Σημειώσεις Μαθήματος Μεταπτυχιακής Άλγεβρας

Δημήτριος Χατζάκος

Χειμερινό έτος 2022-23

Σκοπός του μαθήματος είναι η μελέτη σε βάθος δύο βασικών αλγεβρικών δομών, των Ομάδων και των Προτύπων. Αρχικά υπενθυμίζουμε εν συντομία τα βασικά στοιχεία της στοιχειώδους Θεωρίας ομάδων που θα χρειαστούμε και μετά εμβαθύνουμε στην πιο προχωρημένη Θεωρία ομάδων. Εν συνεχεία θυμίζουμε τα βασικά στοιχεία από την Θεωρία δακτυλίων και σωμάτων. Μελετάμε την έννοια του Προτύπου πάνω από έναν δακτύλιο καθώς και κάποιες βασικές κατηγορίες Προτύπων. Στο τέλος δίνουμε μια επισκόπηση κάποιων βασικών αποτελεσμάτων της Αλγεβρικής θεωρίας αριθμών και της Αλγεβρικής γεωμετρίας.

Περιεχόμενα

1 Εισαγωγή και επανάληψη βασικών στοιχείων της Θεωρίας Ομάδων

1.1 Βασικές έννοιες

Οι έννοιες της ομάδας και του δακτυλίου είναι θεμελιώδεις στην μοντέρνα άλγεβρα. Ξεκινάμε με μια σύντομη σύνοψη των βασικών στοιχείων της Θεωρίας ομάδων όπως διδάχθηκαν στο μάθημα "'Αλγεβρα Ι". Με G θα συμβολίζουμε πάντα μια ομάδα.

Ορισμός 1.1. *Ένα σύνολο G ονομάζεται ομάδα εάν υπάρχει μια απεικόνιση $\cdot : G \times G \to G$ τέτοια ώστε:*

- *Για κάθε δύο στοιχεία $g_1, g_2 \in G$ έχουμε $g_1 \cdot g_2 \in G$.*
- *Υπάρχει ένα ουδέτερο στοιχείο e της πράξης που ικανοποιεί $g \cdot e = g = e \cdot g$ για κάθε $g \in G$.*
- *Για κάθε $g \in G$ υπάρχει ένα αντίστροφο στοιχείο $g^{-1} \in G$ με την ιδιότητα $g \cdot g^{-1} = e$.*

Η απεικόνιση αυτή ονομάζεται πράξη της ομάδας G.

Θα συμβολίζουμε τα στοιχεία μιας ομάδας με $g, h, ...$ ή $x, y, z, ...$ ή $a, b, c, ...$. Για να είμαστε φορμαλιστικά ορθοί, μια ομάδα είναι ένα ζεύγος $(G, \cdot)$, δηλαδή η πράξη $\cdot$ είναι αναπόσπαστο στοιχείο του ορισμού. Αυτό συμβαίνει διότι ένα σύνολο G μπορεί να γίνει ομάδα με πολλές διαφορετικές πράξεις ορισμένες στο G. Συνήθως θα παραλείπουμε τον συμβολισμό $\cdot$ της πράξης της G και θα γράφουμε απλά xy στην θέση του $x \cdot y$, όταν είναι σαφές ποια είναι η αντίστοιχη πράξη που εννοούμε.

Η επόμενη άσκηση έπεται εύκολα και άμεσα από τον ορισμό.

Άσκηση 1.1. *Έστω G μια ομάδα. Τότε το ουδέτερο στοιχείο e είναι μοναδικό. Επίσης, κάθε στοιχείο $g \in G$ έχει μοναδικό αντίστροφο στοιχείο μέσα στην ομάδα G.*

Συμπεραίνουμε από τον ορισμό ότι μια ομάδα είναι ένα σύνολο G εφοδιασμένο με μια πράξη τέτοια ώστε το G να είναι κλειστό ως προς αυτή την πράξη και κάθε στοιχείο του να αντιστρέφεται. Ισοδύναμα, παρατηρούμε ότι τα αξιώματα του Ορισμού 1.1 μας επιτρέπουν να θεωρούμε ότι μια ομάδα είναι ακριβώς ένα σύνολο στο οποίο μπορούμε να επιλύσουμε την πρωτοβάθμια εξίσης $ax = b$ οδηγούμενοι στην μοναδική λύση $x = a^{-1}b$. Υπενθυμίζουμε τώρα μερικά βασικά και χρήσιμα παραδείγματα.

Παράδειγμα 1.1. *Οι πιο οικείες μας ομάδες είναι οι $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \cdot)$.*

Η πράξη μιας ομάδας δεν απαιτείται να είναι αναγκαστικά μεταθετική. Υπενθυμίζουμε τον ακόλουθο βασικό ορισμό.

Ορισμός 1.2. *Μια ομάδα G ονομάζεται αβελιανή (ή μεταθετική) εάν η πράξη της έχει την αντιμεταθετική ιδιότητα, δηλαδή εάν $xy = yx$ για κάθε $x, y \in G$. Σε αυτήν την περίπτωση λέμε ότι τα στοιχεία x και y αντιμετατίθονται.*

Αν και θα μελετήσουμε την Θεωρία δακτυλίων πιο αναλυτική μετά την Θεωρία ομάδων, για λόγους πληρότητας επιθυμούμε να υπενθυμίσουμε εδώ και τον βασικό ορισμό των δακτυλίων (χωρίς όλες τις λεπτομέρειες σε αυτό το στάδιο). Ειδικότερα, ένας δακτύλιος R είναι ένα σύνολο $(R, +, \cdot)$ εφοδιασμένος με δύο πράξεις, μία πράξη 'πρόσθεσης' $+ : R \times R \to R$ και μία πράξη 'πολλαπλασιασμού' $\cdot : R \times R \to R$ τέτοιες ώστε το σύνολο $(R, +)$ να είναι αβελιανή ομάδα και η πράξη του πολλαπλασιασμού $\cdot$ να είναι 'συμβατή' με την πράξη της πρόσθεσης. Ειδικότερα, αν το σύνολο $(R, \cdot)$ αποτελεί κι αυτό αβελιανή ομάδα, τότε ο R ονομάζεται *σώμα*.

Παράδειγμα 1.2. *(α) Τα σύνολα των $n \times n$ πινάκων με συντελεστές από το $\mathbb{R}$ (ή από το $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ ή κάποιον άλλον γενικότερο δακτύλιο R) και με πράξη την πρόσθεση είναι ομάδα και συμβολίζεται με $M_n(\mathbb{R})$ (ή γενικότερα $M_n(R)$).*

(β) Το σύνολο των αντιστρέψιμων $n \times n$ πινάκων με συντελεστές από το $\mathbb{R}$ (ή από το $\mathbb{Q}, \mathbb{C}$ ή από κάποιο γενικότερο σώμα $\mathbb{F}$) και πράξη τον πολλαπλασιασμό πινάκων είναι ομάδα, και συμβολίζεται με $GL_n(\mathbb{R})$ (αντίστοιχα $GL_n(\mathbb{F})$).

(γ) Το σύνολο των $n \times n$ πινάκων ορίζουσας 1 με συντελεστές από το $\mathbb{R}$ (ή κάποιο γενικότερο σώμα $\mathbb{F}$) και πράξη τον πολλαπλασιασμό πινάκων είναι ομάδα, και συμβολίζεται με $SL_n(\mathbb{R})$ (αντίστοιχα $SL_n(\mathbb{F})$). Προφανώς $SL_n(\mathbb{F}) \leqslant GL_n(\mathbb{F})$.

Παράδειγμα 1.3. *Για κάθε φυσικό αριθμό $n \geqslant 2$, θεωρούμε το σύνολο των ακεραίων modulo n, το οποίο συμβολίζουμε με $\mathbb{Z}_n$. Αυτό το σύνολο είναι ομάδα με πράξη της πρόσθεση modulo n.*

Θυμίζουμε πως το $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν το n είναι πρώτος. Το σύνολο των αντιστρέψιμων στοιχείων modulo n είναι ομάδα με πράξη των πολλαπλασιασμό και συμβολίζεται με $U(\mathbb{Z}_n)$ ή $(\mathbb{Z}_n)^{\times}$.

Όπως μας δείχνουν τα παραπάνω παραδείγματα, μια ομάδα μπορεί να είναι είτε άπειρο σύνολο είτε πεπερασμένο. Σε καθέμια από τις παραπάνω περιπτώσεις ονομάζεται αντίστοιχα άπειρη ή πεπερασμένη. Συμβολίζουμε με $|G|$ την *τάξη* της G, δηλαδή την πληθικότητα του συνόλου G. Τα παραπάνω παραδείγματα μας δείχνουν ότι υπάρχει μια πληθώρα πεπερασμένων και άπειρων ομάδων. Ειδικότερα, $|\mathbb{Z}_n| = n$ και $|U(\mathbb{Z}_n)| = \phi(n)$.

Άσκηση 1.2. *Εξετάστε ποιές από τις ομάδες που ορίσαμε παραπάνω είναι αβελιανές και ποιές είναι μη αβελιανές.*

Άσκηση 1.3. *Αν $(G, \cdot), (H, *)$ είναι δύο ομάδες, ορίζουμε το ευθύ γινόμενο τους $G \times H$ να είναι το καρτεσιανό γινόμενο $\{(g, h) : g \in G, h \in H\}$. Δείξτε ότι το ευθύ γινόμενο είναι ομάδα με την πράξη κατά συντεταγμένες. Δείξτε επίσης ότι το ευθύ γινόμενο των G και H είναι αβελιανή ομάδα αν και μόνο αν οι G και H είναι αβελιανές.*

1.2 Υποομάδες

Ένα υποσύνολο μιας ομάδας G μπορεί να παραμένει ομάδα αν περιορίσουμε την πράξη της G σε αυτό. Για παράδειγμα, η προσθετική ομάδα των ακεραίων $(\mathbb{Z}, +)$ εμπεριέχεται μέσα στην προσθετική ομάδα των ρητών αριθμών $(\mathbb{Q}, +)$. Ο παρακάτω ορισμός είναι κρίσιμης σημασίας.

Ορισμός 1.3. *Έστω $(G, \cdot)$ μια ομάδα. Ένα μη κενό υποσύνολο H της G ονομάζεται υποομάδα της G αν η $(H, \cdot)$ είναι ομάδα (δηλαδή εάν ο περιορισμός της πράξης της G στην H εφοδιάζει την H με δομή ομάδας).*

Γράφουμε $H \leqslant G$ για να δηλώσουμε ότι η H είναι υποομάδα της G. Παρατηρήστε επίσης πως ο ορισμός αναγκάζει το ουδέτερο στοιχείο e της G να ανήκει αναγκαστικά στην H. Ως εκ τούτου, κάθε ομάδα G έχει τουλάχιστον δύο υποομάδες, το μονοσύνολο $\{e\}$ (που ονομάζεται *τετριμμένη* υποομάδα) και ολόκληρη την G. Αν η H είναι γνήσιο υποσύνολο της G τότε λέγεται *γνήσια* υποομάδα της και γράφουμε $H < G$. Ενδέχεται όμως να μην έχει άλλες υποομάδες, και ο πιο άμεσος τρόπος για να το δει κανείς αυτό είναι χρησιμοποιώντας το ακόλουθο διάσημο αποτέλεσμα, που αποτελεί το πιο σημαντικό αποτέλεσμα της θεωρίας των πεπερασμένων ομάδων.

Θεώρημα 1.1. *(Lagrange, απλή μορφή) Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της. Τότε η τάξη της H διαιρεί την τάξη της G.*

Θα θυμηθούμε την απόδειξη αυτού του σημαντικού αποτελέσματος παρακάτω, και επίσης θα δούμε μια σημαντική γενίκευση του όταν θα μελετήσουμε τις δράσεις ομάδων σε σύνολα.

Πριν προχωρήσουμε παρακάτω, για λόγους πληρότητας υπενθυμίζουμε ακόμα ένα μικρό αλλά χρήσιμο αποτέλεσμα. Παρατηρούμε πρώτα ότι αν $h \in H \leqslant G$, τότε και $h^{-1} \in H$. Μερικές φορές στην βιβλιογραφία ένα υποσύνολο H μιας ομάδας G ορίζεται να ονομάζεται υποομάδα αν είναι κλειστό ως προς την πράξη και ως προς αντίστροφα στοιχεία (παρατηρήστε ότι ο ορισμός αυτός είναι ισοδύναμος με τον ορισμό που δώσαμε).

Πρόταση 1.1. *Έστω $H \subseteq G$. Τότε $H \leqslant G$ αν και μόνο αν $e \in H$ και για κάθε $x, y \in H$ έχουμε $xy^{-1} \in H$. Αν επιπλέον υποτεθεί ότι $|G| < \infty$, τότε $H \leqslant G$ αν και μόνο αν $x, y \in H$ έχουμε $xy \in H$.*

Απόδειξη. Η απόδειξη αυτής της απλής Πρότασης αφήνεται ως άσκηση. □

Το παραπάνω απλό Λήμμα μας επιτρέπει να ελέγχουμε πιο γρήγορα σε ορισμένες περιπτώσεις εάν ένα υποσύνολο μιας ομάδας είναι υποομάδα της.

Μια θεμελιώδης και πολύ απλή ιδέα της Θεωρίας ομάδων (όπως την διδαχθήκαμε στα προπτυχιακά μας χρόνια) είναι πως η κλειστότητα της πράξης μας επιτρέπει, δοθέντος ενός στοιχείου $g \in G$, να κατασκευάζουμε γρήρορα νέα στοιχεία της ομάδας, απλώς πολλαπλασιάζοντας το g με τον εαυτό του. Ορίζουμε τότε αναδρομικά τις δυνάμεις του g ως $g^2 := g \cdot g$ και $g^n := g^{n-1} \cdot g$, όπου εξ' ορισμού $g^0 = e$. Για αρνητικές δυνάμεις ορίζουμε $g^{-n} := (g^{-1})^n$. Ορίζουμε το *σύνολο που παράγεται* από το g ως το σύνολο

$$\langle g \rangle := \{g^n : n \in \mathbb{Z}\} . \tag{1}$$

Προφανώς $\langle g \rangle \leqslant G$. Δεν ισχύει όμως απαραίτητα πως $\langle g \rangle = G$ για κάποιο $g \in G$ εάν η G είναι αρκετά 'περίπλοκη'.

Ορισμός 1.4. *Μια ομάδα G ονομάζεται κυκλική εάν υπάρχει $g \in G$ τέτοιο ώστε $\langle g \rangle = G$. Σε αυτήν την περίπτωση ένα τέτοιο στοιχείο g ονομάζεται γεννήτορας της G.*

Παρατηρούμε πως κάθε κυκλική ομάδα είναι αναγκαστικά άριθμήσιμη, άρα οι ομάδες $(\mathbb{R}, +)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{C}^*, \cdot)$ κλπ. δεν είναι κυκλικές.

Σχετικός με τον παραπάνω ορισμό είναι ο ορισμός της τάξης ενός στοιχείου g, η οποία ορίζεται ως ο ελάχιστος φυσικός αριθμός n με την ιδιότητα $g^n = e$. Η τάξη του e ορίζεται να είναι ίση με 1, ενώ κάθε μη τετριμμένο στοιχείο έχει τάξη $\geqslant 2$. Εάν για ένα στοιχείο g δεν υπάρχει τέτοιος φυσικός αριθμός n, λέμε ότι το g έχει άπειρη τάξη.

Άσκηση 1.4. *Αποδείξτε πως κάθε κυκλική ομάδα είναι και αβελιανή. Δείξτε ότι το αντίστροφο δεν αληθεύει.*

Άσκηση 1.5. *Μελετήστε ποιές από τις ομάδες του Παραδείγματος 1.1 είναι κυκλικές.*

Άσκηση 1.6. *Αποδείξτε την Πρόταση 1.1.*

Άσκηση 1.7. *Αποδείξτε ότι αν $|G| = p$ με p πρώτο αριθμό, τότε η G είναι κυκλική.*

Άσκηση 1.8. *Έστω $g \in G$ με $|\langle g \rangle| < \infty$. Δείξτε ότι τότε η τάξη της ομάδας $|\langle g \rangle|$ είναι ίση με την τάξη του στοιχείου g.*

Άσκηση 1.9. *Έστω G μία κυκλική ομάδα και $H \leqslant G$. Δείξτε ότι η H είναι κυκλική.*

Άσκηση 1.10. *Έστω G μία κυκλική ομάδα τάξης n. Δείξτε ότι η G έχει $\phi(n)$ στο πλήθος διαφορετικούς γεννήτορες. Δείξτε επίσης ότι για κάθε $d|n$ η G έχει μοναδική υποομάδα τάξης d.*

Άσκηση 1.11. *Χρησιμοποιώντας την προηγούμενη άσκηση δείξτε ότι*

$$\sum_{d|n} \phi(d) = n.$$

Άσκηση 1.12. *Αποδείξτε ότι τομή υποομάδων είναι υποομάδα. Δηλαδή, αν $\{H_i\}_{i\in I}$ είναι μια οικογένεια υποομάδων της G, τότε*

$$\bigcap_{i\in I} H_i \leqslant G.$$

Άσκηση 1.13. *Δείξτε ότι κάθε υποομάδα της προσθετικής ομάδα του $\mathbb{R}$ είναι είτε κυκλική είτε πυκνή.*

Άσκηση 1.14. *Το κέντρο μιας ομάδας G ορίζεται να είναι το σύνολο*

$$Z(G) := \{g \in G : gh = hg \quad \forall h \in G\}.$$

Αποδείξτε ότι το $Z(G)$ είναι υποομάδα της G. Πότε ισχύει $Z(G) = G$;

Άσκηση 1.15. *Βρείτε τα κέντρα $Z(GL_n(\mathbb{R})), Z(SL_n(\mathbb{R}))$.*

Το κέντρο μιας ομάδας μετράει, κατά κάποιον τρόπο, πόσο πολύ απέχει μια ομάδα από το να είναι αβελιανή. Η ακόλουθη ακραία περίπτωση έχει ιδιαίτερο ενδιαφέρον, όπως θα δούμε και παρακάτω στην θεωρία.

Ορισμός 1.5. *Μία υποομάδα που έχει τετριμμένο κέντρο $Z(G) = \{e\}$ λέγεται centerless.*

Άσκηση 1.16. *Έστω G μία centerless ομάδα και $H \leqslant G$. Δείξτε ότι δεν έπεται απαραίτητα πως $Z(H) = \{e\}$.*

Άσκηση 1.17. *Βρείτε όλες τις centerless ομάδες τάξης $\leqslant 10$.*

1.3 Η συμμετρική ομάδα S_n.

Αν θεωρήσουμε το σύνολο $X_n = \{1, 2, 3, ..., n\}$ των πρώτων n φυσικών αριθμών, μας ενδιαφέρει να μελετήσουμε το σύνολο των ένα-προς-ένα και επί συναρτήσεων από το X_n στον εαυτό του.

Ορισμός 1.6. *Μία ένα-προς-ένα και επί συνάρτηση $\sigma : X_n \to X_n$ ονομάζεται μετάθεση βαθμού n.*

Θυμηθείτε (άσκηση) πως το σύνολο των μεταθέσεων του X_n γίνεται ομάδα με πράξη την σύνθεση μεταθέσεων. Η ομάδα αυτή συμβολίζεται με S_n. Για ένα στοιχείο $\sigma \in S_n$ γράφουμε συμβολικά

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}.$$

Παράδειγμα 1.4. *Αν*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

δύο μεταθέσεις της S_5, τότε

$$\sigma\tau := \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}.$$

Άσκηση 1.18. *Δείξτε ότι η τάξη της S_n είναι ίση με $n!$.*

Άσκηση 1.19. *Για $n \geqslant 3$ δείξτε ότι η S_n είναι μη αβελιανή και υπολογείστε το κέντρο της.*

1.4 Ομομορφισμοί ομάδων

Δύο ομάδες G και H μπορεί να είναι πολύ διαφορετικές μεταξύ τους ή μπορεί και να 'μοιάζουν' λίγο μεταξύ τους. Έναν τρόπο να μετρήσουμε σε τι βαθμό μοιάζουν μεταξύ τους δυο ομάδες μας την δίνει η έννοια του *ομομορφισμού* ομάδων, μια ιδέα που είναι καθολική σε όλα τα πεδία των μαθηματικών.

Ορισμός 1.7. *Έστω $(G,\cdot),(H,*)$ δύο ομάδες. Μια απεικόνιση $\phi : G \to H$ λέγεται ομομορφισμός αν για κάθε $x, y \in G$ ισχύει*

$$\phi(x \cdot y) = \phi(x) * \phi(y).$$

Αν η ϕ είναι $1-1$ απεικόνιση, τότε λέγεται μονομορφισμός. Αν είναι επί, λέγεται επιμορφισμός. Αν είναι $1-1$ και επί, λέγεται ισομορφισμός.

Αν επιπλέον έχουμε $G = H$, τότε κάθε επιμορφισμός $\phi : G \to G$ λέγεται και ενδομορφισμός. Κάθε ισομορφισμός $\phi : G \to G$ ονομάζεται αυτομορφισμός.

Αν υπάρχει ένας ισομορφισμός $\phi : G \to H$, τότε οι G, H ονομάζονται *ισόμορφες*, και γράφουμε $G \simeq H$. Δύο ισόμορφες ομάδες είναι αλγεβρικά ίδιες, καθώς ο ορισμός μας λέει ότι οι πράξεις μέσα στην αρχική μεταφέρονται αυτούσιες στην δεύτερη. Μπορούμε λοιπόν στο μυαλό μας να ταυτίζουμε ισόμορφες ομάδες, θεωρώντας τες ουσιαστικά ίδιες.

Παρατηρείστε ότι αν δύο πεπερασμένες ομάδες είναι ισόμορφες μεταξύ τους, τότε θα πρέπει να έχουν αναγκαστικά το ίδιο πλήθος στοιχείων. Η επόμενη άσκηση δείχνει ότι το αντίστροφο δεν είναι ισχύει πάντα.

Άσκηση 1.20. *Δείξτε ότι $S_2 \simeq \mathbb{Z}_2$, ενώ για $n \geqslant 3$ δείξτε ότι οι ομάδες S_n και $\mathbb{Z}_{n!}$ δεν είναι ισόμορφες.*

Άσκηση 1.21. *Έστω δύο πεπερασμένες κυκλικές ομάδες G, H με $|G| = |H|$. Δείξτε ότι $G \simeq H$.*

Έστω $\mathfrak{G}(n)$ η συνάρτηση που απαριθμεί το πλήθος των διαφορετικών (μη ισόμορφων) ομάδων τάξης n. Η παραπάνω άσκηση σε συνδυασμό με την άσκηση 1.7 δίνουν ότι $\mathfrak{G}(p) = 1$ για κάθε πρώτο p. Ο υπολογισμός της συνάρτησης $\mathfrak{G}(n)$ για κάθε n είναι ένα ανοιχτό (και εξαιρετικά περίπλοκο) πρόβλημα. Για γενικό n γνωρίζουμε μόνο άνω φράγματα για την συνάρτηση $\mathfrak{G}(n)$. Θα δούμε πάντως παρακάτω ότι υπάρχουν και σύνθετοι αριθμοί n για τους οποίους έχουμε $\mathfrak{G}(n) = 1$.

Άσκηση 1.22. *Έστω $\phi : G \to H$ ομομορφισμός. Δείξτε ότι $\phi(e_G) = e_H$ και $\phi(g^n) = \phi(g)^n$ για κάθε ακέραιο αριθμό n. Συμπεράνατε πως αν το g έχει πεπερασμένη τάξη τότε η τάξη του $\phi(g)$ διαιρεί την τάξη του g.*

Άσκηση 1.23. *Η απεικόνιση $[\cdot]_n : \mathbb{Z} \to \mathbb{Z}_n$ με $[a]_n = a \mod n$ είναι επιμορφισμός (και ονομάζεται φυσικός επιμορφισμός).*

Άσκηση 1.24. *Εξετάστε εάν η απεικόνιση $\phi : \mathbb{Z}_2 \to SL_2(\mathbb{Z})$*

$$\phi([1]_2) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

είναι ομομορφισμός (είναι 1-1; είναι επί;)

Άσκηση 1.25. *Εξετάστε αν οι παρακάτω ιδιότητες ομάδων διατηρούνται κάτω από ισομορφισμούς: μεταθετικότητα, κυκλικότητα, τάξη ομάδας, τάξεις στοιχείων, τάξη κέντρου, πλήθος διαφορετικών υποομάδων.*

Άσκηση 1.26. *Βρείτε έναν επιμορφισμό*

$$GL_n(\mathbb{F}) \to \mathbb{F}^*.$$

Άσκηση 1.27. *Δείξτε ότι το σύνολο Aut(G) των αυτομορφισμών μιας ομάδας G είναι ομάδα με πράξη την σύνθεση απεικονίσεων.*

Άσκηση 1.28. *Για κάθε $g \in G$ ορίζουμε την απεικόνιση $i_g : G \to G$ με τύπο*

$$i_g(x) = gxg^{-1}.$$

Δείξτε ότι κάθε απεικόνιση i_g είναι αυτομορφισμός της G. Τέτοιου είδους αυτομορφισμοί ονομάζονται εσωτερικοί αυτομορφισμοί της G και το σύνολο τους συμβολίζεται με Inn(G) (ενώ οι υπόλοιποι ονομάζονται εξωτερικοί αυτομορφισμοί). Δείξτε ότι $Inn(G) \leqslant$ Aut(G).

Ο προσδιορισμός της ομάδας των αυτομορφισμών μιας δοσμένης ομάδας G είναι εν γένει ένα αρκετά δύσκολο πρόβλημα. Ο προσδιορισμός της ομάδας των αυτομορφισμών των συμμετρικών ομάδων είναι ένα πρόβλημα με μεγάλο ιστορικό ενδιαφέρον.

Ορισμός 1.8. *Μία ομάδα G λέγεται πλήρης (complete) εάν είναι centerless και Inn(G) = Aut(G).*

Κάθε S_n με $n \neq 2, 6$ είναι πλήρης. Η S_2 δεν είναι πλήρης αφού είναι αβελιανή. Ο Hölder το 1895 απέδειξε πως η S_6 έχει εξωτερικούς αυτομορφισμούς. Θα δούμε επίσης παρακάτω πως η ομάδα Inn(G) μπορεί εύκολα να γίνει κατανοητή ως ομάδα-πηλίκο της G.

Ένα θεμελιώδες γεγονός είναι πως κάθε ομομορφισμός $\phi : G \to H$ ορίζει δύο σημαντικές ομάδες που τον καθορίζουν, τον *πυρήνα* $\ker\phi$ και την *εικόνα* $\operatorname{Im}\phi$, που ορίζονται ως

$$\ker\phi := \{g \in G : \phi(g) = e\} = \phi^{-1}(e),$$

$$\operatorname{Im}\phi = \phi(G) := \{h \in H : \textit{υπάρχει} \quad g \in G \quad \textit{με} \quad \phi(g) = h\}.$$

Ένα γεγονός που το γνωρίζουμε από το μάθημα της Άλγεβρας I (και είναι ρουτίνα να αποδειχθεί) είναι πως

$$\ker\phi \leqslant G, \quad \operatorname{Im}\phi \leqslant H.$$

Άσκηση 1.29. *Έστω $\phi : G_1 \to G_2$ ομομορφισμός υποομάδων και $H_1 \leqslant G_1, H_2 \leqslant G_2$. Δείξτε ότι $\phi(H_1) \leqslant G_2$ και $\phi^{-1}(H_2) \leqslant G_1$. Αν η H_1 είναι κυκλική, τότε και η $\phi(H_1)$ είναι κυκλική.*

Άσκηση 1.30. *Δείξτε ότι η απεικόνιση $\phi : G \to G$ με $\phi(g) = g^{-1}$ είναι ομομορφισμός αν και μόνο αν η G είναι αβελιανή.*

Άσκηση 1.31. *Δείξτε ότι η προσθετική ομάδα $(\mathbb{Z}[x], +)$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $(\mathbb{Q}_{>0}, \cdot)$.*

Άσκηση 1.32. *Δείξτε ότι η προσθετική ομάδα $(\mathbb{R}, +)$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $(\mathbb{R}_{>0}, \cdot)$.*

Άσκηση 1.33. *Έστω G, H δύο ομάδες, $f, g : G \to H$ δύο ομομορφισμοί και ορίζουμε*

$$K = \{a \in G : f(a) = g(a)\}.$$

Ισχύει ότι $K \leqslant G$;

1.5 Γεννήτορες

Ορίσαμε την κυκλική ομάδα $\langle g \rangle$ που παράγεται από ένα στοιχείο $g \in G$. Η υποομάδα αυτή είναι η μικρότερη υποομάδα της G που περιέχει το g, με την έννοια ότι αν μια άλλη υποομάδα της G περιέχει το g τότε θα πρέπει υποχρεωτικά να περιέχει ολόκληρη την $\langle g \rangle$. Η παρατήρηση αυτή μια δίνει την ιδέα πως να ορίσουμε γενικότερα την ομάδα που παράγεται από ένα υποσύνολο X της G.

Ορισμός 1.9. *Έστω $\emptyset \neq X \subset G$. Τότε, η υποομάδα της G που παράγεται από το X ορίζεται ως*

$$\langle X \rangle = \bigcap_{X \subset H \leqslant G} H$$

Μια πιο χρήσιμη περιγραφή της ομάδας $\langle X \rangle$ περιγράφεται στην επόμενη άσκηση. Μια *λέξη* στο X ορίζεται να είναι ένα στοιχείο $w \in G$ με

$$w = x_1^{e_1} x_2^{e_2} ... x_k^{e_k}$$

με $x_i \in X$, $e_i = \pm 1$ και $k \geqslant 1$.

Άσκηση 1.34. *Δείξτε ότι η υποομάδα $\langle X \rangle$ είναι το σύνολο όλων των λέξεων στο X.*

Αν το X είναι ένα πεπερασμένο σύνολο, έστω $X = \{a_1, a_2, ..., a_n\}$, τότε συνήθως γράφουμε $\langle a_1, a_2, ..., a_n \rangle$ αντί για $\langle \{a_1, a_2, ..., a_n\} \rangle$. Ένα τέτοιο υποσύνολο μπορεί να υπάρχει, μπορεί και όχι.

Ορισμός 1.10. *Αν υπάρχει πεπερασμένο $X \subseteq G$ τέτοιο ώστε $\langle X \rangle = G$, τότε η G ονομάζεται πεπερασμένα παραγόμενη.*

Προφανώς κάθε πεπερασμένη ομάδα είναι πεπερασμένα παραγόμενη. Ωστόσο πολλές ενδιαφέρουσες άπειρες ομάδες δεν είναι πεπερασμένα παραγόμενες.

Άσκηση 1.35. *Δείξτε ότι η προσθετική ομάδα των ρητών δεν είναι πεπερασμένα παραγόμενη.*

Άσκηση 1.36. *Δείξτε ότι η πολλαπλασιαστική ομάδα των θετικών ρητών δεν είναι πεπερασμένα παραγόμενη.*

Αν H, K είναι δύο υποομάδες της G, τότε η ένωση τους δεν είναι πάντα ομάδα. Μπορούμε όμως πάντα να θεωρήσουμε την ομάδα που παράγεται από την ένωση τους:

$$H \vee K := \langle H \cup K \rangle$$

Πώς μπορούμε να περιγράψουμε καλύτερα αυτήν την ομάδα; Υπάρχει μια σημαντική ειδική περίπτωση, που θα μας φανεί χρήσιμη και στην διατύπωση του 2ου Θεωρήματος Ισομορφισμών. Ορίζουμε πρώτα το γινόμενο συνόλων: αν G ομάδα και $A, B \subset G$. Ορίζουμε το σύνολο γινόμενο

$$AB = \{ab : a \in A, b \in B\}.$$

Προφανώς αν το ένα από τα δύο σύνολα είναι υποσύνολο του άλλου, τότε τα δύο γινόμενα ταυτίζονται. Όμως στην γενική περίπτωση τα σύνολα AB, BA είναι εν γένει διαφορετικά μεταξύ τους. Αν τα δύο σύνολα είναι υποομάδες της H, K της G, υπό ποιές συνθήκες μπορεί να ισχύει $HK = KH$; Παρατηρούμε ότι πάντα ισχύει ο εγκλεισμός

$$H \cup K \subseteq HK \subseteq H \vee K,$$

$$H \cup K \subseteq KH \subseteq H \vee K.$$

Η επόμενη άσκηση σας καλεί να μελετήσετε πότε ισχύει η ισότητα των γινομένων.

Άσκηση 1.37. *Δείξτε ότι $HK = KH$ αν και μόνο αν $HK \leqslant G$, αν και μόνο αν $HK = H \vee K = KH$ (παρακάτω θα δούμε μία περίπτωση που αυτή η συνθήκη ικανοποιείται).*

Άσκηση 1.38. *(Τύπος γινομένου) Δείξτε ότι αν η G είναι πεπερασμένη και $H, K \leqslant G$, τότε*

$$|HK||H \cap K| = |H||K|.$$

Άσκηση 1.39. *Αν $H < G$, δείξτε ότι $G = \langle G - H \rangle$.*

1.6 Σύμπλοκα, κανονικές υποομάδες και ομάδες-πηλίκα

Μια ειδική περίπτωση του γινομένου συνόλων είναι όταν $A = H \leqslant G$ και $B = \{g\}$ με $g \in G$, και τότε τα γινόμενα

$$Hg := H\{g\},$$
$$gH := \{g\}H$$

ονομάζονται αντίστοιχα το δεξί σύμπλοκο και το αριστερό σύμπλοκο της H στην G που περιέχουν το στοιχείο g. Τα σύνολα αυτά έχουν την ιδιότητα ότι διασπούν την ομάδα G, δηλαδή την διαμερίζουν σε ξένα μεταξύ τους υποσύνολα.

Θεώρημα 1.2. *Αν $H \leqslant G$, τότε $Hx = Hy$ αν και μόνο αν $xy^{-1} \in H$ και $xH = yH$ αν και μόνο αν $y^{-1}x \in H$. Επιπλέον αν δύο δεξιά (αντίστοιχα αριστερά) σύμπλοκα δεν ταυτίζονται, τότε είναι μεταξύ τους ξένα.*

Απόδειξη. Έστω $Hx = Hy$, τότε $x = ex \in Hx = Hy$, άρα υπάρχει $h \in H$ τέτοιο ώστε $x = hy$, δηλαδή $xy^{-1} = h \in H$. Αντίστροφα, αν $xy^{-1} = h \in H$, τότε $x = hy$. Άρα για κάθε $h' \in H$ έχουμε $h'x = h'hy \in Hy$ που μας δίνει $Hx \subseteq Hy$, ενώ ομοίως για κάθε $h' \in H$ έχουμε $h'y = h'h^{-1}x \in Hx$ που μας δίνει $Hy \subseteq Hx$. Η αντίστοιχη σχέση για τα αριστερά σύμπλοκα έπεται ομοίως.

Αν δύο δεξιά σύμπλοκα Hx, Hy δεν είναι μεταξύ τους ξένα, τότε υπάρχει $g \in Hx \cap Hy$, άρα υπάρχουν $h, h' \in H$ τέτοια ώστε $hx = g = h'y$, που συνεπάγεται ότι $xy^{-1} = h^{-1}h' \in H$. Άρα, από το πρώτο σκέλος του θεωρήματος συμπεραίνουμε πως τα δύο σύμπλοκα ταυτίζονται. □

Συμπεραίνουμε πως η σχέση $x \sim y$ αν και μόνο αν $xy^{-1} \in H$ ορίζει μια σχέση ισοδυναμίας μέσα στην G (αντίστοιχα για την σχέση $x^{-1}y \in H$).

Αν και εν γένει τα δεξιά με τα αριστερά σύμπλοκα μιας ομάδας μπορεί να μην ταυτίζονται ως σύνολα, η παραπάνω συζήτηση μας υποδεικνύει ότι το πλήθος τους δείχνει να είναι το ίδιο. Για να το δούμε αυτό πιο ξεκάθαρα, αρκεί να ορίσουμε μια απεικόνιση από την οικογένεια L των αριστερών συμπλόκων της H στην οικογένεια R των δεξιών συμπλόκων της H που είναι αντιστοιχία. Αν ορίσουμε την απεικόνιση

$$f : L \to R$$

με

$$f(xH) = Hx,$$

αυτή η απεικόνιση δεν είναι καλά ορισμένη. Αντιθέτως, η απεικόνιση

$$f(xH) = Hx^{-1},$$

δουλεύει.

Πρόταση 1.2. *Η παραπάνω απεικόνιση είναι αντιστοιχία μεταξύ αριστερών και δεξιών συμπλόκων της H στην G.*

Απόδειξη. Πρώτα δείχνουμε ότι η απεικόνιση είναι καλά ορισμένη. Πράγματι, αν $xH = yH$ τότε $y^{-1}x \in H$, άρα $(y^{-1}x)^{-1} = x^{-1}y \in H$, κι άρα από το προηγούμενο θεώρημα έχουμε $Hx^{-1} = Hy^{-1}$. Για να δείξουμε ότι η απεικόνιση είναι ένα-προς-ένα ακολουθούμε τον παραπάνω συλλογισμό αντίστροφα. Το ότι η απεικόνιση είναι επί είναι άμεσο. □

Συμπεραίνουμε πως, αν και τα αριστερά και τα δεξιά σύμπλοκα μιας υποομάδας H της G μπορεί να διαφέρουν ως σύνολα, εντούτοις ο ακόλουθος ορισμός έχει νόημα.

Ορισμός 1.11. *Το πλήθος των αριστερών (ισοδύναμα, των δεξιών) συμπλόκων της υποομάδας H στην G ονομάζεται δείκτης της H στην G και συμβολίζεται με $[G : H]$.*

Αν έχουμε δύο ξένα μεταξύ τους αριστερά σύμπλοκα xH, yH της H στην G, τότε $|xH| = |yH|$. Αυτό προκύπτει εύκολα από το γεγονός ότι η απεικόνιση

$$f : H \to xH, \quad f(h) = xh$$

είναι αντιστοιχία. Συμπεραίνουμε λοιπόν εύκολα το βασικότερο θεώρημα της Θεωρίας ομάδων.

Θεώρημα 1.3. *(Lagrange) Έστω G μια ομάδα και H μια υποομάδα της. Τότε*

$$|G| = [G : H]|H|.$$

Αν και ίδια σε πλήθος, τα αριστερά και τα δεξιά σύμπλοκα μιας υποομάδας σπανίως ταυτίζονται, και όταν αυτό συμβαίνει είναι ιδιαίτερης σημασίας. Μια τέτοια υποομάδα έχει πολλές καλές ιδιότητες.

Ορισμός 1.12. *Μια υποομάδα H της G ονομάζεται κανονική αν και μόνο αν τα αριστερά και τα δεξιά της σύμπλοκα ταυτίζονται. Δηλαδή, εάν $gH = Hg$ για κάθε $g \in G$ (ισοδύναμα εάν $gHg^{-1} = H$ για κάθε $g \in G$). Σε αυτήν την περίπτωση γράφουμε $H \trianglelefteq G$.*

Συχνά, μια κανονική υποομάδα μιας ομάδας συμβολίζεται με N (από το normal) ή K (η σημασία αυτού του ονόματος θα φανεί σε λίγο). Προφανώς για κάθε ομάδα G έχουμε $G \trianglelefteq G$, $\{e\} \trianglelefteq G$. Ενδέχεται όμως μια ομάδα να μην έχει άλλες (μη τετριμμένες) κανονικές υποομάδες. Ο ακόλουθος ορισμός είναι από τους σημαντικότερους στην Θεωρία ομάδων.

Ορισμός 1.13. *Μια ομάδα G ονομάζεται απλή αν οι μόνες κανονικές υποομάδες της είναι η τετριμμένη και ο εαυτός της.*

Η Θεωρία των απλών ομάδων (ειδικότερα, των απλών πεπερασμένων ομάδων) είναι εξαιρετικά πλούσια. Σημειώνουμε εδώ πως για να αποδειχθεί η κανονικότητα μιας υποομάδας $K \leqslant G$, αρκεί να αποδειχθεί ότι $i_g(K) := gKg^{-1} \leqslant K$ για κάθε $g \in G$.

Αν έχουμε έναν ομομορφισμό ομάδων $\phi : G \to H$, μία πολύ σημαντική ιδιότητα του πυρήνα $\ker \phi$ είναι το γεγονός πως ικανοποιεί την παραπάνω συνθήκη. Με άλλα λόγια, κάθε πυρήνας ομομορφισμού είναι κανονική ομάδα: $\ker \phi \trianglelefteq G$.

Ορισμός 1.14. *Δύο στοιχεία $x, y \in G$ ονομάζονται συζυγή εάν υπάρχει $g \in G$ με $y = i_g(x) = gxg^{-1}$. Η κλάση συζυγίας x^G ενός στοιχείου $x \in G$ είναι το σύνολο όλων των συζυγών στοιχείων του x.*

Η σχέση $x \sim y$ αν και μόνο αν τα x, y είναι συζυγή, είναι σχέση ισοδυναμίας. Άρα οι κλάσεις ισοδυναμίας μιας ομάδας είναι ξένα μεταξύ τους υποσύνολα που διαμερίζουν την ομάδα.

Άσκηση 1.40. *Αποδείξτε ότι δύο συζυγή μεταξύ τους στοιχεία έχουν την ίδια τάξη.*

Παρατηρούμε λοιπόν πως μια υποομάδα είναι κανονική αν και μόνο αν είναι κλειστή υπό συζυγίες, δηλαδή αν και μόνο αν είναι ξένη ένωση κλάσεων συζυγίας.

Οι κανονικές υποομάδες είναι κυρίως σημαντικές διότι μπορούμε να ορίσουμε δομή ομάδας στον χώρο των συμπλόκων τους, τον ονομαζόμενο χώρο-πηλίκο, που συμβολίζεται με G/K. Προσέξτε ότι εδώ δεν έχει σημασία αν θεωρούμε τα αριστερά ή τα δεξιά σύμπλοκα της K αφού η K είναι κανονική.

Θεώρημα 1.4. *Αν $K \trianglelefteq G$, τότε ο χώρος των συμπλόκων της K αποκτά δομή ομάδας που συμβολίζεται με G/K.*

Η ομάδα αυτή ονομάζεται ομάδα-πηλίκο της G modulo K. Παρατηρούμε πως η τάξη της ομάδας πηλίκο G/K είναι προφανώς $[G : K]$.

Απόδειξη. Ορίζουμε την πράξη στα αριστερά σύμπλοκα της K στην G ως εξής:

$$(xK)(yK) = xyK.$$

Εύκολα επαληθεύεται ότι η κανονικότητα της K μας δίνει ότι η η πράξη είναι καλά ορισμένη:

$$xKyK = x(yKy^{-1})yK = xyKK = xyK,$$

όπου στην τελευταία ισότητα χρησιμοποιήσαμε απλά ότι η K είναι υποομάδα της G. Παρατηρούμε ότι το ουδέτερο στοιχείο της πράξης είναι το σύμπλοκο K (το σύμπλοκο του e). Παρατηρούμε επίσης πως $(xK)^{-1} = x^{-1}K$. □

Άσκηση 1.41. *Αν $K \trianglelefteq G$, τότε η απεικόνιση*

$$\pi_K : G \to G/K$$

με $\pi(g) = gK$ είναι επιμορφισμός με $\ker(\pi_K) = K$.

Άρα κάθε κανονική υποομάδα $K \trianglelefteq G$ είναι πυρήνας κάποιου ομομορφισμού $\phi : G \to H$ σε κάποια ομάδα H. Αυτός είναι και ο λόγος που δικαιολογεί τον συμβολισμό K για τις κανονικές υποομάδες (από τον αγγλικό όρο kernel).

Ορίζουμε τέλος ακόμα μια πολύ σημαντική υποομάδα της G, η οποία επίσης μετράει πόσο πολύ απέχει μια ομάδα από το να είναι αβελιανή. Η άσκηση 1.46 δείχνει ότι η ομάδα αυτή ελέγχει πότε μια ομάδα πηλίκο της G είναι αβελιανή.

Ορισμός 1.15. *Αν $x, y \in G$, ορίζουμε τον αντιμεταθέτη τους να είναι η ποσότητα*

$$[x, y] := xyx^{-1}y^{-1}.$$

Η αντιμεταθέτρια (ή παράγουσα) υποομάδα G' της G ορίζεται να είναι η ομάδα που παράγεται από όλους τους αντιμεταθέτες, δηλαδή

$$G' = \langle [x, y] : x, y \in G \rangle .$$

Παρατηρούμε ότι η G είναι αβελιανή αν και μόνο αν $[x, y] = e$ για κάθε $x, y \in G$, δηλαδή αν και μόνο αν $G' = \{e\}$. Δηλαδή οι αβελιανές ομάδες έχουν τετριμμένη παράγουσα υποομάδα. Στο άλλο άκρο, έχει μια ξεχωριστή κλάση ομάδων.

Ορισμός 1.16. *Μια ομάδα G λέγεται τέλεια εάν $G' = G$.*

Πρέπει εδώ να τονίσουμε ότι αν και το κέντρο και η παράγουσα είναι δύο υποομάδες που και οι δύο μετράνε πόσο πολύ απέχει μια ομάδα από το να είναι αβελιανή, εντούτοις δεν υπάρχει άμεση συσχέτιση μεταξύ των μεγεθών τους. Θα επανέλθουμε στην σχετική συζήτηση όταν θα μελετήσουμε τις μηδενοδύναμες ομάδες.

Άσκηση 1.42. *Δείξτε ότι σε μια αβελιανή ομάδα G κάθε υποομάδα της είναι κανονική. Δείξτε επίσης ότι το αντίστροφο δεν ισχύει. Συμπεράνατε πως οι μόνες απλές αβελιανές ομάδες είναι οι κυκλικές με τάξη πρώτο αριθμό.*

Άσκηση 1.43. *Αν $K \leqslant H \leqslant G$ και $K \trianglelefteq G$ τότε και $K \trianglelefteq H$.*

Άσκηση 1.44. *Αν οι H, K είναι κανονικές υποομάδες της G, δείξτε ότι $H \vee K \trianglelefteq G$.*

Άσκηση 1.45. *(a) Αν $[G : H] = 2$, τότε $H \trianglelefteq G$ και $g^2 \in H$ για κάθε $g \in G$.*

(b) Αν $[G : H] = n > 2$ και $H \trianglelefteq G$ τότε $g^n \in H$ για κάθε $g \in G$.

Άσκηση 1.46. *Δείξτε ότι $G' \trianglelefteq G$. Επίσης, αν $H \trianglelefteq G$, τότε η G/H είναι αβελιανή αν και μόνο αν $G' \leqslant H$.*

Άσκηση 1.47. *Δείξτε ότι $Z(G) \trianglelefteq G$. Δείξτε ότι αν η $G/Z(G)$ είναι κυκλική, τότε η G είναι αβελιανή. Συμπεράνατε πως αν η G είναι μη αβελιανή με $|G| = pq$, όπου p, q πρώτοι, τότε η G είναι centerless.*

Άσκηση 1.48. *(a) Δείξτε ότι $G/Z(G) \simeq Inn(G)$ και $Inn(G) \trianglelefteq Aut(G)$.*
(b) Η G είναι αβελιανή αν και μόνο αν η $Inn(G)$ είναι τετριμμένη.
(c) Αν η G δεν είναι αβελιανή τότε η $Aut(G)$ δεν είναι κυκλική.

Άσκηση 1.49. *Δείξτε πως για $n \geqslant 3$ έχουμε $Inn(S_n) \cong S_n$.*

Άσκηση 1.50. *Έστω $H \trianglelefteq G$, $\pi : G \to G/H$ ο φυσικός επιμορφισμός και $X \subseteq G$ ένα σύνολο με $\langle \pi(X) \rangle = G/H$. Δείξτε ότι $G = \langle H \cup X \rangle$.*

Άσκηση 1.51. *Αν το $\mathbb{F}$ είναι σώμα δείξτε ότι $SL_n(\mathbb{F}) \trianglelefteq GL_n(\mathbb{F})$.*

Άσκηση 1.52. *Έστω μια ομάδα G περιττής τάξης και*

$$x = \prod_{g \in G} g^m$$

για κάποιο $m \geqslant 1$. Δείξτε ότι $x \in G'$.

Άσκηση 1.53. *(a) (Νόμος του Dedekind) Αν $A, B, C \leqslant G$ και $A \subseteq B$ τότε*

$$A(B \cap C) = B \cap AC.$$

(b) Έστω $H \leqslant K \leqslant G$ και $N \trianglelefteq G$. Δείξτε ότι αν $HN = KN$ και $H \cap N = K \cap N$ τότε $H = K$.

1.7 Θεωρήματα ισομορφισμών και αντιστοιχίας

Υπάρχουν τρία βασικά θεωρήματα που περιγράφουν την σχέση μεταξύ ομομορφισμών, κανονικών υποομάδων και ομάδων πηλίκα. Τα τρία αυτά θεωρήματα, που διατυπώθηκαν από την E. Noether, είναι γνωστά ως τα Θεωρήματα Ισομορφισμών. Το πρώτο εξ' αυτών ονομάζεται και Θεμελιώδες Θεώρημα ισομορφισμών.

Θεώρημα 1.5. *(Πρώτο Θεώρημα Ισομορφισμών) Αν $\phi : G \to H$ είναι ένας ομομορφισμός με $K = \ker(\phi)$. Τότε $G/K \simeq \operatorname{Im}\phi$.*

Απόδειξη. Ορίζουμε την απεικόνιση $\tilde{\phi} : G/K \to \operatorname{Im}\phi$ με $\tilde{\phi}(gK) = \phi(g)$. Θα δείξουμε ότι η απεικόνιση είναι ισομορφισμός.

Παρατηρούμε πρώτα πως η απεικόνιση $\tilde{\phi}$ είναι καλά ορισμένη, διότι αν έχουμε $g_1K = g_2K$, τότε $g_1g_2^{-1} \in K$, δηλαδή $\phi(g_1g_2^{-1}) = e$, άρα $\phi(g_1) = \phi(g_2)$. Προφανώς η απεικόνιση είναι επί διότι κάθε στοιχείο της εικόνας $\operatorname{Im}\phi$ είναι της μορφής $\phi(g)$ για κάποιο $g \in G$ και τότε έχουμε $\tilde{\phi}(gK) = \phi(g)$. Για να δείξουμε ότι είναι ένα-προς-ένα, παρατηρούμε πως εάν $\phi(g_1) = \phi(g_2)$ τότε $g_1g_2^{-1} \in \ker\phi = K$ και άρα $g_1K = g_2K$.

Ως τελευταίο βήμα, πρέπει να δείξουμε ότι η απεικόνιση που ορίσαμε είναι ομομορφισμός. Αυτό όμως έπεται από το γεγονός ότι η ίδια η απεικόνιση ϕ είναι ομομορφισμός:

$$\tilde{\phi}(g_1Kg_2K) = \tilde{\phi}(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \tilde{\phi}(g_1K)\tilde{\phi}(g_2K),$$

και η απόδειξη είναι πλήρης. □

Εδώ μπορούμε να κάνουμε την εξής κρίσιμη παρατήρηση. Κάθε ομομορφισμός $\phi : G \to H$ ορίζει έναν πυρήνα $\ker\phi \trianglelefteq G$ και μια εικόνα $\operatorname{Im}\phi \leqslant H$. Δοθέντος λοιπόν ενός ομομορφισμού, πρέπει πάντα να ψάχνουμε τον πυρήνα του και την εικόνα του καθώς αυτά τα δύο σύνολα τον καθορίζουν. Αντίστροφα, δοθείσης κανονικής υποομάδας $K \trianglelefteq G$, θα πρέπει πάντα να ψάχνουμε έναν ομομορφισμό ϕ που να έχει πυρήνα την K.

Για να περιγράψουμε το Δεύτερο Θεώρημα ισομορφισμών, επανερχόμαστε στο ερώτημα πότε το γινόμενο δύο υποομάδων $H, K \leqslant G$ είναι υποομάδα της G (άσκηση 1.37). Όπως δείχνει η επόμενη άσκηση, μία ικανή συνθήκη είναι όταν η μία εκ των δύο υποομάδων είναι κανονική.

Άσκηση 1.54. *Αν η μία εκ των υποομάδων H, K είναι κανονική στην G, τότε $HK = KH$.*

Μία ακόμη πολύ χρήσιμη παρατήρηση είναι η ακόλουθη: εάν $K \trianglelefteq G$ και η H δεν περιέχει την K, τότε $K \leqslant HK \leqslant G$ και επιπλέον $K \trianglelefteq HK$. Σε αυτήν την περίπτωση η ομάδα πηλίκο HK/K αποτελείται από όλα τα σύμπλοκα της μορφής $hkK = hK$, με $h \in H, k \in K$.

Εάν λοιπόν θεωρήσουμε τον φυσικό επιμορφισμό $\pi_K : G \to G/K$, που έχει πυρήνα την υποομάδα K, και θεωρήσουμε τον περιορισμό της $\pi_K|_H$ σε μια υποομάδα $H \leqslant G$, τότε από το Πρώτο Θεώρημα Ισομορφισμών παίρνουμε

$$\frac{H}{\ker(\pi_K|_H)} \simeq \mathrm{Im}(\pi_K|_H).$$

Θέλουμε τώρα να περιγράψουμε καλύτερα τον παραπάνω πυρήνα και την αντίστοιχη εικόνα. Ο πυρήνας του $\pi_K|_H$ δίνεται ως

$$\begin{aligned} \ker(\pi_K|_H) &= \{h \in H : hK = K\} \\ &= \{h \in H : h \in K\} \\ &= H \cap K. \end{aligned}$$

Ειδικότερα, συμπεραίνουμε πως $H \cap K \trianglelefteq H$. Η εικόνα $\mathrm{Im}(\pi_K|_H)$ δίνεται ως το σύνολο $\{hK : h \in H\}$ όλων των συμπλόκων της K που περιέχουν τα στοιχεία $h \in H$, και από την προηγούμενη συζήτηση αυτό το σύνολο είναι ακριβώς η ομάδα πηλίκο HK/K. Άρα αποδείξαμε το Δεύτερο Θεώρημα Ισομορφισμών:

Θεώρημα 1.6. *Έστω $H \leqslant G$ και $K \trianglelefteq G$. Τότε $H \cap K \trianglelefteq H$ και*

$$\frac{H}{H \cap K} \simeq \frac{HK}{K}.$$

Ερχόμαστε τώρα στο τρίτο Θεώρημα ισομορφισμών, το οποίο μας δίνει περισσότερη πληροφορία για την δομή της G όταν έχω δύο υποομάδες της που η μία να περιέχει την άλλη, δηλαδή $K \leqslant H \leqslant G$ και επιπλέον $K, H \trianglelefteq G$.

Θεώρημα 1.7. *Έστω $K \leqslant H \leqslant G$ με $H \trianglelefteq G$ και $K \trianglelefteq G$. Τότε $H/K \trianglelefteq G/K$ και*

$$\frac{G/K}{H/K} \simeq \frac{G}{H}.$$

Απόδειξη. Θεωρούμε την απεικόνιση $\phi : G/K \to G/H$ με $\phi(gK) = gH$. Η απεικόνιση αυτή είναι καλά ορισμένη διότι αν $g_1K = g_2K$ τότε $g_1g_2^{-1} \in K \leqslant H$ άρα $g_1H = g_2H$. Προφανώς η απεικόνιση είναι επί ενώ εύκολα αποδεικνύεται πως είναι ομομορφισμός. Ο πυρήνας της ϕ είναι η ομάδα

$$\ker \phi = \{gK : gH = H\} = \{gK : g \in H\} = H/K$$

και το ζητούμενο έπεται. □

Μία φυσιολογική επέκταση του τρίτου Θεωρήματος ισομορφισμών είναι το Θεώρημα της αντιστοιχίας, που περιγράφει τις υποομάδες μια ομάδας πηλίκο.

Θεώρημα 1.8. *(Αντιστοιχίας) Έστω $K \trianglelefteq G$. Τότε οι υποομάδες (αντίστ. κανονικές υποομάδες) της ομάδας πηλίκο G/K βρίσκονται σε ένα-προς-ένα αντιστοιχία με της υποομάδες (αντίστ. κανονικές υποομάδες) της G που περιέχουν την K.*

Απόδειξη. Περιγράφουμε την βασική ιδέα της απόδειξης και αφήνουμε τις λεπτομέρειες στον αναγνώστη. Η βασική ιδέα εδώ είναι η εξής: αν $K \leqslant H \leqslant G$, τότε ο φυσικός επιμορφισμός $\pi_K : G \to G/K$ απεικονίζει την H στην $\pi_K(H) = H/K \leqslant G/K$. Η απεικόνιση αυτή είναι αντιστοιχία (ένα-προς-ένα και επί). Επιπλέον, το Τρίτο Θεώρημα Ισομορφισμών συνεπάγεται την αντιστοιχία όταν οι αντίστοιχες υποομάδες είναι κανονικές. □

Άσκηση 1.55. *Μία $H \leqslant G$ λέγεται μέγιστη (maximal) υποομάδα εάν δεν υπάρχει άλλη $K \leqslant G$ με $H \leqslant K$. Δείξτε ότι αν μία τέτοια H είναι κανονική υποομάδα της G, τότε ο δείκτης της στην G είναι ίσος με κάποιον πρώτο αριθμό p.*

Άσκηση 1.56. *Μία $K \trianglelefteq G$ λέγεται μέγιστη (maximal) κανονική υποομάδα εάν δεν υπάρχει άλλη $N \trianglelefteq G$ με $K \leqslant N$. Δείξτε ότι η $K \trianglelefteq G$ είναι μέγιστη κανονική αν και μόνο αν η G/K είναι απλή.*

Άσκηση 1.57. *Έστω $H \leqslant G$ απλή και δείκτου 2. Αν η H δεν είναι η μοναδική κανονική υποομάδα της G, δείξτε ότι υπάρχει $K \trianglelefteq G$ με $|K| = 2$ και $G \simeq H \times K$.*

Άσκηση 1.58. *Έστω $K \trianglelefteq G$ με $G/K \simeq \mathbb{Z}$. Δείξτε ότι για κάθε $n \geqslant 1$ υπάρχει $K_n \trianglelefteq G$ τέτοια ώστε $[G : K_n] = n$.*

Άσκηση 1.59. *Εάν $H \trianglelefteq G$, έπεται ότι η G περιέχει υποομάδα ισόμορφη με την G/H;*

Άσκηση 1.60. *Συμπληρώστε τις λεπτομέρειες της απόδειξης του Θεωρήματος Αντιστοιχίας.*

1.8 Ευθέα γινόμενα

Έχουμε ήδη δει στην άσκηση 1.3 πως αν H, K είναι δύο ομάδες, τότε ορίζεται το ευθύ γινόμενο $H \times K$ τους με την πράξη που ορίζεται κατά συντεταγμένες. Επιπλέον $H \simeq H \times \{e\} \trianglelefteq H \times K$ και $K \simeq \{e\} \times K \trianglelefteq H \times K$.

Μας απασχολεί το αντίστροφο ερώτημα. Αν μας δοθεί μια ομάδα G, μπορούμε να εξετάσουμε αν $G \simeq H \times K$ για κάποιες υποομάδες της H και K;

Θεώρημα 1.9. *Έστω $H, K \trianglelefteq G$. Αν $G = HK$ και $H \cap K = \{e\}$, τότε $G \simeq H \times K$.*

Απόδειξη. Για κάθε $g \in G$ μπορούμε εξ' υποθέσεως να βρούμε $h \in H, k \in K$ τέτοια ώστε $g = hk$. Ισχυριζόμαστε ότι αυτή η γραφή είναι μοναδική. Διότι αν υποθέσουμε πως $h_1k_1 = g = h_2k_2$, τότε $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, άρα $h_1 = h_2$ και $k_1 = k_2$.

Ορίζουμε την απεικόνιση $f : G \to H \times K$ με $f(g) = (h, k)$. Η προηγούμενη παρατήρηση δείχνει ότι η απεικόνιση αυτή είναι καλά ορισμένη. Θέλουμε να δείξουμε ότι είναι και ισομορφισμός. Η απόδειξη πως η f είναι ένα-προς-ένα και επί είναι πάρα πολύ απλή και αφήνεται ως άσκηση για τον προσεκτικό αναγνώστη.

Η μέθοδος που χρησιμοποιούμε για να αποδείξουμε ότι η f είναι ομομορφισμός είναι λίγο λεπτή. Θέλουμε να δείξουμε ότι $f(g_1)f(g_2) = f(g_1g_2)$ για κάθε δύο στοιχεία $g_1 = h_1k_1, g_2 = h_2k_2$ της G. Με άλλα λόγια, αρκεί να δείξουμε ότι ισχύει

$$(h_1, k_1)(h_2, k_2) = f(h_1k_1h_2k_2)$$

για κάθε $h_1, h_2 \in H$, $k_1, k_2 \in K$. ’Ομως το αριστερό μέρος είναι απλά ίσο με (h_1h_2, k_1k_2). Αν ξέραμε ότι $k_1h_2 = h_2k_1$ θα είχαμε δείξει το ζητούμενο. Με άλλα λόγια, ζητάμε κάθε στοιχείο της H να αντιμετατίθεται με κάθε στοιχείο της K. Για να το αποδείξουμε αυτό, αρκεί να παρατηρήσουμε ότι η κανονικότητα των H, K συνεπάγεται πως για κάθε h, k ο αντιμεταθέτης

$$khk^{-1}h^{-1} = (khk^{-1})h^{-1} \in H \times H = H$$

και ομοίως

$$khk^{-1}h^{-1} = k(hk^{-1}h^{-1}) \in K \times K = K.$$

Άρα $khk^{-1}h^{-1} = e$ και έχουμε τελειώσει. □

Πόρισμα 1.1. *Αν $A \trianglelefteq H$ και $B \trianglelefteq K$, τότε $A \times B \trianglelefteq H \times K$ και*

$$\frac{H \times K}{A \times B} \simeq \frac{H}{A} \times \frac{K}{B}.$$

Απόδειξη. Ορίζουμε τον επιμορφισμό

$$\phi : H \times K \to \frac{H}{A} \times \frac{K}{B}$$

με τύπο $\phi(h, k) = (hA, kB)$. Ο πυρήνας του είναι η υποομάδα

$$\ker \phi = \{(h, k) : hA = A, kB = B\} = \{(h, k) : h \in A, k \in B\} = A \times B,$$

και το συμπέρασμα έπεται από το 1ο Θεώρημα ισομορφισμών. □

Υπάρχει μία λεπτή διαφορά ανάμεσα στους δύο τρόπους που μπορεί κανείς να αντιλαμβάνεται ένα ευθύ γινόμενο ομάδων, όπως αυτοί περιγράφονται από το Θεώρημα 1.9. Η θέαση της G ως το ευθύ (καρτεσιανό) γινόμενο $H \times K$ δύο κανονικών υποομάδων της ονομάζεται *εξωτερική* σκοπιά. Αντίθετα, η (ισομορφική) θέαση της G ως το γινόμενο HK δύο κανονικών υποομάδων της με τετριμμένη τομή ονομάζεται και *εσωτερική* σκοπιά. Για παράδειγμα, η εσωτερική σκοπιά μας επιτρέπει να γράφουμε εν συντομία

$$\frac{H \times K}{H} \simeq K,$$

αντί για

$$\frac{H \times K}{H \times \{e\}} \simeq \{e\} \times K.$$

Άσκηση 1.61. *Αν $N \trianglelefteq H \times K$ ισχύει ότι $N \simeq A \times B$ για κάποια $A \trianglelefteq H$ και $B \trianglelefteq K$; Αν όχι, ισχύει αν υποθέσουμε έξτρα συνθήκες στις H, K; Υπάρχει κάποιος εύχρηστος γενικός τρόπος να περιγράψουμε τις κανονικές υποομάδες του γινομένου $H \times K$;*

1.9 Περισσότερη θεωρία συμμετρικών ομάδων

Κλείνουμε με μια επανάληψη κάποιων ακόμα βασικών στοιχείων της θεωρίας των ομάδων μεταθέσεων.

Το πρώτο σημαντικό γεγονός για την ομάδα S_n είναι πως κάθε στοιχείο της σ επιδέχεται δύο ειδών παραγοντοποιήσεις, η κάθεμια εκ των οποίων έχει την δική της ξεχωριστή σημασία. Η πρώτη παραγοντοποίηση είναι η ανάλυση σε *γινόμενο ξένων κύκλων με μοναδικό τρόπο* και η δεύτερη είναι η ανάλυση σε *ανάλυση σε γινόμενο αντιμεταθέσεων*. Η δεύτερη ανάλυση δεν είναι μοναδική, διαμερίζει όμως τα στοιχεία της S_n σε δύο ξένα σύνολα.

Μία τυχαία μετάθεση $\sigma \in S_n$ που στέλνει κάθε $x \in X_n$ στο στοιχείο $\sigma(x) \in X_n$ την συμβολίζουμε, όπως είπαμε και νωρίτερα, με

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \sigma(1) & \sigma(2) & \sigma(3) & ... & \sigma(n) \end{pmatrix}.$$

Για να περιγράψουμε την ανάλυση σε ξένους κύκλους, χρειαζόμαστε τον εξής ορισμό:

Ορισμός 1.17. *Μία $\sigma \in S_n$ σταθεροποιεί ένα στοιχείο $x \in X_n$ εάν $\sigma(x) = x$.*

Ορισμός 1.18. *Αν μία $\sigma \in S_n$, για κάποια $i_1, i_2, ..., i_k \in X_n$ με $k \leqslant n$, ικανοποιεί την συνθήκη $\sigma(i_m) = i_{m+1}$ και $\sigma(i_k) = i_1$ και σταθεροποιεί όλα τα υπόλοιπα στοιχεία του X_n τότε λέμε ότι η σ είναι ένας κύκλος μήκους k (ή πιο σύντομα, ένας k-κύκλος) και συμβολίζεται με $(i_1\, i_2 \ldots i_k)$.*

Ορισμός 1.19. *Δύο μεταθέσεις $\sigma, \tau \in S_n$ λέγονται ξένες εάν $\sigma(x) \neq x$ συνεπάγεται $\tau(x) = x$ και $\tau(x) \neq x$ συνεπάγεται $\sigma(x) = x$.*

Προσέξτε πως δύο ξένες μεταθέσεις δεν απαγορεύεται να σταθεροποιούν κάποια κοινά στοιχεία, δηλαδή μπορεί να ισχύει $\sigma(x) = x = \tau(x)$ για κάποια $x \in X$.

Θεώρημα 1.10. *Κάθε $\sigma \in S_n$ μπορεί να αναλυθεί με μοναδικό τρόπο σαν γινόμενο ξένων κύκλων.*

Απόδειξη. Η απόδειξη γίνεται με επαγωγή στο n και αφήνεται σαν άσκηση. □

Αυτή λοιπόν είναι η πρώτη ανάλυση που μπορούμε να κάνουμε σε κάθε μετάθεση. Για να την κάνουμε πιο σαφή, μελετάμε ένα απλό παράδειγμα.

Παράδειγμα 1.5. *Αν θεωρήσουμε τις μεταθέσεις που είχαμε και στην Υποενότητα 1.3, δηλαδή τις*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 5 & 3 \end{pmatrix}$$

που η σύνθεση τους έδινε την μετάθεση

$$\sigma\tau := \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix},$$

τότε οι μεταθέσεις αυτές αναλύονται σε ξένους κύκλους ως εξής:

$$\sigma = (1\,2)(3\,5\,4), \quad \tau = (1)(2\,4\,5\,3),$$

ενώ τα γινόμενα τους δίνονται ως

$$\sigma\tau = (1\,2\,3)(4)(5), \quad \tau\sigma = (1\,4\,2)(3)(5).$$

Το παραπάνω παράδειγμα μας δείχνει πως εν γένει δύο μεταθέσεις δεν αντιμετατίθονται (κάτι που το ξέραμε ήδη από την άσκηση 1.19). Ισχύει όμως το ακόλουθο:

Άσκηση 1.62. *Δείξτε πως δύο ξένοι κύκλοι αντιμετατίθονται.*

Ένας 2-κύκλος $(i\,j)$ καλείται και *αντιμετάθεση*. Αν και οι αντιμεταθέσεις είναι οι απλούστερες μεταθέσεις, εντούτοις είναι εξαιρετικά σημαντικές. Το επόμενο αποτέλεσμα δείχνει πως κάθε μετάθεση σαν γράφεται σαν γινόμενο αντιμεταθέσεων.

Θεώρημα 1.11. *Κάθε k-κύκλος γράφεται σαν γινόμενο $k-1$ το πλήθος αντιμεταθέσεων. Άρα κάθε μετάθεση γράφεται ως γινόμενο αντιμεταθέσεων.*

Απόδειξη. Αρκεί κανείς να ελέγξει ότι

$$(i_1\, i_2 \ldots i_k) = (i_1\, i_k)(i_1\, i_{k-1})\ldots(i_1\, i_3)(i_1\, i_2).$$

□

Η γραφή μιας μετάθεσης όμως σε γινόμενο αντιμεταθέσεων δεν είναι μοναδική, πχ. $(i\,j) = (i\,j)(i\,j)(i\,j)$. Αυτό που μένει όμως αναλλοίωτο είναι το πλήθος των αντιμεταθέσεων στην ανάλυση της σ modulo 2.

Ορισμός 1.20. *Αν η $\sigma \in S_n$ γράφεται ως γινόμενο r στο πλήθος κύκλων (συμπεριλαμβάνοντας και τους 1-κύκλους) τότε ορίζουμε το πρόσημο της σ ως*

$$sgn(\sigma) := (-1)^{n-r}.$$

Ο ορισμός αυτός μας δίνει άμεσα ότι αν $\tau = (i\,j)$ είναι μια αντιμετάθεση τότε η τ αποτελείται από $n-1$ στο πλήθος κύκλους (μαζί με τους τετριμμένους 1-κύκλους) κι άρα

$$sgn(\tau) = (-1)^{n-(n-1)} = -1.$$

Ακόμα, εάν $\sigma = \sigma_1 \dots \sigma_r$ είναι η ανάλυση μιας $\sigma \in S_n$ σε ξένους κύκλους, τότε έχουμε το ακόλουθο αποτέλεσμα.

Πρόταση 1.3. *Αν $\sigma = \sigma_1 \dots \sigma_r$ είναι η ανάλυση μιας $\sigma \in S_n$ σε ξένους κύκλους και $\tau = (i\,j)$ μια αντιμετάθεση τότε*

$$sgn(\tau\sigma) = -sgn(\sigma).$$

Απόδειξη. Η απόδειξη διακρίνει δύο περιπτώσεις, ανάλογα με το εάν τα i και j ανήκουν ή όχι στον ίδιο κύκλο της σ.

Αν ανήκουν στον ίδιο κύκλο της σ, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι ανήκουν στο σ_1. Τότε αν

$$\sigma_1 = (i\,c_1 \dots. c_k\, j\, d_1 \dots d_l), \quad k, l \geqslant 0$$

παίρνουμε

$$\tau\sigma_1 = (i\,c_1 \dots. c_k)(j\,d_1 \dots d_l),$$

δηλαδή ο πολλαπλασιασμός με τ αυξάνει κατά έναν το πλήθος των ξένων κύκλων:

$$\tau\sigma = (i\,c_1 \dots. c_k)\,(j\,d_1 \dots d_l)\,\sigma_2 \dots \sigma_r.$$

Τότε

$$sgn(\tau\sigma) = (-1)^{n-(r+1)} = -sgn(\sigma).$$

Αντίθετα, αν τα i και j δεν ανήκουν στον ίδιο κύκλο της σ, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι ανήκουν στα σ_1 και σ_2. Τότε αν γράψουμε

$$\sigma_1 = (i\,c_1 \dots. c_k), \quad k \geqslant 0$$

και

$$\sigma_2 = (j\,d_1 \dots. d_l), \quad l \geqslant 0$$

τότε παίρνουμε

$$\tau\sigma_1\sigma_2 = (i\,c_1 \dots. c_k\, j\, d_1 \dots d_l),$$

δηλαδή ο πολλαπλασιασμός με τ τώρα μειώνει κατά έναν το πλήθος των ξένων κύκλων, κι άρα

$$\tau\sigma = (i\,c_1 \dots. c_k)\,(j\,d_1 \dots d_l)\,\sigma_3 \dots \sigma_r,$$

οπότε

$$sgn(\tau\sigma) = (-1)^{n-(r-1)} = -sgn(\sigma).$$

□

Η απόδειξη πως η απεικόνιση του προσήμου είναι πάντα πολλαπλασιαστική, δηλαδή πως

$$sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$$

για κάθε $\sigma, \tau \in S_n$ είναι τώρα άμεση, αν θεωρήσουμε την σ σταθερή, γράψουμε την τ ως γινόμενο αντιμεταθέσεων και εφαρμόσουμε επαγωγή στο πλήθος των αντιμεταθέσεων της τ. Καλούμε τον αναγνώστη να γράψει αυτήν την ιδέα αυστηρά.

Άσκηση 1.63. *Αποδείξτε πως $sgn(\sigma\tau) = sgn(\sigma)sgn(\tau)$ για κάθε $\sigma, \tau \in S_n$.*

Ορισμός 1.21. *Αν μια $\sigma \in S_n$ μπορεί να γραφτεί ως γινόμενο άρτιου πλήθους αντιμεταθέσεων, τότε καλείται άρτια. Αλλιώς, καλείται περιττή.*

Θεώρημα 1.12. *Η $\sigma \in S_n$ είναι άρτια αν και μόνο αν $sgn(\sigma) = 1$. Άρα η σ είναι περιττή αν και μόνο αν $sgn(\sigma) = -1$.*

Απόδειξη. Γράφουμε την σ ως γινόμενο αντιμεταθέσεων

$$\sigma = \tau_1\, \tau_2 \ldots \tau_m.$$

Τότε, από την πολλαπλασιαστικότητα του προσήμου έχουμε

$$sgn(\sigma) = sgn(\tau_1)\, sgn(\tau_2) \ldots sgn(\tau_m) = (-1)^m.$$

Το ζητούμενο τώρα έπεται. □

Το σύνολο των άρτιων αντιμεταθέσεων της S_n αποτελεί υποομάδα της S_n. Η υποομάδα αυτή είναι εξαιρετικής σημασίας για την Θεωρία ομάδων.

Ορισμός 1.22. *Η υποομάδα των άρτιων αντιμεταθέσεων της S_n λέγεται εναλλάσουσα υποομάδα της S_n και συμβολίζεται με A_n.*

Άσκηση 1.64. *Δείξτε ότι η απεικόνιση $f : A_n \to S_n \backslash A_n$ με $f(\sigma) = (1\,2)\,\sigma$ είναι αντιστοιχία, κι άρα $|A_n| = |S_n|/2$. Δείξτε επίσης ότι η απεικόνιση $sgn : S_n \to \{\pm 1\}$ είναι επιμορφισμός. Συμπεράνατε πως $A_n \trianglelefteq S_n$.*

Άσκηση 1.65. *Αν η $\sigma \in S_n$ γράφεται ως γινόμενο ξένων κύκλων $\sigma = \sigma_1\sigma_2 \ldots \sigma_r$ και ο σ_i έχει μήκος k_i, δείξτε ότι η σ έχει τάξη ίση με εκπ$\{k_1, k_2, \ldots, k_r\}$.*

Άσκηση 1.66. *Αποδείξτε το Θεώρημα 1.10.*

Άσκηση 1.67. *Δείξτε ότι $Z(A_n) = \{e\}$ για $n \geqslant 4$.*

Άσκηση 1.68. *Δείξτε ότι δύο μεταθέσεις $\sigma, \tau \in S_n$ είναι συζυγείς αν και μόνο αν έχουν τον ίδιο τύπο ανάλυσης σε ξένους κύκλους, δηλαδή αν και μόνο αν η ανάλυση τους σε γινόμενο ξένων κύκλων έχει το ίδιο πλήθος r-κύκλων για κάθε $r \geqslant 1$.*

Άσκηση 1.69. *Δείξτε πως για $n \geqslant 4$ έχουμε $Inn(A_n) \cong A_n$.*

Άσκηση 1.70. ** Δείξτε ότι η A_n είναι απλή για $n \geqslant 5$ ενώ η A_4 έχει κανονική υποομάδα τάξης 4.*

1.10 Επαναληπτικές ασκήσεις πρώτου κεφαλαίου

Άσκηση 1.71. *Δείξτε ότι $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ αν $(m, n) = 1$, ενώ δεν ισχύει $\mathbb{Z}_{p^2} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$.*

Άσκηση 1.72. *Έστω G μια ομάδα που έχει ακριβώς τρεις υποομάδες. Δείξτε ότι $G \simeq \mathbb{Z}_{p^2}$.*

Άσκηση 1.73. *Αν μια ομάδα G έχει πεπερασμένο πλήθος διαφορετικών υποομάδων τότε είναι πεπερασμένη.*

Άσκηση 1.74. *Αν μια πεπερασμένη ομάδα G έχει άρτια τάξη, τότε έχει περιττό πλήθος στοιχείων τάξης 2. Αν $|G| = 2m$ με m περιττό και η G είναι αβελιανή, δείξτε ότι η G έχει μοναδικό στοιχείο τάξης 2.*

Άσκηση 1.75. *Έστω G πεπερασμένη ομάδα και $K \trianglelefteq G$ με μκδ$(|K|, |G/K|) = 1$. Δείξτε ότι η K είναι η μοναδική υποομάδα της G τάξης $|K|$.*

Άσκηση 1.76. *Δείξτε ότι η S_n είναι ισόμορφη με υποομάδα της A_{n+2} αλλά όχι της A_{n+1}.*

Άσκηση 1.77. *Δείξτε ότι αν το $\mathbb{F}$ είναι ένα πεπερασμένο σώμα, η πολλαπλασιαστική ομάδα του $\mathbb{F}^{\times}$ είναι κυκλική.*

Άσκηση 1.78. *Αν δύο στοιχεία $g, h \in G$ έχουν πεπερασμένη τάξη, μπορεί το γινόμενο τους να έχει άπειρη τάξη;*

Άσκηση 1.79. *Δείξτε ότι η ομάδα $(\mathbb{Z}, +)$ δεν είναι ισόμορφη με την $(\mathbb{Q}, +)$. Δείξτε επίσης ότι η $(\mathbb{Q}, +)$ δεν είναι ισόμορφη με την ομάδα $(\mathbb{Q}_{+}, \cdot)$.*

Άσκηση 1.80. *Αν $G \times K \cong G \times H$, τότε ισχύει ότι $K \cong H$?*

Άσκηση 1.81. *Αν $H \trianglelefteq G$ με H και G/H αβελιανές, έπεται ότι η G είναι αβελιανή;*

Άσκηση 1.82. *Πόσες (μη ισόμορφες) μη αβελιανές ομάδες τάξης 8 υπάρχουν; Πόσες μη αβελιανές ομάδες τάξης 12;*

Άσκηση 1.83. *Δείξτε ότι το αντίστροφο του Θεωρήματος του Lagrange δεν ισχύει για μη κυκλικές ομάδες: αν $d||G|$ δεν είναι απαραίτητο ότι υπάρχει υποομάδα $H \leqslant G$ τάξης d.*

Άσκηση 1.84. *Έστω G μία πεπερασμένη centerless ομάδα. Έπεται ότι η G είναι τέλεια;*

Άσκηση 1.85. *Εξηγήστε πως μπορούμε να ορίσουμε ευθέα γινόμενα περισσότερων ομάδων $G_1 \times G_2 \times ... \times G_n$ και αποδείξτε τα αντίστοιχα αποτελέσματα που δείξαμε για το ευθύ γινόμενο δύο ομάδων.*

Άσκηση 1.86. *Αν G, H είναι δύο ομάδες, τότε συμβολίζουμε με $Hom(G, H)$ το σύνολο των ομομορφισμών από την G στην H. Αν η H είναι αβελιανή, δείξτε ότι το σύνολο $Hom(G, H)$ είναι κι αυτό αβελιανή ομάδα.*

Άσκηση 1.87. * *Υπάρχει πεπερασμένη ομάδα G και H γνήσια κανονική υποομάδας της τέτοιες ώστε να ισχύει $|Aut(H)| > |Aut(G)|$;*

Άσκηση 1.88. * *Υπάρχει πεπερασμένη ομάδα G με την $Aut(G)$ να είναι απλή;*

Άσκηση 1.89. * *Έστω p πρώτος και $|G| = p^n$. Δείξτε ότι η G είναι κυκλική αν και μόνο αν είναι αβελιανή με μοναδική υποομάδα τάξης p.*

2 Δράσεις ομάδων

Σε αυτό το κεφάλαιο θα ορίσουμε και θα μελετήσουμε μία από τις πιο θεμελειώδεις έννοιες στην θεωρία ομάδων, την έννοια της δράσης μιας ομάδας G σε ένα σύνολο X. Η ιδέα της δράσης μιας ομάδας σε ένα σύνολο είναι πάρα πολύ γόνιμη, καθώς βρίσκεται στην καρδιά της γέννησης και της ιστορικής εξέλιξης της θεωρίας ομάδων.

Η ιδέα της δράσης μιας ομάδας σε ένα σύνολο κρύβει μέσα της την κατανόηση μιας ομάδας ως ένα δυναμικό αντικείμενο. Από αυτή την οπτική, μια ομάδα δεν είναι απλά ένα σύνολο με κάποια αλγεβρική δομή, αλλά ένα σύνολο 'μετασχηματισμών' κάποιου γεωμετρικού αντικειμένου ή ένα σύνολο 'αναδιατάξεων' κάποιου διακριτού συνόλου. Η πρώτη οπτική άνθησε μέσα από τις ιδέες των Klein, Lie και Poincaré. Η δεύτερη οπτική βρίσκεται στην καρδιά των πρώτων αποτελεσμάτων των Lagrange, Abel και Galois σχετικά με τις αναδιατάξεις των ριζών πολυωνύμων. Οι ομάδες μετασχηματισμών του κύκλου (που αποτελεί έναν από τους πιο απλούς ομογενείς χώρους) και των κανονικών πολυγώνων (διεδρικές ομάδες) περιγράφουν πολύ καλά την ιστορική σύνδεση και την αλληλεπίδραση ανάμεσα σε αυτές τις δύο διαφορετικές ιστορικές οπτικές, την συνεχή (Ομάδες Lie) και την διακριτή (Ομάδες Coxeter, κλπ.). Αυτός ήταν και ένας κύριος λόγος που, παρ' ότι οι απαρχές της θεωρίας ομάδων βρίσκονται στην μελέτη των ριζών πολυωνύμων, η θεωρία ομάδων βρήκε ευρεία εφαρμογή στην φυσική, στην γεωμετρία, στην γεωμετρία, στην θεωρία αριθμών και σε σχεδόν κάθε άλλον κλάδο των μαθηματικών.

Ξεκινάμε δίνοντας τους βασικούς γενικούς ορισμούς και μετά θα επικεντρωθούμε σε δύο πολύ σημαντικά παραδείγματα, αλγεβρικής φύσεως. Παραδείγματα που έρχονται μέσα από την ίδια την θεωρία ομάδων. Το κεφάλαιο αυτό επικεντρώνεται στην μελέτη των δράσεων ομάδων από αλγεβρικής/συνδυαστικής σκοπιάς. Στο επόμενο κεφάλαιο θα μελετήσουμε δράσεις ομάδων από πιο γεωμετρική σκοπιά.

2.1 Η έννοια της δράσης και παραδείγματα

Ορισμός 2.1. *Έστω G μια ομάδα και X ένα σύνολο. Λέμε ότι η G δρα στο X ή ότι το X είναι ένα G-σύνολο εάν υπάρχει μια απεικόνιση $f : G \times X \to X$ με $f(g,x) = g \cdot x$ τέτοια ώστε:*
(i) $e \cdot x = x$ για κάθε $x \in X$,
(ii) $g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$ για κάθε $g_1, g_2 \in G$ και για κάθε $x \in X$.

Αν η G δρα στο X για λόγους συντομίας και κομψότητας συνήθως θα γράφουμε απλά $G \circlearrowleft X$. Πριν προχωρήσουμε παρακάτω στην θεωρία, περιγράφουμε μερικά βασικά παραδείγματα.

(i) Η ομάδα S_n δρα στο σύνολο X_n: πράγματι, η ομάδα S_n ορίστηκε ως ένα σύνολο μεταθέσεων, δηλαδή κάθε στοιχείο της μετατοπίζει κάθε $x \in X_n$. Ο τρόπος που ορίσαμε την πράξη στην S_n (σύνθεση μεταθέσεων) δείχνει ότι η απεικόνιση $f(\sigma, x) := \sigma \cdot x := \sigma(x)$ για κάθε $\sigma \in S_n$ είναι δράση της S_n στο X_n.

Πιο γενικά κάθε δράση $f : G \times X \to X$ ορίζει μια απεικόνιση $\tilde{f} : G \to S_X$ με $f(g) := \{x \to g \cdot x\}$, όπου S_X είναι η *ομάδα μεταθέσεων του* X. Ειδικότερα, αν $X = X_n$ τότε $S_X = S_n$.

(ii) Κάθε ομάδα G δρα στον εαυτό της (δηλαδή παίρνοντας $X = G$), με την δράση να δίνεται ως $g \cdot x := gx$ (η πράξη της ομάδας). Η προσεταιριστική ιδιότητα της πράξης της ομάδας μας δίνει ότι αυτή η απεικόνιση είναι δράση.

(iii) Αν $H \leqslant G$, τότε η G δρα στα σύμπλοκα της H (παίρνουμε δηλαδή ως X τον χώρο G/H) με την απεικόνιση $g \cdot (xH) := (gx)H$. Εύκολα επαληθεύεται ότι αυτή η απεικόνιση είναι δράση.

Παρατηρούμε πως αν η $G \circlearrowright X$ και $H \leqslant G$ τότε προφανώς και $H \circlearrowright X$ (με τον περιορισμό της δράσης).

Άσκηση 2.1. *Βρείτε κι άλλα παραδείγματα δράσεων για μια γενική ομάδα G καθώς και για συγκεκριμμένες οικείες ομάδες.*

2.2 Τροχιές και σταθεροποιούσες υποομάδες

Η έννοια της δράσης είναι αρκετά γενική ώστε να χτίζει μία πλούσια θεωρία. Ένα από τα πλεονεκτήματα του ορισμού της δράσης είναι η γενικότητα του χώρου στον οποίο μπορεί να δρα η G: *οποιοδήποτε σύνολο*. Αναλόγως με την δομή που έχει κάθε φορά το X μπορεί κανείς να παίρνει και πιο συγκεκριμμένα αποτελέσματα. Μια γενική παρατήρηση όμως είναι πως, από τον ορισμό της δράσης, η σχέση

$$x \sim y \iff \text{υπάρχει } g \in G : y = g \cdot x$$

είναι σχέση ισοδυναμίας (εξηγήστε γιατί). Άρα η σχέση $\sim$ που ορίζεται από την δράση διαμερίζει το X σε ξένα μεταξύ τους υποσύνολα. Καθένα από αυτά τα υποσύνολα καλείται *τροχιά της δράσης* και αν διαλέξουμε ένα σημείο x που ανήκει σε μία τέτοια τροχιά, τότε μπορούμε να περιγράψουμε όλα τα άλλα στοιχεία της τροχιάς αυτής.

Ορισμός 2.2. *Η τροχιά του $x \in X$ ορίζεται να είναι το σύνολο*

$$G \cdot x := \{g \cdot x : g \in G\} \subseteq X.$$

Έτσι λοιπόν το X διαμερίζεται σε ξένες μεταξύ τους τροχιές. Έχουμε λοιπόν προφανώς ότι $y \in G \cdot x \iff x \in G \cdot y$. Από τον ορισμό της δράσης έχουμε επίσης ότι το $e \in G$ σταθεροποιεί (δηλαδή δεν μετακινεί) κάθε $x \in X$. Κάθε $x \in X$ όμως μπορεί να σταθεροποιείται κι από άλλα στοιχεία της G. Μπορεί επίσης ένα $g \in G$ να σταθεροποιεί ένα ή περισσότερα στοιχεία του X. Ορίζουμε λοιπόν τα παρακάτω πολύ σημαντικά σύνολα.

Ορισμός 2.3. *Η σταθεροποιούσα ομάδα του x είναι το σύνολο*

$$G_x := \{g \in G : g \cdot x = x\}.$$

Άσκηση 2.2. *Αποδείξτε ότι το σύνολο G_x είναι όντως υποομάδα της G.*

Ορίζουμε τέλος, για κάθε $g \in G$, το σύνολο

$$X_g := \{x \in X : g \cdot x = x\}.$$

Υπάρχει μια σημαντική σχέση που συνδέει την τροχιά ενός $x \in X$ με την σταθεροποιούσα ομάδα του και δίνεται από το ακόλουθο Θεώρημα τροχιάς-σταθεροποιούσας.

Θεώρημα 2.1. *Έστω $G \circlearrowright X$ και $x \in X$. Τότε*

$$|G \cdot x| = [G : G_x].$$

Απόδειξη. Ορίζουμε την απεικόνιση $f : G \cdot x \to G/G_x$ που απεικονίζει το στοιχείο $g \cdot x$ στο σύμπλοκο gG_x. Θα δείξουμε ότι η απεικόνιση αυτή είναι αντιστοιχία.

Πρώτα δείχνουμε ότι η f είναι καλά ορισμένη. Πράγματι, αν $g_1 \cdot x = g_2 \cdot x$ τότε $(g_1 g_2^{-1}) \cdot x = x$, δηλαδή $(g_1 g_2^{-1}) \in G_x$ κι άρα $g_1 G_x = g_2 G_x$. Άρα η f είναι καλά ορισμένη. Η f είναι ένα-προς-ένα: πράγματι, αν $g_1 G_x = g_2 G_x$ τότε $(g_1 g_2^{-1}) \in G_x$ κι άρα $g_1 \cdot x = g_2 \cdot x$. Το γεγονός ότι η f είναι επί είναι προφανές. □

Το παραπάνω αποτέλεσμα είναι αρκετά ισχυρό και μας δίνει κάποια πρώτα συμπεράσματα. Ειδικότερα, παίρνουμε

$$|G| = |G_x| \cdot |G \cdot x|.$$

Έτσι, αν η G είναι άπειρη, τότε για κάθε $x \in X$ τουλάχιστον μία εκ των G_x και $G \cdot x$ είναι άπειρη.

Δίνουμε κάποιους ακόμα γενικούς και πολύ χρήσιμους ορισμούς.

Ορισμός 2.4. *Μια δράση $G \circlearrowright X$ λέγεται μεταβατική (και το X λέγεται μεταβατικό G-σύνολο) εάν η δράση έχει μόνο μία τροχιά. Η δράση λέγεται πιστή εάν το μόνο στοιχείο της ομάδας G που σταθεροποιεί κάθε στοιχείο του X είναι το ταυτοτικό. Η δράση λέγεται ελεύθερη εάν για κάθε $x \in X$ έχουμε $G_x = \{e\}$.*

Με άλλα λόγια, η δράση είναι ελεύθερη εάν $G_x = \{e\}$ για κάθε $x \in X$, ενώ η δράση είναι πιστή εάν

$$\bigcap_{x \in X} G_x = \{e\}.$$

Προφανώς κάθε ελεύθερη δράση είναι πιστή.

Άσκηση 2.3. *Δείξτε ότι αν $G \circlearrowright X$ πιστά, τότε η $\tilde{f}$ που ορίσαμε στο Παράδειγμα (i) της υποενότητας 2.1 είναι ένα-προς-ενα.*

Ορισμός 2.5. *Ο χώρος των τροχιών (ή χώρος πηλίκο) $X/\sim$ μιας δράσης $G \circlearrowright X$ είναι ο χώρος των αντιπροσώπων των κλάσεων ισοδυναμίας.*

Προφανώς ο παραπάνω ορισμός γενικεύει την έννοια της ομάδας-πηλίκο που ορίσαμε στο πρώτο κεφάλαιο.

Άσκηση 2.4. *Μελετήστε τις σταθεροποιούσες υποομάδες, τις τροχιές καθώς και τα σύνολα X_g για κάθε μία από τις δράσεις που είδαμε στα παραδείγματα της υποενότητας 2.1. Ποιές από αυτές είναι πιστές, μεταβατικές, πιστές ή ελεύθερες; Ποιός είναι ο χώρος των τροχιών σε κάθε μία από αυτές τις περιπτώσεις;*

Άσκηση 2.5. *Δείξτε ότι μία δράση $G \circlearrowright X$ είναι μεταβατική αν και μόνο αν ο χώρος πηλίκο είναι μονοσύνολο.*

Άσκηση 2.6. *Θεωρούμε την δράση του Παραδείγματος (iii) της υποενότητας 2.1. Τι μας δίνει σε αυτήν την περίπτωση το Θεώρημα τροχιάς-σταθεροποιούσας;*

Άσκηση 2.7. *Αν $G \circlearrowright X$ τότε κάθε τροχιά $G \cdot x$ είναι μεταβατικό G-σύνολο.*

Άσκηση 2.8. *Δείξτε ότι η ομάδα $SL_2(\mathbb{R})$ δρα στο άνω μιδαγικό ημιεπίπεδο $\mathbb{H}^2 := \{z \in \mathbb{C} : \Im(z) > 0\}$ (το οποίο, όταν εφοδιαστεί με την υπερβολική μετρική ονομάζεται υπερβολικό επίπεδο). Βρείτε την τροχιά και την σταθεροποιούσα στο σημείου $z = i$.*

2.3 Η εξίσωση κλάσεων

Αφού η δράση $G \circlearrowright X$ διαμερίζει το X σε ξένες κλάσεις ισοδυναμίας, που η κάθεμια κλάση είναι μία τροχιά κάποιου σημείου $x_i \in X$:

$$X = \bigcup_{[x_i] \in X/\sim} G \cdot x_i$$

έπεται ότι

$$|X| = \sum_{[x_i] \in X/\sim} |G \cdot x_i|.$$

Κάποιες από τις τροχιές μπορεί να είναι τετριμμένες, δηλαδή μπορεί ολόκληρη η G να σταθεροποιεί κάποιο $x_i \in X$. Σε αυτήν την περίπτωση έχουμε $G \cdot x_i = \{x_i\}$ άρα $|G \cdot x_i| = 1$. Συμβολίζουμε με X_G το σύνολο όλων αυτών των x_i. Παίρνουμε λοιπόν

$$\begin{aligned} |X| &= \sum_{|G\cdot x_i|=1} |G \cdot x_i| + \sum_{|G\cdot x_i|>1} |G \cdot x_i| \\ &= |X_G| + \sum_{|G\cdot x_i|>1} |G \cdot x_i|. \end{aligned} \tag{2}$$

Η σχέση αυτή ονομάζεται εξίσωση κλάσεων και θα αποδειχθεί ιδιαιτέρως σημαντική για την πορεία της μελέτης μας. Παρατηρήστε επίσης πως

$$X_G = \bigcap_{g \in G} X_g.$$

Άσκηση 2.9. *Αν $G \circlearrowleft X$ και $H \leqslant G$, πώς σχετίζεται η εξίσωση των κλάσεων για την δράση $H \circlearrowleft X$ σε σχέση με την δράση της G στο X;*

Άσκηση 2.10. *Υπολογίστε το σύνολο X_G για κάθε μία από τις δράσεις που έχουμε δει ως τώρα στα παραδείγματα.*

Άσκηση 2.11. *Αν $G \circlearrowleft X$ με X πεπερασμένο και $|G| = p^k$, όπου $p \geqslant 2$ είναι κάποιος πρώτος αριθμός, τότε*

$$|X| \equiv |X_G| \mod p.$$

Συμπεράνετε πως αν ο p δεν διαιρεί τον πληθάριθμο $|X|$, τότε υπάρχει $x \in X$ με $G_x = G$.

2.4 Κλάσεις συζυγίας και κεντροποιούσα ομάδα

Στην υποενότητα 2.1 είδαμε μία δράση της G στον εαυτό της με την πράξη από αριστερά. Υπάρχει άλλη μία δράση της ομάδας G στον εαυτό της που έχει ξεχωριστό ενδιαφέρον. Όπως έχουμε ήδη αναφέρει, δύο στοιχεία $x, y \in G$ ονομάζονται συζυγή εάν υπάρχει $g \in G$ τέτοια ώστε

$$y = gxg^{-1}.$$

Η σχέση αυτή μας είναι γνώριμη από το πρώτο κεφάλαιο. Το κρίσιμο στοιχείο εδώ της νέας οπτικής μας, είναι ότι μπορούμε να δούμε την συζυγία ως μία δράση.

Πράγματι, αν G είναι μια ομάδα τότε $G \circlearrowleft G$ με την δράση συζυγίας

$$g \cdot x = gxg^{-1}$$

για κάθε $g, x \in G$. Ο λόγος που συμβολίζουμε το στοιχείο x με αυτόν τον τρόπο είναι για να δώσουμε έμφαση στο γεγονός ότι είναι στοιχείο του συνόλου X που δέχεται την δράση της G (ανεξαρτήτως του ότι σε αυτήν την ειδική περίπτωση έχουμε $X = G$).

Θέλουμε να εξετάσουμε την τροχιά $G \cdot x$, το σύνολο X_g καθώς και την σταθεροποιούσα υποομάδα G_x για αυτήν την δράση. Αν $x \in X$ τότε η τροχιά του

$$G \cdot x = \{gxg^{-1} : g \in G\} \subseteq G$$

είναι απλά η κλάση συζυγίας x^G που ορίσαμε στην υποενότητα 1.6. Η σταθεροποιούσα ομάδα του σε αυτήν την περίπτωση ονομάζεται *κεντροποιούσα του* x και συμβολίζεται με

$$C_G(x) = \{g \in G,\, gxg^{-1} = x\} = \{g \in G,\, gx = xg\} \leqslant G,$$

δηλαδή είναι η υποομάδα της G που περιέχει όλα τα στοιχεία της ομάδας που μετατίθονται με το x. Παρατηρούμε ότι $Z(G) \leqslant C_G(x)$ και

$$\bigcap_{x \in G} C_G(x) = Z(G).$$

Ειδικότερη, η δράση συζυγίας σε μια ομάδα G είναι πιστή αν και μόνο αν η ομάδα είναι centerless. Σε αυτήν την περίπτωση, το Θεώρημα τροχιάς-σταθεροποιούσας μας δίνει ότι για κάθε $x \in G$ ισχύει

$$|G| = |C_G(x)| \cdot |x^G|.$$

Αξίζει να δούμε πως ποσοτικοποιείται τώρα κάτι που ήδη γνωρίζουμε: για ένα $x \in G$ έχουμε $x \in Z(G)$ αν και μόνο αν $x^G = \{x\}$ αν και μόνο αν $C_G(x) = G$.

Άσκηση 2.12. *Δείξτε ότι αν x^G είναι μία κλάση συζυγίας της G τότε η $|x^G|$ διαιρεί τον δείκτη $[G : Z(G)]$.*

Η εξίσωση των κλάσεων για την δράση της συζυγίας έχει ιδιαίτερη σημασία. Πιο συγκεκριμμένα, σε αυτήν την περίπτωση έχουμε

$$X_G = \{x \in G : gx = xg \, \forall g \in G\} = Z(G)$$

και

$$|G \cdot x_i| = |x_i^G| = [G : C_G(x_i)].$$

Άρα η εξίσωση κλάσεων τώρα παίρνει την μορφή

$$|G| = |Z(G)| + \sum_{|x_i^G|>1} |G : C_G(x_i)|.$$

Μία άμεση και χρήσιμη εφαρμογή της εξίσωσης αυτής είναι για την ειδική περίπτωση που έχουμε $|G| = p^k$, όπου $p \geqslant 2$ είναι κάποιος πρώτος αριθμός (θα συναντήσουμε πολλές τέτοιες ομάδες παρακάτω καθώς έχουν ιδιαίτερη σημασία). Αν $k = 1$, τότε ξέρουμε ότι η G είναι κυκλική τάξης p και απλή. Ας δούμε τι συμβαίνει όταν $k \geqslant 2$. Κάθε όρος του αθροίσματος πάνω από τις μη τετριμμένες τροχιές διαιρείται από p, αφού είναι δείκτης γνήσιας υποομάδας της ομάδας G. Ειδικότερα

$$|G| \equiv |Z(G)| \mod p.$$

Αφού όμως $p||G|$, παίρνουμε πως $p||Z(G)|$. Αφού $|Z(G)| \geqslant 1$, έπεται ότι $|Z(G)| \geqslant p$. Αν το κέντρο είναι γνήσια υποομάδα της G, τότε η G δεν είναι απλή (γιατί το κέντρο είναι κανονική υποομάδα). Αν η G είναι αβελιανή (άρα $G = Z(G)$), τότε θα δούμε παρακάτω ότι η G έχει υποομάδες τάξης p^i για κάθε $1 \leqslant i \leqslant k$ και άρα δεν είναι απλή.

Άσκηση 2.13. *Δείξτε ότι για κάθε $x, g \in G$ ισχύει $C_G(gxg^{-1}) = gC_G(x)g^{-1}$. Πιο γενικά, αν $G \circlearrowright X$ τότε $C_{g \cdot x} = gC_xg^{-1}$ και $|C_{g \cdot x}| = |C_x|$.*

Άσκηση 2.14. *Αν $x^G = \{a_1, ..., a_k\}$, δείξτε ότι $(x^{-1})^G = \{a_1^{-1}, ..., a_k^{-1}\}$.*

Άσκηση 2.15. *Αν μια πεπερασμένη ομάδα G έχει ακριβώς δύο ξένες κλάσεις συζυγίας, δείξτε ότι $|G| = 2$.*

Άσκηση 2.16. *Αν μια πεπερασμένη ομάδα G έχει ακριβώς τρεις ξένες κλάσεις συζυγίας, δείξτε ότι $|G| = 3$ ή 6.*

Άσκηση 2.17. *Δείξτε ότι δεν υπάρχει ομάδα G με εξίσωση κλάσεων συζυγίας $1+1+2+2+2+2$ ενώ υπάρχει ομάδα με εξίσωση κλάσεων $1+2+2+5$.*

Θα δούμε τώρα μια γενίκευση των ασκήσεων 2.15 και 2.16. Ειδικότερα, θα δείξουμε ότι για κάθε $n \geqslant 1$ υπάρχουν πεπερασμένες στο πλήθος πεπερασμένες ομάδες που έχουν ακριβώς n κλάσεις συζυγίας. Θα χρειαστούμε το ακόλουθο Λήμμα.

Λήμμα 2.1. *(Landau) Δοθέντων $n \geqslant 1$, $q \in \mathbb{Q}$, υπάρχουν πεπερασμένες n-άδες $k_1, ..., k_n$ φυσικών αριθμών που ικανοποιούν την εξίσωση*

$$q = \sum_{i=1}^{n} \frac{1}{k_i}.$$

Θεώρημα 2.2. *Για κάθε $n \geqslant 1$ υπάρχουν πεπερασμένες στο πλήθος (μη ισόμορφες) πεπερασμένες ομάδες που έχουν ακριβώς n κλάσεις συζυγίας*

Απόδειξη. Έστω G μια τέτοια ομάδα και έστω $|Z(G)| = m|n$. Τότε για $q = 1$ παίρνουμε

$$1 = \frac{1}{|G|} + ... + \frac{1}{|G|} + \sum_{i=m+1}^{n} \frac{1}{k_i}$$

με $k_i = 1/|G|$ για τα στοιχεία που ανήκουν στο κέντρο της G και με $k_i = [G : C_G(x_i)]/|G|$ για ένα σύνολο αντιπροσώπων x_i των μη τετριμμένων κλάσεων συζυγίας. Η απόδειξη έπεται εφαρμόζωντας το Λήμμα του Landau: υπάρχει καθολικό $M > 0$ που φράσσει από πάνω όλα τα k_i κι άρα $|G| \leqslant M$. Όμως για κάθε $M \geqslant 1$ υπάρχουν πεπερασμένες (μη ισόμορφες) ομάδες τάξης $\leqslant M$ (εξηγήστε γιατί). □

Άσκηση 2.18. *Χρησιμοποιώντας επαγωγή στο n δείξτε το Λήμμα του Landau.*

2.5 Συζυγίες υποομάδων και κανονικοποιούσα ομάδα

Εκτός από την δράση μιας G στον εαυτό της ή σε έναν χώρο συμπλόκων της, υπάρχει μία ακόμα δράση της G που είναι ιδιαιτέρως σημαντική για εμάς. Αν θεωρήσουμε το σύνολο X των υποομάδων της G, δηλαδή $X = \{H : H \leqslant G\}$, τότε η G δρα στο X με την δράση συζυγίας: αν $g \in G$ και $H \leqslant G$ ορίζουμε

$$g \cdot H := gHg^{-1}.$$

Εύκολα επαληθεύουμε ότι αυτή η απεικόνιση είναι όντως δράση (διότι αν $H \leqslant G$ τότε και $gHg^{-1} \leqslant G$). Επιπλέον, μπορούμε να περιορίσουμε αυτήν την δράση σε κατάλληλα υποσύνολα του X αν θυμηθούμε πως $|H| = |gHg^{-1}|$. Συμβολίζουμε με H^g την συζυγή υποομάδα gHg^{-1} και θυμίζουμε πως $H \trianglelefteq G$ αν και μόνο αν $H^g = H$ για κάθε $g \in G$. Συμπεραίνουμε πως η τροχιά της H υπό την δράση συζυγίας είναι η οικογένεια $[H] = \{H^g,\, g \in G\}$ των συζυγών υποομάδων της H.

Η σταθεροποιούσα ομάδα της $H \in X$ σε αυτήν την περίπτωση ονομάζεται *κανονικοποιούσα της H* και συμβολίζεται με

$$N_G(H) = \{g \in G,\, gHg^{-1} = H\} = \{g \in G,\, gH = Hg\} \leqslant G.$$

Η $N_G(H)$ είναι η μεγαλύτερη υποομάδα της G μέσα στην οποία η H είναι κανονική: $H \trianglelefteq N_G(H) \leqslant G$, κι άρα $H \trianglelefteq G$ αν και μόνο αν $N_G(H) = G$. Το Θεώρημα τροχιάς-σταθεροποιητή σε αυτήν την περίπτωση μας δίνει την σχέση

$$|[H]| = [G : N_G(H)].$$

Σε αυτήν την περίπτωση η εξίσωση των κλάσεων γίνεται πιο περίπλοκη. Θα δούμε παρακάτω την χρησιμότητα αυτής της δράσεως και την κανονικοποιούσας στην Θεωρία Sylow.

Άσκηση 2.19. *Δείξτε ότι $N_G(gHg^{-1}) = gN_G(H)g^{-1}$.*

Άσκηση 2.20. *Αν $H \leqslant K \leqslant G$ τότε $N_K(H) = N_G(H) \cap K$.*

Άσκηση 2.21. *Αν $H, K \leqslant G$ τότε $N_G(H) \cap N_G(K) \leqslant N_G(H \cap K)$.*

Άσκηση 2.22. *Γράψτε την εξίσωση των κλάσεων για την δράση $H \circlearrowright G/H$ της H στα αριστερά σύμπλοκα της που δίνεται ως*

$$h \cdot (gH) = (hg)H.$$

Χρησιμοποιώντας αυτήν την εξίσωση κλάσεων δείξτε ότι αν $|G| < \infty$ και $H \leqslant G$ με $H = p^k$, τότε

$$[G : H] \equiv [N_G(H) : H] \mod p.$$

2.6 Απαρίθμηση τροχιών

Όταν μία πεπερασμένη ομάδα G δρα σε ένα πεπερασμένο σύνολο X, το επόμενο όμορφο αποτέλεσμα του Burnside μετράει το πλήθος n των τροχιών της δράσης. Υπενθυμίζουμε τον ορισμό του συνόλου X_g από την υποενότητα 2.2.

Θεώρημα 2.3. *(Burnside) Αν $G \circlearrowright X$ με $|G| < \infty, |X| < \infty$, τότε*

$$n = \frac{1}{|G|} \sum_{g \in G} |X_g|.$$

Απόδειξη. Το επιχείρημα της απόδειξης εδώ είναι μία μέτρηση ενός κατάλληλου συνόλου S με δύο διαφορετικούς τρόπους. Πιο συγκεκριμμένα, ορίζουμε

$$S = \{(g, x) \in G \times X : \, g \cdot x = x\}.$$

Τότε πόσα στοιχεία έχει το S; Παρατηρείστε ότι

$$X_g := \{x \in X : \, g \in G_x\}.$$

Τότε αφ' ενός

$$|S| = \sum_{g \in G} |X_g|.$$

ενώ από την άλλη, έχουμε

$$|S| = \sum_{x \in X} |G_x|.$$

Όμως $|G_x| = |G|/|G \cdot x|$. Επίσης, για κάθε $y \in G \cdot x$ θυμηθείτε πως $|G_x| = |G_y|$ (άσκηση 2.13). Άρα

$$\begin{aligned} |S| &= \sum_{x \in X} \frac{|G|}{|G \cdot x|} = |G| \sum_{x \in X} \frac{1}{|G \cdot x|} \\ &= |G| \sum_{i=1}^{n} \sum_{y \in G \cdot x_i} \frac{1}{|G \cdot y|} = |G| \sum_{i=1}^{n} \sum_{y \in G \cdot x_i} \frac{1}{|G \cdot x_i|} \\ &= |G| \sum_{i=1}^{n} 1 = |G| \cdot n, \end{aligned} \tag{3}$$

και το ζητούμενο έπεται. □

Άσκηση 2.23. *Ως πόρισμα του Θεωρήματος Burnside, δείξτε ότι αν G πεπερασμένη, $1 < |X| < \infty$ και $G \circlearrowright X$ μεταβατικά, τότε υπάρχει $g \in G$ χωρίς σταθερό σημείο (δηλαδή $X_g = \varnothing$).*

Άσκηση 2.24. *Αν G πεπερασμένη και c είναι το πλήθος των κλάσεων συζυγίας της G, τότε*

$$c = \frac{1}{|G|} \sum_{g \in G} |C_G(g)|.$$

2.7 p-Ομάδες και το Θεώρημα του Cauchy

Έχουμε τονίσει πολλές φορές ότι η τάξη μιας πεπερασμένης ομάδας G επηρρεάζει την δομή της ομάδας με ουσιώδη τρόπο. Η πιο απλή περίπτωση (η "τοπική περίπτωση") είναι η περίπτωση όπου η τάξη της G είναι ίση με την δύναμη ενός πρώτου αριθμού. Τις ομάδες αυτές τις έχουμε ήδη συναντήσει. Ήρθε η ώρα να τους δώσουμε ένα όνομα και να τις μελετήσουμε ξεχωριστά.

Ορισμός 2.6. *Αν p είναι ένας πρώτος αριθμός, μια p-ομάδα ονομάζεται μια ομάδα όπου κάθε στοιχείο της έχει τάξη μία δύναμη του p.*

Αντίστοιχα, μια $H \leqslant G$ ονομάζεται p-υποομάδα της G αν είναι p-ομάδα. Το επόμενο Θεώρημα μας επιτρέπει να χαρακτηρίσουμε τις πεπερασμένες p-ομάδες.

Θεώρημα 2.4. *(Cauchy) Αν G είναι μια πεπερασμένη ομάδα και p ένας πρώτος με $p||G|$, τότε η G έχει στοιχείο τάξης p.*

Για να αποδείξουμε αυτό το σημαντικό αποτέλεσμα θα χρειαστεί να σπάσουμε την απόδειξη σε δύο βήματα. Το πρώτο βήμα είναι η ακόλουθη Πρόταση, που δείχνει πως το Θεώρημα αληθεύει στην αβελιανή περίπτωση.

Πρόταση 2.1. *Αν G είναι μια πεπερασμένη αβελιανή ομάδα και p ένας πρώτος με $p||G|$, τότε η G έχει στοιχείο τάξης p.*

Απόδειξη. Έστω $|G| = pm$ με $m \geqslant 1$. Η απόδειξη θα γίνει με ισχυρή επαγωγή στο m. Αν $m = 1$ τότε το ζητούμενο προφανώς ισχύει. Έστω ότι ισχύει για κάθε αβελιανή ομάδα τάξης pk, με $k \leqslant m - 1$. Θα δείξουμε ότι ισχύει και για κάθε αβελιανή ομάδα τάξης pm.

Έστω λοιπόν μια τέτοια αβελιανή ομάδα και έστω ένα $g \in G$ τάξης $n > 1$. Αν $p|n$ τότε επιλέγουμε το στοιχείο $g^{n/p}$ το οποίο έχει τάξη p.

Αν $p \nmid n$, τότε $\langle g \rangle \trianglelefteq G$ και

$$\left| \frac{G}{\langle g \rangle} \right| = \frac{pm}{n} < pm.$$

Προφανώς, αφού $(p, n) = 1$ παίρνουμε $n|m$, κι άρα η τάξη της ομάδας $G/\langle g \rangle$ διαιρείται από p. Άρα η ομάδα πηλίκο ικανοποιεί την επαγωγική υπόθεση, κι έτσι υπάρχει ένα $y^* \in G/\langle g \rangle$ τάξης p. Ο φυσικός επιμορφισμός

$$\pi_{\langle g \rangle} : G \to G/\langle g \rangle$$

μας δίνει ένα $y \in G$ τέτοιο ώστε $\pi_{\langle g \rangle}(y) = y^*$. Από τις ιδιότητες ενός ομομορφισμού έχουμε ότι η τάξη του $\pi_{\langle g \rangle}(y)$ διαιρεί την τάξη του y. Συμπεραίνουμε ότι η τάξη του y διαιρείται από p. Αυτό μας φέρνει στην προηγούμενη περίπτωση: αν η τάξης του y είναι pt αρκεί να επιλέξουμε το στοιχείο y^t κι έχουμε τελειώσει. □

Απόδειξη. (του Θεωρήματος Cauchy). Θεωρούμε την εξίσωση κλάσεων για την δράση συζυγίας $G \circlearrowleft G$, η οποία είναι

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)].$$

Μπορούμε επίσης εύκολα να επαληθεύσουμε πως το Θεώρημα ισχύει για $|G| \leqslant 7$. Η απόδειξη θα γίνει με γενικευμένη επαγωγή στην τάξη της G: έστω ότι ισχύει για κάθε ομάδα τάξης $< n$. Θα δείξουμε ότι ισχύει για κάθε ομάδα τάξης n.

Αν η G είναι αβελιανή τότε το Θεώρημα ισχύει. Έστω ότι η G δεν είναι αβελιανή. Τότε για κάθε $x \notin Z(G)$ έχουμε $1 < |C_G(x)| < |G|$. Αν για κάποιο x_i έχουμε

$$p \mid |C_G(x_i)|$$

τότε παίρνουμε το ζητούμενο θεωρώντας την αβελιανή υποομάδα $C_G(x_i)$ και εφαρμόζοντας την προηγούμενη Πρόταση. Αν

$$p \nmid |C_G(x_i)|$$

για κάθε x_i, $i = 1, 2, ..., m$, τότε

$$p \mid [G : C_G(x_i)]$$

για κάθε x_i, $i = 1, 2, ..., m$. Αφού $p \mid |G|$, η εξίσωση κλάσεων σε αυτήν την περίπτωση μας δίνει ότι $p \mid |Z(G)|$, και το ζητούμενο έπεται εφαρμόζωντας την προηγούμενη Πρόταση για την αβελιανή ομάδα $Z(G)$. □

Το Θεωρημα του Cauchy μας δίνει ότι μια πεπερασμένη ομάδα G είναι p-ομάδα αν και μόνο αν η τάξη της είναι ίση με p^k για κάποιο $k \geqslant 1$. Θυμίζουμε πως κάθε τέτοια ομάδα έχει μη τετριμμένο κέντρο, όπως δείξαμε στην υποενότητα 2.4 και άρα δεν είναι απλή, εκτός αν είναι αβελιανή τάξης p. Τονίζουμε πως αυτό δεν αληθεύει για άπειρες p-ομάδες.

Άσκηση 2.25. *Χρησιμοποιώντας την άσκηση 1.47 δείξτε ότι αν $|G| = p^2$ τότε η G είναι αβελιανή.*

Άσκηση 2.26. *Αν p πρώτος και G μη αβελιανή με τάξη $|G| = p^3$, δείξτε ότι $|Z(G)| = p$, $G/Z(G) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ και $Z(G) = G'$.*

Άσκηση 2.27. *Αν G μη αβελιανή με $|G| = p^k$ με $k \geqslant 3$, τότε $|Z(G)| \in \{p, p^2, p^3, ..., p^{k-2}\}$.*

Άσκηση 2.28. *Αν $H \trianglelefteq G$ και οι $H, G/H$ είναι p-ομάδες, δείξτε ότι και η G είναι p-ομάδα.*

Άσκηση 2.29. *Χρησιμοποιώντας την άσκηση 2.21 δείξτε ότι αν η G είναι μια πεπερασμένη p-ομάδα και $H < G$ είναι μια γνήσια υποομάδα της τότε $H < N_G(H)$.*

2.8 Θεωρία Sylow

Στην πραγματικότητα το Θεώρημα του Cauchy είναι το πρώτο σημαντικό αποτέλεσμα της θεωρίας των πεπερασμένων p-Ομάδων. Τα Θεωρήματα του Sylow γενικεύουν το αποτέλεσμα του Cauchy και παρέχουν πολλή πληροφορία για όλες τις p-υποομάδες μιας πεπερασμένης ομάδας. Θα μας χρειαστούν οι παρακάτω ορισμοί και ασκήσεις, τους οποίους και τις οποίες έχουμε ξαναδεί αλλά παραθέτουμε εδώ για λόγους πληρότητας (δείτε ασκήσεις 1.55, 1.56).

Ορισμός 2.7. *Έστω $H \leqslant G$. Η H θα λέγεται μέγιστη υποομάδα της G εάν δεν υπάρχει άλλη υποομάδα K της G που να περιέχει την H.*

Ορισμός 2.8. *Έστω $K \trianglelefteq G$. Η K θα λέγεται μέγιστη κανονική υποομάδα της G εάν δεν υπάρχει άλλη κανονική υποομάδα N της G που να περιέχει την K.*

Άσκηση 2.30. *Δείξτε ότι αν μια μέγιστη υποομάδα H της G είναι και κανονική στην G, τότε $[G : H] = p$ για κάποιο πρώτο αριθμό p.*

Άσκηση 2.31. *Δείξτε ότι η K είναι μέγιστη κανονική υποομάδα της G αν και μόνο αν η ομάδα-πηλίκο G/K είναι απλή.*

Στόχος μας είναι να αποδείξουμε τα τρία Θεωρήματα του Sylow. Για το πρώτο Θεώρημα θα χρησιμοποιήσουμε την εξής κρίσιμη παρατήρηση (δείτε και τις ασκήσεις 2.21 και 2.26): αν G είναι μια πεπερασμένη ομάδα και H μια πεπερασμένη p-υποομάδα της τότε

$$H < N_G(H).$$

Αυτό το γεγονός θα μας βοηθήσει να φτιάξουμε μια άυξουσα ακολουθία υποομάδων της G που ικανοποιούν την ζητούμενη ιδιότητα.

Θεώρημα 2.5. *(1ο Θεώρημα Sylow) Έστω G μια πεπερασμένη ομάδα τάξης $p^n m$, με $n \geqslant 1$ και $(p, m) = 1$. Τότε για κάθε $1 \leqslant i \leqslant n$, η G περιέχει υποομάδα H_i τάξης p^i. Επιπλέον κάθε υποομάδα της G τάξης p^i είναι κανονική σε κάποια υποομάδα της G τάξης p^{i+1}.*

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στο i για $1 \leqslant i \leqslant n$. Η περίπτωση $i = 1$ είναι ακριβώς το Θεώρημα Cauchy. Έστω λοιπόν ότι υπάρχει μία υποομάδα H_i της G τάξης p^i όπου $i < n$. Θα κατασκευάσουμε μία υποομάδα H_{i+1} της G τάξης p^{i+1}.

Αφού $i < n$ έχουμε πως $p \mid [G : H_i]$, άρα από την άσκηση 2.21 συμπεραίνουμε πως $p \mid [N_G(H_i) : H_i]$. Αφού $H_i \lhd N_G(H_i)$, έχουμε πως ο χώρος πηλίκο $N_G(H_i)/H_i$ είναι ομάδα, της οποίας η τάξη διαιρείται από p. Άρα ικανοποιείται το Θεώρημα του Cauchy, δηλαδή υπάρχει $K_i \leqslant N_G(H_i)/H_i$ με $|K_i| = p$. Ο φυσικός επιμορφισμός

$$\pi_{H_i} : N_G(H_i) \to \frac{N_G(H_i)}{H_i}$$

μας δίνει της υποομάδα $H_{i+1} := \pi_{H_i}^{-1}(K_i)$ της $N_G(H_i)$ που περιέχει και την H_i. Άρα $H_i \lhd H_{i+1}$. Από το Θεώρημα της αντιστοιχίας συμπεραίνουμε πως $K_i \simeq H_{i+1}/H_i$, άρα $|H_{i+1}| = |K_i||H_i| = p \cdot p^i = p^{i+1}$. □

Βλέπουμε τώρα πόσο κομμάτι του αντίστροφου του Lagrange διασώζεται. Αν $d \mid |G|$ έχουμε δει πως δεν υπάρχει πάντα υποομάδα της G τάξης d, ισχύει όμως αν το d είναι δύναμη πρώτου.

Ορισμός 2.9. *Έστω G μία ομάδα. Μία Sylow p-υποομάδα P της G είναι μία μέγιστη p-υποομάδα της (δηλαδή δεν υπάρχει άλλη p-υποομάδα P' της G με $P < P'$).*

Αν $|G| = p^n m$ με $(p, m) = 1$, το πρώτο Θεώρημα Sylow μας δίνει πως κάθε Sylow p-υποομάδα της G έχει τάξη p^n. Επιπλέον, αν P είναι μία τέτοια υποομάδα και $g \in G$, τότε και η συζυγής υποομάδα gPg^{-1} της G έχει την ίδια τάξη (γιατί;), άρα είναι Sylow. Το δεύτερο Θεώρημα του Sylow μας λέει πως όλες οι Sylow p-υποομάδες της G είναι συζυγείς μεταξύ τους.

Θεώρημα 2.6. *(2ο Θεώρημα Sylow) Κάθε δύο Sylow p-υποομάδες P_1, P_2 μιας πεπερασμένης ομάδας G είναι συζυγείς, δηλαδή $P_1 = gP_2g^{-1}$ για κάποιο $g \in G$.*

Απόδειξη. Αφήνουμε την P_1 να δράσει στον χώρο των συμπλόκων της P_2 μέσα στην G, δηλαδή $P_1 \circlearrowright X = G/P_2$, όπου η δράση δίνεται ως

$$y \cdot (gP_2) = (yg)P_2,$$

για κάθε $y \in P_1$, $g \in G$. Επειδή η P_1 είναι p-υποομάδα της G η εξίσωση των κλάσεων μας δίνει

$$[G : P_2] = |X| \equiv |X_{P_1}| \mod p.$$

Όμως $[G : P_2] = m$ (επειδή η P_2 είναι μέγιστη) το οποίο είναι σχετικά πρώτο ως προς τον p, άρα $|X_{P_1}| \equiv m \not\equiv 0 \mod p$. Ειδικότερα $X_{P_1} \neq \varnothing$, άρα υπάρχει σύμπλοκο $gP_2 \in X$ τέτοιο ώστε $y \cdot (gP_2) = gP_2$ για κάθε $y \in P_1$. Συμπεραίνουμε πως

$$g^{-1}ygP_2 = P_2 \Longrightarrow g^{-1}yg \in P_2$$

για κάθε $y \in P_1$. Αυτό σημαίνει πως

$$g^{-1}P_1g \leqslant P_2$$

κι αφού $|g^{-1}P_1g| = |P_2|$ έπεται πως $g^{-1}P_1g = P_2$, δηλαδή $P_1 = gP_2g^{-1}$. □

Πόρισμα 2.1. *Έστω μια πεπερασμένη ομάδα G. Τότε η G έχει μοναδική Sylow p-υποομάδα P για κάποιο $p \mid |G|$ αν και μόνο αν $P \trianglelefteq G$.*

Τό τρίτο Θεώρημα του Sylow μας επιτρέπει να μετρήσουμε το πλήθος των Sylow p-υποομάδων μιας πεπερασμένης ομάδας G. Το πρόβλημα που προκύπτει εδώ είναι πως δεν μπορούμε να μετρήσουμε το πλήθος τους επακριβώς, μπορούμε όμως να το μετρήσουμε modulo p.

Θεώρημα 2.7. *(3ο Θεώρημα Sylow) Έστω G μια πεπερασμένη ομάδα τάξης $p^n m$ και έστω s_p το πλήθος των Sylow p-υποομάδων της. Τότε $s_p \mid |G|$ και επιπλέον $s_p \equiv 1 \mod p$.*

Με άλλα λόγια, το τρίτο Θεώρημα Sylow μας δίνει πως αν $|G| = p^n m$ με $(p, m) = 1$, τότε $s_p \mid m$ και $p \mid s_p - 1$. Οι δύο αυτές συνθήκες είναι πολύ ισχυρές, τόσο ώστε πολύ συχνά επιβάλλουν σε μια ομάδα να έχει μοναδική λύση $s_p = 1$ για κάποιο $p \mid |G|$. Σε αυτήν την περίπτωση, όπως είδαμε και παραπάνω, η μοναδική Sylow p-υποομάδα P θα είναι αναγκαστικά κανονική στην G. Ειδικότερα, αν $m > 1$ τότε η G δεν μπορεί να είναι απλή (όταν $m = 1$ έχουμε ήδη εξηγήσει ότι η G δεν μπορεί να είναι απλή για $n \geqslant 2$).

Απόδειξη. (3ο Θεώρημα Sylow). Έστω $|G| = p^n m$ με $(p, m) = 1$. Θεωρούμε το σύνολο

$$X = \{X_1, X_2, ..., X_s\}$$

των Sylow p-υποομάδων της G (δηλαδή $s_p = s$). Θεωρούμε την δράση της ομάδας $G \circlearrowright X$ με συζυγία, και τον περιορισμό της δράσης αυτής στην υποομάδα $P = P_1 \circlearrowright X$. Δηλαδή

$$x \cdot P_i = xP_ix^{-1}$$

για $P_i \in X$ και για $x \in P$. Θέλουμε να μετρήσουμε το σύνολο X_P των τετριμμένων τροχιών για να χρησιμοποιήσουμε την εξίσωση των κλάσεων. Το σύνολο αυτό X_P δίνεται ως

$$\{P_i \in X : xP_ix^{-1} = P_i, \forall x \in P\}.$$

Άρα, αν $P_i \in X_P$ τότε $P \leqslant N_G(P_i) \leqslant G$. Όμως επίσης έχουμε και $P_i \trianglelefteq N_G(P_i) \leqslant G$. Το κρίσιμο στοιχείο εδώ είναι πως αφού οι P, P_i είναι Sylow p-υποομάδες της G, είναι και Sylow p-υποομάδες της $N_G(P_i)$. Από το 2ο Θεώρημα Sylow, οι P, P_i είναι συζυγείς μέσα στην $N_G(P_i)$, δηλαδή $P = yP_iy^{-1}$ για κάποιο $y \in N_G(P_i)$. Όμως $P_i \trianglelefteq N_G(P_i)$, δηλαδή $yP_iy^{-1} = P_i$. Άρα $P_i = P$. Συμπεραίνουμε πως $X_P = \{P\}$, κι άρα η εξίσωση κλάσεων μας δίνει

$$s_p = |X| \equiv |X_P| = 1 \mod p.$$

Αν θεωρήσουμε την δράση συζυγίας $G \circlearrowright X$ (χωρίς δηλαδή να περιορίσουμε την δράση σε μία Sylow p-υποομάδα), τότε ξέρουμε (από το 2ο Θεώρημα Sylow) ότι όλες οι Sylow p-υποομάδες είναι μεταξύ τους συζυγείς. Άρα η δράση στο X είναι μεταβατική (υπάρχει μόνο μία τροχιά). Αν επιλέξουμε μία οποιαδήποτε $P_i \in X$, τότε η σταθεροποιούσα της είναι η ομάδα

$$G_{P_i} = \{g \in G : gP_ig^{-1} = P_i\} = N_G(P_i).$$

Από το Θεώρημα τροχιάς-σταθεροποιούσας συμπεραίνουμε πως

$$s_p = |X| = |G \cdot P_i| = [G : N_G(P_i)] \mid |G|$$

και η απόδειξη είναι πλήρης. □

Μπορούμε τώρα, ως εφαρμογή του 3ου Θεωρήματος Sylow, να αποδείξουμε για αρκετά n πως αν $|G| = n$ τότε η G δεν μπορεί να είναι απλή. Ένα απλό παράδειγμα είναι για $n = 20$. Σε αυτήν την περίπτωση, αφού $20 = 2^2 \cdot 5$ μας δίνει ότι $n_5 \mid 4$ και $n_5 \equiv 1$ mod 6. Η μόνη λύση αυτού του συστήματος είναι η $n_5 = 1$, άρα υπάρχει μοναδική Sylow 5-υποομάδα της G, η οποία είναι αναγκαστικά κανονική υποομάδα της. Θα δούμε τώρα κι άλλα πιο δύσκολα παραδείγματα.

Στο δεύτερο παράδειγμα μας, θεωρούμε $|G| = 30 = 2 \cdot 3 \cdot 5$. Τότε η G δεν είναι απλή. Πράγματι, το 3ο Θεώρημα Sylow μας δίνει $s_3 = 1$ ή 10 και $s_5 = 1$ ή 6. Αν η G δεν είναι απλή, τότε θα πρέπει αναγκαστικά να ισχύει $s_3 = 10$ και $s_5 = 6$. Αφού η G έχει 10 διαφορετικές υποομάδες τάξης 3, αυτές θα έχουν αναγκαστικά τετριμμένη τομή, κι άρα θα υπάρχουν τουλάχιστον $10(3-1) = 20$ στοιχεία τάξης 3. Ομοίως θα υπάρχουν τουλάχιστον

$6(5-4) = 24$ στοιχεία τάξης 5. Συνολικά λοιπόν η G θα πρέπει να περιέχει τουλάχιστον 44 στοιχεία, το οποίο αντιβαίνει στο γεγονός ότι η G έχει τάξη 30.

Το παραπάνω επιχείρημα μας λέει πως εάν μία G έχει k διαφορετικές ομάδες τάξης p, τότε η G θα περιέχει τουλάχιστον $k(p-1)$ στοιχεία τάξης p.

Ερχόμαστε τώρα σε ένα τρίτο, πιο περίπλοκο, παράδειγμα. Έστω $|G| = 48 = 2^4 \cdot 3$. Τότε η G δεν είναι απλή. Για να το αποδείξουμε αυτό, παρατηρούμε πρώτα ότι $s_2 = 1$ ή 3. Αν $s_2 = 1$ τότε έχει κανονική Sylow 2-υποομάδα τάξης 16. Αν $s_2 = 3$, έστω H_1, H_2, H_3 οι Sylow 2-υποομάδες της. Τότε $|H_i| = 16$ για κάθε i. Η κρίσιμη παρατήρηση εδώ είναι πως η τομή οποιονδήποτε δύο εξ' αυτών έχει τάξη 8. Αν όχι, τότε για κάποια $i \neq j$ θα είχαμε $|H_i \cap H_j| \leqslant 4$ κι άρα, από τον τύπο γινομένου (άσκηση 1.38) θα παίρναμε

$$|H_i \cdot H_j| = \frac{|H_i||H_j|}{|H_i \cap H_j|} \geqslant \frac{16^2}{4} = 64$$

το οποίο είναι άτοπο διότι $H_i \cdot H_j \subseteq G$. Άρα

$$H_i \cap H_j \trianglelefteq H_i,$$

$$H_i \cap H_j \trianglelefteq H_j$$

ως υποομάδες δείκτου 2. Συμπεραίνουμε πως η κανονικοποιούσα της τομής $N_G(H_i \cap H_j)$ περιέχει τις H_i, H_j γνήσια κι άρα $N_G(H_i \cap H_j) = G$. Αυτό όμως σημαίνει πως $H_i \cap H_j \trianglelefteq G$.

Για $|G| = p^n m$ ορίζουμε $s_{p,i}$ το πλήθος των υποομάδων της G τάξης p^i με $1 \leqslant i \leqslant n$. Το 1ο Θεώρημα Sylow δίνει πως $s_{p,i} \geqslant 1$ για κάθε i. Το 3ο Θεώρημα Sylow μας λέει πως το $s_p := s_{p,n} \equiv 1 \mod p$ και διαιρεί το m. Στην πραγματικότητα, μπορούμε να αποδείξουμε πως $s_{p,i} \equiv 1 \mod p$ για κάθε $1 \leqslant i \leqslant n$. Η απόδειξη, που είναι λίγο πιο εκτενής και θα την παραλείψουμε, βασίζεται στην απόδειξη της επαγωγικής σχέσης $s_{p,i} \equiv s_{p,i+1} \mod p$. Για $i = 1$ όμως μπορούμε να δώσουμε μία πιο στοιχειώδη απόδειξη του ισχυρισμού για p-ομάδες.

Θεώρημα 2.8. *Έστω G μια πεπερασμένη ομάδα τάξης p^n και έστω $m_p = s_{p,1}$ το πλήθος των υποομάδων της τάξης p. Τότε $m_p \equiv 1 \mod p$.*

Απόδειξη. Για να μετρήσω το πλήθος των υποομάδων της G τάξης p, αρκεί να μετρήσω το πλήθος των στοιχείων της G τάξης p, αφού κάθε τέτοια υποομάδα παράγεται από αυτά τα στοιχεία. Για την ακρίβεια, κάθε τέτοια υποομάδα περιέχει ακριβώς $p-1$ στοιχεία τάξης p, άρα αν m_p είναι το πλήθος των ζητούμενων υποομάδων τότε υπάρχουν συνολικά $m_p(p-1)$ στοιχεία τάξης p μέσα στην G.

Από την άλλη, μπορούμε να μετρήσουμε ξεχωριστά τα στοιχεία τάξης p χωρίζοντας τα σε δύο υποκατηγορίες: εκείνα που ανήκουν στο κέντρο και εκείνα που είναι εκτός κέντρου. Αν $g \in Z(G)$ είναι ένα στοιχείο τάξης p, τότε το υποσύνολο

$$H_p = \{g \in Z(G) : g^p = e\}$$

είναι υποομάδα του κέντρου (αφού το κέντρο είναι αβελιανή υποομάδα της G). Ειδικότερα, το $Z(G)$ είναι μη τετριμμένη p-ομάδα τάξης p^k για κάποιο $k \leqslant n$. Άρα το κέντρο περιέχει $p^k - 1$ στοιχεία τάξης p. Αν $g \notin Z(G)$, τότε ο πληθάριθμος της κλάσης συζυγίας

$$|g^G| = [G : C_G(g)] = p^\ell > 1.$$

Όμως όλα τα στοιχεία της g^G έχουν την ίδια τάξη με το g, άρα έχουν τάξη p. Αθροίζοντας πάνω από όλες τις κλάσεις συζυγίας που δεν συμπεριλαμβάνονται στο κέντρο, συμπεραίνουμε πως το πλήθος των στοιχείων τάξης p εκτός κέντρου είναι αθροιστικά $\equiv 0 \mod p$, έστω ap.

Συνολικά, το πλήθος των στοιχείων τάξης p είναι ίσο με $p^k - 1 + ap$, ενώ από την άλλη είναι ίσο με $m_p(p-1)$. Άρα

$$p^k - 1 + ap = m_p(p-1) \Longrightarrow -1 \equiv -m_p \mod p \tag{4}$$

κι άρα $m_p \equiv 1 \mod p$. □

Χρησιμοποιώντας τα Θεωρήματα Sylow μπορούμε να χαρακτηρίσουμε (να κατατάξουμε) τις ομάδες που η τάξη τους έχει σχετικά απλή γραφή σε γινόμενο πρώτων.

Θεώρημα 2.9. *Έστω $n = pq$ με $p > q$. Τότε υπάρχουν το πολύ δύο (έως ισομορφισμού) ομάδες τάξης n. Η μία είναι η κυκλική τάξης n και, εάν $q|p-1$, τότε υπάρχει και μία δεύτερη μη αβελιανή ομάδα $G = \langle a, b\rangle$ με $a^q = 1$, $b^p = 1$ και $aba^{-1} = b^m$, όπου $m^q \equiv 1 \mod p$ αλλά $m \not\equiv 1 \mod p$.*

Απόδειξη. Έστω $|G| = pq$. Από το Θεώρημα του Cauchy συμπεραίνουμε πως υπάρχει $b \in G$ τάξης p και $a \in G$ τάξης q. Έστω $K = \langle b\rangle$ και $H = \langle a\rangle$.

Το 3ο Θεώρημα Sylow μας δίνει ότι $s_p = 1$ άρα $K \trianglelefteq G$. Επιπλέον $s_q = 1$ ή p. Αν $s_q = 1$ τότε $H \trianglelefteq G$. Επιπλέον $H \cap K = \{e\}$ και $HK = G$ (εξηγήστε γιατί) κι έτσι $G = H \times K \simeq \mathbb{Z}_q \times \mathbb{Z}_p \simeq \mathbb{Z}_{pq}$.

Στην δεύτερη περίπτωση έχουμε $s_q = p$. Σε αυτήν την περίπτωση το 3ο Θεώρημα Sylow μας δίνει επιπλέον $s_q \equiv 1 \mod q$, άρα $q \mid p-1$. Αφού $K \trianglelefteq G$ έχουμε $aba^{-1} = b^m \in K$ για κάποιο $m \mod q$ με $m \neq 1$ (διότι αν $m = 1$ αναγόμαστε στην προηγούμενη περίπτωση). Επαγωγικά μπορούμε να δείξουμε πως $a^j ba^{-j} = b^{m^j}$ για κάθε $j \geqslant 1$. Ειδικότερα, για $j = q$ παίρνουμε $b = b^{m^q}$ άρα $m^q \equiv 1 \mod p$. □

Παρατηρήστε πως αν $q = 2$ τότε το παραπάνω Θεώρημα μας εγγυάται την ύπαρξη μιας μη αβελιανής ομάδας τάξης $2p$. Θα δούμε παρακάτω στο επόμενο κεφάλαιο πως η μη αβελιανή περίπτωση του παραπάνω Θεωρήματος μπορεί να περιγραφεί ως ένα *ημιευθές* γινόμενο δύο κυκλικών ομάδων.

Μπορούμε επίσης να χρησιμοποιήσουμε τα Θεωρήματα Sylow για να περιγράψουμε όλες τις ομάδες τάξης 8 και 12 (άσκηση 1.82), αυτό όμως το αφήνουμε ως άσκηση για την 3η ενότητα, αφού μιλήσουμε πρώτα για τις διεδρικές ομάδες.

Άσκηση 2.32. *Χρησιμοποιώντας μόνο το 1ο Θεώρημα Sylow, εξηγήστε γιατί κάθε ομάδα τάξης $2p^n$ δεν είναι απλή.*

Άσκηση 2.33. *Αν p είναι ο μικρότερος πρώτος που διαιρεί την τάξη της G και υπάρχει $H \leqslant G$ με $[G : H] = p$, δείξτε ότι $H \trianglelefteq G$. Γενικεύοντας την προηγούμενη άσκηση, χρησιμοποιώντας μόνο το 1ο Θεώρημα Sylow συμπεράνετε πως εάν $|G| = p^n q$ με $p > q$ και q πρώτος, τότε η G δεν είναι απλή. Πιο γενικά, χρησιμοποιώντας το 3ο Θεώρημα Sylow, δείξτε ότι αν $|G| = p^n m$ με $p > m$ τότε η G δεν είναι απλή.*

Άσκηση 2.34. *Βρείτε όλους τους $n = pq \leqslant 100$ για τους οποίους ισχύει πως κάθε ομάδα τάξης n είναι κυκλική.*

Άσκηση 2.35. *Αν $|G| = p^n$ και $\{e\} < H \trianglelefteq G$ δείξτε ότι $H \cap Z(G) \neq \{e\}$. Ειδικότερα, εάν $|H| = p$ τότε $H \leqslant Z(G)$.*

Άσκηση 2.36. *Έστω H μία Sylow p-υποομάδα μιας πεπερασμένης ομάδας G. Τότε η H είναι η μοναδική Sylow p-υποομάδα της $N_G(H)$.*

Άσκηση 2.37. *Έστω $|G| = p^3$ η οποία δεν είναι αβελιανή. Υπολογίστε το πλήθος των κλάσεων συζυγίας της G. Κάντε το ίδιο για μια ομάδα G με $|G| = p^n$ αν σας δίνεται ότι $|Z(G)| = p^{n-2}$.*

Άσκηση 2.38. *(Frattini argument) Έστω $K \trianglelefteq G$ με G πεπερασμένη. Έστω p ένας σταθερός πρώτος αριθμός που διαιρεί την τάξη της G και P μία Sylow p-υποομάδα της K. Τότε $G = K \cdot N_G(P)$.*

Άσκηση 2.39. *Αν X είναι ένα πεπερασμένο G-σύνολο και μια $H \leqslant G$ δρα μεταβατικά στο X, τότε $G = H \cdot G_x$ για κάθε $x \in X$. Παρατηρήστε ότι αυτό συνεπάγεται την προηγούμενη άσκηση.*

Άσκηση 2.40. *Έστω G μια πεπερασμένη ομάδα και P μία Sylow p-υποομάδα της G. Τότε, για κάθε $H \leqslant G$ με $N_G(P) \leqslant H$ έχουμε $N_G(H) = H$.*

Άσκηση 2.41. *Δείξτε ότι κάθε μη αβελιανή ομάδα τάξης $\leqslant 59$ δεν είναι απλή.*

Άσκηση 2.42. *Δείξτε ότι δεν υπάρχει απλή ομάδα τάξης $10 \cdot 7^n$.*

2.9 Θεώρημα Cayley και εισαγωγικές έννοιες αναπαραστάσεων ομάδων

Πολλές φορές μπορούμε να αντιληφθούμε ένα περίπλοκο αντικείμενο καλύτερα εάν το ενσωματώσουμε μέσα σε ένα πιο οικείο και κατανοητό περιβάλλον. Αυτή η απλή ιδέα έχει φυσικά εφαρμογή και στην θεωρία ομάδων (καθώς και σε όλα τα μαθηματικά), όταν προσπαθούμε να απεικονίσουμε αφηρημένες ομάδες μέσα σε ομάδες τις οποίες πιστεύουμε ότι καταλαβαίνουμε κάπως καλύτερα. Το πρώτο αποτέλεσμα σε αυτήν την κατεύθυνση ήταν το ακόλουθο αποτέλεσμα του Cayley. Θυμίζουμε πως στην υποενότητα 2.1 ορίσαμε για κάθε σύνολο X την ομάδα μεταθέσεων του S_X που είναι όλες οι ένα-προς-ένα και επί απεικονίσης από το X στον εαυτό του. Ειδικότερα, εάν $|X| = n$ τότε $S_X \simeq S_n$.

Θεώρημα 2.10. *(Cayley) Για κάθε ομάδα G υπάρχει μονομορφισμός*

$$G \to S_G.$$

Ειδικότερα, εάν $|G| = n$ τότε η G είναι ισόμορφη με κάποια υποομάδα της S_n.

Απόδειξη. Στην πραγματικότητα η απόδειξη είναι άμεση συνέπεια της θεωρίας των δράσεων. Η G δρα στον εαυτό της με την μετατόπιση και για κάθε $g \in G$ η απεικόνιση $L_g : G \to G$ με $L_g(x) = gx$ είναι ένα-προς-ένα και επί. Άρα $L_g \in S_G$. Η απεικόνιση

$$L : G \to S_G,\ L(g) = L_g$$

είναι ένα-προς-ένα και ομομορφισμός (άρα $G \simeq \operatorname{Im} L \leqslant S_{|G|}$). Πρώτα δείχνουμε πως η L είναι καλά ορισμένη. Πράγματι, εάν $L_{g_1} \neq L_{g_2}$ τότε υπάρχει $x \in G$ με $L_{g_1}(x) \neq L_{g_2}(x)$, δηλαδή $g_1 x \neq g_2 x$ κι άρα $g_1 \neq g_2$. Αντίστροφα, εάν $g_1 \neq g_2$ τότε $L_{g_1}(e) \neq L_{g_2}(e)$ κι άρα $L_{g_1} \neq L_{g_2}$. Τέλος, το γεγονός ότι η L είναι ομομορφισμός έπεται εύκολα καθώς

$$L_{g_1} \circ L_{g_2}(x) = g_1(g_2 x) = (g_1 g_2)x = L_{g_1 g_2}(x)$$

το οποίο ολοκληρώνει την απόδειξη. □

Ο ομομορφισμός L ονομάζεται και αριστερή αναπαράσταση της G. Συχνά, προτιμάμε να δούμε μια ομάδα ως ομάδα πινάκων αντί ως ομάδα μεταθέσεων. Το Θεώρημα Cayley μας δίνει το εξής όμορφο συμπέρασμα.

Πόρισμα 2.2. *Έστω $\mathbb{F}$ σώμα. Κάθε ομάδα G τάξης n μπορεί να αναπαρασταθεί μέσα στην $GL_n(\mathbb{F})$, δηλαδή υπάρχει μονομορφισμός $G \to GL_n(\mathbb{F})$.*

Απόδειξη. Έστω I_n ο ταυτοτικός $n \times n$ πίνακας και γράφουμε ϵ_i για την i-στήλη του, δηλαδή $I_n = (\epsilon_1, \epsilon_2, ..., \epsilon_n)$. Η ομάδα $P(n, \mathbb{F})$ των $n \times n$ που έχουν ως στήλες αναδιατάξεις των ϵ_i (πίνακες μεταθέσεων) είναι υποομάδα της $\mathrm{GL}(n, \mathbb{F})$. Επιπλέον, αν $P \in P(n, \mathbb{F})$ με $P = (\epsilon_{\sigma(1)}, \epsilon_{\sigma(2)}, ..., \epsilon_{\sigma(n)})$, τότε η απεικόνιση $P(n, \mathbb{F}) \to S_n$ με

$$P = (\epsilon_{\sigma(1)}, \epsilon_{\sigma(2)}, ..., \epsilon_{\sigma(n)}) \to \sigma$$

είναι ισομορφισμός. Το Cayley μας δίνει έναν μονομορφισμό $G \to P(n, \mathbb{F}) \leqslant \mathrm{GL}(n, \mathbb{F})$. □

Θεώρημα 2.11. *(Γενίκευση του Cayley) Αν $H \leqslant G$ και $[G : H] = n$, τότε υπάρχει ομομορφισμός $f : G \to S_n$ με $\ker f \leqslant H$ (ο ομομορφισμός αυτός καλείται αναπαράσταση της G στα σύμπλοκα της H).* .

Απόδειξη. Η G δρα στο σύνολο των αριστερών συμπλόκων της H στην G και για $g \in G$ ορίζουμε την συνηθισμένη δράση

$$f_g : X \to X, \ f_g(xH) = (gx)H.$$

Αφήνουμε ως άσκηση στον αναγνώστη να ελέγξει πως η f_g είναι μετάθεση του X και ότι η $f : G \to S_X$ με $f(g) = f_g$ είναι ομομορφισμός. Αν τώρα $g \in \ker f$ δηλαδή $f_g = e_{S_X}$, τότε $gxH = xH$ για κάθε $x \in G$. Επιλέγοντας το στοιχείο $x = e$ παίρνουμε $g \in H$, κι άρα $\ker f \leqslant H$. □

Παρατηρήστε πως το προηγούμενο Θεώρημα είναι όντως γενίκευση του Cayley στην περίπτωση της τετριμμένης υποομάδας $H = \{e\}$.

Πόρισμα 2.3. *Αν η G είναι απλή και $H \leqslant G$ με $[G : H] = n$, τότε η G μπορεί να αναπαρασταθεί στην S_n, κι ειδικότερα $|G| \mid n!$.*

Απόδειξη. Από το προηγούμενο Θεώρημα βρίσκουμε ομομορφισμό $f : G \to S_n$ με $\ker f \leqslant H < G$. Αφού η G είναι απλή και ο πυρήνας $\ker f$ είναι κανονική υποομάδα της, τότε $\ker f = \{e\}$ και άρα ο f είναι μονομορφισμός. □

Πόρισμα 2.4. *Μια άπειρη απλή ομάδα G δεν έχει γνήσιες υποομάδες πεπερασμένου δείκτη.*

Το Πόρισμα 2.3 δίνει πολύ ισχυρά αποτελέσματα για απλές ομάδες. Για παράδειγμα, για την απλή ομάδα $G = A_n$ με τάξη $n!/2$, το Θεώρημα του Cayley μας δίνει μονομορφισμό $G \to S_{n!/2}$, η οποία είναι τεράστια ομάδα. Το Πόρισμα 2.3 όμως μας δίνει (καθώς $[A_n : A_{n-1}] = n$) μονομορφισμό $G \to S_n$ (το οποίο είναι το βέλτιστο δυνατό).

Πιο γενικά, αν $|G| = p^n m$ με $(p, m) = 1$, τότε ξέρουμε ότι κάθε Sylow p-υποομάδα της έχει τάξη p^n και δείκτη m. Αν η G είναι απλή, τότε το Πόρισμα 2.3 μας δίνει $p^n m = |G| \mid m!$, δηλαδή

$$p^n \mid (m-1)!.$$

Αν αυτή η ανισότητα δεν ισχύει για κάποιον πρώτο $p \mid |G|$, τότε συμπεραίνουμε ότι η G δεν μπορεί να είναι απλή. Για παράδειγμα, μια ομάδα τάξης $|G| = 36 = 2^2 \cdot 3^2$ δεν μπορεί να είναι απλή, καθώς αν ήταν για $p = 3$ θα παίρναμε $9 \mid 3! = 6$. Επιπλέον, αυτή η συνθήκη μας επιβάλλει έναν περιορισμό που πρέπει να ισχύει για τις πρώτες δυνάμεις που διαιρούν την τάξη μιας απλής ομάδας G. Για παράδειγμα, αν p, m είναι δύο σταθεροί αριθμοί με p πρώτο και $(p, m) = 1$, Η τελευταία ανισότητα μας λέει ότι μια ομάδα τάξης $p^n m$ μπορεί να είναι απλή μόνο για πεπερασμένες τιμές του n.

Μας νοιάζει λοιπόν να μελετήσουμε με ποιούς τρόπους μπορούμε να φέρουμε μια τυχαία ομάδα G σε μια πιο οικεία μορφή. Γενικότερα έχουμε τον ακόλουθο ορισμό:

Ορισμός 2.10. *Μια αναπαράσταση μιας ομάδας G επί ενός διανυσματικού χώρου V που ορίζεται υπεράνω ενός σώματος K είναι ένας ομομορφισμός ομάδων $G \to GL(V)$, την γενική γραμμική ομάδα του V. Δηλαδή, μια αναπαράσταση είναι μια απεικόνιση*

$$\rho\colon G \to \mathrm{GL}\,(V)$$

τέτοια ώστε

$$\rho(g_1 g_2) = \rho(g_1)\rho(g_2),$$

για κάθε $g_1, g_2 \in G$. Όταν ο V είναι πεπερασμένης διάστασης n υπεράνω του $\mathbb{F}$ γράφουμε πιο απλά

$$\rho\colon G \to \mathrm{GL}\,(n, \mathbb{F}).$$

Ο αριθμός $n \geqslant 1$ ονομάζεται βαθμός της αναπαράστασης ρ.

Ορισμός 2.11. *Μια αναπαράσταση ρ της G ονομάζεται πιστή εάν $\ker \rho = \{e\}$, δηλαδή αν και μόνο αν είναι μονομορφισμός.*

Για κάθε $n \geqslant 1$ υπάρχει η αναπαράσταση $\rho : G \to \mathrm{GL}\,(n, \mathbb{F})$ με $\rho(g) = I_n$ για κάθε $g \in G$. Προφανώς αυτός ο ομομορφισμός δεν κρατάει καμία πληροφορία για την δομή της G και είναι πρακτικά άχρηστος. Μας δείχνει όμως ότι κάθε ομάδα G επιδέχεται αναπαράσταση οσοδήποτε μεγάλου βαθμού. Ειδικότερα, για $n = 1$, η αναπαράσταση $\rho : G \to \mathrm{GL}\,(1, \mathbb{F})$ με $\rho(g) = (1)$ για κάθε $g \in G$ ονομάζεται η *τετριμμένη* αναπαράσταση της G.

Έστω τώρα $G \simeq \mathbb{Z}_n$ και g ένας γεννήτορας της G. Τότε οι αναπαραστάσεις βαθμού 1 επί του $\mathbb{C}$ είναι όλοι οι ομομορφισμοί $\rho : G \to \mathbb{C}^\times = \mathbb{C} - \{0\}$. Κάθε τέτοιος ομομορφισμός προφανώς καθορίζεται από την εικόνα του γεννήτορα g, άρα αν $\rho(g) = z \in \mathbb{C}^\times$, τότε $z^n = \rho(e) = 1$ κι άρα $z = \zeta$ για κάποιο $\zeta \in S^1$ τέτοιο ώστε $\zeta^n = 1$ (οι n-οστές ρίζες της μονάδας). Καθορίζοντας την εικόνα του γεννήτορα g καθορίζεται φυσικά και η εικόνα κάθε στοιχείου της G. Αν επιπλέον το $\rho(g)$ είναι γεννήτορας της ομάδας των n-οστών ριζών της μονάδας, τότε

$$\rho(g) = e^{\frac{2\pi i k}{n}},$$

για κάποιο $(k, n) = 1$ κι έτσι

$$\rho(g^m) = e^{\frac{2\pi i k m}{n}}.$$

Σε αυτήν την περίπτωση η αναπαράσταση είναι προφανώς πιστή.

Άσκηση 2.43. *Ολοκληρώστε την απόδειξη του Θεωρήματος 2.11.*

Άσκηση 2.44. *Βρείτε όλες τις αναπαραστάσεις*

$$\rho\colon \mathbb{Z}_n \to \mathrm{GL}\,(2, \mathbb{C}).$$

Άσκηση 2.45. *Έστω δύο αναπαραστάσεις $\rho_1 : G \to \mathrm{GL}\,(n, \mathbb{F})$ και $\rho_2 : G \to \mathrm{GL}\,(m, \mathbb{F})$ της G υπεράνω του $\mathbb{F}$. Οι ρ_1, ρ_2 ονομάζονται ισοδύναμες εάν $n = m$ και υπάρχει $T \in \mathrm{GL}\,(n, \mathbb{F})$ τέτοιος ώστε*

$$\rho_2(g) = T\rho_1(g)T^{-1}$$

για κάθε $g \in G$. Δείξτε ότι αυτή η σχέση είναι όντως σχέση ισοδυναμίας.

2.10 Επαναληπτικές ασκήσεις δευτέρου κεφαλαίου

Άσκηση 2.46. *Έστω G μια πεπερασμένη ομάδα, $g \in G$ και $x \in Z(G)$. Δείξτε ότι $|g^G| = |(gx)^G|$.*

Άσκηση 2.47. *Έστω μια ομάδα G που δρα στο X με $|X| = 19$, $|G| = 35$ και $X_G = \varnothing$. Βρείτε τον αριθμό των τροχιών της δράσης και τον πληθάριθμο κάθε τροχιάς.*

Άσκηση 2.48. *Χρησιμοποιώντας την άσκηση 1.68, δείξτε ότι* $|(12)^{S_n}| = \binom{n}{2}$ *και βρείτε την* $C_{S_n}((12))$. *Επιβεβαιώστε ότι οι απαντήσεις σας ικανοποιούν το Θεώρημα τροχιάς-σταθεροποιούσας.*

Άσκηση 2.49. *Δείξτε ότι αν η* G *είναι πεπερασμένη και* $s_p = 1$ *για κάθε* $p \mid |G|$ *τότε η* G *είναι ευθύ γινόμενο των Sylow* p*-υποομάδων της.*

Άσκηση 2.50. *Αν* $G_1 \circlearrowright X_1$ *και* $G_2 \circlearrowright X_2$, *δείξτε ότι η* $G := G_1 \times G_2$ *δρα στο* $X := X_1 \times X_2$. *Για* $x \in X$ *υπολογίστε την τροχιά και την σταθεροποιούσα του.*

Άσκηση 2.51. *Έστω* G *μία άπειρη απλή ομάδα. Δείξτε ότι για κάθε μη τετριμμένο* $x \in G$ *και μη τετριμμένη υποομάδα* $H < G$ *έχουμε ότι τα σύνολα* x^G *και* $[H]$ *είναι άπειρα.*

Άσκηση 2.52. *Έστω* $|G| = p^n$ *με* $n \geqslant 3$ *και* $|Z(G)| = p$. *Δείξτε ότι υπάρχει κλάση συζυγίας με* p *στοιχεία, δηλαδή* $|x^G| = p$ *για κάποιο* $x \in G$.

Άσκηση 2.53. *Έστω* K *μία Sylow* p*-υποομάδα της* G *και* $H \leqslant G$. *Έπεται ότι η* $K \cap H$ *είναι Sylow* p*-υποομάδα της* H;

Άσκηση 2.54. *Δείξτε ότι υπάρχει πεπερασμένη ομάδα* G *με τρεις Sylow* p*-υποομάδες* P_1, P_2 *και* P_3 *τέτοιες ώστε* $P_1 \cap P_2 = \{e\}$ *και* $P_1 \cap P_3 \neq \{e\}$.

Άσκηση 2.55. *Έστω* K *μία Sylow* p*-υποομάδα της* G *και* $f : G \to G$ *ένας αυτομορφισμός της* G. *Έπεται ότι* $f(K) = K$;

Άσκηση 2.56. *Έστω* G *μια πεπερασμένη ομάδα και* $k(G)$ *το πλήθος των ξένων κλάσεων συζυγίας της* G. *Δείξτε ότι αν το* $k(G)$ *είναι άρτιο, τότε η τάξη της* G *είναι άρτια. Δείξτε επίσης ότι το αντίστροφο δεν ισχύει.*

Άσκηση 2.57. *Αν* G *είναι μια πεπερασμένη ομάδα με κλάσεις συζυγίας* $C_1, C_2, ..., C_m$ *και* $x_i \in C_i$, *δείξτε ότι* $G = \langle x_1, ..., x_m \rangle$.

Άσκηση 2.58. *Έστω* G *πεπερασμένη ομάδα,* $H \trianglelefteq G$ *και* P *μία* p*-υποομάδα της* G. *Αν* $|H| \not\equiv 1 \mod p$ *τότε* $H \cap C_G(P) \neq \{e\}$.

Άσκηση 2.59. *Έστω* G *ομάδα,* $H \leqslant G$ *και* $X = [H] = \{gHg^{-1}, g \in G\}$. *Δείξτε ότι υπάρχει ομομορφισμός* $f : G \to S_X$ *με* $\ker f \leqslant N_G(H)$ *(ο ομομορφισμός αυτός καλείται αναπαράσταση της* G *στις συζυγίες της* H*).*

Άσκηση 2.60. *Εστω* $|G| = p^n$ *με* $p > n$ *και η* G *δρα σε ένα πεπερασμένο σύνολο* X *με* m *στοιχεία. Αν* $G \to S_m$ *μονομορφικά και υπάρχει* $x \in X$ *με* $g \cdot x = x$ *για κάθε* $g \in G$ *τότε* $m \geqslant np + 1$.

Άσκηση 2.61. *Αν* $|G| = p^2 q$ *όπου* p, q *δύο οποιοιδήποτε πρώτοι, δείξτε ότι η* G *δεν είναι απλή.*

Άσκηση 2.62. *Αν* G *μη αβελιανή με* $61 \leqslant |G| \leqslant 100$ *τότε η* G *δεν είναι απλή.*

Άσκηση 2.63. *Αν η* G *είναι πεπερασμένη μη αβελιανή απλή ομάδα και* $H < G$, *τότε* $[G : H] \geqslant 5$.

Άσκηση 2.64. *Για* $\sigma \in A_n$, *δείξτε ότι* $\sigma^{S_n} = \sigma^{A_n}$ *αν και μόνο αν η* σ *μετατίθεται με κάποια περιττή μετάθεση της* S_n.

Άσκηση 2.65. * *Έστω* G *πεπερασμένη,* $H \trianglelefteq G$ *με* $[G : H] = p$ *και* $x \in H$ *με* $C_H(x) < C_G(x)$. *Αν* $y \in H$ *συζυγές του* x *στην* G, *δείξτε ότι το* y *είναι συζυγές του* x *μέσα στην* H. *Πώς συνδέεται αυτό με την προηγούμενη άσκηση;*

Άσκηση 2.66. *Χρησιμοποιώντας την άσκηση 1.68 και την άσκηση 2.65 (ή απλούστερα την άσκηση 2.64) δείξτε ότι η A_n είναι απλή για $n \geqslant 5$.*

Άσκηση 2.67. * *Έστω G μια υποομάδα της S_n τέτοια ώστε για κάθε $\sigma \in G - \{id\}$ υπάρχει μοναδικό $k \in X_n$ που σταθεροποιείται από την σ. Δείξτε ότι αυτό το k είναι το ίδιο για τα στοιχεία της $G - \{id\}$.*

3 Γεωμετρία

Σε αυτήν την ενότητα μελετάμε εν συντομία ορισμένες πτυχές της θεωρίας ομάδων που συνδέονται άμεσα με την γεωμετρία. Και πάλι εδώ η έννοια της δράσης είναι κεντρική, καθώς ενδιαφερόμαστε για ομάδες που δρουν σε διαφόρων ειδών χώρους (πχ. πολλαπλότητες). Σε αυτό το κεφάλαιο δεν δίνουμε πολλές αποδείξεις, αλλά κυρίως μια περιγραφή ορισμένων σημαντικών παραδειγμάτων.

3.1 Διεδρικές ομάδες και ημιευθέα γινόμενα

Ορίζουμε πρώτα μία συγκεκριμμένη οικογένεια ομάδων που εμφανίζονται συχνά σε διάφορα μέρη μέσα στην Θεωρία ομάδων και έχουν έντονη γεωμετρική υφή.

Ορισμός 3.1. *Για κάθε $n \geqslant 2$ ορίζουμε την διεδρική ομάδα D_{2n} ως μια ομάδα τάξης $2n$ που παράγεται από δύο στοιχεία x, y (δηλαδή $D_{2n} = \langle x, y \rangle$) τα οποία ικανοποιούν τις σχέσεις $x^n = e$, $y^2 = e$ και $yxy = x^{-1}$.*

Είναι χρήσιμο εδώ να επισημάνουμε πως πολλές φορές στην βιβλιογραφία η D_{2n} συμβολίζεται με D_n.

Αν και την ορίσαμε αφηρημένα, αλγεβρικά είναι απλό να δει κανείς ότι η διεδρική ομάδα τάξης $2n$ είναι η ομάδα αυτομορφισμών του κανονικού n-γώνου, όπου το στοιχείο x είναι μια στροφή κατά $\frac{2\pi}{n}$ μοίρες, y είναι μια ανάκλαση ως προς έναν σταθερό άξονα και η σχέση $yxy = x^{-1}$ περιγράφει την σχέση που ικανοποιούν μεταξύ τους οι δύο γεννήτορες της στροφής και της ανάκλασης.

Η ομάδα D_4 είναι απλά η ομάδα του Klein $V = \mathbb{Z}_2 \times \mathbb{Z}_2$. Είναι απλό να δει κανείς ότι αυτή είναι η μόνη αβελιανή διεδρική ομάδα.

Άσκηση 3.1. *Η D_{2n} δεν είναι αβελιανή για $n \geqslant 3$. Ειδικότερα, $D_{2n} \not\simeq \mathbb{Z}_n \times \mathbb{Z}_2$.*

Θα δούμε παρακάτω ότι η D_{2n} είναι το *ημιευθές* γινόμενο των $\mathbb{Z}_n$ και $\mathbb{Z}_2$. Το επόμενο Θεώρημα μας λέει ότι οι διεδρικές ομάδες εμφανίζονται συχνά.

Θεώρημα 3.1. *Αν η G είναι μια πεπερασμένη ομάδα και υπάρχουν $a, b \in G$ με $a^2 = e = b^2$ τότε $\langle a, b \rangle \simeq D_{2n}$.*

Απόδειξη. Αφού η G είναι πεπερασμένη, έπεται ότι η τάξη του στοιχείου ab είναι πεπερασμένη. Έστω n η τάξη του. Θα δείξουμε ότι $|\langle a, b \rangle| = 2n$.

Έστω $s = ab$. Τότε $asa = a^2ba = ba = (ab)^{-1} = s^{-1}$. Βλέπουμε λοιπόν πως το a θα παίξει τον ρόλο της ανάκλασης και το s θα παίξει τον ρόλο του στοιχείου της στροφής. Για αυτόν τον λόγο θεωρούμε τώρα τα στοιχεία as^i, με $i \geqslant 0$. Κάθε τέτοιο στοιχείο είναι $\neq e$. Αν όχι, τότε θα υπήρχε ένα ελάχιστο k με $as^{k=e}$ (το οποίο εύκολα ελέγχουμε ότι θα έπρεπε αναγκαστικά να είναι $\geqslant 3$) και τότε θα παίρναμε

$$e = as^k = a^2bs^{k-1} = bs^{k-1}.$$

Αφού το b έχει τάξη 2 αυτή η σχέση τώρα μας δίνει

$$e = s^{k-1}b = s^{k-2}ab^2 = s^{k-2}a$$

η οποία, αφού και το a έχει τάξη 2, γράφεται ως

$$e = as^{k-2}.$$

Αυτό όμως αντιβαίνει στην αρχική μας υπόθεση για το k. Άρα $as^i \neq e$ το οποίο άμεσα συνεπάγεται πως $as^i \neq s^j$ για κάθε i, j. Άρα

$$\langle s \rangle \cup a\langle s \rangle \subseteq \langle a, b \rangle,$$

όπου η αριστερή ξένη ένωση περιέχει ακριβώς $2n$ στοιχεία. Αντίστροφα όμως, το σύνολο

$$A = \{a^i s^j,\ 0 \leqslant 1 \leqslant 1, 0 \leqslant j \leqslant n-1$$

είναι κλειστό ως προς την πράξη καθώς οι λέξεις στα στοιχεία a, b είναι ακριβώς οι λέξεις στα στοιχεία a, s (δηλαδή $\langle a, b\rangle = \langle a, s\rangle = \langle s\rangle \cup a\langle s\rangle$) και το ζητούμενο έπεται. □

Άσκηση 3.2. *Υπολογίστε τις τάξεις όλων των στοιχείων των* D_6, D_8, D_{10}.

Άσκηση 3.3. *Δείξτε ότι* $D_6 \simeq S_3$.

Άσκηση 3.4. *Δείξτε ότι* $D_{12} \simeq S_3 \times \mathbb{Z}_2$.

Ο παρακάτω ορισμός γενικεύει τον ορισμό του ευθέους γινομένου ώστε να συμπεριλαμβάνει και τις διεδρικές ομάδες.

Ορισμός 3.2. *Έστω G ομάδα και $K \leqslant G$. Μια άλλη υποομάδα $H \leqslant G$ λέγεται συμπλήρωμα της K στην G εάν $K \cap H = \{e\}$ και $KH = G$.*

Δεν είναι απαραίτητο πως μια υποομάδα της G έχει συμπλήρωμα. Επίσης, εάν μια υποομάδα K έχει συμπλήρωμα, αυτό δεν είναι απαραιτήτως μοναδικό. Όλα τα συμπληρώματα όμως της K είναι ισόμορφα μεταξύ τους. Πράγματι, εάν H είναι ένα συμπλήρωμα της K, τότε το δεύτερο Θεώρημα ισομορφισμών μας δίνει

$$\frac{G}{K} = \frac{KH}{K} \simeq \frac{H}{K \cap H} = \frac{H}{\{e\}} \simeq H.$$

Προφανώς, εάν οι K, H είναι κανονικές υποομάδες της G τότε η G είναι το ευθύ γινόμενο $K \times H$. Μπορεί όμως να είναι κανονική στην G μόνο η μία από τις δύο.

Ορισμός 3.3. *Μια ομάδα G είναι το ημιευθύ γινόμενο της K επί H εάν $K \trianglelefteq G$ και η K έχει συμπλήρωμα $H_1 \simeq H$. Γράφουμε $K \rtimes H = G$.*

Προφανώς, εάν το συμπλήρωμα H_1 της K είναι κανονική υποομάδα της G, τότε η G είναι το ευθύ γινόμενο τους. Άρα κάθε ευθύ γινόμενο είναι και ημιευθές γινόμενο.

Σε αυτό το σημείο, είναι απλό να συμπεράνουμε πως η διεδρική ομάδα D_{2n} είναι το ημιευθές γινόμενο $\mathbb{Z}_n \rtimes \mathbb{Z}_2$, η συμμετρικη΄ομάδα S_n είναι το ημιευθές γινόμενο $A_n \rtimes \langle\tau\rangle$ για οποιαδήποτε αντιμετάθεση τ, ενώ το Θεώρημα 2.9 μας λέει πως αν $p > q$ πρώτοι με $q \mid p-1$ τότε υπάρχει μια μη αβελιανή ομάδα τάξης pq, το ημιευθές γινόμενο τους $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

Είπαμε παραπάνω πως κάθε ευθύ γινόμενο είναι και ημιευθές γινόμενο, ενώ το αντίστροφο προφανώς δεν ισχύει. Αυτό που καθορίζει την διαφορά τους είναι το ”με ποιόν τρόπο” είναι κανονική η K μέσα στην G.

Έστω λοιπόν ένα ημιευθές γινόμενο $G = K \rtimes H$. Αφού $K \trianglelefteq G$, τότε προφανώς

$$xgx^{-1} \in K$$

για κάθε $x \in H, g \in K$. Ορίζεται έτσι ένας ομομορφισμός

$$\theta : H \to \mathrm{Aut}(K),\ \theta(x) = \theta_x$$

όπου θ_x είναι ο περιορισμός του αυτομορφισμού συζυγίας i_x στην K:

$$\theta_x = i_x|_K\,.$$

Κάθε ημιευθές γινόμενο της K επί H λοιπόν αντιστοιχεί σε κάποιον ομομορφισμό

$$\theta : K \to \mathrm{Aut}(H).$$

Λέμε ότι ο θ *υλοποιεί* το αντίστοιχο ημιευθές γινόμενο και γράφουμε $G = K \rtimes_\theta H$. Για παράδειγμα, αν ο θ είναι ο τετριμμένος ομομορφισμός (ο οποίος υπάρχει πάντα), δηλαδή αν $\theta_x(g) = g$ για κάθε $g \in K$ και για κάθε $x \in H$, τότε αυτό σημαίνει πως

$$xg = gx$$

$g \in K$ και για κάθε $x \in H$. Τότε αυτό μας δίνει πως $H \trianglelefteq G$ (εξηγήστε γιατί) κι άρα η G είναι το ευθύ γινόμενο $K \times H$. Αυτό μας εξηγεί γιατί ενώ το ευθύ γινόμενο δύο ομάδων K και H ορίζεται πάντα, μπορεί να ορίζονται ή να μην ορίζονται άλλα ημιευθέα γινόμενα τους.

Άσκηση 3.5. *Περιγράψτε όλους τους πιθανούς ομομορφισμούς $\theta : H \to Aut(K)$ για καθένα από τα παρακάτω ημιευθέα γινόμενα:*

α) $\mathbb{Z}_p \rtimes_\theta \mathbb{Z}_q$,
β) $A_n \rtimes_\theta \langle\tau\rangle$,
γ) $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2$.

Άσκηση 3.6. *Βρείτε το κέντρο της $Z(D_{2n})$ της διεδρικής ομάδας τάξης $2n$. (Υπόδειξη: διακρίνετε περιπτώσεις για n άρτιο και n περιττό).*

Άσκηση 3.7. *Περιγράψτε τις κλάσεις συζυγίας της D_{2n}.*

Άσκηση 3.8. *Δείξτε ότι η D_{2n} είναι υποομάδα της D_{4n}.*

Άσκηση 3.9. *Δείξτε ότι υπάρχουν ακριβώς δύο μη αβελιανές ομάδες τάξης 8, η μία εκ των οποίων είναι η D_8 ενώ η δεύτερη ονομάζεται ομάδα των Quaternions και συμβολίζεται με Q_8.*

Άσκηση 3.10. *Δείξτε ότι κάθε υποομάδα της ομάδας Q_8 των Quaternions είναι κανονική, απαντώντας έτσι στην αντίστροφη κατεύθυνσης της άσκησης 1.42.*

Άσκηση 3.11. **Δείξτε ότι υπάρχουν ακριβώς τρεις μη αβελιανές ομάδες τάξης 12, η μία εκ των οποίων είναι η D_{12} και η δεύτερη είναι η A_4. Για να βρείτε την τρίτη ομάδα, εξετάστε τα ημιευθέα γινόμενα της $\mathbb{Z}_3$ επί $\mathbb{Z}_4$ (η τρίτη ομάδα που θα βρείτε συμβολίζεται συνήθως με T).*

Άσκηση 3.12. *Έστω $n \geqslant 3$ ένας περιττός ακέραιος. Δείξτε ότι κάθε Sylow p-υποομάδα της D_{2n} είναι κυκλική.*

Άσκηση 3.13. *Δείξτε ότι η απεικόνιση $\rho : D_8 \to \mathrm{GL}(2, \mathbb{F})$ με*

$$\rho(x^i y^j) = A^i B^j,$$

όπου οι πίνακες A, B είναι οι

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

είναι μια αναπαράσταση της D_8 βαθμού 2.

Άσκηση 3.14. *Αν $\mathbb{F}$ σώμα, δείξτε ότι $GL_n(\mathbb{F}) = SL_n(\mathbb{F}) \rtimes \mathbb{F}$.*

Άσκηση 3.15. *Έστω $|G| = mn$ με $(m, n) = 1$. Αν $K \leqslant G$ με $|K| = m$ και $H \leqslant G$, δείξτε ότι η H είναι συμπλήρωμα της K αν και μόνο αν $|H| = n$.*

Μία υποομάδα $K \leqslant G$ που έχει την ιδιότητα που περιγράφει η προηγούμενη άσκηση (δηλαδή η τάξη της K είναι σχετικά πρώτη ως προς τον δείκτη της K μέσα στην G) ονομάζεται Hall υποομάδα της G. Η άσκηση 1.75 μας δίνει ότι αν μια Hall υποομάδα K της G είναι κανονική, τότε είναι η μοναδική υποομάδα τάξης $|K|$. Ο Hall έδειξε ότι αν η G είναι επιλύσιμη (θα μελετήσουμε τις επιλύσιμες ομάδες στο επόμενο κεφάλαιο) και $|G| = mn$ με m, n σχετικά πρώτους, τότε υπάρχει πάντα υποομάδα της G τάξης m. Το Θεώρημα Schur-Zassenhaus λέει πως αν μια Hall υποομάδα K της G είναι κανονική, τότε $G \simeq K \rtimes (G/K)$.

Άσκηση 3.16. *Ολοκληρώστε την απόδειξη ότι το ημιευθές γινόμενο $K \rtimes_\theta H$ είναι ευθύ αν και μόνο αν ο θ είναι ο τετριμμένος ομομορφισμός.*

Άσκηση 3.17. ** Αν $K \trianglelefteq G$ και η K είναι πλήρης, δείξτε ότι η K έχει συμπλήρωμα στην G. Μπορείτε να δείξτε ότι αληθεύει κάτι ισχυρότερο: η K έχει ευθύ παράγοντα, δηλαδή υπάρχει $H \trianglelefteq G$ με $G = K \times H$. (Υπόδειξη: Θεωρείστε την υποομάδα $H = C_G(K) := \bigcap_{k\in K} C_G(k)$).*

3.2 Σύντομη εισαγωγή στις ελεύθερες ομάδες

Σε αυτό το σημείο είναι χρήσιμο το εξής σχόλιο: ορίσαμε την ομάδα D_{2n} ως μια ομάδα με δύο γεννήτορες που ικανοποιούν μεταξύ τους κάποιες σχέσεις. Η ύπαρξη της D_{2n} ήταν εγγυημένη λόγω γεωμετρίας (ως ομάδα αυτομορφισμών του κανονικού n-γώνου) και για να την μελετήσουμε αλγεβρικά έπρεπε να ψάξουμε τις σχέσεις που συνδέουν τους δύο γεννήτορες της x, y. Πιο γενικά, αν μας δοθεί ένα σύνολο γεννητόρων X και κάποιες σχέσεις που ικανοποιούν αυτοί μεταξύ τους, πότε αυτές ορίζουν ομάδα;

Σε αυτό το σημείο δίνουμε μια ιδέα της κατάστασης χωρίς να είμαστε πολύ αυστηροί. Έστω σύνολο X, το οποίο ας υποθέσουμε για λόγους απλότητας πως είναι πεπερασμένο, δηλαδή $X = \{x_1, x_2, ..., x_n\}$. Κάθε σχέση μεταξύ των γεννητόρων μπορεί να γραφτεί στην μορφή $w(x_1, ..., x_n) = e$, οπου w είναι μία λέξη των x_i. Για παράδειγμα, οι τρεις σχέσεις που ορίζουν την D_{2n} είναι οι $w_1(x, y) = x^n$, $w_2(x, y) = y^2$, $w_3(x, y) = (yx)^2$. Η ομάδα που παράγεται από τα n αυτά στοιχεία, αν δεν ικανοποιούν καμία σχέση μεταξύ τους, ορίζεται ως

$$F_n = \langle x, x_2, ..., x_n\rangle$$

και καλείται *η ελέυθερη* ομάδα ομάδα σε n στοιχεία (γράφουμε $n = (F_n)$. Κάθε άλλη ομάδα G που παράγεται από n στοιχεία μπορεί να γίνει αντιληπτή ως ισόμορφη με κάποια ομάδα πηλίκο της F_n:

$$G \simeq F_n/I,$$

οπου η υποομάδα I σχετίζεται με τις έξτρα συνθήκες που ικανοποιούν οι γεννότηρες της G. Για παράδειγμα, αν $n = 1$, τότε $F_1 \simeq \mathbb{Z}$ και κάθε ομάδα που παράγεται από ένα στοιχείο (δηλαδή κάθε κυκλική ομάδα) είναι ισόμορφη με κάποια $\mathbb{Z}_n$. Σε αυτήν την περίπτωση έχουμε

$$G \simeq \frac{F_1}{I} := \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n,\ n = |G|.$$

Αν $n \geqslant 2$ τότε η F_n είναι άπειρη αριθμήσιμη, καθώς κάθε στοιχείο της F_n είναι πεπερασμένη λέξη επί των x_i. Απο την άλλη, κάθε F_n έχει τετριμμένο κέντρο (γιατί;)

Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα είναι εξ' ορισμού πεπερασμένη παραγόμενη, και μπορεί να προκύψει από την F_n αν ζητήσουμε κάθε δύο γεννήτορες να μετατίθονται, δηλαδή $w_{ij} := x_i x_j x_i^{-1} x_j^{-1} = e$. Για παράδειγμα, έχουμε

$$\mathbb{Z}^n \simeq \langle x_1, x_2, ..., x_n | w_{ij} = e,\ \forall\, i < j\rangle,$$

ενώ με παρόμοιο τρόπο βλέπουμε πως

$$\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z} \simeq \langle x_1, x_2, x_3 | w_{12} = e,\ w_{13} = e,\ w_{23} = e,\ x_1^2 = e,\ x_2^5 = e\rangle.$$

Από την άλλη, κάθε πεπερασμένη ομάδα G είναι προφανώς πεπερασμένα παραγόμενη κι έτσι η G είναι πηλίκο κάποιας F_n, και αν επιλέξουμε ένα σύνολο γεννητόρων $G = \langle X\rangle$, τότε η G είναι αβελιανή αν και μόνο αν $w_{ij} = e$ για κάθε $x_i, x_j \in X$.

Άσκηση 3.18. *Εξηγήστε γιατί η F_n είναι centerless για $n \geqslant 2$.*

3.3 Ισομετρίες Ευκλείδιων χώρων

Εστιάζουμε τώρα την μελέτη μας στον n-διάστατο ευκλείδιο χώρο $\mathbb{R}^n$, ο οποίος είναι n-διάστατος διανυσματικός χώρος πάνω από το σώμα των πραγματικών αριθμών με βάση $\{e_1, ..., e_n\}$ οπου $e_i = (0, ..., 0, 1, 0, ..., 0)$ στην i-συντεταγμένη. Ο χώρος $\mathbb{R}^n$ είναι εφοδιασμένος με το σύνηθες εσωτερικό γινόμενο $\langle x, y\rangle = x_1y_1 + ... + x_ny_n$ για $x = (x_i)_{i=1}^n$, $y = (y_i)_{i=1}^n$ και θεωρούμε την συνήθη ευκλείδια μετρική $d(x, y)$ που δίνεται από την 2-νόρμα $d(x, y) = \|x-y\|_2$, όπου $\|x\|_2^2 := \langle x, x\rangle$, είναι χώρος Hilbert. Γενικότερα, μια ορθοκανονική βάση $\{u_1, ..., u_n\}$ του $\mathbb{R}^n$ είναι ένα υποσύνολο του με $\langle u_i, u_j\rangle = \delta_{ij}$ (το δ του Kronecker).

Ορισμός 3.4. *Μια ευκλείδια ισομετρία $T : \mathbb{R}^n \to \mathbb{R}^n$ είναι μια απεικόνιση που διατηρεί την ευκλείδια μετρική, δηλαδή $d(T(x), T(y)) = d(x, y)$ (ισοδύναμα $\|T(x) - T(y)\|_2 = \|x - y\|_2$) για κάθε $x, y \in \mathbb{R}^n$.*

Προφανώς, για κάθε $w \in \mathbb{R}^n$ η απεικόνιση *μεταφοράς* $T_w(x) := x + w$ είναι ισομετρία. Υπάρχουν όμως και άλλες ισομετρίες του $\mathbb{R}^n$, το σύνολο των οποίων θα προσπαθήσουμε να περιγράψουμε. Θα χρειαστούμε την ακόλουθη έννοια.

Ορισμός 3.5. *Ένας γραμμικός μετασχηματισμός $S : \mathbb{R}^n \to \mathbb{R}^n$ ονομάζεται ορθογώνιος εάν $\|S(x)\|_2 = \|x\|_2$ για κάθε $x \in \mathbb{R}^n$.*

Παρατηρήστε πως κάθε ορθογώνιος μετασχηματισμός είναι αντιστρέψιμος (γιατί;). Πολύ περισσότερο, κάθε ορθογώνιος μετασχηματισμός είναι ισομετρία.

Άσκηση 3.19. *Αποδείξτε πως κάθε ισομετρία είναι $1-1$.*

Άσκηση 3.20. *Η απεικόνιση μεταφοράς T_w είναι γραμμική αν και μόνο αν $w = 0$.*

Άσκηση 3.21. *Αποδείξτε πως κάθε ορθογώνιος μετασχηματισμός είναι αντιστρέψιμος.*

Λήμμα 3.1. *Κάθε ορθογώνιος γραμμικός μετασχηματισμός $S : \mathbb{R}^n \to \mathbb{R}^n$ είναι ισομετρία.*

Απόδειξη. Έστω δύο σημεία $x, y \in \mathbb{R}^n$. Τότε έχουμε

$$\|S(x) - S(y)\|_2 = \|S(x - y)\|_2 = \|x - y\|_2$$

και το ζητούμενο έπεται. □

Άσκηση 3.22. *Ένας γραμμικός μετασχηματισμός S είναι ορθογώνιος αν και μόνο αν απεικονίζει την βάση $(e_i)_{i=1}^n$ σε ορθοκανονική βάση.*

Παρατηρήστε επίσης πως ισχύει και το αντίστροφο του παραπάνω λήμματος: αν ένας γραμμικός μετασχηματισμός S είναι ισομετρία τότε είναι ορθογώνιος (γιατί;). Για την εύρεση όλων των ισομετριών του $\mathbb{R}^n$ θα μας χρειαστεί το ακόλουθο λήμμα, του οποίου η απόδειξη χρησιμοποιεί ένα στάνταρ τρικ.

Πρόταση 3.1. *Κάθε ισομετρία $T : \mathbb{R}^n \to \mathbb{R}^n$ με $T(0) = 0$ είναι γραμμικός μετασχηματισμός (άρα και ορθογώνιος).*

Ως πόρισμα των παραπάνω έχουμε τώρα το ακόλουθο Θεώρημα που περιγράφει τις ισομετρίες του n-διάστατου Ευκλείδιου χώρου $\mathbb{R}^n$.

Θεώρημα 3.2. *Η ομάδα των ισομετριών του $S : \mathbb{R}^n \to \mathbb{R}^n$ με $S(0) = 0$ είναι υποομάδα της $GL_n(\mathbb{R})$, ονομάζεται ορθογώνια ομάδα και συμβολίζεται με $O(n, \mathbb{R})$.*

Επιπλέον, κάθε ισομετρία $T : \mathbb{R}^n \to \mathbb{R}^n$ είναι σύνθεση μιας μεταφοράς T_w και ενός ορθογώνιου μετασχηματισμού S. Η ομάδα όλων των ισομετριών του $\mathbb{R}^n$ συμβολίζεται με $M(n, \mathbb{R})$.

Απόδειξη. Η απόδειξη του γεγονότος ότι το σύνολο των ισομετριών που σταθεροποιούν την αρχή των αξόνων είναι ομάδα είναι πολύ απλή αφήνεται ως άσκηση. Προφανώς, από την προηγούμενη Πρόταση, κάθε τέτοια ισομετρία είναι ορθογώνιος μετασχηματισμός $S \in \mathrm{GL}(n, \mathbb{R})$, άρα το σύνολο των ορθογώνιων μετασχηματισμών αποτελεί υποομάδα της $\mathrm{GL}(n, \mathbb{R})$.

Για το δεύτερο σκέλος του Θεωρήματος, αν T είναι μια τυχούσα ισομετρία με $T(0) = w$ θεωρούμε την απεικόνιση μεταφοράς T_{-w} και παίρνουμε την σύνθεση $T_{-w} \circ T$. Αυτή η σύνθεση κρατάει σταθερό το $x = 0$, άρα από την προηγούμενη Πρόταση έπεται ότι $T_{-w} \circ T = S$ για κάποιον ορθογώνιο μετασχηματισμό S, άρα $T = T_w \circ S$. □

Άσκηση 3.23. *Αποδείξτε την Πρόταση 3.1.*

Άσκηση 3.24. *Ολοκληρώστε την απόδειξη του Θεωρήματος 3.2.*

Άσκηση 3.25. *Μια απεικόνιση $f : \mathbb{R}^n \to \mathbb{R}^n$ με $f(0) = 0$ είναι ισομετρία αν και μόνο αν διατηρεί τις γωνίες, δηλαδή αν και μόνο αν $\langle f(x), f(y)\rangle = \langle x, y\rangle$.*

Άσκηση 3.26. *Ένας πίνακας $A \in GL(n, \mathbb{R})$ είναι ορθογώνιος (δηλαδή ορίζει ορθογώνιο γραμμικό μετασχηματισμό του $\mathbb{R}^n$ που διατηρεί την νόρμα) αν και μόνο $AA^t = I_n$.*

Από την τελευταία άσκηση και το γεγονός ότι $\det(A^t) = \det(A)$ έπεται ότι $\det(A) = \pm 1$ για κάθε $A \in O(n, \mathbb{R})$.

Ορισμός 3.6. *Μια ισομετρία S με $S(0) = 0$ διατηρεί τον προσανατολισμό εάν $\det S = 1$ (αλλιώς λέμε ότι η S αντιστρέφει τον προσανατολισμό). Η ομάδα των ισομετριών που διατηρούν τον προσανατολισμό συμβολίζεται με $SO(n, \mathbb{R})$.*

Άσκηση 3.27. *Δείξτε ότι η ομάδα $SO(2, \mathbb{R})$ είναι ισόμορφη με την ομάδα $\mathbb{T} \simeq \mathbb{R}/\mathbb{Z}$ του κύκλου.*

Άσκηση 3.28. *Δείξτε ότι $[O(n, \mathbb{R}) : SO(n, \mathbb{R})] = 2$. Συμπεράνατε πως η ομάδα των ορθογώνιων μετασχηματισμών δίνεται ως ημιευθύ γινόμενο $O(n, \mathbb{R}) = SO(n, \mathbb{R}) \rtimes \langle A\rangle$ για κάθε ορθογώνιο πίνακα A με $\det(A) = -1$ και $A^2 = I_n$.*

Άσκηση 3.29. *Έστω $Tr(n, \mathbb{R})$ το σύνολο όλων των μεταφορών T_w του $\mathbb{R}^n$. Δείξτε ότι $Tr(n, \mathbb{R}) \simeq \mathbb{R}^n$.*

Άσκηση 3.30. *Το Θεώρημα 3.2 μας δίνει ότι $M(n, \mathbb{R}) = Tr(n, \mathbb{R}) \cdot O(n, \mathbb{R})$. Έχουμε επίσης παρατηρήσει ότι*

$$Tr(n, \mathbb{R}) \cap O(n, \mathbb{R}) = \{id\}.$$

Δείξτε ότι $Tr(n, \mathbb{R}) \trianglelefteq M(n, \mathbb{R}) = \{id\}$. Συμπεράνατε πως

$$M(n, \mathbb{R}) \simeq \mathbb{R}^n \rtimes O(n, \mathbb{R}).$$

Άσκηση 3.31. ** Αληθεύει πως κάθε υποομάδα της $M(n, \mathbb{R})$ είναι ισόμορφη με ένα ημιευθές γινόμενο $T \rtimes Q$ με $T \leqslant Tr(n, \mathbb{R})$ και $Q \leqslant O(n, \mathbb{R})$;*

3.4 Τοπολογικές ομάδες

Θα δούμε τώρα εν συντομία πως μπορεί να γενικευτεί το παραπάνω παράδειγμα και μετά θα δούμε και άλλα σημαντικά παραδείγματα.

Μία τοπολογική ομάδα είναι μία ομάδα G που είναι και τοπολογικός χώρος. Θεωρούμε δηλαδή την G εφοδιασμένη με μια τοπολογία, η οποία όμως θέλουμε να είναι συμβατή με την αλγεβρική δομή της G.

Ορισμός 3.7. *Μια ομάδα G εφοδιασμένη με μια τοπολογία τέτοια ώστε οι απεικονίσεις*

$$(g, h) \in G \times G \to gh \in G,$$

$$g \in G \to g^{-1} \in G$$

να είναι συνεχείς λέγεται τοπολογική ομάδα.

Ορισμός 3.8. *Εστω ότι η G δρα σε έναν τοπολογικό χώρο X μέσω μιας δράσης*

$$G \times X \to X : (g, x) \to gx.$$

Αν η απεικόνιση αυτή είναι συνεχής, τότε λέμε ότι η G δρα συνεχώς στον X.

Οι συνθήκες που επιβάλλουμε στον ορισμό της τοπολογικής ομάδας είναι πολύ ισχυρές. Ειδικότερα, ο ορισμός της τοπολογικής ομάδας μας λέει ότι η G δρα στον εαυτό της από αριστερά και η δράση είναι συνεχής. Η δράση αυτή μεταφέρει γειτονιές κάθε στοιχείο $g \in G$ σε γειτονιές του ταυτοτικού στοιχείου $e \in G$ (η G δηλαδή ως τοπολογικός χώρος έχει μεγάλη συμμετρία). Ειδικότερα, αποδεικνύεται ότι η G είναι χώρος Hausdorff (T_2-χώρος) αν και μόνο αν είναι χώρος Kolmogorov (T_0-χώρος). Οι συνθήκες αυτές είναι ισοδύναμες με την υπόθεση ότι το μονοσύνολο $\{e\}$ είναι κλειστό. Επιπλέον, οποιαδήποτε από τις παραπάνω συνθήκες είναι ισοδύναμες με την συνθήκη ότι η G είναι χώρος Tychonoff ($T_{3\frac{1}{2}}$-χώρος). Το Θεώρημα των Birkhoff–Kakutani λέει πως η τοπολογία της G είναι μετρικοποιήσιμη αν και μόνο αν το μονοσύνολο $\{e\}$ είναι κλειστό και το ταυτοτικό στοιχείο e έχει αριθμήσιμη βάση περιοχών.

Άσκηση 3.32. *Δείξτε την ισοδυναμία ότι η G είναι Hausdorff αν και μόνο αν το μονοσύνολο $\{e\}$ είναι κλειστό. (Υπόδειξη: ένας χώρος X είναι Hausdorff αν και μόνο αν η διαγώνιος $\Delta_X \subseteq X \times X$ είναι κλειστό υποσύνολο. Θεωρείστε την συνεχή απεικόνιση $G \times G \to G$ με $(x, y) \to xy^{-1}$. Ποιά είναι η αντίστροφη εικόνα του μονοσυνόλου $\{e\}$; Αντίστροφα, αν $x \neq y$, συσχετίστε κατάλληλες γειτονιές τους με γειτονιές του ταυτοτικού στοιχείου.)*

Σε αυτό το σημείο πρέπει επίσης να παρατηρήσουμε ότι για κάθε $g \in G$ ο πολλαπλασιασμός με g είναι ομοιομορφισμός $X \to X$. Για κάθε $x \in X$ θεωρούμε την σταθεροποιούσα G_x, η οποία σε αυτήν την περίπτωση ονομάζεται και *ομάδα ισοτροπίας* ή *ισοτροπική ομάδα* του x. Αν συμβολίσουμε με $f_x : G \to X$ την απεικόνιση με $f_x(g) = gx$, τότε αυτή η απεικόνιση είναι συνεχής και η αντίστροφη εικόνα ενός σημείου δίνεται από την ομάδα ισοτροπίας του:

$$G_x = f_x^{-1}(x).$$

Άρα αν ο χώρος X είναι Hausdorff τότε η $G_x \leqslant G$ είναι κλειστό υποσύνολο της G.

Επίσης, η δράση μιας τοπολογικής ομάδας G στον X ορίζει μία φυσιολογική τοπολογία πηλίκο στον χώρο των τροχιών $X/\sim$: η τοπολογία αυτή είναι η η μικρότερη τοπολογία για την οποία η απεικόνιση πηλίκο

$$\pi : X \to X/\sim, \; \pi(x) = Gx$$

είναι συνεχής.

Άσκηση 3.33. *Δείξτε ότι η απεικόνιση πηλίκο $\pi : X \to X/\sim$ είναι ανοιχτή.*

Πρόταση 3.2. *Έστω G Hausdorff τοπολογική ομάδα, $H \leqslant G$ και $X = G/H$. Τότε ο X είναι χώρος Hausdorff αν και μόνο αν η H είναι κλειστή υποομάδα της G.*

Απόδειξη. Αν ο χώρος πηλίκο $X = G/H$ είναι Hausdorff, τότε το ταυτοτικό του X είναι το σύμπλοκο $eH = H$, το οποίο είναι κλειστό σύνολο (ως μονοσύνολο). Έπεται πως, αν $\pi : G \to G/H$ είναι η συνηθισμένη συνάρτηση προβολής, τότε $H = \pi^{-1}(eH)$, άρα η H είναι κλειστό υποσύνολο της G ως αντίστροφη εικόνα κλειστού. Η αντίστροφη κατεύθυνση αφήνεται ως άσκηση. □

Γενικότερα, εάν έχουμε μία μεταβατική δράση $G \circlearrowright X$ τότε $X = G \cdot x$ για κάθε $x \in X$, και το Θεώρημα τροχιάς-σταθεροποιούσας μας λέει ότι $[G : G_x] = |X|$. Στην περίπτωση των συνεχών δράσεων τοπολογικών ομάδων αυτό το αποτέλεσμα ισχυροποιείται.

Θεώρημα 3.3. *Έστω G τοπολογική ομάδα που δρα σε έναν τοπολογικό χώρο X μεταβατικά. Υποθέτουμε ότι οι G, X είναι τοπικά συμπαγείς (δηλαδή κάθε σημείο τους έχει συμπαγή γειτονιά) Hausdorff τοπολογικοί χώροι. Υποθέτουμε ακόμη ότι η G έχει αριθμήσιμη βάση για την τοπολογία της. Τότε, η απεικόνιση $\phi : G/G_x \to X$ με*

$$\phi(gG_x) = g \cdot x$$

είναι ομοιομορφισμός (δηλαδή $1-1$, επί και αμφισυνεχής) για κάθε $x \in X$.

Άσκηση 3.34. *Σε πολλά σημαντικά παραδείγματα η δράση $G \circlearrowright X$ είναι proper. Αυτό σημαίνει πως η απεικόνιση $G \times X \to X \times X$ με*

$$(g, x) \to (g \cdot x, x)$$

είναι proper, δηλαδή αντίστροφη εικόνα συμπαγούς συνόλου είναι συμπαγές. Δείξτε ότι σε μια proper δράση κάθε ισοτροπική υποομάδα είναι συμπαγής. Δείξτε επίσης ότι αν οι G, X είναι όπως στο Θεώρημα 3.3 τότε ο χώρος τροχιών $X/\sim$ είναι Hausdorff.

Αφού $G \circlearrowright X$, κάθε υποομάδα της δρα στον X. Θέλουμε να μελετήσουμε καλές συνθήκες κάτω από τις οποίες ο αντίστοιχος χώρος τροχιών είναι Hausdorff. Μια σημαντική περίπτωση τέτοιων δράσεων είναι ότι η υποομάδα που δρα είναι αρκούντως μικρή μέσα στην G. Οδηγούμαστε λοιπόν στην εξής έννοια.

Ορισμός 3.9. *Αν μια τοπολογική ομάδα G δρα στον τοπολογικό χώρο X και $\Gamma \leqslant G$, λέμε ότι η δράση της Γ στον X είναι:*

α) ασυνεχής, αν για κάθε $x \in X$ και ακολουθία στοιχείων $\gamma_n \in \Gamma$ η ακολουθία $\gamma_n \cdot x$ δεν έχει σημείο συσσώρευσης μέσα στον X.

β) γνήσια ασυνεχής, αν για κάθε $x, y \in X$ υπάρχουν ανοιχτές περιοχές τους U_x, U_y τέτοιες ώστε να ισχύει

$$|\{\gamma \in \Gamma : \gamma U_x \cap U_y \neq \emptyset\}| < \infty.$$

Αν οι G και X είναι όπως στο Θεώρημα 3.3 και $\Gamma \leqslant G$, τότε η δράση $\Gamma \circlearrowright X$ είναι ασυνεχής αν και μόνο αν είναι γνήσια ασυνεχής, και αυτό συμβαίνει αν και μόνο αν η Γ είναι διακριτή υποομάδα της G με την επαγόμενη τοπολογία. Ο χαρακτηρισμός αυτός των διακριτών υποομάδων της G (ως ομάδων που δρουν ασυνεχώς σε χώρους Hausdorff) έχει αποδειχθεί ιστορικά πολύ σημαντικός. Σε αυτήν την περίπτωση έχουμε τα ακόλουθα συμπεράσματα:

Πόρισμα 3.1. *Αν οι $\Gamma \leqslant G \circlearrowright X$ είναι όπως στον Ορισμό 3.9 και $x \in X$ τότε η ομάδα ισοτροπίας Γ_x είναι πεπερασμένη για κάθε $x \in X$.*

Πόρισμα 3.2. *Αν οι G, X, Γ, K είναι όπως παραπάνω, τότε ο χώρος ... είναι Hausdorff.*

3.5 Υπερβολικοί χώροι και άλλα παραδείγματα

Θεωρούμε πρώτα τον 2-διάστατο υπερβολικό χώρο (δηλαδή το υπερβολικό επίπεδο) που ορίζεται ως

$$\mathbb{H}^2 := \{z \in \mathbb{C} : \Im(z) > 0\}.$$

Το υπερβολικό επίπεδο εφοδιάζεται με την μετρική

$$ds^2 = \frac{dx^2 + dy^2}{y^2}.$$

Αυτό σημαίνει πως για κάθε μονοπάτι $\gamma(t) = (x(t), y(t)) : [0,1] \to \mathbb{H}^2$ το μήκος της ορίζεται ως

$$\ell(\gamma) = \int_0^1 \frac{\sqrt{x(t)^2 + y(t)^2}}{y(t)} dt.$$

Συμβολίζουμε συνήθως με $d(z,w)$ την υπερβολική απόσταση δύο στοιχείων z, w του υπερβολικού επιπέδου που επάγεται από την μετρική ds. Η ομάδα $\mathrm{SL}(2,\mathbb{R})$ δρα μεταβατικά στο $\mathbb{H}^2$ δρα με μετασχηματισμούς Möbius (δείτε την άσκηση 2.7) ως εξής:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

Η δράση αυτή διατηρεί τις αποστάσεις, δηλαδή $d(\gamma z, \gamma w) = d(z,w)$ για κάθε $\gamma \in \mathrm{SL}(2,\mathbb{R})$. Αφού κάθε πίνακας $\gamma \in \mathrm{SL}(2,\mathbb{R})$ ορίζει την ίδια δράση με τον πίνακα $-\gamma$, έπεται ότι η ομάδα των ισομετριών του $\mathbb{H}^2$ που διατηρούν τον προσανατολισμό είναι ισόμορφη με την ομάδα

$$\mathrm{PSL}(2,\mathbb{R}) = \mathrm{SL}(2,\mathbb{R})/\langle -I \rangle.$$

Το $\mathbb{H}^2$ έχει επίσης τον αυτομορφισμό της ανάκλασης $\phi(z) = -\overline{z}$, κι αποδεικνύεται πως η ομάδα όλων των ισομετριών είναι ισόμορφη με την

$$G \simeq \mathrm{PSL}(2,\mathbb{R}) \rtimes \langle \phi \rangle.$$

Οι διακριτές υποομάδες Γ της $\mathrm{PSL}(2,\mathbb{R})$ ονομάζονται ομάδες Fuchsian και οι χώροι πηλίκα της δράσης ... ονομάζονται επιφάνειες Riemann.

Αξίζει εδώ να κάνουμε ορισμένα σχόλια για αυτές τις πολλαπλότητες.

Άσκηση 3.35. *Δείξτε ότι η PSL$(2,\mathbb{R})$ δρα όντως μεταβατικά στο $\mathbb{H}^2$ θεωρώντας την δράση του πίνακα*

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$$

στο κέντρο του $\mathbb{H}^2$ που είναι το σημείο $z = i$.

Άσκηση 3.36. *Δείξτε ότι η G που ορίστηκε στην προηγούμενη άσκηση δρα όντως με ισομετρίες, δηλαδή για κάθε $\gamma \in G$ έχουμε $d(\gamma z, \gamma w) = d(z,w)$.*

Πιο γενικά, ορίζεται ο n-διάστατος υπερβολικός χώρος

$$\mathbb{H}^n := \{\mathbf{x} + jy \,:\, \mathbf{x} \in \mathbb{R}^{n-1},\, y > 0\},$$

όπου με j συμβολίζεται

3.6 Επαναληπτικές ασκήσεις τρίτου κεφαλαίου

Άσκηση 3.37. *Την αναπαράσταση των quaternions με πίνακες.*

Άσκηση 3.38. *Για κάθε $n \geqslant 2$ δώστε παράδειγμα centerless ομάδας G με $[G : G'] = n$. (Συγκρίνετε την με την άσκηση 1.84)*

Άσκηση 3.39. **** Μία ομάδα G ονομάζεται τοπολογικοποιήσιμη εάν επιδέχεται μία μη-διακριτή Hausdorff τοπολογία αλλιώς ονομάζεται μη-τοπολογικοποιήσιμη. Υπάρχει άπειρη ομάδα που είναι μη-τοπολογικοποιήσιμη; (Αυτό το πρόβλημα του Markov (1946) λύθηκε στα τέλη της δεκαετίας του '70 από τον Shelah).*

4 Προχωρημένη θεωρία ομάδων

Θα δούμε τώρα λίγη προχωρημένη Θεωρία ομάδων, οι βασικές έννοιες της οποίας έρχονται από την Θεωρία Galois. Οι δύο πιο βασικές κατηγορίες ομάδων που θα μας απασχολήσουν εδώ είναι οι επιλύσιμες και οι μηδενοδύναμες ομάδες.

4.1 Σειρές ομάδων

Μία από τις κεντρικές ιδέες της θεωρία ομάδων που έχουμε μελετήσει έως τώρα είναι η εξής: μπορούμε να καταλάβουμε μια ομάδα G αν καταλάβουμε όλες τις υποομάδες της $H \leqslant G$. Μέχρι τώρα μελετούσαμε την περίπτωση, ως πορίσματα των Θεωρημάτων του Lagrange και του Sylow, την 'τοπική ' περίπτωση $|H| = p$ ή $|H| = p^k$. Θα δούμε τώρα πως μπορούμε να μελετήσουμε ταυτόχρονα υποομάδες μιας G που έχουν διαφορετική τάξη.

Ορισμός 4.1. *Έστω G μια ομάδα. Μία σειρά της G είναι μια σειρά υποομάδων G_i της G τέτοιες ώστες*

$$\{e\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_1 \leqslant G_0 = G.$$

Μήκος μιας τέτοιας σειράς ονομάζεται το πλήθος των μη τετριμμένων εγκλεισμών της σειράς.

Για λόγους που έρχονται από την Θεωρία Galois (την οποία δεν θα αναπτύξουμε εδώ), ο επόμενος ορισμός είναι εξαιρετικά σημαντικός.

Ορισμός 4.2. *Μια σειρά της G ονομάζεται κανονική σειρά εάν $G_{i+1} \trianglelefteq G_i$ για κάθε $0 \leqslant i \leqslant n-1$. Σε αυτήν την περίπτωση, κάθε ομάδα πηλίκο G_i/G_{i+1} ονομάζεται παράγοντας της σειράς.*

Μια σειρά της G λέγεται επιλύσιμη εάν όλοι οι παράγοντες της σειράς είναι αβελιανές ομάδες. Μία ομάδα G ονομάζεται επιλύσιμη εάν έχει επιλύσιμη σειρά.

Μία κανονική σειρά ονομάζεται συνθετική εάν για κάθε i έχουμε ότι η G_{i+1} είναι μέγιστη κανονική υποομάδα της G_i ή $G_{i+1} = G_i$.

Άσκηση 4.1. *Δείξτε ότι μια κανονική σειρά της G είναι συνθετική εάν κάθε παράγοντας της σειράς είναι απλή ή τετριμμένη ομάδα.*

Άσκηση 4.2. *Έστω G μια πεπερασμένη ομάδα. Δείξτε ότι η G είναι επιλύσιμη αν και μόνο αν υπάρχει σειρά της με κάθε παράγοντα G_i/G_{i+1} να είναι κυκλική τάξης p για κάποιον πρώτο p (όχι ο ίδιος για όλους τους διαφορετικούς παράγοντες).*

Αν τώρα θεωρήσουμε μια κανονική σειρά της G της μορφής

$$\{e\} = H_m \leqslant H_{m-1} \leqslant ... \leqslant H_1 \leqslant H_0 = G,$$

τότε μία άλλη σειρά

$$\{e\} = G_n \leqslant G_{n-1} \leqslant ... \leqslant G_1 \leqslant G_0 = G$$

της G ονομάζεται εκλέπτυνση της αρχικής σειράς εάν κάθε υποομάδα H_i εμφανίζεται στην δεύτερη σειρά, δηλαδή εάν το σύνολο $\{H_i\}_{i=1}^m$ είναι υποσύνολο του συνόλου $\{G_i\}_{i=1}^n$.

Παρατηρούμε πως εκλέπτυνση συνθετικής σειράς είναι συνθετική σειρά (γιατί;). Αυτό μας επιτρέπει, όταν θέλουμε να δείξουμε κάποιο αποτέλεσμα για κάποια σειρά της G, να περιορίζουμε την μελέτη μας μόνο στις συνθετικές σειρές της G.

Αν και, σύμφωνα με τους ορισμούς που δώσαμε, μία G έχει πολλές συνθετικές σειρές, διαισθητικά όλες φαίνονται να μοιάζουν μεταξύ τους. Μπορούμε να δούμε ένα εύκολο παράδειγμα που εξηγεί αυτό το φαινόμενο εάν θεωρήσουμε μία εύκολη περίπτωση, την κυκλική ομάδα $G = \mathbb{Z}_{30} = \langle 1 \rangle$ και τις εξής σειρές της

$$\begin{aligned}
\{e\} &\trianglelefteq \mathbb{Z}_{30}, \\
\{e\} = \langle 0 \rangle &\trianglelefteq \mathbb{Z}_{15} \simeq \langle 2 \rangle \trianglelefteq \mathbb{Z}_{30}, \\
\{e\} = \langle 0 \rangle &\trianglelefteq \mathbb{Z}_{5} \simeq \langle 6 \rangle \trianglelefteq \mathbb{Z}_{15} \simeq \langle 2 \rangle \trianglelefteq \mathbb{Z}_{30}, \\
\{e\} = \langle 0 \rangle &\trianglelefteq \mathbb{Z}_{3} \simeq \langle 10 \rangle \trianglelefteq \mathbb{Z}_{6} \simeq \langle 5 \rangle \trianglelefteq \mathbb{Z}_{30}.
\end{aligned}$$

Η πρώτη σειρά της G είναι η τετριμμένη σειρά (μήκους 1). Προφανώς η κανονική σειρά $\{e\} \trianglelefteq G$ υπάρχει για κάθε ομάδα G. Αν η G είναι απλή, τότε αυτή η σειρά είναι συνθετική και δεν εκλεπτύνεται (με μη τετριμμένο τρόπο). Στο παράδειγμα μας η G είναι αβελιανή, οπότε η τετριμμένη σειρά της μπορεί να εκλεπτυνθεί περισσότερο. Μια εκλέπτυνση της είναι η τρίτη κανονική σειρά. Η σειρά αυτή είναι συνθετική, γιατί κάθε πηλίκο είναι κυκλική τάξης πρώτου αριθμού (άρα και αβελιανή). Η τέταρτη κανονική σειρά είναι επίσης συνθετική, αλλά είναι διαφορετική από την τρίτη κανονική σειρά. Όμως και οι δύο αυτές συνθετικές σειρές έχουν παράγοντες ισόμορφους με τις ομάδες $\mathbb{Z}_2, \mathbb{Z}_3$ και $\mathbb{Z}_5$ (όχι όμως διατεταγμένους με την ίδια σειρά). Αυτή η παρατήρηση μας οδηγεί φυσιολογικά στον ακόλουθο ορισμό.

Ορισμός 4.3. *Δύο κανονικές σειρές μιας ομάδας G ονομάζονται ισοδύναμες εάν υπάρχει ένα-προς-ένα και επί αντιστοιχία μεταξύ των μη-τετριμμένων παραγόντων τους με τις αντίστοιχες ομάδες πηλίκα να είναι ισόμορφες.*

Στο προηγούμενο παράδειγμα βρήκαμε δύο συνθετικές σειρές της $\mathbb{Z}_{30}$ που είναι ισοδύναμες. Το Θεώρημα Jordan-Hölder μας λέει ότι αυτό ισχύει για κάθε ομάδα G. Το Θεώρημα αυτό έπεται άμεσα από το Θεώρημα του Schreier.

Θεώρημα 4.1. *(Schreier) Κάθε δύο κανονικές σειρές μιας ομάδας G έχουν ισοδύναμες εκλεπτύνσεις.*

Δεν θα αποδείξουμε το Θεώρημα Schreier, όμως αξίζει να σημειώσουμε πως η πιο απλή απόδειξη του βασίζεται στο ακόλουθο Λήμμα (γνωστός και ως Λήμμα της πεταλούδας).

Λήμμα 4.1. *(Zassenhaus) Έστω G ομάδα με $B, D \leqslant G$ και $A \trianglelefteq B$, $C \trianglelefteq D$. Τότε:*

(α) $A(B \cap C) \trianglelefteq A(B \cap D)$ και $C(A \cap D) \trianglelefteq C(B \cap D)$,

(β) τα αντίστοιχα πηλίκα είναι ισόμορφα:

$$\frac{A(B \cap D)}{A(B \cap C)} \simeq \frac{C(B \cap D)}{C(A \cap D)} \simeq \frac{B \cap D}{(A \cap D)(B \cap C)}.$$

Ως Πόρισμα του Θεωρήματος Schreier παίρνουμε το Θεώρημα Jordan-Hölder.

Θεώρημα 4.2. *(Jordan-Hölder) Κάθε δύο συνθετικές σειρές μιας ομάδας G είναι ισοδύναμες.*

Απόδειξη. Έστω δύο συνθετικές σειρές μιας G. Τότε από το Θεώρημα Schreier αυτές οι δύο σειρές έχουν ισοδύναμες εκλεπτύνσεις. $\square$

Οι ομάδες-παράγοντες μιας συνθετικής σειράς μιας ομάδας ονομάζονται συνθετικοί παράγοντες της σειράς. Είδαμε ότι είναι απλές ομάδες και (υπό μία έννοια) μοναδικές για κάθε δοσμένη G. Αν εφαρμόσουμε αυτή την παρατήρηση για την κυκλική ομάδα τάξης n, δηλαδή για $G \simeq \mathbb{Z}_n$, τότε το Θεώρημα Jordan-Hölder μας δίνει ως πόρισμα το Θεμελιώδες Θεώρημα της αριθμητικής (εξηγείστε γιατί).

Άσκηση 4.3. *Δείξτε πως εκλέπτυνση συνθετικής σειράς είναι όντως συνθετική σειρά.*

Άσκηση 4.4. *Δείξτε πως μία κανονική σειρά είναι συνθετική αν και μόνο αν είναι μέγιστου μήκους (δηλαδή κάθε εκλέπτυνση της έχει ίδιο μήκος).*

Άσκηση 4.5. *Δείξτε πως κάθε πεπερασμένη ομάδα G έχει συνθετική σειρά.*

Άσκηση 4.6. *Δείξτε πως μία αβελιανή ομάδα έχει σειρά αν και μόνο αν είναι πεπερασμένη.*

Άσκηση 4.7. *Δώστε παράδειγμα άπειρης ομάδας με συνθετική σειρά.*

Άσκηση 4.8. *Βρείτε την συνθετική σειρά της S_n για κάθε $n \geqslant 2$.*

Άσκηση 4.9. *Αν G πεπερασμένη τότε*

$$|G| = \prod_{i=0}^{n-1} |G_i/G_{i+1}| \,.$$

Ο βαθύτερος λόγος που δώσαμε τους παραπάνω ορισμούς είναι η Θεωρία Galois και η επιλυσιμότητα πολυωνύμων. Σε αυτό το μάθημα δεν θα μελετήσουμε Θεωρία Galois, ωστόσο θα μελετήσουμε τις επιλύσιμες (και μηδενοδύναμες) ομάδες ξεχωριστά.

4.2 Επιλύσιμες ομάδες

Επαναλαμβάνουμε τον επόμενο ορισμό, λόγω της εξαιρετικής σημασίας του.

Ορισμός 4.4. *(Galois) Μία κανονική σειρά της G, δηλαδή μια σειρά της μορφής*

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \ldots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

λέγεται επιλύσιμη εάν κάθε παράγοντας G_i/G_{i+1} είναι αβελιανή ομάδα. Μια ομάδα G λέγεται επιλύσιμη εάν υπάρχει μια σειρά της που να είναι επιλύσιμη.

Ισοδύναμα, μία G είναι επιλύσιμη εάν μια συνθετική σειράς της είναι επιλύσιμη σειρά. Άρα για να αποφανθούμε εάν μία πεπερασμένη G είναι επιλύσιμη, αρκεί να ελέγξουμε εαν οι παράγοντες μιας συνθετικής σειράς της είναι κυκλικοί. Έτσι λοιπόν εύκολα συμπεραίνουμε ότι η S_n (καθώς και η A_n) δεν είναι επιλύσιμη για $n \geqslant 5$ (εξηγείστε γιατί).

Άσκηση 4.10. *Χρησιμοποιώντας το γεγονός ότι η μικρότερη μη αβελιανή απλή ομάδα έχει τάξη 60, δείξτε ότι κάθε ομάδα τάξης $\leqslant 59$ είναι επιλύσιμη.*

Άσκηση 4.11. *Δείξτε ότι η διεδρική ομάδα D_{2n} είναι επιλύσιμη για κάθε $n \geqslant 1$.*

Άσκηση 4.12. *Πιο γενικά, δείξτε ότι αν οι K, H είναι επιλύσιμες, τότε και το ημιευθές γινόμενο $K \rtimes_\theta H$ είναι επιλύσιμη ομάδα.*

5 Επαναληπτικές ασκήσεις μαθήματος

Άσκηση 5.1. *Δείξτε ότι η G είναι αβελιανή αν και μόνο αν η απεικόνιση $g \to g^{-1}$ είναι αυτομορφισμός.*

Άσκηση 5.2. *Έστω G ομάδα και $H \leqslant G$. Δείξτε ότι η HG' είναι κανονική υποομάδα της G.*

Άσκηση 5.3. *Έστω G μη αβελιανή ομάδα τάξης $|G| = pq$ με $p > q$. Βρείτε την G'.*

Άσκηση 5.4. *Αν G είναι μια μη αβελιανή, πεπερασμένη p-ομάδα, δείξτε ότι $p^2 \mid |Aut(G)|$.*

Άσκηση 5.5. *Βρείτε το κέντρο $Z(G)$ και την παράγουσα υποομάδα G' της $G = \mathbb{Z}_3 \times S_3$.*

Άσκηση 5.6. *(Putnam 1997) Έστω G και $\phi : G \to G$ μια απεικόνιση τέτοια ώστε*

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

για όλα τα στοιχεία που ικανοποιούν

$$g_1g_2g_3 = h_1h_2h_3 = e.$$

Δείξτε ότι υπάρχει ένα στοιχείο $a \in G$ τέτοιο ώστε η απεικόνιση $\psi(g) := a\phi(g)$ να είναι ομομορφισμός.

Άσκηση 5.7. *Έστω G μία ομάδα και H_1, H_2 δύο αβελιανές υποομάδες της. Έστω $H = H_1 \vee H_2$. Τότε η $H_1 \cap H_2$ είναι κανονική υποομάδα της H. Δείξτε επίσης ότι αν η G είναι πεπερασμένη μη αβελιανή και κάθε γνήσια υποομάδα της είναι αβελιανή, τότε η G δεν είναι απλή.*

Άσκηση 5.8. *Έστω G μια ομάδα και N μια υποομάδα της με την ιδιότητα $N \cap G' = \{e\}$. Δείξτε ότι η N είναι αβελιανή. Αν επιπλέον η N είναι κανονική υποομάδα της G, δείξτε ότι $N \leqslant Z(G)$.*

Άσκηση 5.9. *Έστω G πεπερασμένη ομάδα περιττής τάξης $|G| = n$. Δείξτε ότι η ομάδα $A_4 \times G$ δεν έχει υποομάδα δείκτου 2.*

Άσκηση 5.10. *Έστω G πεπερασμένη με $|G| = pqr$, όπου p, q, r διαφορετικοί πρώτοι αριθμοί. Δείξτε ότι η G δεν είναι απλή. Δειξτε επίσης ότι η G είναι επιλύσιμη.*

Άσκηση 5.11. *** Έστω G πεπερασμένη με $|G| = n$. Αν $(n, \phi(n)) = 1$, δείξτε ότι η G είναι αβελιανή.*

Άσκηση 5.12. *** (Dedekind) Μία μη αβελιανή ομάδα που κάθε υποομάδα της είναι κανονική ονομάζεται Hamiltonian. Είδαμε ότι η ομάδα Q_8 των Quaternions είναι Hamiltonian. Βρείτε όλες τις πεπερασμένες Hamiltonian ομάδες.*

Άσκηση 5.13. *** Μια πεπερασμένη ομάδα λέγεται CLT αν ικανοποιεί το αντίστροφο του Θεωρήματος Lagrange, δηλαδή αν για κάθε $d \| G|$ υπάρχει $H \leqslant G$ τάξης d. Έστω A, B, C οι κλάσεις των πεπερασμένων υπερεπιλύσιμων, των CLT και των πεπερασμένων επιλύσιμων ομάδων. Δείξτε τους γνήσιους εγκλεισμούς $A \subset B \subset C$.*

Άσκηση 5.14. *** Υπάρχει άπειρη μη αβελιανή ομάδα G που κάθε πεπερασμένη υποομάδα της να είναι κυκλική;*

Άσκηση 5.15. **** Υπάρχει άπειρη μη αβελιανή ομάδα G που κάθε γνήσια ομάδα της $H \neq 1$ της G είναι κυκλική τάξης p για κάποιον σταθερό πρώτο p; (Μια τέτοια ομάδα ονομάζεται Tarski monster group και είναι απαραιτήτως απλή).*