_j$. Προφανώς, στην πρώτη περίπτωση θα έχουμε $p \mid a = a_1 \cdots a_{i-1} p u a_{i+1} \cdots a_n$, και στην δεύτερη περίπτωση θα έχουμε $p \mid b = b_1 \cdots b_{j-1} p v b_{j+1} \cdots b_m$. Αν το στοιχείο c δεν είναι αντιστρέψιμο, τότε από την ιδιότητα (ΠΜΑ1), μπορούμε να γράψουμε $c = c_1 c_2 \cdots c_k$ για κάποια ανάγωγα στοιχεία $c_i \in R$, $1 \le i \le k$. Τότε θα έχουμε

$$ab = a_1 a_2 \cdots a_n \cdot b_1 b_2 \cdots b_m = pc = pc_1 c_2 \cdots c_k$$

και άρα από την ιδιότητα (ΠΜΑ2), το στοιχείο p είναι συντροφικό με κάποιο από τα ανάγωγα στοιχεία $a_1, a_2, \cdots a_n, b_1, b_2, \cdots b_m$. Τότε, όπως και παραπάνω, το στοιχείο p θα διαιρεί ένα εκ των a και b. Επομένως το ανάγωγο στοιχείο p είναι πρώτο. ■

Ορισμός 11.4.10. *Ένας μεταθετικός δακτύλιος R ικανοποιεί τη* **συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη**, *αν για κάθε αύξουσα ακολουθία*

$$(a_1) \subseteq (a_2) \subseteq \cdots (a_n) \subseteq (a_{n+1}) \subseteq \cdots$$

κύριων ιδεωδών του R, υπάρχει δείκτης $m \geq 1$, έτσι ώστε: $(a_m) = (a_{m+1}) = \cdots$.

Το ακόλουθο Θεώρημα παρουσιάζει κάποιες σημαντικές ιδιότητες οι οποίες αφορούν την ύπαρξη και μοναδικότητα παραγοντοποίησης στοιχείων σε ανάγωγους παράγοντες.

Θεώρημα 11.4.11. *Έστω R μια ακέραια περιοχή.*

1. *Αν ο R είναι περιοχή μονοσήμαντης ανάλυσης, τότε ο R ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη.*
2. *Αν ο R ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη, τότε ο R ικανοποιεί την ιδιότητα (ΠΜΑ1).*
3. *Αν ο R ικανοποιεί την ιδιότητα (ΠΜΑ1) και κάθε ανάγωγο στοιχείο του R είναι πρώτο, τότε ο R είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. 1. Θεωρούμε μια αύξουσα ακολουθία

$$(a_1) \subseteq (a_2) \subseteq \cdots (a_n) \subseteq (a_{n+1}) \subseteq \cdots$$

κύριων ιδεωδών. Επειδή γενικά ισχύει ότι $(b) \subseteq (c)$ αν και μόνο αν $c \mid b$, έπεται ότι θα έχουμε:

$$\forall n \geq 1: \quad a_{n+1} \mid a_n \qquad \text{και άρα} \qquad \exists x_n \in R: \quad a_n = x_n a_{n+1}$$

Επομένως στην ανάλυση του a_{n+1} σε ανάγωγους παράγοντες, τα ανάγωγα στοιχεία τα οποία εμφανίζονται θα αποτελούνται από κάποια (μπορεί και όλα) από τα ανάγωγα στοιχεία τα οποία εμφανίζονται στην ανάλυση του a_n σε ανάγωγους παράγοντες. Επειδή το στοιχείο a_1 διαιρείται από όλα τα στοιχεία a_n, $n \geq 1$, και επειδή το στοιχείο a_1 γράφεται μοναδικά ως γινόμενο πεπερασμένου πλήθους αναγώγων στοιχείων, έπεται ότι υπάρχει κάποιος δείκτης $m \geq 1$, έτσι ώστε τα ανάγωγα στοιχεία τα οποία εμφανίζονται στις αναλύσεις των στοιχείων a_k, $k \geq m$ είναι τα ίδια. Αυτό σημαίνει ότι τα στοιχεία a_k, $k \geq m$, διαφέρουν μόνο ως προς τον πολλαπλασιασμό με αντιστρέψιμα στοιχεία, δηλαδή είναι συντροφικά. Επειδή συντροφικά στοιχεία παράγουν το ίδιο κύριο ιδεώδες, έπεται ότι $(a_m) = (a_{m+k})$, $\forall k \geq 1$, και επομένως η αύξουσα ακολουθία σταθεροποιείται.

2. Υποθέτουμε ότι ο R ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη. Έστω a_1 ένα μη μηδενικό στοιχείο του R. Αν το a_1 είναι ανάγωγο, δεν υπάρχει τίποτα να αποδείξουμε. Αν το a_1 δεν είναι ανάγωγο, τότε μπορούμε να γράψουμε $a_1 = a_2 b_2$, όπου τα στοιχεία a_2, b_2 δεν είναι αντιστρέψιμα. Επειδή $a_2 \mid a_1$, θα έχουμε $(a_1) \subseteq (a_2)$ και μάλιστα $(a_1) \neq (a_2)$ διότι αν $(a_1) = (a_2)$, τότε τα στοιχεία a_1, a_2 θα ήταν συντροφικά, και άρα $a_1 = a_2 u$, όπου το u είναι αντιστρέψιμο. Τότε $a_2 b_2 = a_1 = a_2 u$ και άρα $a_2(b_2 - u) = 0$. Επειδή $a_2 \neq 0$ (αν $a_2 = 0$, τότε $a_1 = 0$ και αυτό είναι άτοπο), θα έχουμε $b_2 = u$ και άρα το b_2 είναι αντιστρέψιμο. Αυτό είναι άτοπο διότι το b_2 είναι ανάγωγο. Άρα $(a_1) \subsetneqq (a_2)$. Αν το στοιχείο $a_2 b_2$ είναι ανάγωγα, τότε έχουμε το ζητούμενο. Αν αυτό δεν ισχύει, τότε ένα εκ των a_2 και b_2, έστω χωρίς βλάβη της γενικότητας το a_2, δεν είναι ανάγωγο. Τότε μπορούμε να γράψουμε $a_2 = a_3 b_3$, όπου τα στοιχεία a_3 και b_3 δεν είναι αντιστρέψιμα, και όπως παραπάνω θα έχουμε μια γνήσια έγκλειση κύριων ιδεωδών $(a_2) \subsetneqq (a_3)$. Η διαδικασία αυτή, η οποία μπορεί να συνεχιστεί όταν κάποιος από τους παράγοντες δεν είναι ανάγωγο στοιχείο, παράγει μια ακολουθία στοιχείων $a_1, a_2, a_3, \cdots$ του R στην οποία κάθε στοιχείο είναι γνήσιος διαιρέτης του προηγούμενου. Η ακολουθία αυτή με τη σειρά της παράγει μια αύξουσα ακολουθία κύριων ιδεωδών

$$(a_1) \subsetneqq (a_2) \subsetneqq \cdots (a_n) \subsetneqq (a_{n+1}) \subseteq \cdots$$

για την οποία, από την υπόθεση, υπάρχει δείκτης $m \geq 1$ έτσι ώστε: $(a_m) = (a_{m+1}) = (a_{m+2}) = \cdots$. Αυτό όμως είναι άτοπο διότι $(a_n) \neq (a_{n+1})$ από την κατασκευή της ακολουθίας κύριων ιδεωδών. Επομένως

σε κάποιο βήμα της διαδικασίας όλοι οι παράγοντες της ανάλυσης του a_1 είναι ανάγωγοι. Επομένως θα έχουμε μια παραγοντοποίηση του a_1 σε γινόμενο αναγώγων στοιχείων και έτσι ικανοποιείται η ιδιότητα (ΠΜΑ1).

3. Αρκεί να δείξουμε ότι η παραγοντοποίηση ενός μη μηδενικού στοιχείου σε γινόμενο ανάγωγων στοιχείων είναι μοναδική. Υποθέτουμε ότι $\{p_i\}_{i=1}^n$ και $\{q_j\}_{j=1}^m$ είναι δύο σύνολα ανάγωγων στοιχείων του R, και ισχύει ότι:
$$a := p_1 p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m$$
Θα δείξουμε τον ισχυρισμό, δηλαδή ότι ισχύει στον δακτύλιο R η ιδιότητα (ΠΜΑ2), με χρήση της Αρχής Μαθηματικής Επαγωγής. Αν $n = 1$, τότε $a = p_1$ είναι ανάγωγο στοιχείο του R. Επομένως αναγκαστικά $m = 1$ και $q_1 = a = p_1$. Υποθέτουμε ότι η ιδιότητα (ΠΜΑ2) είναι αληθής, για $n-1$ ανάγωγους παράγοντες, δηλαδή κάθε στοιχείο το οποίο μπορεί να γραφεί ως γινόμενο $n-1$ το πλήθος ανάγωγων στοιχείων έχει μοναδική παραγοντοποίηση, και θεωρούμε το στοιχείο a όπως παραπάνω. Επειδή το στοιχείο p_1 είναι ανάγωγο, από την υπόθεση θα είναι πρώτο, και άρα από το Λήμμα 11.4.4 έπεται ότι $p_1 \mid q_j$ για κάποιο $j = 1, 2, \cdots, m$. Χωρίς βλάβη της γενικότητας, εν ανάγκη μετά από κάποια αναδιάταξη των στοιχείων $q_1, q_2, \cdots, q_m$, μπορούμε να υποθέσουμε ότι $j = 1$ και άρα $p_1 \mid q_1$. Επειδή το q_1 είναι ανάγωγο, έπεται ότι τα στοιχεία p_1 και q_1 είναι συντροφικά, και άρα $q_1 = u_1 p_1$, όπου το στοιχείο u_1 είναι αντιστρέψιμο. Τότε θα έχουμε $p_1 p_2 \cdots p_n = u_1 p_1 \cdot q_2 \cdots q_m$. Επειδή ο δακτύλιος R είναι ακέραια περιοχή, ισχύει ο Νόμος Διαγραφής και επομένως η παραπάνω σχέση γράφεται
$$b := p_2 \cdots p_n = u_1 \cdot q_2 \cdots q_m = q_2' \cdots q_m'$$
όπου $q_2' = u_1 q_2$, και $q_j' = q_j$, $3 \le j \le m$, είναι ανάγωγα στοιχεία του R. Από την επαγωγική υπόθεση έπεται ότι θα έχουμε $n-1 = m-1$ και μετά από κάποια αναδιάταξη των στοιχείων $p_2, \cdots, p_n$ και $q_2', \cdots, q_m'$, θα έχουμε ότι τα στοιχεία p_k και q_k' είναι συντροφικά, $2 \le k \le n$. Τότε όμως θα έχουμε $n = m$ και τα στοιχεία p_k και q_k είναι συντροφικά, $1 \le k \le n$. Επομένως από την Αρχή Μαθηματικής Επαγωγής, η ιδιότητα (ΠΜΑ2) ισχύει για κάθε πεπερασμένο γινόμενο αναγώγων στοιχείων του R. Συνεπώς ο δακτύλιος R είναι περιοχή μονοσήμαντης ανάλυσης. ■

Ως άμεση συνέπεια του Θεωρήματος 11.4.11 και της Πρότασης 11.4.9, έχουμε το ακόλουθο Θεώρημα το οποίο χαρακτηρίζει τις περιοχές μονοσήμαντης ανάλυσης.

Θεώρημα 11.4.12. *Για μια ακέραια περιοχή R, τα ακόλουθα είναι ισοδύναμα:*

1. *Η R είναι περιοχή μονοσήμαυτης ανάλυσης.*
2. *(α′) Η R ικανοποιεί την ιδιότητα (ΠΜΑ1), δηλαδή κάθε μη-μηδενικό στοιχείο του R είναι είτε αντιστρέψιμο είτε (πεπερασμένο) γινόμενο ανάγωγων στοιχείων, και*
   (β′) κάθε ανάγωγο στοιχείο της R είναι πρώτο.
3. *(α′) Η R ικανοποιεί την συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη και*
   (β′) κάθε ανάγωγο στοιχείο της R είναι πρώτο.

Το ακόλουθο Θεώρημα δείχνει ότι μια σημαντική κλάση ακέραιων περιοχών είναι περιοχές μονοσήμαντης ανάλυσης.

Θεώρημα 11.4.13. *Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μονοσήμαυτης ανάλυσης.*

Απόδειξη. Έστω R μια περιοχή κυρίων ιδεωδών. Τότε από την Πρόταση 11.1.9, ο δακτύλιος R είναι δακτύλιος της Noether και επομένως ικανοποιείται η συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη του R. Από το Θεώρημα 11.4.6 έπεται ότι κάθε ανάγωγο στοιχείο της R είναι πρώτο. Επομένως από το Θεώρημα 11.4.12, η περιοχή R είναι περιοχή μονοσήμαντης ανάλυσης. ■

Επειδή κάθε Ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών, θα έχουμε την ακόλουθη συνέπεια.

Πόρισμα 11.4.14. *Κάθε Ευκλείδεια περιοχή είναι περιοχή μονοσήμαντης ανάλυσης.*

Τα ακόλουθα παραδείγματα δείχνουν την ευρύτητα εφαρμογής του Θεωρήματος 11.4.13.

Παράδειγμα 11.4.15. Το πρώτο παράδειγμα μας είναι οικείο από τη στοιχειώδη Θεωρία Αριθμών.

1. Ο δακτύλιος των ακεραίων, ως περιοχή κυρίων ιδεωδών, είναι περιοχή μονοσήμαντης ανάλυσης. Τα πρώτα στοιχεία συμπίπτουν με τα ανάγωγα, και είναι τα στοιχεία του συνόλου $\{\pm p \in \mathbb{Z} \mid p : \text{πρώτος}\}$. Παρατηρούμε ότι τα στοιχεία $p, -p$ είναι συντροφικά, και κάθε θετικός ακέραιος $a > 1$ μπορεί να γραφεί μοναδικά ως γινόμενο: $a = p_1 p_2 \cdots p_n$, όπου οι αριθμοί $p_1, p_2, \cdots, p_n$ είναι πρώτοι, όπου κάποιοι από αυτούς μπορεί να συμπίπτουν. Ισοδύναμα μπορούμε να γράψουμε μοναδικά $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, όπου οι πρώτοι $p_1, p_2, \cdots, p_k$ είναι διακεκριμένοι, και $a_i \geq 1$. Η παραπάνω ανάλυση του a είναι γνωστή ως η πρωτογενής ανάλυση του a.

2. Ο δακτύλιος πολυωνύμων $\mathbb{K}[t]$, όπου ο δακτύλιος $\mathbb{K}$ είναι σώμα, ως περιοχή κυρίων ιδεωδών, είναι περιοχή μονοσήμαντης ανάλυσης. Τα πρώτα στοιχεία του $\mathbb{K}[t]$ συμπίπτουν με τα ανάγωγα, και είναι τα ανάγωγα πολυώνυμα. Κάθε μη μηδενικό πολυώνυμο είναι είτε αντιστρέψιμο, δηλαδή σταθερό μη μηδενικό πολυώνυμο, ή μπορεί να γραφεί μοναδικά ως $P(t) = P_1(t)^{a_1} P_2(t)^{a_2} \cdots P_k(t)^{a_k}$, όπου τα πολυώνυμα $P_i(t)$ είναι ανάγωγα και $a_k \geq 1$, $1 \leq i \leq k$.

3. Θεωρούμε το σύνολο
$$R = \{P(t) \in \mathbb{Q}[t] \mid P(0) \in \mathbb{Z}\}$$
των πολυωνύμων υπεράνω του $\mathbb{Q}$ με σταθερό όρο από τον δακτύλιο $\mathbb{Z}$ των ακεραίων. Εύκολα βλέπουμε ότι το σύνολο R είναι ένας υποδακτύλιος του $\mathbb{K}[t]$ και άρα είναι μια ακέραια περιοχή. Ο δακτύλιος R δεν είναι περιοχή μονοσήμαντης ανάλυσης διότι δεν ικανοποιεί την συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη. Για παράδειγμα, η ακολουθία
$$(t) \subseteq \left(\frac{t}{2}\right) \subseteq \left(\frac{t}{2^2}\right) \subseteq \cdots \subseteq \left(\frac{t}{2^n}\right) \subseteq \left(\frac{t}{2^{n+1}}\right) \subseteq \cdots$$
είναι μια ακολουθία κύριων ιδεωδών του R η οποία δεν σταθεροποιείται. Κατ' αρχήν, επειδή $\frac{t}{2^n} = \frac{t}{2^{n+1}} 2 \in \left(\frac{t}{2^{n+1}}\right)$ και άρα $\left(\frac{t}{2^n}\right) \subseteq \left(\frac{t}{2^{n+1}}\right)$. Αν $\left(\frac{t}{2^n}\right) = \left(\frac{t}{2^{n+1}}\right)$, τότε $\frac{t}{2^{n+1}} = \frac{t}{2^n} P(t)$ για κάποιο πολυώνυμο $P(t) = a_0 + a_1 t + \cdots a_k t^k \in \mathbb{K}[t]$, όπου $a_0 \in \mathbb{Z}$. Επομένως $\frac{t}{2} = t(a_0 + a_1 t + \cdots + a_k t^k$ και άρα $a_0 = \frac{1}{2}$ το οποίο είναι άτοπο. Άρα ο δακτύλιος R δεν ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη και επομένως από το Θεώρημα 11.4.12 έπεται ότι ο R δεν είναι περιοχή μονοσήμαντης ανάλυσης.

4. Υπάρχουν περιοχές μονοσήμαντης ανάλυσης οι οποίες δεν είναι περιοχές κυρίων ιδεωδών. Πράγματι, έχουμε δει ότι ο δακτύλιος πολυωνύμων $\mathbb{K}[t_1, t_2, \cdots, t_n]$, $n \geq 2$, όπου $\mathbb{K}$ είναι σώμα, και ο δακτύλιος $\mathbb{Z}[t]$ δεν είναι περιοχές κυρίων ιδεωδών. Θα δούμε στην επόμενη ενότητα ότι ο δακτύλιος πολυωνύμων $\mathbb{K}[t_1, t_2, \cdots, t_n]$, όπου $\mathbb{K}$ είναι σώμα, και ο δακτύλιος πολυωνύμων $\mathbb{Z}[t_1, t_2, \cdots, t_n]$ είναι περιοχές μονοσήμαντης ανάλυσης, $\forall n \geq 1$. $\surd$

Μέγιστος Κοινός Διαιρέτης σε Περιοχές Μονοσήμαντης Ανάλυσης

Έστω R μια περιοχή μονοσήμαντης ανάλυσης και $a, b \in R$. Αν ένα εκ των στοιχείων a, b είναι αντιστρέψιμο, τότε προφανώς ένας μέγιστος κοινός διαιρέτης (a, b) των στοιχείων a, b είναι το στοιχείο a και ένα ελάχιστο κοινό πολλαπλάσιο $[a, b]$ των στοιχείων a, b είναι το στοιχείο b. Υποθέτουμε ότι τα στοιχεία a, b δεν είναι αντιστρέψιμα. Τότε το a γρέφεται μοναδικά ως γινόμενο ανάγωγων στοιχείων $a = p_1 p_2 \cdots p_n$. Συλλέγοντας τους ανάγωγους παράγοντες οι οποίοι εμφανίζονται στην παραπάνω παραγοντοποίηση και αντικαθιστώντας συντροφικά στοιχεία με έναν αντιπρόσωπό τους πολλαπλασιασμένο με κατάλληλο αντιστρέψιμο στοιχείο, μπορούμε να γράψουμε για το a, και παρόμοια για το b:
$$a = u p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \qquad \text{και} \qquad b = v q_1^{b_1} q_2^{b_2} \cdots q_l^{b_l}$$

όπου τα στοιχεία u, v είναι αντιστρέψιμα και τα $p_1, p_2, \cdots, p_k$ και $q_1, q_2, \cdots, q_l$ είναι ανά δύο μη συντροφικά ανάγωγα στοιχεία, και οι αριθμοί a_i και b_j είναι θετικοί ακέραιοι, όπου $1 \leq i \leq k$ και $1 \leq j \leq l$. Αν $d = u' p_1^{a_1'} p_2^{a_2'} \cdots p_k^{a_k'}$, όπου a_i' είναι ακέραιοι με $0 \leq a_i' \leq a_i$, $1 \leq i \leq k$, τότε είναι άμεσο ότι το στοιχείο d είναι διαιρέτης του a. Αντίστροφα, αν d είναι διαιρέτης του a, γράφουμε τη μοναδική ανάλυσή του ως γινόμενο ανάγωγων στοιχείων του $d = w r_1^{d_1} r_2^{d_2} \cdots r_t^{d_t}$, όπου το στοιχείο w είναι αντιστρέψιμο, τα $r_1, r_2, \cdots, r_t$ είναι ανά δύο μη συντροφικά ανάγωγα στοιχεία, και $d_i \geq 1$, $1 \leq i \leq t$. Επειδή $r_i \mid d$ και $d \mid a$, έπεται ότι $r_1 \mid a$, $1 \leq i \leq t$. Επειδή τα ανάγωγα στοιχεία του R συμπίπτουν με τα πρώτα στοιχεία, έπεται ότι κάθε r_i διαιρεί ένα από τα ανάγωγα στοιχεία p_j, και άρα τα στοιχεία r_i και p_j είναι συντροφικά. Προφανώς τότε $1 \leq t \leq k$ και $d_l \leq a_l$, $1 \leq l \leq t$. Συνοψίζοντας, έχουμε ότι οι διαιρέτες του $a = u p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ είναι της μορφής $d = w r_1^{d_1} r_2^{d_2} \cdots r_t^{d_t}$, όπου το στοιχείο w είναι αντιστρέψιμο, τα $r_1, r_2, \cdots, r_t$ είναι ανά δύο μη συντροφικά ανάγωγα στοιχεία, και $d_i \leq a_i \geq 1$, $1 \leq i \leq t$.

Αν κάποιο ανάγωγο στοιχείο p_i είναι διαφορετικό από ένα ανάγωγο στοιχείο q_j, τότε, εισάγοντας τα ανάγωγα στοιχεία που λείπουν στις παραπάνω παραγοντοποιήσεις με μηδενικούς εκθέτες, μπορούμε να γράψουμε:

$$a = u p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m} \qquad \text{και} \qquad b = v p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m}$$

όπου τα στοιχεία u, v είναι αντιστρέψιμα και τα $p_1, p_2, \cdots, p_m$ και $q_1, q_2, \cdots, q_l$ είναι ανά δύο μη συντροφικά ανάγωγα στοιχεία, και οι αριθμοί a_i και b_j είναι μη αρνητικοί ακέραιοι, όπου $1 \leq i, j \leq m$.

Ισχυρισμός: Θέτοντας:

$$d = u p_1^{\min\{a_1, b_1\}} p_2^{\min\{a_2, b_2} \cdots p_k^{\min\{a_k, b_k\}} \qquad \text{και} \qquad e = v p_1^{\max\{a_1, b_1\}} p_2^{\max\{a_2, b_2\}} \cdots p_m^{\max\{a_m, b_m}$$

έπεται ότι το στοιχείο c είναι ένας μέγιστος κοινός διαιρέτης των a και b, και το στοιχείο c είναι ένα ελάχιστο κοινό πολλαπλάσιο των a και b.

Πράγματι θα έχουμε προφανώς ότι $d \mid a$ και $d \mid b$. Έστω $c \in R$ και υποθέτουμε ότι $c \mid a$ και $c \mid b$. Τότε μπορούμε να γράφουμε όπως παραπάνω $c = w p_1^{c_1} p_2^{c_2} \cdots p_m^{c_m}$, όπου το w είναι αντιστρέψιμο και $0 \leq c_i \leq a_i, b_i$, όπου $1 \leq i \leq m$. Οι παραπάνω ανισότητες δείχνουν ότι $c_i \leq \min\{a_i, b_i\}$ και επομένως $c \mid d$. Δηλαδή το στοιχείο d είναι ένας μέγιστος κοινός διαιρέτης των a, b. Παρόμοια προκύπτει ότι το στοιχείο e είναι ένα ελάχιστο κοινό πολλαπλάσιο των a, b.

Συνοψίζοντας την παραπάνω ανάλυση, θα έχουμε ότι:

Πρόταση 11.4.16. *Για κάθε δύο μη μηδενικά στοιχεία μιας περιοχής μονοσήμαντης ανάλυσης, υπάρχει ένας μέγιστος κοινός διαιρέτης και ένα ελάχιστο κοινό πολλαπλάσιο.*

Είναι εύκολο να αποδειχθεί με χρήση της Αρχής Μαθηματικής Επαγωγής ότι σε μια περιοχή μονοσήμαντης ανάλυσης κάθε πεπερασμένο σύνολο $a_1, a_2, \cdots, a_n \in R$ μη μηδενικών στοιχείων έχει έναν μέγιστο κοινό διαιρέτη $(a_1, a_2, \cdots, a_n)$, βλέπε την Άσκηση 11.5.24.

Για τον μέγιστο κοινό διαιρέτη στοιχείων σε μια περιοχή μονοσήμαντης ανάλυσης R ισχύουν ανάλογες ιδιότητες με τις γνωστές μας ιδιότητες μέγιστου κοινού διαιρέτη ακεραίων αριθμών, όπου συνήθως η ισότητα αντικαθίσταται από τη σχέση συντροφικότητας.

Για παράδειγμα ισχύει ότι:

$$\forall a, b, c \in R^*: \quad (ca, cb) \sim c(a, b)$$

Πράγματι, έστω $d = (a, b)$ και $e = (ca, cb)$. Επειδή $d \mid a$ και $d \mid b$, θα έχουμε $dc \mid ca$ και $dc \mid cb$. Επομένως θα έχουμε $dc \mid (ca, cb) = e$, και άρα $e = dcu$ για κάποιο στοιχείο $u \in R$. Επειδή $e \mid ca$, έπεται ότι $ca = ex$ για κάποιο στοιχείο $x \in R$, και τότε $ca = cdux$. Επειδή σε μια ακέραια περιοχή ισχύει ο Νόμος Διαγραφής και $c \neq 0$, θα έχουμε $a = dux$, δηλαδή $du \mid a$. Ακριβώς παρόμοια θα έχουμε $du \mid b$. Επομένως $du \mid d$ και άρα $d = duz$ για κάποιο $z \in R$. Τότε, επειδή $d \neq 0$, πάλι από τον Νόμο Διαγραφής θα έχουμε $xu = 1$ και άρα το u είναι αντιστρέψιμο. Αυτό σημαίνει ότι τα στοιχεία e και cd είναι συντροφικά, δηλαδή: $(ca, cb) \sim c(a, b)$.

Με χρήση της Αρχής Μαθηματικής Επαγωγής, εύκολα βλέπουμε ότι, αν $a_1, a_2, \cdots, a_n, c \in R$ είναι μη μηδενικά στοιχεία, τότε:

$$(ca_1, ca_2, \cdots, ca_n) \sim c(a_1, a_2, \cdots, a_n) \tag{11.2}$$

Η μέχρι τώρα ιεραρχία ακέραιων περιοχών που έχουμε μελετήσει είναι:

Ευκλείδειες Περιοχές $\subseteq$ Περιοχές Κυρίων Ιδεωδών $\subseteq$ Περιοχές Μονοσήμαντης Ανάλυσης $\subseteq$ Ακέραιες Περιοχές

και κάθε έγκλειση είναι γνήσια:

1. Ο δακτύλιος R του Παραδείγματος 11.4.15 είναι μια ακέραια περιοχή η οποία δεν είναι περιοχή μονοσήμαντης ανάλυσης.

2. Ο δακτύλιος πολυωνυμων $\mathbb{Z}[t]$ είναι περιοχή μονοσήμαντης ανάλυσης η οποία δεν είναι περιοχή κυρίων ιδεωδών, διότι, για παράδειγμα, το ιδεώδες $(2,t)$ του $\mathbb{Z}[t]$ το οποίο παράγεται από το σταθερό πολυώνυμο 2 και το πολυώνυμο t δεν είναι κύριο, βλέπε την Άσκηση 11.5.1.

   Παρόμοια, το ιδεώδες (t_1,t_2) του δακτυλίου πολυωνύμων $\mathbb{K}[t_1,t_2]$, όπου $\mathbb{K}$ είναι σώμα, το οποίο παράγεται από τα πολυώνυμα t_1 και t_2, δεν είναι κύριο, βλέπε την Άσκηση 11.5.2.

3. Ο δακτύλιος $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ είναι περιοχή κυρίων ιδεωδών η οποία δεν είναι Ευκλείδεια περιοχή, βλέπε την Παρατήρηση 11.3.6.

Οι περιοχές μονοσήμαντης ανάλυσης διαδραματίζουν σημαντικό ρόλο στην Αλγεβρική Θεωρία Αριθμών καθώς, όπως αποδεικύεται, η αριθμητική τους έχει πολλά κοινά σημεία με την αριθμητική στον δακτύλιο $\mathbb{Z}$ των ακεραίων. Επίσης οι ακέραιες περιοχές και οι περιοχές μονοσήμαντης ανάλυσης διαδραματίζουν σημαντικό ρόλο στην Αλγεβρική Γεωμετρία, καθώς αυτοί οι δακτύλιοι, ως δακτύλιοι συναρτήσεων, περιγράφουν ιδιότητες γεωμετρικών σχημάτων, όπως το αν ένα γεωμετρικό σχήμα είναι ανάγωγο ή αν μπορεί να οριστεί με μια εξίσωση.

11.4.3 Πολυωνυμικές Επεκτάσεις Περιοχών Μονοσήμαντης Ανάλυσης

Βασικός σκοπός της παρούσας ενότητας είναι να αποδείξουμε ότι πολυωνυμικές επεκτάσεις περιοχών μονοσήμαντης ανάλυσης παραμένουν περιοχές μονοσήμαντης ανάλυσης.

Από τώρα και μέχρι το τέλος της παρούσας ενότητας, R συμβολίζει μια περιοχή μονοσήμαντης ανάλυσης. Χάριν ευκολίας θα γράφουμε $a=b$, αντί «$a\sim b$», όταν $a\sim b$, $a,b\in R$. Αν $a_1,a_2,\cdots,a_n$ είναι μη-μηδενικά στοιχεία μιας ακέραιας περιοχής, τότε θα συμβολίζουμε με $(a_1,a_2,\cdots,a_n)$ έναν μέγιστο κοινό διαιρέτη τους. Συμβατικά θα θέτουμε $(a_1,a_2,\cdots,a_n)=0$, αν όλα τα στοιχεία $a_i=0$.

Έστω $P(t)=a_0+a_1t+\cdots+a_nt^n$ ένα μη μηδενικό πολυώνυμο με στοιχεία από την περιοχή μονοσήμαντης ανάλυσης R.

Ορισμός 11.4.17. *Η* **περιεκτικότητα** *του μη μηδενικού πολυωνύμου $P(t)=\sum_{k=0}^n a_kt^k\in R[t]$ ορίζεται να είναι το στοιχείο*

$$\mathsf{c}(P(t))=(a_0,a_1,a_2,\cdots,a_n)$$

Έστω $P(t)=\sum_{k=0}^n a_kt^k\in R[t]$ ένα μη μηδενικό πολυώνυμο υπεράνω του R με περιεκτικότητα $d=\mathsf{c}(P(t))=(a_0,a_1,a_2,\cdots,a_n)$. Επειδή $d\mid a_k$, έπεται ότι θα έχουμε $a_k=a_k'd$, για κάποια στοιχεία $a_k'\in R$, $0\le k\le n$. Τότε, από τη σχέση (11.2) θα έχουμε $d=(da_0',da_1',\cdots,da_n')=d(a_0',a_1',\cdots,a_n')$, από όπου έπεται ότι $(a_0',a_1',\cdots,a_n')=1$. Θεωρούμε το πολυώνυμο $P_1(t)=\sum_{k=0}^n a_k't^k\in R[t]$ με περιεκτικότητα $\mathsf{c}(P_1(t))=(a_0',a_1',a_2',\cdots,a_n')=1$. Το πολυώνυμο $P_1(t)$ είναι πρωταρχικό με την έννοια του ακόλουθου ορισμού:

Ορισμός 11.4.18. *Ένα πολυώνυμο $P(t)=\sum_{k=0}^n a_kt^k$ καλείται* **πρωταρχικό**, *αν* $\mathsf{c}(P(t))=1$.

Επομένως κάθε πολυώνυμο $P(t)\in R[t]$ γράφεται ως $P(t)=\mathsf{c}(P(t))P_1(t)$, όπου $\mathsf{c}(P(t))\in R$ και το πολυώνυμο $P_1(t)$ είναι πρωταρχικό. Αυτή η γραφή είναι «μοναδική» με την ακόλουθη έννοια: έστω $P(t)=dP_2(t)$, όπου $d\in R$ και το πολυώνυμο $P_2(t)=\sum_{k=0}^m b_kt^k$ είναι πρωταρχικό, τότε $d\sim\mathsf{c}(P(t))$. Πράγματι θα έχουμε $a_0+a_1t+\cdots+a_nt^n=db_0+db_1t+\cdots+db_mt^m$, απ' όπου επειδή ο δακτύλιος είναι ακέραια περιοχή έπεται ότι $n=m$ και $a_k=db_k$, $0\le k\le n$. Επειδή το πολυώνυμο $P_2(t)$ είναι πρωταρχικό, έπεται ότι $\mathsf{c}(P(t))=(a_0,a_1,\cdots,a_n)=(db_0,db_1,\cdots,db_n)=d(b_0,b_1,\cdots,b_n)=d$, δηλαδή τα στοιχεία $\mathsf{c}(P(t))$ και d είναι συντροφικά.

Η επόμενη βοηθητική Πρόταση περιγράφει τι συμβαίνει όταν ξεκινήσουμε με ένα πολυώνυμο με συντελεστές στο σώμα κλασμάτων της ακέραιας περιοχής R.

Λήμμα 11.4.19. *Έστω $Q(R)$ το σώμα κλασμάτων της περιοχής μονοσήμαντης ανάλυσης R, και $P(t) \in Q(R)[t]$ ένα ένα μη μηδενικό πολυώνυμο υπεράνω του σώματος $Q(R)$. Τότε $P(t) = \omega P_1(t)$, όπου $\omega \in Q(R)$ και το πολυώνυμο $P_1(t) \in R[t]$ είναι πρωταρχικό. Αν $P(t) = \rho P_2(t)$, όπου $\rho \in Q(R)$ και το πολυώνυμο $P_2(t) \in R[t]$ είναι πρωταρχικό, τότε: $\omega = u\rho$, όπου $u \in \mathsf{U}(R)$.*

Απόδειξη. Έστω $P(t) = \sum_{k=0}^{n} a_k t^k$, ένα πολυώνυμο βαθμού n, οπότε $a_n \neq 0$, με συντελεστές στο σώμα $Q(R)$. Τότε θα έχουμε $a_i = r_i s_i^{-1}$, όπου $r_i, s_i \in R$, $0 \leq i \leq n$. Θέτοντας $s = s_1 s_2 \cdots s_n$, θα έχουμε $sP(t) = s\sum_{k=0}^{n} r_k s_k^{-1} t^k \in R[t]$ και επομένως, σύμφωνα με την παραπάνω ανάλυση, μπορούμε να γράψουμε $sP(t) = cP_1(t)$, όπου $c \in R$ και το πολυώνυμο $P_1(t) \in R[t]$ είναι πρωταρχικό. Τότε $\omega := cs^{-1} \in Q(R)$ και $P(t) = \omega P_1(t)$.

Υποθέτουμε ότι $P(t) = \rho P_2(t)$, όπου $\rho \in Q(R)$ και το πολυώνυμο $P_2(t) \in R[t]$ είναι πρωταρχικό. Επειδή $\rho \in Q(R)$, μπορούμε να γράψουμε $\rho = fg^{-1}$, όπου $f, g \in R$, και τότε $P(t) = cs^{-1}P_1(t) = fg^{-1}P_2(t)$, δηλαδή $cgP_1(t) = sfP_2(t)$. Επειδή τα πολυώνυμα $P_1(t)$ και $P_2(t)$ είναι πρωταρχικά, όπως παραπάνω εύκολα βλέπουμε ότι τα στοιχεία cg και sf είναι συντροφικά, και άρα υπάρχει αντιστρέψιμο στοιχείο $u \in R$ έτσι ώστε $usf = cg$ και τότε $ufg^{-1} = cs^{-1}$ στο σώμα $Q(R)$, δηλαδή $\omega = u\rho$. ■

Πόρισμα 11.4.20. *Έστω $P(t)$ και $Q(t)$ πρωταρχικά πολυώνυμα υπεράνω του R. Αν τα $P(t)$ και $Q(t)$ είναι συντροφικά ως στοιχεία του $Q(R)[t]$, τότε είναι και συντροφικά ως στοιχεία του $R[t]$.*

Απόδειξη. Έστω ότι τα $P(t)$ και $Q(t)$ είναι συντροφικά ως στοιχεία του $Q(R)[t]$. Τότε $P(t) = \omega Q(t)$ για κάποιο μη-μηδενικό στοιχείο $\omega = ab^{-1} \in Q(R)$, όπου $a, b \in R$. Τότε $P(t) = \omega Q(t)$ και $P(t) = 1P(t)$, και άρα επειδή τα πολυώνυμα $P(t)$ και $Q(t)$ είναι πρωταρχικά, από το Λήμμα 11.4.19 έπεται ότι υπάρχει αντιστρέψιμο στοιχείο $u \in R$ έτσι ώστε $\omega ab^{-1} = u \cdot 1 = u$. Άρα τα $P(t)$ και $Q(t)$ είναι συντροφικά ως στοιχεία του $R[t]$. ■

Το ακόλουθο σημαντικό αποτέλεσμα είναι γνωστό ως Λήμμα του Gauss.

Λήμμα 11.4.21 (Λήμμα του Gauss)**.** *Αν $P(t)$ και $Q(t)$ είναι μη μηδενικά πολυώνυμα υπεράνω του R, τότε*

$$\mathsf{c}\big(P(t)Q(t)\big) = \mathsf{c}(P(t))\,\mathsf{c}(R(t))$$

Ιδιαίτερα το γινόμενο πρωταρχικών πολυωνύμων είναι πρωταρχικό πολυώνυμο.

Απόδειξη. Μπορούμε να γράψουμε $P(t) = cP_1(t)$ και $Q(t) = c'Q_1(t)$, όπου $c := \mathsf{c}(P(t))$, $c' := \mathsf{c}(Q(t))$, και $\mathsf{c}(P_1(t)) = 1 = \mathsf{c}(Q_1(t))$. Τότε $P(t)Q(t) = cc'P_1(t)Q_1(t)$, και αρκεί να δείξουμε ότι $\mathsf{c}(P_1(t)Q_1(t)) = 1$, διότι τότε θα έχουμε $\mathsf{c}(P(t)Q(t)) = \mathsf{c}(cc'P_1(t)Q_1(t)) = cc'\mathsf{c}(P_1(t)Q_1(t)) = cc' = \mathsf{c}(P(t))\mathsf{c}(Q(t))$. Άρα αρκεί να δείξουμε ότι το γινόμενο $P(t)Q(t)$ μη μηδενικών πρωταρχικών πολυωνύμων $P(t)$ και $Q(t)$ είναι πρωταρχικό πολυώνυμο. Υποθέτουμε ότι το πολυώνυμο $H(t) = P(t)Q(t)$ δεν είναι πρωταρχικό. Αυτό σημαίνει ότι η περιεκτικότητα του $H(t)$ δεν είναι αντιστρέψιμο στοιχείο του R, και άρα υπάρχει ανάγωγο, και επομένως πρώτο, στοιχείο $p \in R$ έτσι ώστε $p \mid H(t)$ και προφανώς $p \nmid P(t)$ και $p \nmid Q(t)$ διότι τα πολυώνυμα $P(t), Q(t)$ είναι πρωταρχικά. Από την Παρατήρηση 11.4.7 έπεται ότι το κύριο ιδεώδες (p) είναι πρώτο και άρα ο δακτύλιος πηλίκο $R/(p)$ είναι ακέραια περιοχή. Αυτό έχει ως συνέπεια ότι και ο δακτύλιος πολυωνύμων $R/(p)[t]$ είναι ακέραια περιοχή. Θεωρούμε την απεικόνιση

$$\phi\colon R[t] \longrightarrow R/(p)[t], \quad \phi\Big(\sum_{k=0}^{n} a_k t^k\Big) = \sum_{k=0}^{n} (a_k + (p))t^k)$$

η οποία εύκολα βλέπουμε ότι είναι επιμορφισμός δακτυλίων (η απεικόνιση ϕ είναι η επέκταση του κανονικού επιμορφισμού $\pi\colon R \longrightarrow R/(p)$, $\pi(a) = a + (p)$, όπως εξασφαλίζεται από την Πρόταση 8.2.22). Επειδή $p \nmid P(t)$, $p \nmid Q(t)$ και $p \mid H(t)$, θα έχουμε αντίστοιχα $\phi(P(t)) \neq 0_{R/(p)[t]}0$, $\phi(Q(t)) \neq 0_{R/(p)[t]}0$, και $\phi(H(t)) = 0_{R/(p)[t]}$. Επειδή

$$\phi(P(t))\phi(Q(t)) = \phi(P(t)Q(t)) = \phi\big(H(t)\big) = 0_{R/(p)[t]}$$

και ο δακτύλιος $R/(p)[t]$ είναι ακέραια περιοχή, θα πρέπει είτε $\phi(P(t)) = 0$ είτε $\phi(Q(t)) = 0$ το οποίο είναι άτοπο. Άρα το πολυώνυμο $H(t)$ είναι πρωταρχικό. ■

Λήμμα 11.4.22. *Αν $P(t), Q(t) \in R[t]$ και $P(t) \mid Q(t)$ στον δακτύλιο $Q(R)[t]$, και το πολυώνυμο $P(t)$ είναι πρωταρχικό, τότε $P(t) \mid Q(t)$ στον δακτύλιο $R[t]$.*

Απόδειξη. Επειδή $P(t) \mid Q(t)$ στον δακτύλιο $Q(R)[t]$, υπάρχει πολυώνυμο $A(t) \in Q(R)[t]$ έτσι ώστε $Q(t) = A(t)P(t)$. Προφανώς υπάρχει $d \in R$ έτσι ώστε $dA(t) \in R[t]$ (μπορούμε να θωρήσουμε d να είναι το γινόμενο των παρονομαστών των συντελεστών του $A(t)$). Τότε θα έχουμε $dQ(t) = dA(t)P(t)$ και

$$\mathsf{c}(dQ(t)) = d\mathsf{c}(Q(t)) = \mathsf{c}(dP(t)A(t)) = \mathsf{c}(P(t))\mathsf{c}(dA(t)) = \mathsf{c}(dA(t))$$

και άρα $d \mid \mathsf{c}(dA(t))$, δηλαδή το d διαιρεί στον δακτύλιο R όλους τους συντελεστές του $dA(t)$. Αν $A(t) = \sum_{k=0}^{n} \frac{a_k}{b_k} t^k$, τότε $dA(t) = \sum_{k=0}^{n} d\frac{a_k}{b_k} t^k$, και άρα υπάρχουν στοιχεία $r_i \in R$, έτσι ώστε $d\frac{a_k}{b_k} = dr_k$, $0 \le k \le n$. Τότε $da_k = db_k r_k$, δηλαδή $d(a_k - b_k r_k) = 0$ και επομένως, επειδή ο δακτύλιος R είναι ακέραια περιοχή, θα έχουμε $a_k = b_k r_k$, $0 \le k \le n$. Αυτό σημαίνει ότι οι συντελεστές του $A(t)$ ανήκουν στον δακτύλιο R και άρα $A(t) \in R[t]$, δηλαδή $P(t) \mid Q(t)$ στον δακτύλιο $R[t]$. ■

Πόρισμα 11.4.23. *Κάθε πρώτο στοιχείο του δακτυλίου R είναι πρώτο θεωρούμενο ως στοιχείο του δακτυλίου πολυωνύμων $R[t]$.*

Απόδειξη. Έστω $p \in R$ ένα πρώτο στοιχείο, και υποθέτουμε ότι $p \mid P(t)Q(t)$, όπου $P(t), Q(t)$ είναι μη-μηδενικά στοιχεία του $R[t]$. Προφανώς τότε το στοιχείο p διαιρεί κάθε συντελεστή του πολυωνύμου $P(t)Q(t)$ και άρα $p \mid \mathsf{c}(P(t)Q(t))$. Από το Λήμμα του Gauss 11.4.21, έπεται ότι $p \mid \mathsf{c}(P(t))\mathsf{c}(Q(t))$, και επειδή το στοιχείο p είναι πρώτο στον δακτύλιο R, έπεται ότι είτε $p \mid \mathsf{c}(P(t))$ είτε $p \mid \mathsf{c}(Q(t))$. Δηλαδή είτε το p διαιρεί κάθε συντελεστή του $P(t)$ είτε το p διαιρεί κάθε συντελεστή του $Q(t)$. Αυτό προφανώς σημαίνει ότι είτε $p \mid P(t)$ είτε $p \mid Q(t)$, και επομένως το p είναι πρώτο θεωρούμενο ως στοιχείο του $R[t]$. ■

Λήμμα 11.4.24. *Για ένα πολυώνυμο $P(t) \in R[t]$ βαθμού ≥ 1, τα ακόλουθα είναι ισοδύναμα:*

1. *Το $P(t)$ είναι πρώτο στοιχείο του $R[t]$.*
2. *Το $P(t)$ είναι ανάγωγο στοιχείο του $R[t]$.*
3. *Το $P(t)$ είναι ανάγωγο πρωταρχικό στοιχείο του $Q(R)[t]$.*

Απόδειξη. «1. $\implies$ 2.» Από την Πρόταση 11.4.5 γνωρίζουμε ότι σε μια ακέραια περιοχή κάθε πρώτο στοιχείο είναι ανάγωγο.

«2. $\implies$ 3.» Αν το $P(t)$ είναι ανάγωγο στοιχείο του $R[t]$ και δεν είναι πρωταρχικό, τότε η περιεκτικότητα του $c := \mathsf{c}(P(t))$ δεν είναι αντιστρέψιμο στοιχείο. Έτσι μπορούμε να γράψουμε $P(t) = cP_1(t)$ και αναγκαστικά $\deg P(t) = \deg P_1(t)$. Επειδή $\deg P(t) \ge 1$, αυτό σημαίνει ότι το $P(t)$ δεν είναι ανάγωγο, καθώς τα c και $P_1(t)$ δεν είναι αντιστρέψιμα. Άρα το c είναι αντιστρέψιμο και χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $c = 1$. Υποθέτουμε ότι το $P(t)$ δεν είναι ανάγωγο θεωρούμενο ως πολυώνυμο του $Q(R)[t]$, και τότε μπορούμε να γράψουμε $P(t) = Q(t)R(t)$, όπου $Q(t)$ και $R(t)$ είναι πολυώνυμα βαθμού ≥ 1 υπεράνω του $Q(R)$. Όπως και στην απόδειξη του Λήμματος 11.4.19, θα έχουμε ότι $aQ(t) \in R[t]$ και $bR(t) \in R[t]$, όπου a και b είναι τα γινόμενα των παρονομαστών των συντελεστών των πολυωνύμων $Q(t)$ και $R(t)$ αντίστοιχα. Τότε $abP(t) = abQ(t)R(t)$ και $\mathsf{c}(abP(t)) = ab\mathsf{c}(P(t)) = \mathsf{c}(aQ(t)bR(t)) = \mathsf{c}(aP(t))\mathsf{c}(bR(t))$, και μπορούμε να γράψουμε $aQ(t) = \mathsf{c}(aQ(t))Q_1(t)$ και $bR(t) = \mathsf{c}(bR(t))R_1(t)$ και τα πολυώνυμα $Q_1(t) \in R[t]$ και $R_1(t) \in R[t]$ είναι πρωταρχικά και βαθμού ≥ 1. Τότε όμως θα έχουμε $P(t) = Q_1(t)R_1(t)$ και αυτό είναι άτοπο διότι το $P(t)$ είναι ανάγωγο υπεράνω του $R[t]$.

«3. $\implies$ 1.» Υποθέτουμε ότι το $P(t)$ είναι ανάγωγο πρωταρχικό στοιχείο του $Q(R)[t]$, και έστω $Q(t), R(t) \in R[t]$ έτσι ώστε $P(t) \mid Q(t)R(t)$. Τότε προφανώς $P(t) \mid Q(t)R(t)$ στην ακέραια περιοχή $Q(R)[t]$. Επειδή ο δακτύλιος $Q(R)$ είναι σώμα, έπεται ότι η ακέραια περιοχή $Q(R)[t]$ είναι περιοχή κυρίων ιδεωδών, και άρα το ανάγωγο στοιχείο $P(t)$ είναι πρώτο και επομένως $P(t) \mid Q(t)$ ή $P(t) \mid R(t)$ στον δακτύλιο $Q(R)[t]$. ■

Μπορούμε τώρα να αποδείξουμε το ακόλουθο σημαντικό Θεώρημα το οποίο πιστοποιεί ότι δακτύλιοι πολυωνύμων υπεράνω περιοχών μονοσήμαντης ανάλυσης είναι περιοχές μονοσήμαντης ανάλυσης.

Θεώρημα 11.4.25. *Αν ο δακτύλιος R είναι περιοχή μονοσήμαντης ανάλυσης, τότε ο δακτύλιος πολυωνύμων $R[t]$ είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. Από τα Λήμματα 11.4.23 και 11.4.24, έπεται ότι κάθε ανάγωγο στοιχείο του $R[t]$ είναι πρώτο. Επομένως, σύμφωνα με το Θεώρημα 11.4.12, για να δείξουμε ότι ο δακτύλιος $R[t]$ είναι περιοχή μονοσήμαντης ανάλυσης, αρκεί να δείξουμε ότι κάθε μη μηδενικό στοιχείο του $R[t]$ το οποίο δεν είναι αντιστρέψιμο, μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους ανάγωγων, ή ισοδύναμα πρώτων, στοιχείων.

Υποθέτουμε ότι αυτό δεν ισχύει, δηλαδή υπάρχουν μη μηδενικά μη αντιστρέψιμα στοιχεία του $R[t]$ τα οποία δεν μπορούν να γραφούν ως γινόμενο πεπερασμένου πλήθους ανάγωγων, ή ισοδύναμα πρώτων, στοιχείων. Από όλα αυτά τα πολυώνυμα, έστω $P(t)$ εκείνο το πολυώνυμο με τον μικρότερο δυνατό βαθμό. Προφανώς το $P(t)$ δεν είναι σταθερό πολυώνυμο, διότι διαφορετικά το $P(t)$ θα ανήκε στον δακτύλιο R ο οποίος είναι περιοχή μονοσήμαντης ανάλυσης και άρα κάθε στοιχείο του είναι γινόμενο πεπερασμένου πλήθους ανάγωγων, ή ισοδύναμα πρώτων, στοιχείων. Επομένως $\deg P(t) \geq 1$ και όπως παραπάνω μπορούμε να γράψουμε $P(t) = cP_1(t)$, όπου $c = \mathsf{c}(P(t))$ είναι η περιεκτικότητα του $P(t)$, και $\mathsf{c}(P_1(t)) = 1$. Επειδή ο δακτύλιος R είναι περιοχή μονοσήμαντης ανάλυσης, έπεται ότι το στοιχείο c είναι είτε αντιστρέψιμο είτε γινόμενο πεπερασμένου πλήθους ανάγωγων στοιχείων, τα οποία είναι ανάγωγα και στον δακτύλιο $R[t]$. Έτσι το $P_1(t)$ δεν μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους ανάγωγων, ή ισοδύναμα πρώτων, στοιχείων του $R[t]$, καθώς διαφορετικά το $P(t)$ θα είχε αυτή την ιδιότητα, και αυτό είναι άτοπο από την επιλογή του. Ιδιαίτερα το $P_1(t)$ δεν είναι ανάγωγο και άρα μπορεί να γραφεί ως γινόμενο $P_1(t) = A(t)B(t)$, όπου τα πολυώνυμα $A(t), B(t)$ δεν είναι αντιστρέψιμα. Όμως, από το Λήμμα του Gauss 11.4.21, θα έχουμε $1 = \mathsf{c}(P_1(t)) = \mathsf{c}(A(t)B(t)) = \mathsf{c}(A(t))\mathsf{c}(B(t))$ και άρα οι περιεκτικότητες των $A(t)$ και $B(t)$ είναι αντιστρέψιμα στοιχεία του R. Αυτό σημαίνει ότι τα πολυώνυμα $A(t)$ και $B(t)$ είναι βαθμού ≥ 1, καθώς διαφορετικά, ένα εξ αυτών θα ήταν αντιστρέψιμο στον δακτύλιο $R[t]$ και αυτό είναι άτοπο από την κατασκευή τους. Επειδή $\deg A(t) \leq \deg P_1(t) = \deg P(t)$ και $\deg B(t) \leq \deg P_1(t) = \deg P(t)$, από την επιλογή του $P(t)$, τα πολυώνυμα $A(t)$ και $B(t)$ μπορούν να γραφούν ως πεπερασμένα γινόμενα πεπερασμένου πλήθους ανάγωγων στοιχείων. Αυτό όμως είναι άτοπο από την επιλογή του $P(t)$. Επομένως το πολυώνυμο $P(t)$ μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους ανάγωγων, ή ισοδύναμα πρώτων, στοιχείων του $R[t]$ και άρα ο δακτύλιος $R[t]$ είναι περιοχή μονοσήμαντης ανάλυσης. ■

Τα επόμενα πορίσματα είναι άμεσες συνέπειες του Θεωρήματος 11.4.25.

Πόρισμα 11.4.26. *Αν ο δακτύλιος R είναι περιοχή μονοσήμαντης ανάλυσης, τότε ο δακτύλιος πολυωνύμων $R[t_1, t_2, \cdots, t_n]$, $\forall n \geq 1$, είναι περιοχή μονοσήμαντης ανάλυσης.*

Πόρισμα 11.4.27.

1. *Ο δακτύλιος $\mathbb{Z}[t_1, t_2, \cdots, t_n]$, $\forall n \geq 1$, είναι περιοχή μονοσήμαντης ανάλυσης.*
2. *Αν $\mathbb{K}$ είναι ένα σώμα, τότε ο δακτύλιος $\mathbb{K}[t_1, t_2, \cdots, t_n]$, $\forall n \geq 1$, είναι περιοχή μονοσήμαντης ανάλυσης.*

Παρατήρηση 11.4.28. Αν και δακτύλιοι πολυωνύμων υπεράνω περιοχών μονοσήμαντης ανάλυσης είναι περιοχές μονοσήμαντης ανάλυσης, δεν συμβαίνει το ίδιο για δακτυλίους τυπικών δυναμοσειρών. Πράγματι υπάρχει παράδειγμα[7] περιοχής μονοσήματης ανάλυσης R, η οποία επιπλέον είναι τοπικός δακτύλιος, αλλά η ακέραια περιοχή $R[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του R δεν είναι περιοχή μονοσήμαντης ανάλυσης. Ο δακτύλιος R του παραδείγματος δεν μπορεί να είναι σώμα, διότι, σύμφωνα με την Πρόταση 11.1.5, για κάθε σώμα $\mathbb{K}$, ο δακτύλιος $\mathbb{K}[\![t]\!]$ των τυπικών δυναμοσειρών είναι περιοχή κυρίων ιδεωδών και άρα περιοχή μονοσήμαντης ανάλυσης. ▲

Κλείνουμε την παρούσα ενότητα με την ακόλουθη εφαρμογή της εκτεθείσας θεωρίας στη στοιχειώδη Θεωρία Αριθμών.

[7] Βλέπε P. Samuel: "*On unique factorization domains*", Ill. J. Math. **5** (1961), 1–17.

Θεώρημα 11.4.29. *Έστω p ένας περιττός πρώτος αριθμός. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Ο p είναι άθροισμα δύο τετραγώνων.*
2. *Ο p είναι της μορφής $4n+1$, $n \geq 1$.*

Απόδειξη. «1. $\Longrightarrow$ 2.» Υποθέτουμε ότι ο πρώτος p είναι άθροισμα δύο τετραγώνων: $p = a^2+b^2$, $a, b \in \mathbb{Z}$. Αν $a = 2k$, τότε $a^2 = 4k^2$ και αν $a = 2k+1$, τότε $a^2 = 4k^2+4k+1 = 4(k^2+k)+1$. Παρόμοια, αν $b = 2l$, τότε $b^2 = 4l^2$, και αν $b = 2l+1$, τότε $b^2 = 4l^2+4l+1 = 4(l^2+l)+1$. Άρα, αν $a = 2k$ και $b = 2l$, τότε $p = a^2+b^2 = 4(k^2+l^2)$, το οποίο είναι άτοπο διότι ο p είναι πρώτος. Αν $a = 2k+1$ και $b = 2l+1$, τότε $p = a^2+b^2 = 4(k^2+k)+1+4(l^2+l)+1 = 4(k^2+k+l^2+l)+2$, το οποίο είναι άτοπο διότι ο p είναι πρώτος. Αν $a = 2k+1$ και $b = 2l$, τότε $p = a^2+b^2 = 4(k^2+k)+1+4l^2 = 4(k^2+k+l^2)+1$, και παρόμοια, αν $a = 2k$ και $b = 2l+1$, τότε $p = a^2+b^2 = 4(k^2+l^2+l)+1$. Άρα, αν ο p είναι άθροισμα δυο τετραγώνων, τότε ο p είναι της μορφής $4n+1$.

«2. $\Longrightarrow$ 1.» Υποθέτουμε ότι ο πρώτος p είναι της μορφής $4n+1$, όπου $n \geq 1$. Τότε $(p-1)! = (2n)! \cdot (2n+1)(2n+2)\cdots 4n = (2n)! \cdot (p-2n)\cdots(p-1)$. Θεωρώντας αυτή τη σχέση mod p, θα έχουμε:

$$(p-1)! \equiv 1\cdot 2\cdots(2n)! \cdot (-2n)\cdots(-1) \,(\mathrm{mod}\ p) \equiv (1\cdot 2\cdots 2n)^2(-1)^{2n} \,(\mathrm{mod}\ p) = (2n)!(-1)^n \,(\mathrm{mod}\ p)$$

Θέτοντας $x = (2n)!(-1)^n$, χρησιμοποιώντας ότι από το Θεώρημα του Wilson, βλέπε το Θεώρημα 3.8.3, έχουμε $(p-1)! \equiv -1 (\mathrm{mod}\ p)$, έπεται ότι: $x^2 \equiv -1 \,(\mathrm{mod}\ p)$, και επομένως $p \mid x^2+1$. Τότε εργαζόμενοι στην περιοχή μονοσήμαντης ανάλυσης $\mathbb{Z}[i]$, θα έχουμε $p \mid (x+i)(x-i)$. Αν $p \mid x+i$, τότε θα έχουμε $p(a+bi) = x+i$, για κάποιο $a+bi \in \mathbb{Z}[i]$, δηλαδή $pa+pbi = x+i$, από όπου $pb = 1$ και αυτό είναι άτοπο διότι $p > 2$. Παρόμοια, αν $p \mid x-i$, τότε θα έχουμε $p(c+di) = x-i$, για κάποιο $c+di \in \mathbb{Z}[i]$, δηλαδή $pc+pdi = x-i$, από όπου $pd = -1$ και αυτό είναι άτοπο διότι $p > 2$. Άρα το στοιχείο p δεν είναι πρώτο και επομένως δεν είναι ανάγωγο. Αυτό σημαίνει ότι υπάρχουν μη-αντιστρέψιμα στοιχεία $a+bi, c+di \in \mathbb{Z}$ έτσι ώστε $p = (a+bi)(c+di)$ και τότε χρησιμοποιώντας την Ευκλείδεια στάθμη $\delta\colon \mathbb{Z}[i] \longrightarrow \mathbb{N}_0$, $\delta(a+bi) = a^2+b^2$, έπεται ότι

$$\delta(p) = p^2 = \delta\big((a+bi)(c+di)\big) = \delta(a+bi)\delta(c+di) = (a^2+b^2)(c^2+d^2)$$

Άρα $p \cdot p = (a^2+b^2)(c^2+d^2)$, από όπου θα έχουμε ότι $p = a^2+b^2 = c^2+d^2$. ■

11.5 Ασκήσεις

Άσκηση 11.5.1. *Να δειχθεί ότι το ιδεώδες $(2, t)$ του δακτυλίου πολυωνύμων $\mathbb{Z}[t]$ το οποίο παράγεται από το σταθερό πολυώνυμο 2 και το πολυώνυμο t δεν είναι κύριο.*

Άσκηση 11.5.2. *Να δειχθεί ότι το ιδεώδες (t_1, t_2) του δακτυλίου πολυωνύμων $\mathbb{K}[t_1, t_2]$, όπου $\mathbb{K}$ είναι ένα σώμα, το οποίο παράγεται από τα πολυώνυμα t_1 και t_2, δεν είναι κύριο.*

Άσκηση 11.5.3. *Έστω ότι R είναι μια ακέραια περιοχή και υποθέτουμε ότι κάθε ζεύγος μη μηδενικών στοιχείων της R αποτελείται από συντροφικά στοιχεία. Να δειχθεί ότι η ακέραια περιοχή R είναι σώμα.*

Άσκηση 11.5.4. *Έστω p είναι ένας πρώτος αριθμός και θεωρούμε τον υποδακτύλιο*

$$\mathbb{Q}_p = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; p \nmid b \right\}$$

του $\mathbb{Q}$. Να δειχθεί ότι ο δακτύλιος είναι τοπικός και περιοχή κυρίων ιδεωδών, και $\mathbb{Q}_p/\mathfrak{m} \cong \mathbb{Z}_p$, όπου $\mathfrak{m}$ είναι το μοναδικό μεγιστοτικό ιδεώδες του $\mathbb{Q}_p$.

Άσκηση 11.5.5. *Έστω p ένας πρώτος ακέραιος αριθμός. Θεωρούμε το σύνολο*

$$\mathbb{Z}_p(i) = \left\{ [a]_p + [b]_p i \mid [a]_p, [b]_p \in \mathbb{Z}_p \right\}$$

στο οποίο ορίζουμε πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·» ως εξής:

$$\left([a]_p + [b]_p i\right) + \left([c]_p + [d]_p i\right) = \left([a]_p + [c]_p\right) + \left([b]_p + [d]_p\right) i$$

$$([a]_p + [b]_p i) \cdot ([c]_p + [d]_p i) = \left([a]_p [c]_p - [b]_p [d]_p\right) + \left([a]_p [d]_p + [b]_p [c]_p\right) i$$

1. *Να δειχθεί ότι το σύνολο $\mathbb{Z}_p(i)$ είναι ένας μεταθετικός δακτύλιος με μονάδα.*
2. *Να δειχθεί ότι το σύνολο $R := \mathbb{Z}_p \times \mathbb{Z}_p$ το οποίο είναι εφοδιασμένο με τις ακόλουθες πράξεις πρόσθεσης «+» και πολλαπλασιασμού «·»*

$$\left([a]_p, [b]_p\right) + \left([c]_p, [d]_p\right) = \left([a]_p + [c]_p,\, [b]_p + [d]_p\right)$$

$$([a]_p, [b]_p) \cdot ([c]_p, [d]_p) = \left([a]_p [c]_p - [b]_p [d]_p,\, [a]_p [d]_p + [b]_p [c]_p\right)$$

   είναι ένας δακτύλιος ισόμορφος με τον δακτύλιο $\mathbb{Z}_p(i)$, μέσω ενός ισομορφισμού ο οποίος στέλνει το στοιχείο $([0]_p, [1]_p) \in \mathbb{Z}_p \times \mathbb{Z}_p$ στο στοιχείο $i \in \mathbb{Z}_p(i)$.
3. *Να εξεταστεί αν ο δακτύλιος $\mathbb{Z}_p(i)$ είναι ακέραια περιοχή η σώμα.*

Άσκηση 11.5.6. *Αν p είναι ένας πρώτος αριθμός, να δειχθεί ότι υπάρχουν ισομορφισμοί δακτυλίων:*

$$\mathbb{Z}_p(i) \;\cong\; \mathbb{Z}[i]/(p) \;\cong\; \mathbb{Z}_p[t]/(t^2+1)$$

Άσκηση 11.5.7. *Αν p είναι ένας πρώτος αριθμός, να δειχθεί ότι τα ακόλουθα είναι ισοδύναμα:*

1. *Ο πρώτος αριθμός p είναι πρώτο στοιχείο του δακτυλίου $\mathbb{Z}[i]$.*
2. *Το κύριο ιδεώδες $(p) \subseteq \mathbb{Z}[i]$ είναι μεγιστοτικό ιδεώδες του $\mathbb{Z}[i]$.*
3. *Ο δακτύλιος $\mathbb{Z}_p(i)$ είναι σώμα.*

Άσκηση 11.5.8 (Ο Ευκλείδειος Αλγόριθμος)**.** *Έστω (R, δ) μια Ευκλείδεια περιοχή, και a_1, a_2 δύο μη μηδενικά στοιχεία του R. Ορίζουμε στοιχεία a_k, $\forall\, k \geq 3$, ως εξής:*

$$\begin{aligned}
a_1 &= a_2 q_2 + a_3, \qquad 0 \leq \delta(a_3) < \delta(a_2) \\
a_2 &= a_3 q_3 + a_4, \qquad 0 \leq \delta(a_4) < \delta(a_3) \\
&\vdots \\
a_k &= a_{k+1} q_{k+1} + a_{k+2}, \qquad 0 \leq \delta(a_{k+2}) < \delta(a_{k+1}) \\
&\vdots
\end{aligned}$$

1. *Να δειχθεί ότι υπάρχει $n \geq 2$ έτσι ώστε $a_n \neq 0$ και $a_{n+1} = 0$, και τότε*

$$a_n = (a_1, a_2)$$

2. *Να χρησιμοποιηθούν οι παραπάνω σχέσεις για να γραφεί ο μέγιστος κοινός διαιρέτης (a_1, a_2) στη μορφή $(a_1, a_2) = x_1 a_1 + x_2 a_2$, όπου $x_1, x_2 \in R$.*

Άσκηση 11.5.9. *Να βρεθεί ο μέγιστος κοινός διαιρέτης $(11 + 7i, 18 - i)$ των στοιχείων $11 + 7i$, $18 - i \in \mathbb{Z}[i]$.*

Άσκηση 11.5.10. *Να βρεθεί ο μέγιστος κοινός διαιρέτης των πολυωνύμων*

$$P(t) = t^3 + t^2 + t - 3 \quad \text{και} \quad Q(t) = t^4 - t^3 + 3t^2 + t - 4$$

στην Ευκλείδεια περιοχή $\mathbb{Q}[t]$.

Άσκηση 11.5.11. *Έστω ότι* R *είναι μια περιοχή κυρίων ιδεωδών, και* $0 \neq a \in R$. *Να δειχθεί ότι αν, το στοιχείο* a *είναι πρώτο, τότε ο δακτύλιος πηλίκο* $R/(a)$ *είναι σώμα, και, αν το στοιχείο* a *δεν είναι πρώτο, τότε ο δακτύλιος πηλίκο* $R/(a)$ *δεν είναι ούτε ακέραια περιοχή.*

Άσκηση 11.5.12. *Να δειχθεί ότι οι ακόλουθοι δακτύλιοι είναι Ευκλείδειες περιοχές, όπου* $\zeta = e^{\frac{2\pi i}{3}}$ *:*

$$\mathbb{Z}[\zeta] \quad \text{και} \quad \mathbb{Z}[\sqrt{-2}]$$

Άσκηση 11.5.13. *Να γραφεί το πολυώνυμο* $P(t) = 4t^2 - 4t + 8$ *ως γινόμενο ανάγωγων στοιχείων στις ακέραιες περιοχές:*

$$\mathbb{Z}[t], \quad \mathbb{Q}[t], \quad \mathbb{Z}_{11}[t]$$

Άσκηση 11.5.14. *Να δειχθεί ότι ο μέγιστος κοινός διαιρέτης* (m, n) *δύο ακεραίων* m, n *στο* $\mathbb{Z}$ *συμπίπτει με τον μέγιστο κοινό διαιρέτη των* m, n *στο* $\mathbb{Z}[i]$.

Άσκηση 11.5.15. *Να δειχθεί ότι οι ακέραιες περιοχές* $\mathbb{Z}[\sqrt{2}]$ *και* $\mathbb{Z}[\sqrt{3}]$ *είναι Ευκλείδειες περιοχές.*
Υπόδειξη: Θεωρήστε την απεικόνιση $\delta(x + y\sqrt{d}) = |x^2 - dy^2|$, *όπου* $d = 2, 3$.

Άσκηση 11.5.16. *Έστω* I *ένα μη μηδενικό ιδεώδες του δακτυλίου* $\mathbb{Z}[i]$. *Να δειχθεί ότι ο δακτύλιος πηλίκο* $\mathbb{Z}[i]/I$ *έχει πεπερασμένο πλήθος στοιχείων. Πόσα στοιχεία έχουν οι δακτύλιοι*

$$\mathbb{Z}[i]/(3), \quad \mathbb{Z}[i]/(1+i), \quad \mathbb{Z}[i]/(1+2i);$$

Ποιοι από τους παραπάνω δακτύλιους είναι σώματα;

Άσκηση 11.5.17. *Να δειχθεί ότι στην ακέραια περιοχή* $\mathbb{Z}[\sqrt{-3}]$ *το στοιχείο* 2 *είναι ανάγωγο αλλά όχι πρώτο. Να συμπεράνετε ότι ο δακτύλιος* $\mathbb{Z}[\sqrt{-3}]$ *δεν είναι περιοχή μονοσήμαντης ανάλυσης.*

Άσκηση 11.5.18. *Να δειχθεί ότι ο δακτύλιος* $\mathbb{Z}[\sqrt{d}]$, *όπου* $d < 1$ *είναι ένας περιττός ακέραιος, δεν είναι περιοχή μονοσήμαντης ανάλυσης.*
Υπόδειξη: Δείξτε ότι το 2 *είναι ανάγωγο αλλά όχι πρώτο στοιχείο του* $\mathbb{Z}[\sqrt{d}]$.

Άσκηση 11.5.19. *Να δειχθεί ότι ο πυρήνας του μοναδικού ομομορφισμού δακτυλίων*

$$f : \mathbb{Z}[t] \longrightarrow \mathbb{R}, \quad \text{έτσι ώστε} \quad t \longmapsto 1 + \sqrt{2}$$

είναι ένα κύριο ιδεώδες.

Άσκηση 11.5.20. *Να δειχθεί ότι σε μια ακέραια περιοχή* R, *τα ακόλουθα είναι ισοδύναμα:*

1. *Ικανοποιείται η συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη.*
2. *Δεν υπάρχει άπειρη ακολουθία μη μηδενικών στοιχείων* $a_1, a_2, \cdots$, *του* R *έτσι ώστε το στοιχείο* a_{n+1} *να είναι γνήσιος διαιρέτης του* a_n, $\forall n \geq 1$.

Άσκηση 11.5.21. *Έστω ότι R είναι μια ακέραια περιοχή έτσι ώστε κάθε μη-μηδενικό στοιχείο της είναι είτε ανάγωγο είτε αντιστρέψιμο. Να δειχθεί ότι η ακέραια περιοχή R είναι σώμα.*

Άσκηση 11.5.22. *Να γραφεί ο αριθμός 30 ως γινόμενο πρώτων στοιχείων στον δακτύλιο $\mathbb{Z}[i]$.*

Άσκηση 11.5.23. *Να δειχθεί ότι τα μεγιστοτικά ιδεώδη του δακτυλίου πολυωνύμων $\mathbb{Z}[t]$ είναι της μορφής*

$$(p)+(A(t)) = \{pP(t)+Q(t)A(t) \in \mathbb{Z}[t] \mid p : \text{πρώτος ακέραιος, } A(t) : \text{μονικό πολυώνυμο, ανάγωγο στο σώμα } \mathbb{Z}_p\}$$

όπου ένα πολυώνυμο $P(t) = \sum_{k=0}^{n} a_k t^k \in \mathbb{Z}[t]$ καλείται ανάγωγο στο σώμα $\mathbb{Z}_p$ αν το πολυώνυμο $\widetilde{P}(t) = \sum_{k=0}^{n} [a_k]_p t^k \in \mathbb{Z}_p[t]$ είναι ανάγωγο στο σώμα $\mathbb{Z}_p$.

Οι επόμενες πέντε ασκήσεις αποτελούν τα βήματα για την απόδειξη του ακόλουθου χαρακτηρισμού περιοχών μονοσήμαντης ανάλυσης:

- *Μια ακέραια περιοχή R είναι περιοχή μονοσήμαντης ανάλυσης αν και μόνο αν: (α) ο R ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη, και (β) κάθε δύο στοιχεία του R^* έχουν μέγιστο κοινό διαιρέτη.*

Πρώτα υπενθυμίζουμε ότι στο σύνολο των μη μηδενικών στοιχείων μιας ακέραιας περιοχής R έχουμε ορίσει τη σχέση συντροφικότητας «$\sim$»: $a \sim b$ αν και μόνο αν τα στοιχεία είναι συντροφικά, δηλαδή υπάρχει αντιστρέψιμο στοιχείο u έτσι ώστε $a = ub$. Στις επόμενες πέντε ασκήσεις R συμβολίζει μια ακέραια περιοχή στην οποία κάθε δύο μη μηδενικά στοιχεία του R έχουν μέγιστο κοινό διαιρέτη. Αν $a_1, a_2, \cdots, a_n \in R^*$, τότε, χάριν ευκολίας, συμβολίζουμε με $(a_1, a_2, \cdots, a_n)$ έναν μέγιστο κοινό διαιρέτη των στοιχείων $a_1, a_2, \cdots, a_n$.

Οι ιδιότητες οι οποίες περιγράφονται στις επόμενες ασκήσεις είναι οικείες από τη θεωρία διαιρετότητας στην στοιχειώδη Θεωρία Αριθμών.

Άσκηση 11.5.24. *Κάθε πεπερασμένο πλήθος μη μηδενικών στοιχείων του R έχει έναν μέγιστο κοινό διαιρέτη.*

Άσκηση 11.5.25. $\forall a, b, c \in R^*$: $((a,b),c) \sim (a,(b,c))$.

Άσκηση 11.5.26. $\forall a, b, c \in R^*$: $c(a,b) \sim (ca, cb)$.

Άσκηση 11.5.27. $\forall a, b, c \in R^*$: $(a,b) \sim 1$ και $(a,c) \sim 1 \implies (a,bc) \sim 1$.

Άσκηση 11.5.28. *Κάθε ανάγωγο στοιχείο της ακέραιας περιοχής R είναι πρώτο.*

Άσκηση 11.5.29. *Για μια ακέραια περιοχή R τα ακόλουθα είναι ισοδύναμα:*

1. *Η ακέραια περιοχή R είναι περιοχή μονοσήμαντης ανάλυσης.*
2. *(α') Η ακέραια περιοχή R ικανοποιεί τη συνθήκη αύξουσας αλυσίδας για κύρια ιδεώδη.*
   (β') Κάθε δύο μη μηδενικά στοιχεία της ακέραιας περιοχής R έχουν μέγιστο κοινό διαιρέτη.

Άσκηση 11.5.30. *Να δειχθεί ότι ο δακτύλιος $\mathbb{R}[\![t]\!]$ των τυπικών δυναμοσειρών υπεράνω του $\mathbb{R}$ είναι περιοχή μονοσήμαντης ανάλυσης.*

Άσκηση 11.5.31. *Να δειχθεί ότι ο δακτύλιος $\mathbb{Z}_{p^n}$, όπου p είναι ένας πρώτος αριθμός, είναι δακτύλιος μονοσήμαντης ανάλυσης ο οποίος δεν είναι ακέραια περιοχή.*

Άσκηση 11.5.32. *Έστω ότι R είναι ένας δακτύλιος ο οποίος περιέχει τον δακτύλιο $\mathbb{Z}$ των ακεραίων ως υποδακτύλιο, και έστω $n, m \in \mathbb{N}$. Αν $n, m \in I$, όπου I είναι ένα γνήσιο ιδεώδες του R, τότε οι n, m έχουν έναν ακέραιο κοινό παράγοντα ≥ 2.*

Άσκηση 11.5.33. *Να δειχθεί ότι, αν R είναι μια ακέραια περιοχή η οποία δεν είναι σώμα, τότε ο δακτύλιος πολυωνύμων $R[t]$ δεν είναι περιοχή κυρίων ιδεωδών.*

Άσκηση 11.5.34. *Να δειχθεί ότι υπάρχει άπειρο πλήθος ανάγωγων (= πρώτων) στοιχείων στην Ευκλείδεια περιοχή $\mathbb{Z}[i]$.*

Άσκηση 11.5.35. *Έστω R μια περιοχή μονοσήμαντης ανάλυσης η οποία περιέχει πεπερασμένο πλήθος αντιστρέψιμων στοιχών, π.χ. $R = \mathbb{Z}$ ή $R = \mathbb{Z}[i]$ ή $R = \mathbb{F}[t]$, όπου $\mathbb{F}$ είναι ένα πεπερασμένο σώμα.*

Να δειχθεί ότι η περιοχή R περιέχει άπειρο πλήθος ανάγωγων (= πρώτων) στοιχείων.

Υπόδειξη: Υπενθυμίζουμε ότι, σύμφωνα με το Θεώρημα του Ευκλείδη, το πλήθος των πρώτων θετικών ακέραιων αριθμών είναι άπειρο. Προσπαθήστε να ακολουθήσετε την απόδειξη του Ευκλείδη.

Παράρτημα Α΄

Μεγιστοτικά Ιδεώδη σε Δακτύλιους Συνεχών Συναρτήσεων

Στό παρόν Παράρτημα θα μελετήσουμε μεγιστοτικά ιδεώδη δακτυλίων συνεχών συναρτήσεων επί ενός κλειστού διαστήματος της πραγματικής ευθείας.

Υπενθυμίζουμε ότι το σύνολο

$$\mathscr{C}([0,1],\mathbb{R}) = \{f\colon [0,1] \longrightarrow \mathbb{R} \mid f\colon \text{συνεχής}\}$$

εφοδιασμένο με τις πράξεις

$$\forall f,g \in \mathscr{C}([0,1],\mathbb{R})\colon \quad (f+g)(x) = f(x)+g(x)$$

$$\forall f,g \in \mathscr{C}([0,1],\mathbb{R})\colon \quad (f\cdot g)(x) = f(x)g(x)$$

είναι ένας μεταθετικός δακτύλιος με μονάδα την σταθερή συνάρτηση $1\colon [0,1] \longrightarrow \mathbb{R}$, $1(x) = 1$.

Αυτό προκύπτει από το γεγονός ότι το άθροισμα και το γινόμενο συνεχών συναρτήσεων $[0,1] \longrightarrow \mathbb{R}$ είναι συνεχής συνάρτηση, και επομένως το σύνολο $\mathscr{C}([0,1],\mathbb{R})$ είναι ένας υποδακτύλιος του δακτυλίου $\mathscr{F}([0,1],\mathbb{R})$ όλων των συναρτήσεων από το διάστημα $[0,1]$ στο $\mathbb{R}$. Γενικά ο δακτύλιος $\mathscr{C}([0,1])$ περιέχει διαιρέτες του μηδενός και επομένως ο δακτύλιος $\mathscr{C}([0,1])$ δεν είναι ούτε σώμα ούτε ακέραια περιοχή.

Θα προσδιορίσουμε τα μεγιστοτικά ιδεώδη του δακτυλίου

$$\mathscr{C}([0,1],\mathbb{R}) = \{f\colon [0,1] \longrightarrow \mathbb{R} \mid f\colon \text{συνεχής}\}$$

Θέτουμε $R := \mathscr{C}([0,1],\mathbb{R})$, και τότε για κάθε πραγματικό αριθμό $r \in [0,1]$, θεωρούμε την σταθερή συνάρτηση

$$\mathsf{r}\colon [0,1] \longrightarrow \mathbb{R}, \quad \mathsf{r}(x) = r$$

Προφανώς η r είναι συνεχής και άρα $\mathsf{r} \in R$, $\forall r \in [0,1]$. Θεωρούμε την απεικόνιση

$$\Phi_r\colon R \longrightarrow \mathbb{R}, \quad \Phi_r(f) = f(r)$$

Τότε $\Phi_r(1) = 1(r) = 1$, και, αν $f,g \in R$, τότε θα έχουμε:

$$\Phi_r(f+g) = (f+g)(r) = f(r)+g(r) = \Phi_r(f)+\Phi_r(g)$$

$$\Phi_r(f\cdot g) = (f\cdot g)(r) = f(r)\cdot g(r) = \Phi_r(f)\cdot\Phi_r(g)$$

Άρα η απεικόνιση Φ_r είναι ένας ομομορφισμός δακτυλίων και ο οποίος είναι επιμορφισμός, διότι, αν $s \in \mathbb{R}$, τότε για την σταθερή συνάρτηση $\mathsf{s}\colon [0,1] \longrightarrow \mathbb{R}$, $\mathsf{s}(x) = s$, θα έχουμε: $\Phi_r(\mathsf{s}) = \mathsf{s}(r) = s$. Από το Πρώτο Θεώρημα Ισομορφισμών δακτυλίων, θα έχουμε έναν ισομορφισμό δακτυλίων

$$R/M_r \;\cong\; \mathbb{R}, \qquad \text{όπου} \qquad M_r = \{f \in R \mid \Phi_r(f) = f(r) = 0\}$$

Επομένως, για κάθε $r \in [0,1]$, το υποσύνολο M_r είναι ένα μεγιστοτικό ιδεώδες του R. Το ακόλουθο Θεώρημα δείχνει ότι κάθε μεγιστοτικό ιδεώδες του R είναι της μορφής M_r για κατάλληλο $r \in \mathbb{R}$.

Υπενθυμίζουμε ότι με

$$\mathsf{Max}(R) = \big\{ I \subseteq R \mid I : \text{μεγιστοτικό ιδελωδες του } R \big\}$$

συμβολίζουμε το σύνολο όλων των μεγιστοτικών ιδεωδών του δακτυλίου R.

Θεώρημα Α΄.0.1. *Έστω $R = \mathscr{C}([0,1],\mathbb{R})$ ο δακτύλιος των συνεχών πραγματικών συναρτήσεων επί του κλειστού διαστήματος $[0,1]$ της πραγματικής ευθείας. Τότε η απεικόνιση*

$$\Omega : [0,1] \longrightarrow \mathsf{Max}(R), \quad \Omega(r) = M_r = \big\{ f \in R \mid f(r) = 0 \big\}$$

είναι «1-1» και «επί».

Απόδειξη. Η ανάλυση που προηγήθηκε δείχνει ότι η απεικόνιση Ω είναι καλά ορισμένη. Αν $\Omega(r) = \Omega(s)$, όπου $r,s \in [0,1]$, τότε θα έχουμε $M_r = M_s$. Θεωρούμε τις συναρτήσεις $\phi_r, \phi_s : [0,1] \longrightarrow \mathbb{R}$, όπου $\phi_r(x) = x - r$ και $\phi_s(x) = x - s$. Επειδή προφανώς οι συναρτήσεις ϕ_r, ϕ_s είναι συνεχείς, θα έχουμε $\phi_r, \phi_s \in R$. Επειδή προφανώς $\phi_r(r) = r - r = 0$, θα έχουμε $\phi_r \in M_r$, και επειδή $M_r = M_s$, θα έχουμε $\phi_r \in M_s$ και επομένως $\phi_r(s) = 0$, δηλαδή $s - r = 0$, και άρα $s = r$. Αυτό σημαίνει ότι η απεικόνιση Ω είναι «1-1».

Έστω M ένα μέγιστο ιδεώδες του R. Θα δείξουμε πρώτα ότι υπάρχει $r \in [0,1]$ έτσι ώστε $M \subseteq M_r$, δηλαδή θα δείξουμε ότι:

$$\exists\, r \in [0,1] : \quad f \in M \implies f \in M_r$$

Ισοδύναμα θα δείξουμε ότι:

$$\exists\, r \in [0,1] : \quad \forall\, f \in M : \quad f(r) = 0 \tag{†}$$

Έστω ότι ο ισχυρισμός (†) δεν ισχύει. Τότε θα έχουμε ότι:

$$\forall\, x \in [0,1], \quad \exists\, f_x \in M : \quad f_x(x) \neq 0 \tag{††}$$

– Μεσω μιας σειρας 4 βηματων θα δουμε οτι ο ισχυρισμος (††) μας οδηγει σε ατοπο:

Βήμα 1: Επειδή, $\forall x \in [0,1]$, η συνάρτηση f_x ανήκει στο ιδεώδες M, έπεται ότι η f_x είναι συνέχης. Επειδή $f_x(x) \neq 0$, λόγω της συνέχειας της f_x, έπεται ότι υπάρχει ένα ανοιχτό διάστημα I_x το οποίο περιέχει το x: $x \in I_x$, έτσι ώστε $f_x(y) \neq 0$, $\forall y \in I_x$:

$$\forall x \in [0,1], \ \exists \text{ ανοιχτό διάστημα } I_x \subseteq [0,1] \text{ έτσι ώστε } x \in I_x \text{ και } \forall y \in I_x : \ f_x(y) \neq 0 \tag{1}$$

Προφανώς τότε θα έχουμε ότι η ένωση όλων των ανοιχτών διαστημάτων I_x τα οποία περιέχουν τα στοιχεία x του $[0,1]$ θα μας δίνει το διάστημα $[0,1]$:

$$[0,1] = \bigcup_{x \in [0,1]} I_x \tag{2}$$

Βήμα 2: Από τη σχέση (2) βλέπουμε ότι η συλλογή ανοιχτών διαστημάτων

$$\mathscr{I} = \big\{ I_x \subseteq [0,1] \mid x \in [0,1] \big\} \quad \text{την οποία ορίσαμε στη σχέση (1)}$$

αποτελεί μια ανοιχτή κάλυψη του κλειστού διαστήματος $[0,1]$.

Από το Θεώρημα των Heine-Borel [1] της Πραγματικής Ανάλυσης: «*κάθε ανοιχτή κάλυψη ενός κλειστού διαστήματος της πραγματικής ευθείας, περιέχει μια πεπερασμένη υποκάλυψη*», έπεται ότι υπάρχει πεπερασμένο πλήθος στοιχείων $x_1, x_2, \cdots, x_n \in [0,1]$, έτσι ώστε η ένωση των ανοιχτών διαστημάτων $I_{x_1}, \cdots, I_{x_n}$, όπου κάθε ανοιχτό διάστημα I_{x_j} περιέχει το στοιχείο x_j, μας δίνει το κλειστό διάστημα $[0,1]$:

$$\exists\, x_1, x_2, \cdots, x_n \in [0,1] : \quad I_{x_j} \in \mathscr{I}, \quad j = 1,2,\cdots,n, \quad \text{και} \quad [0,1] = \bigcup_{j=1}^{n} I_{x_j} \tag{3}$$

[1] - Félix Édouard Justin Émile Borel (7 Ιανουαρίου 1871 - 3 Φεβρουαρίου 1956) [https://en.wikipedia.org/wiki/?mile_Borel]: Γάλλος μαθηματικός και πολιτικός, γνωστός για τη συμβολή του στην Ανάλυση, και ιδιαίτερα στη Θεωρία Μέτρου, και στη Θεωρία Πιθανοτήτων.

- Heinrich Eduard Heine (16 Μαρτίου 1821 - 21 Οκτωβρίου 1881) [https://en.wikipedia.org/wiki/Eduard_Heine]: Γερμανός μαθηματικός με συμβολή στην Πραγματική Ανάλυση (υπεργεωμετρικές σειρές, ειδικές συναρτήσεις).

Βήμα 3: Θεωρούμε την συνάρτηση

$$f = f_{x_1}^2 + f_{x_2}^2 + \cdots + f_{x_n}^2 : [0,1] \longrightarrow \mathbb{R}, \quad f(x) = f_{x_1}^2(x) + f_{x_2}^2(x) + \cdots + f_{x_n}^2(x)$$

Σημειώνουμε ότι $f_{x_j}^2(x) = f_{x_j}(x) f_{x_j}(x) = (f_{x_j}(x))^2$, $1 \le j \le n$.

Η συνάρτηση f είναι προφανώς συνεχής και επομένως $f \in \mathscr{C}([0,1],\mathbb{R})$. Επιπρόσθετα επειδή οι συναρτήσεις f_x, $x \in [0,1]$, ανήκουν εκ κατασκευής στο ιδεώδες M έπεται ότι προφανώς θα έχουμε:

$$f = f_{x_1}^2 + f_{x_2}^2 + \cdots + f_{x_n}^2 \in M$$

Βήμα 4: Θα δείξουμε ότι η συνάρτηση f είναι αντιστρέψιμο στοιχείο του δακτυλίου $\mathscr{C}([0,1],\mathbb{R})$ και

$$M = \mathscr{C}([0,1],\mathbb{R})$$

Για να το δείξουμε αυτό, δείχνουμε πρώτα ότι η f δεν μηδενίζεται πουθενά στο διάστημα $[0,1]$:

$$f(z) \neq 0, \quad \forall z \in [0,1]$$

Πραγματικά: έστω ότι υπάρχει $z \in [0,1]$ έτσι ώστε $f(z) = 0$. Τότε:

$$f(z) = 0 \implies f_{x_1}^2(z) + f_{x_2}^2(z) + \cdots + f_{x_n}^2(z) = 0 \implies (f_{x_j}(z))^2 = 0, \quad 1 \le j \le n$$

και άρα

$$f_{x_j}(z) = 0, \quad \forall j = 1,2,\cdots,n \tag{4}$$

Επειδή $z \in [0,1]$ και επειδή από τη σχέση (3) έχουμε $[0,1] = \bigcup_{j=1}^n I_{x_j}$, έπεται ότι

$$z \in I_{x_k}, \quad \text{για κάποιο} \quad k = 1,2,\cdots,n$$

Όμως τότε από τον ορισμό τουμ διαστήματος I_{x_k}, έπεται ότι

$$f_{x_k}(z) \neq 0 \tag{5}$$

Επομένως οι σχέσεις (4), (5) μας οδηγούν σε άτοπο, και άρα πράγματικά έχουμε:

$$f(z) \neq 0, \quad \forall z \in [0,1] \tag{6}$$

Επειδή η f δεν μηδενίζεται σε κανένα σημείο του $[0,1]$, έπεται ότι μπορούμε να ορίσουμε μια συνάρτηση

$$g : [0,1] \longrightarrow \mathbb{R}, \quad g(x) = \frac{1}{f(x)}$$

και εύκολα βλέπουμε ότι η g είναι συνεχής και άρα ανήκει στον δακτύλιο $\mathscr{C}([0,1],\mathbb{R})$. Επειδή

$$(f \cdot g)(x) = f(x)g(x) = 1 = g(x)f(x) = (g \cdot f)(x), \quad \forall x \in [0,1]$$

έπεται ότι η f είναι αντιστρέψιμο στοιχείο του δακτυλίου $\mathscr{C}([0,1],\mathbb{R})$ και $g = f^{-1}$.

Επομένως το ιδεώδες M περιέχει το αντιστρέψιμο στοιχείο f και άρα το ιδεώδες M συμπίπτει με τον δακτύλιο $\mathscr{C}([0,1],\mathbb{R})$. Αυτό όμως είναι άτοπο διότι το M είναι μεγιστοτικό και άρα εξ ορισμού είναι γνήσιο.

Τα βήματα (1) - (4) μας οδηγήσαν σε άτοπο, υποθέτοντας ότι ισχύει η σχέση (††). Επομένως η σχέση (††) δεν ισχύει, και άρα θα έχουμε:

$$\exists r \in [0,1] : \quad \forall f \in M : \quad f(r) = 0 \tag{†}$$

Όπως είδαμε, αυτό σημαίνει ότι:

$$M \subseteq M_r \subseteq \mathscr{C}([0,1]) \tag{7}$$

Επειδή το ιδεώδες M είναι μεγιστοτικό, και επειδή κάθε ιδεώδες της μορφής M_r είναι μεγιστοτικό, και άρα γνήσιο, θα έχουμε από τη σχέση (7) ότι:

$$M = M_r = \Omega(r)$$

Επομένως η απεικόνιση Ω είναι «επί». ■

Παρατήρηση Α΄.0.2. Το αποτέλεσμα του Θεωρήματος Α΄.0.1 έχει ενδιαφέρουσες γενικεύσεις. Θα δούμε εν συντομία μια από αυτές.

(**I**) Ένας από τους λόγους που εξηγούν γιατί το αποτέλεσμα του Θεωρήματος Α΄.0.1 είναι σημαντικό, είναι γιατί μας επιτρέπει να «ανακαλύψουμε» το κλειστό διάστημα $[0,1]$ αλγεβρικά ως το σύνολο των μεγιστοτικών ιδεωδών του δακτυλίου των συνεχών πραγματικών συναρτήσεων οι οποίες ορίζονται επί του $[0,1]$. Αυτή η παρατήρηση μπορεί να γίνει περισσότερο ακριβής:

Το σύνολο $\mathsf{Max}(R)$ των μέγιστων ιδεωδών του δακτυλίου $R = \mathscr{C}([0,1],\mathbb{R})$ μπορεί να εφοδιαστεί με κατάλληλη τοπολογία (βλέπε παρακάτω το Θεώρημα των Gelfand-Kolmogorov), και έτσι να γίνει τοπολογικός χώρος. Αποδεικνύεται τότε ότι η απεικόνιση την οποία ορίσαμε στο Θεώρημα Α΄.0.1

$$\Omega : [0,1] \longrightarrow \mathsf{Max}(R), \quad \Omega(r) = M_r$$

είναι **ομοιομορφισμός** μεταξύ τοπολογικών χώρων, δηλαδή η Ω είναι «1-1» και «επί», συνεχής και η αντίστροφή της ϕ είναι συνεχής. Επομένως οι τοπολογικοί χώροι $[0,1]$ και $\mathsf{Max}(R)$ είναι (τοπολογικά) ίδιοι.

(**II**) Προσεκτική παρατήρηση της απόδειξης του Θεωρήματος Α΄.0.1 δείχνει ότι ένα από τα κρίσιμα σημεία στην απόδειξη είναι η δυνατότητα εφαρμογής του Θεωρήματος των Heine-Borel (κάθε ανοιχτή κάλυψη ενός κλειστού διαστήματος της πραγματικής ευθείας περιέχει μια πεπερασμένη υποκάλυψη), και αυτό είναι εφικτό διότι εργαζόμαστε στο κλειστό διάστημα $[0,1]$, το οποίο ως τοπολογικός χώρος είναι χώρος Hausdorff,[2], και **συμπαγής**, δηλαδή κάθε ανοιχτή του κάλυψη έχει μια πεπερασμένη υποκάλυψη.

Γενικότερα, ισχύει το ακόλουθο σημαντικό Θεώρημα των Kolmogorov-Gelfand.[3] Πριν το διατυπώσουμε, χρειαζόμαστε κάποιους ορισμούς (ότι ακολουθεί προαπαιτεί από τον αναγνώστη στοιχειώδεις γνώσεις τοπολογίας):

Έστω X ένας συμπαγής τοπολογικός χώρος Hausdorff, και έστω

$$\mathscr{C}(X,\mathbb{R}) = \{f : X \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$$

Μπορούμε να δούμε εύκολα ότι το σύνολο $\mathscr{C}(X,\mathbb{R})$ εφοδιασμένο με τις ακόλουθες πράξεις

$$\forall f,g \in \mathscr{C}(X,\mathbb{R}) : \quad (f+g)(x) = f(x) + g(x)$$

$$\forall f,g \in \mathscr{C}(X,\mathbb{R}) : \quad (f\cdot g)(x) = f(x)\cdot g(x)$$

είναι ένας μεταθετικός δακτύλιος με μονάδα την σταθερή συνάρτηση $1 : X \longrightarrow \mathbb{R}$, $1(x) = 1$.

Για κάθε στοιχείο $x \in X$, θεωρούμε το σύνολο

$$M_x = \{f \in \mathscr{C}(X,\mathbb{R}) \mid f(x) = 0\}$$

Θεώρημα [Kolmogorov-Gelfand (1939)] *Έστω X ένας συμπαγής τοπολογικός χώρος Hausdorff, και έστω*[4]

$$\mathscr{C}(X,\mathbb{R}) = \{f : X \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$$

ο δακτύλιος των συνεχών πραγματικών συναρτήσεων επί του X.

[2] Felix Hausdorff (8 Νοεμβρίου 1868 - 26 Ιανουαρίου 1942) [https://en.wikipedia.org/wiki/Felix_Hausdorff]: Γερμανός μαθηματικός, εκ των ιδρυτών της σύγχρονης Τοπολογίας, με συμβολή στη Θεωρία Συνόλων, στη Συναρτησιακή Ανάλυση, στη Θεωρία Μέτρου, και στη Θεωρία Συναρτήσεων.

[3] Israel Moiseevich Gelfand (2 Σεπτεμβρίου 1913 - 5 Οκτωβρίου 2009) [https://en.wikipedia.org/wiki/Israel_Gelfand]: Ρώσος, εκ των επιφανέστερων μαθηματικών του 20ού αιώνα. Το έργο του σε πολλούς κλάδους θεωρείται θεμελιώδες και εκτείνεται από την Άλγεβρα και τη Θεωρία Ομάδων, τη Θεωρία Αναπαραστάσεων, μέχρι την Συναρτησιακή Ανάλυση, τη Γεωμετρία, και τις Διαφορικές Εξισώσεις.

[4] Σε ό, τι ακολουθεί το σώμα $\mathbb{R}$ μπορεί να αντικατασταθεί με το σώμα των μιγαδικών αριθμών $\mathbb{C}$.

(**1**) *Το σύνολο* $\mathsf{Max}(R)$ *των μέγιστων ιδεωδών του δακτυλίου* $R = \mathscr{C}(X,\mathbb{R})$*, εφοδιασμένο με κατάλληλη τοπολογία,*[5] *είναι ένας τοπολογικός χώρος και η απεικόνιση*

$$\Omega : X \longrightarrow \mathsf{Max}(R), \quad \Omega(x) = M_x$$

είναι ομοιομορφισμός.

(**2**) *Κάθε συνεχής απεικόνιση* $\phi : X \longrightarrow Y$ *μεταξύ συμπαγών τοπολογικών χωρών Hausdorff επάγει έναν ομομορφισμό δακτυλίων*

$$\phi^* : \mathscr{C}(Y,\mathbb{R}) \longrightarrow \mathscr{C}(X,\mathbb{R}), \quad \phi^*(f) = f \circ \phi$$

και κάθε ομομορφισμός δακτυλίων $\mathscr{C}(Y,\mathbb{R}) \longrightarrow \mathscr{C}(X,\mathbb{R})$*, προκύπτει με τον παραπάνω τρόπο από μια συνεχή απεικόνιση* $\phi : X \longrightarrow Y$*.*

(**3**) *Δύο συμπαγείς τοπολογικοί χώροι Hausdorff* X *και* Y *είναι ομοιομορφικοί αν και μόνο αν οι δακτύλιοι* $\mathscr{C}(X,\mathbb{R})$ *και* $\mathscr{C}(Y,\mathbb{R})$ *είναι ισόμορφοι.*

Το Θεώρημα των Kolmogorov-Gelfand, ιστορικά, αποτέλεσε ένα απο τα πρώτα αποτελέσματα τα οποία συσχετίζουν με γόνιμο τρόπο γενικές ιδιότητες τοπολογικών χώρων με ανάλογες αλγεβρικές ιδιότητες κατάλληλων δακτυλίων. Προς αυτή την κατεύθυνση υπάρχει πληθώρα αποτελεσμάτων με μεγάλο ενδιαφέρον, αναφέρουμε για παράδειγμα ανάλογα αποτελέσματα των Gelfand-Naimark,[6] Banach-Stone[7] κτλ.

Ιδιαίτερα το ακόλουθο Θεώρημα των Banach-Stone χρησιμοποιεί το γεγονός ότι ο δακτύλιος $\mathscr{C}(X,\mathbb{R})$, όπου X είναι ένας συμπαγής τοπολογικός χώρος Hausdorff, είναι και χώρος Banach[8] με στάθμη

$$\forall f \in \mathscr{C}(X,\mathbb{R}) : \quad \|f\| = \sup\{|f(x)| \mid x \in X\}$$

Θεώρημα [Banach (1932) - Stone (1935)] *Έστω* X *και* Y *συμπαγείς τοπολογικοί χώροι Hausdorff, και έστω*

$$\mathscr{C}(X,\mathbb{R}) = \{f : X \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\} \quad \text{και} \quad \mathscr{C}(Y,\mathbb{R}) = \{f : Y \longrightarrow \mathbb{R} \mid f : \text{συνεχής}\}$$

οι δακτύλιοι των συνεχών πραγματικών συναρτήσεων επί των X *και* Y *αντίστοιχα, θεωρούμενοι ως χώροι Banach με στάθμη όπως παραπάνω. Τότε τα ακόλουθα είναι ισοδύναμα:*

1. *Οι χώροι Banach* $\mathscr{C}(X,\mathbb{R})$ *και* $\mathscr{C}(Y,\mathbb{R})$ *είναι ισομετρικά ισόμορφοι.*
2. *Οι τοπολογικοί χώροι* X *και* Y *είναι ομοιομορφικοί.* ▲

[5] Τη λεγόμενη τοπολογία του Stone της οποίας τα ανοιχτά υποσύνολα είναι τα σύνολα της μορφής $\mathfrak{M}(I) = \{M \in \mathsf{Max}(R) \mid I \nsubseteq M\}$, όπου I είναι ένα ιδεώδες του δακτυλίου $\mathscr{C}(X,\mathbb{R})$.

[6] Mark Naimark (5 Δεκεμβρίου 1909 - 30 Δεκεμβρίου 1978) [https://en.wikipedia.org/wiki/Mark_Naimark]: Ρώσος μαθηματικός, με συμβολή στη Συναρτησιακή Ανάλυση και στη Θεωρία Αναπαραστάσεων.

[7] - Stefan Banach (30 Μαρτίου 1892 - 31 Αυγούστου 1945) [https://en.wikipedia.org/wiki/StefanBanach]: Πολωνός μαθηματικός, από τους επιδραστικότερους Μαθηματικούς του 20ου αιώνα, με σημαντική συμβολή στην Συναρτησιακή Ανάλυση, όπου υπήρξε εκ των θεμελιωτών της.

- Marshall Harvey Stone (8 Απριλίου 1903 - 9 Ιανουαρίου 1989) [https://en.wikipedia.org/wiki/Marshall_Harvey_Stone]: Σημαντικός Αμερικανός μαθηματικός, με συμβολή στην Πραγματική Ανάλυση, στη Συναρτησιακή Ανάλυση, στην Τοπολογία, και στη Θεωρία των αλγεβρών Boole.

[8] Ακριβέστερα είναι μια (μεταθετική) άλγεβρα Banach. Για την έννοια της άλγεβρας Banach ο αναγνώστης μπορεί να ανατρέξει στο κλασικό βιβλίο «*Real and complex analysis*» του Walter Rudin.

Παράρτημα Β΄

Πότε μια Ακέραια Περιοχή είναι Περιοχή Κυρίων Ιδεωδών;

Στην παρούσα υποενότητα θα χαρακτηρίσουμε τις περιοχές κυρίων ιδεωδών ως εκείνες τις ακέραιες περιοχές οι οποίες μπορούν να δεχθούν μια στάθμη του Hasse στο σώμα κλασμάτων τους.

Ορισμός Β΄.0.1. *Έστω R ένας μεταθετικός δακτύλιος. Μια απεικόνιση*

$$\delta\colon R \longrightarrow \mathbb{N}_0, \quad a \longmapsto \delta(a)$$

καλείται **ασθενής πολλαπλασιαστική στάθμη**, *αν ικανοποιεί τις ακόλουθες ιδιότητες:*

1. $\delta(0) = 0$ *και* $\delta(a) \geq 1$, $\forall\, a \in R \setminus \{0\}$.
2. $\forall\, a, b \in R$: $\delta(ab) = \delta(a)\delta(b)$.

Η ασθενής πολλαπλασιαστική στάθμη δ καλείται **πολλαπλασιαστική στάθμη**, *αν η απεικόνιση δ ικανοποιεί επιπλέον την ιδιότητα:*

3. $\forall\, a \in R$: $\delta(a) = 1 \implies a \in \mathsf{U}(R)$.

Η επόμενη Πρόταση καταγράφει κάποιες στοιχεώδεις ιδιότητες (ασθενών) πολλαπλασιαστικών σταθμών.

Πρόταση Β΄.0.2. *Έστω R ένας μεταθετικός δακτύλιος.*

1. *Ο δακτύλιος R είναι ακέραια περιοχή αν και μονο αν η απεικόνιση*

$$\delta_0\colon R \longrightarrow \mathbb{N}_0, \quad \delta_0(0) = 0 \quad \textit{και} \quad \delta_0(a) = 1, \ \ \forall\, a \neq 0$$

   είναι μια ασθενής πολλαπλασιαστική στάθμη επί του R.

2. *Αν στον δακτύλιο R μπορεί να οριστεί μια ασθενής πολλαπλασιαστική στάθμη, τότε ο R είναι ακέραια περιοχή.*

3. *Ο δακτύλιος R είναι σώμα αν και μόνο αν η απεικόνιση δ_0 είναι μια πολλαπλασιαστική στάθμη επί του R.*

4. *Αν δ είναι μια ασθενής πολλαπλασιαστική στάθμη επί του R, τότε: $a \in \mathsf{U}(R) \implies \delta(a) = 1$.*

Απόδειξη. 1. Έστω ότι ο δακτύλιος R είναι ακέραια περιοχή, και έστω $a, b \in R$. Αν ένα εκ των a, b είναι ίσο με 0, για παράδειγμα το $a = 0$, τότε $0 = 0\delta_0(b) = \delta_0(a)\delta_0(b) = \delta_0(0) = \delta_0(ab)$. Αν $a, b \neq 0$, τότε, επειδή ο δακτύλιος R είναι ακέραια περιοχή, θα έχουμε $ab \neq 0$, και επομένως $1 = 1 \cdot 1 = \delta_0(a)\delta_0(b) = \delta_0(ab) = 1$.

Άρα η απεικόνιση δ_0 είναι μια ασθενής πολλαπλασιαστική στάθμη. Αντίστροφα, αν αυτό ισχύει, έστω $a,b\in R$ τέτοια ώστε $ab=0$, οπότε $\delta_0(ab)=0$. Αν $a\neq 0\neq b$, τότε $\delta_0(a)=1=\delta_0(b)$ και άρα θα καταλήξουμε στο άτοπο: $0=\delta_0(ab)=\delta_0(a)\delta_0(b)=1\cdot 1=1$. Άρα τουλάχιστον ένα εκ των a,b είναι ίσο με 0 και επομένως ο δακτύλιος R είναι ακέραια περιοχή.

2. Έστω δ μια ασθενής πολλαπλασιαστική στάθμη ορισμένη επί του R. Αν $a,b\in R$ είναι τέτοια ώστε $ab=0$, τότε $\delta(ab)=0$. Αν $a\neq 0\neq b$, τότε $\delta(a)\neq 0\neq\delta(b)$ και άρα θα καταλήξουμε στο άτοπο: $0=\delta(ab)=\delta(a)\delta(b)\neq 0$. Άρα τουλάχιστον ένα εκ των a,b είναι ίσο με 0 και επομένως ο δακτύλιος R είναι ακέραια περιοχή.

3. Αν ο δακτύλιος R είναι σώμα, τότε είναι ιδιαίτερα ακέραια περιοχή και έτσι από το μέρος 1. η απεικόνιση δ_0 είναι μια ασθενής πολλαπλασιαστική στάθμη επί του R. Αν $a\in R$ είναι τέτοιο ώστε $\delta_0=1$, τότε προφανώς $a\neq 0$ και, επειδή ο δακτύλιος R είναι σώμα, έπεται ότι $a\in\mathsf{U}(R)$. Έτσι η απεικόνιση δ_0 είναι μια πολλαπλασιαστική στάθμη. Αντίστροφα, αν αυτό ισχύει, έστω $0\neq a\in R$. Τότε $\delta_0(a)=1$ και άρα από την υπόθεση $a\in\mathsf{U}(R)$. Επομένως ο δακτύλιος R είναι σώμα.

4. Έστω δ μια ασθενής πολλαπλασιαστική στάθμη επί του R. Τότε $\delta(1)=\delta(1\cdot 1)=\delta(1)\delta(1)$, από όπου $\delta(1)=1$. Αν το στοιχείο a είναι αντιστρέψιμο, τότε $ab=1$, για κάποιο $b\in R$. Τότε $1=\delta(1)=\delta(ab)=\delta(a)\delta(b)$ και άρα $\delta(a)=1=\delta(b)$. ■

Έστω R μια ακέραια περιοχή με σώμα κλασμάτων $Q(R)$. Αν $\delta\colon R\longrightarrow\mathbb{N}_0$ είναι μια πολλαπλασιαστική στάθμη επί της R, τότε μπορούμε να επεκτείνουμε την απεικόνιση δ σε μια απεικόνιση

$$\delta^*\colon Q(R)\longrightarrow\mathbb{Q},\quad \delta^*\big(\frac{a}{b}\big)=\frac{\delta(a)}{\delta(b)}$$

Η απεικόνιση δ^* είναι καλά ορισμένη διότι, αν $\frac{a}{b}=\frac{c}{d}$, τότε θα έχουμε $ad=bc$ και άρα $\delta(a)\delta(d)=\delta(ad)=\delta(bc)=\delta(b)\delta(c)$, από όπου, χρησιμοποιώντας ότι $\delta(b)\neq 0\neq\delta(d)$, έπεται ότι:

$$\delta^*\big(\frac{a}{b}\big)=\frac{\delta(a)}{\delta(b)}=\frac{\delta(b)}{\delta(c)}=\delta^*\big(\frac{c}{d}\big)$$

Επιπλέον η δ^* είναι επίσης πολλαπλασιαστική (χρησιμοποιούμε ότι αν $b,d\neq 0$, τότε $bd\neq 0$ και άρα $\delta(b),\delta(d)\neq 0$):

$$\delta^*\big(\frac{a}{b}\cdot\frac{c}{d}\big)=\delta^*\big(\frac{ac}{bd}\big)=\frac{\delta(ac)}{\delta(bd)}=\frac{\delta(a)\delta(c)}{\delta(b)\delta(d)}=\frac{\delta(a)}{\delta(b)}\cdot\frac{\delta(c)}{\delta(d)}=\delta^*\big(\frac{a}{b}\big)\cdot\delta^*\big(\frac{c}{d}\big)$$

Η πολλαπλασιαστική συνάρτηση $\delta^*\colon Q(R)\longrightarrow\mathbb{N}_0$ καλείται **επέκταση** της πολλαπλασιαστικής στάθμης $\delta\colon R\longrightarrow\mathbb{N}_0$ στο σώμα κλασμάτων της ακέραιας περιοχής R.

Ορισμός Β΄.0.3. *Έστω R μια ακέραια περιοχή με σώμα κλασμάτων $Q(R)$ και $\delta\colon R\longrightarrow\mathbb{N}_0$ μια πολλαπλασιαστική στάθμη. Η δ καλείται* **στάθμη του Hasse** *επί της R, αν η επέκτασή της $\delta^*\colon Q(R)\longrightarrow\mathbb{N}_0$ στο σώμα κλασμάτων της R ικανοποιεί την ακόλουθη ιδιότητα:*

$$\forall\, x\in Q(R)\setminus R,\quad \exists\, a,b\in R\colon\quad 0<\delta^*(ax-b)<1$$

Όταν γραφουμε $x\in Q(R)\setminus R$, φυσικά εννοούμε ότι $x\in Q(R)\setminus\phi(R)$, όπου $\phi\colon R\longrightarrow Q(R)$, $\phi(r)=\frac{r}{1}$, είναι ο φυσικός μονομορφισμός.

Παράδειγμα Β΄.0.4. Η συνήθης απόλυτη τιμή $|\cdot|\colon\mathbb{Z}\longrightarrow\mathbb{N}_0$ είναι μια πολλαπλασιαστική στάθμη επί του $\mathbb{Z}$ και η επέκτασή της στο σώμα κλασμάτων $\mathbb{Q}$ είναι η συνήθης απόλυτη τιμή επί του $\mathbb{Q}$, και είναι μια στάθμη Hasse επί του $\mathbb{Z}$. Πράγματι, για κάθε ρητό αριθμό x ο οποίος δεν είναι ακέραιος, μπορούμε να θέσουμε $a=1$ και b να είναι το ακέραιο μέρος του x, δηλαδή ο μαγαλύτερος ακέραιος ο οποίος είναι μικρότερος ή ίσος με τον x. Τότε προφανώς θα έχουμε $0<|x-b|<1$. $\surd$

Μπορούμε τώρα να αποδείξουμε το ακόλουθο αποτέλεσμα το οποίο χαρακτηρίζει τις περιοχές κυρίων ιδεωδών ως εκείνες τις ακέραιες περιοχές επί των οποίων μπορεί να οριστεί μια στάθμη Hasse.

Θεώρημα Β΄.0.5 (Θεώρημα του Hasse)**.** *Για μια ακέραια περιοχή R, τα ακόλουθα είναι ισοδύναμα:*

1. *Η ακέραια περιοχή R είναι περιοχή κυρίων ιδεωδών.*
2. *Υπάρχει μια στάθμη Hasse ορισμένη επί της R.*

Απόδειξη. 1. Υποθέτουμε ότι η περιοχή R είναι περιοχή κυρίων ιδεωδών. Αν x είναι ένα τυχόν στοιχείο του R, τότε θα ορίσουμε μια στάθμη του Hasse $\delta\colon R \longrightarrow \mathbb{N}_0$ επί του R. Πρώτα ορίζουμε $\delta(0) = 0$. Αν $u \in \mathsf{U}(R)$ είναι ένα αντιστρέψιμο στοιχείο του R, ορίζουμε $\delta(u) = 1$. Αν $0 \neq x \in R \setminus \mathsf{U}(R)$, επειδή ο δακτύλιος R είναι περιοχή κυρίων ιδεωδών, από το Θεώρημα 11.4.13, έπεται ότι ο δακτύλιος R είναι περιοχή μονοσήμαντης ανάλυσης, και άρα μπορούμε να γράψουμε μοναδικά $x = x_1 \cdot x_2 \cdots x_n$, όπου κάθε x_i είναι ανάγωγο στοιχείο του R, $1 \leq i \leq n$. Ορίζουμε τότε $\delta(x) = 2^n$. Αν $0 \neq y \in R \setminus \mathsf{U}(R)$, και $y = y_1 \cdot y_2 \cdots y_m$ είναι η μοναδική γραφή του (μετρώντας πολλαπλότητες) ως γινόμενο πεπερασμένου πλήθους ανάγωγων στοιχείων του R, τότε προφανώς θα έχουμε $\delta(x \cdot y) = 2^{n+m} = 2^n 2^m = \delta(x)\delta(y)$. Η τελευταία σχέση ισχύει προφανώς και αν ένα ή και τα δύο εκ των x, y είναι ίσα με μηδέν ή είναι αντιστρέψιμα στοιχεία. Έτσι η απεικόνιση δ είναι μια καλά ορισμένη πολλαπλασιαστική στάθμη επί του R. Μένει να δείξουμε ότι η δ είναι στάθμη του Hasse.

Έστω $x \in Q(R) \setminus R$, και τότε μπορούμε να γράψουμε $x = \frac{a}{b}$, όπου $a, b \in R$, $b \neq 0$, και $(a, b) = 1$ και $b \in R \setminus \mathsf{U}(R)$. Τότε όμως από τον ορισμό της δ, έπεται ότι $\delta(b) > 1$. Επειδή $(a, b) = 1$, έπεται ότι υπάρχουν στοιχεία $k, l \in R$: $ka + lb = 1$ ή ισοδύναμα $ka - tb = 1$, όπου $t = -b$. Από την τελευταία σχέση θα έχουμε $\frac{1}{b}(ka - tb) = k\frac{a}{b} - t = kx - t = \frac{1}{b}$. Τότε θα έχουμε:

$$0 \;<\; \delta\big(kx - t\big) = \delta\big(\frac{1}{b}\big) \;<\; 1$$

Άρα η δ είναι στάθμη του Hasse.

2. Έστω $\delta\colon R \longrightarrow \mathbb{N}_0$ μια στάθμη του Hasse ορισμένη επί της ακέραιας περιοχής R, και έστω $\delta^*\colon Q(R) \longrightarrow \mathbb{Q}$ η επέκτασή της στο σώμα κλασμάτων της R. Αν I είναι το μηδενικό ιδεώδες του R, τότε το I είναι κύριο: $I = (0)$. Έστω I ένα μη μηδενικό ιδεώδες του R. Τότε το I περιέχει μη μηδενικά στοιχεία και επομένως το I περιέχει και στοιχεία στα οποία η στάθμη δ λαμβάνει θετικές τιμές. Έστω $d \in I$ ένα στοιχείο για το οποίο $\delta(d) > 0$ και το d είναι ελάχιστο μεταξύ των στοιχείων του I στα οποία η στάθμη λαμβάνει θετικές τιμές. Θα δείξουμε ότι $I = (d)$. Επειδή $d \in I$, θα έχουμε $(d) \subseteq I$ και αρκεί να δείξουμε ότι $I \subseteq (d)$. Έστω a ένα στοιχείο του I και θέτουμε $x = \frac{a}{d} \in Q(R)$. Αν $d \mid a$, τότε προφανώς $x \in R$. Υποθέτουμε ότι $x \notin R$ και άρα $x \in Q(R) \setminus R$. Επειδή η στάθμη δ είναι στάθμη του Hasse, θα έχουμε για κάποια στοιχεία $c, b \in R$:

$$0 < \delta^*\big(c\frac{a}{d} - b\big) < 1$$

Πολλαπλασιάζοντας με $\delta(d) = \delta^*(d)$, θα έχουμε:

$$0 < \delta^*(d)\delta^*(c\frac{a}{d} - b) = \delta^*(dc\frac{a}{d} - db) = \delta(ca - db) < \delta(d)$$

Το στοιχείο $ca - db$ ανήκει στο ιδεώδες I, διότι $d, a \in I$, και έχει στάθμη γνήσια μικρότερη της στάθμης του στοιχείου d. Αυτό είναι άτοπο από την επιλογή του I. Άρα $x = \frac{a}{d} \in R$ το οποίο σημαίνει ότι $d \mid a$, και άρα $a \in (d)$, δηλαδή $I \subseteq (d)$. Επομένως θα έχουμε $I = (d)$, δηλαδή το I είναι κύριο. Άρα η περιοχή R είναι περιοχή κυρίων ιδεωδών. ■

Ευρετήριο

Βιβλιογραφία

[1] **M.A. Armstrong**. Ομαδες και Συμμετρια. *Leader Books*, (2002).

[2] **M. Artin**. Algebra. *Prentice Hall*, (1991).

[3] **Δ. Βάρσος, Δ. Δεριζιώτης, Μ. Μαλιάκας, Ο. Ταλλέλη, Ι. Εμμανουήλ**. Μια Εισαγωγη στην Αλγεβρα. *Εκδόσεις Σοφία*, (2007).

[4] **Ayman Badawi**. Abstract algebra manual: problems and solutions. *Nova Science*, (2001).

[5] **John A. Beachy, William D. Blair**. Abstract algebra. *Waveland Press, Inc.*, (2005).
Για μια διαδικτυακή έκδοση βλέπε τον ιστότοπο: http://www.math.niu.edu/~beachy/abstract_algebra/study_guide/contents.html

[6] **B. Birkhoff, S. MacLane**. A survey of Modern Algebra. *MacMillan*, (1965).

[7] **N.J. Bloch**. Abstract Algebra with Applications. *Willey*, (1987).

[8] **A. Clark**. Elements of Abstract Algebra. *Dover*, (1984).

[9] **G. Calugareanu, P. Hamburg**. Exercises in Basic Ring Theory. *Kluwer*, (1998).

[10] **P. M. Cohn**. Algebra, Vol. 1-3. *Wiley*, (1982), (1989), (1991).

[11] **J. D. Dixon**. Problems in Group Theory. *Dover*, (1973).

[12] **D.S. Dummit, R. M. Foote**. Abstract algebra. *John Wiley and Sons, Inc.*, (2004).

[13] **J.B. Fraleigh**. Εισαγωγη στην Αλγεβρα. *Πανεπιστημιακές Εκδόσεις Κρήτης*, (2005).

[14] **J. Gallian**. Contemporary Abstract Algebra. *D.C. Heath and Company*, (1994).

[15] **R. Godement**. Cours d' Algèbre. *Hermann*, (1963).

[16] **M. Hall**. Theory of Groups. *Macmillan*, (1959).

[17] **I. N. Herstein**. Non Commutative Rings. *Carus Mathematical Monographs, Vol.* **15**, *MAA*, (1968).

[18] **I. N. Herstein**. Topics in Algebra. *Wiley*, (1975).

[19] **I. N. Herstein**. Abstract Algebra. *Prentice Hall*, (1990).

[20] **T. W. Hungerford**. Algebra. *Holt, Rinehart and Winston*, (1974).

[21] **I. M. Isaacs**. Algebra (A Graduate Course). *Brooks.Cole Publishing Company*, (1994).

[22] **N. Jacobson**. Basic Algebra I. *W.H. Freeman*, (1974).

[23] **I. Kaplansky**. Fields and Rings. *Chicago University Press*, (1974).

[24] **S. Lang**. Algebra. *Addison-Wesley*, (1965).

[25] **N. Μαρμαρίδης**. Αλγεβρα: Πανεπιστημιακες Παραδοσεις. *Ιωάννινα*, (2013).

[26] **N. Μαρμαρίδης**. Θεωρια Ομαδων. *Ιωάννινα*, (2015).

[27] **A. Μπεληγιάννης**. Ασκησεις Βασικης Αλγεβρας: Πανεπιστημιακες Παραδοσεις. *Ιωάννινα*, (2015).

[28] **Δ. Πουλάκης**. Θεωρια Αριθμων. *Εκδόσεις Ζήτη*, (1997).

[29] **Δ. Πουλάκης**. Αλγεβρα. *Εκδόσεις Ζήτη*, (2015).

[30] **J. Rotman**. A First Course in Abstract Algebra. *Prentice Hall*, (2000).

[31] **J. Rotman**. An Introduction to the Theory of Groups. *Springer*, (1995).

[32] **W.R. Scott**. Group Theory. *Dover*, (1987).

[33] **J. Silverman**. A Friendly Introduction to Number Theory. *Prentice Hall*, (2001).

[34] **S. Warner**. Modern Algebra (2 Volumes). *Prentice Hall*, (1965).