Πρόταση: $\forall n \in \mathbb{N},\ |\mathbb{Z}_n| = n$

Απόδειξη: Έστω $n \in \mathbb{N}$ και $[a]_n \in \mathbb{Z}_n$.

Από την Ευκλείδεια Διαίρεση του a με το n έχουμε $a = qn + r$, όπου $q, r \in \mathbb{Z}$ με $0 \le r < n-1$. Συνεπώς, $[a]_n = [qn+r]_n$

$= [qn]_n + [r]_n \overset{(*)}{=} [0]_n + [r]_n = [r]_n \in \{[0]_n, \dots, [n-1]_n\}$

οπότε: $\mathbb{Z}_n \subseteq \{[0]_n, \dots, [n-1]_n\}$.

$(*)$ $n \mid qn \Rightarrow n \mid qn - 0 \Rightarrow [qn]_n = [0]_n$.

Απ' την άλλη, $\{[0]_n, \dots, [n-1]_n\} \subseteq \mathbb{Z}_n$.

Τελικά, $\mathbb{Z}_n = \{[0]_n, \dots, [n-1]_n\} \Rightarrow$

$\Rightarrow |\mathbb{Z}_n| = |\{[0]_n, \dots, [n-1]_n\}| = n$. ∎

Παραδείγματα

(I) mod 2: $[0]_2, [1]_2$

$[0]_2 = \{\dots, -4, -2, 0, 2, 4, \dots\}$: άρτιοι

$[1]_2 = \{\dots, -5, -3, -1, 1, 3, 5, \dots\}$: περιττοί

(II) mod 3: $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\}$

$[1]_3 = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$

$[2]_3 = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$

▶ Στο σύνολο $\mathbb{Z}_n$ μπορούμε επιπλέον να ορίσουμε:

$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, \quad [a]_n \cdot [c]_n := [ac]_n$

Εύκολα πάλι μπορούμε να αποδείξουμε ότι $n \cdot$ είναι καλά ορισμένη απεικόνιση

δηλ: $\left.\begin{matrix} [a]_n = [a']_n \\ [c]_n = [c']_n \end{matrix}\right\} \Rightarrow [ac]_n = [a'c']_n$

Εύκολα επίσης μπορούμε να δούμε ότι η πράξη $\cdot$ είναι προσεταιριστική και ότι η κλάση $[1]_n$ είναι ουδέτερο στοιχείο του $\mathbb{Z}_n$ ως προς την πράξη αυτή. Οπότε $\forall [a]_n \in \mathbb{Z}_n : [0]_n \cdot [a]_n = [0]_n \neq [1]_n$ και συνεπώς το $[0]_n$ δεν έχει αντίστροφο.

Άρα, $(\mathbb{Z}_n, \cdot)$: όχι ομάδα.

! Ακόμα και αν πάρουμε $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]_n\}$ με την πράξη του πολ/μού, πάλι δεν έχουμε ομάδα (εν γένει).

πχ: $\mathbb{Z}_4^* = \{[1]_4, [2]_4, [3]_4\}$

Ισχύει: $[2]_4 \cdot [2]_4 = [4]_4 = [0]_4 \notin \mathbb{Z}_4^*$

▸ Πρέπει να περιοριστούμε και άλλο:

Η ομάδα $U(\mathbb{Z}_n)$ και η συνάρτηση Euler

Έστω $n \in \mathbb{N}$. Θεωρούμε το σύνολο

$$U(\mathbb{Z}_n) = \{ [a]_n \in \mathbb{Z}_n \mid \exists\, [b]_n \in \mathbb{Z}_n : [a]_n [b]_n = [1]_n \} \subseteq \mathbb{Z}_n.$$

Επειδή $[1]_n \in \mathbb{Z}_n$ και $[1]_n [1]_n = [1 \cdot 1]_n = [1]_n$

έπεται ότι $[1]_n \in U(\mathbb{Z}_n) \Rightarrow U(\mathbb{Z}_n) \neq \emptyset$.

Βήμα 1: $[a]_n, [a']_n \in U(\mathbb{Z}_n) \Rightarrow [a]_n [a']_n \in U(\mathbb{Z}_n)$

Απόδειξη: $[a]_n \in U(\mathbb{Z}_n) \Rightarrow \exists\, [b]_n \in U(\mathbb{Z}_n)$:

$$[a]_n [b]_n = [1]_n$$

- $[a']_n \in U(\mathbb{Z}_n) \Rightarrow \exists\, [b']_n \in U(\mathbb{Z}_n) : [a']_n [b']_n = [1]_n$

Για το $[a]_n [a']_n = [aa']_n \in \mathbb{Z}_n$ υπάρχει το

$[bb']_n \in \mathbb{Z}_n$ ώστε:

$$[a]_n [a']_n [bb']_n = [aa'bb']_n = [(ab)(a'b')]_n =$$

$$[ab]_n [a'b']_n = \underbrace{[a]_n [b]_n}_{[1]_n} \underbrace{[a']_n [b']_n}_{[1]_n} = [1]_n [1]_n = [1]_n$$

Άρα, $[a]_n [a']_n \in U(\mathbb{Z}_n)$.

n. είναι κλειστή στο $U(\mathbb{Z}_n)$

Βήμα 2: Για κάθε $[a]_n, [a']_n, [a'']_n \in U(\mathbb{Z}_n)$ ισχύει: $[a]_n \cdot ([a']_n \cdot [a'']_n) = [a]_n \cdot [a'a'']_n =$

$[a \cdot (a' \cdot a'')]_n = [(a \cdot a')a'']_n = [aa']_n [a'']_n =$

$([a]_n \cdot [a']_n) \cdot [a'']_n$

η · είναι προσεταιριστική στο $U(\mathbb{Z}_n)$

Βήμα 3: Υπάρχει το $[1]_n \in U(\mathbb{Z}_n)$ ώστε:

$[a]_n [1]_n = [a]_n = [1]_n [a]_n, \forall [a]_n \in U(\mathbb{Z}_n)$

το $[1]_n$ είναι ουδέτερο ως προς την · στο $U(\mathbb{Z}_n)$

Βήμα 4: Έστω $[a]_n \in U(\mathbb{Z}_n)$. Εξ' ορισμού της $U(\mathbb{Z}_n)$, υπάρχει $[b]_n \in \mathbb{Z}_n$ με $[a]_n [b]_n = [1]_n$

Επίσης, $[b]_n [a]_n = [ba]_n = [ab]_n = [a]_n [b]_n = [1]_n$

Οι σχέσεις $[a]_n [b]_n = [1]_n = [b]_n [a]_n$ δηλώνουν ότι $[b]_n \in U(\mathbb{Z}_n)$ και ταυτόχρονα το $[b]_n$ είναι το αντίστροφο του $[a]_n$ ως προς την ·.

Από Βήμα 1 - Βήμα 4 συμπεραίνουμε ότι το ζεύγος $(U(\mathbb{Z}_n), \cdot)$ είναι ομάδα με ουδέτερο στοιχείο το $[1]_n \in U(\mathbb{Z}_n)$.

Ερωτήματα: 1) $|U(\mathbb{Z}_n)| = ;$

2) Πώς χαρακτηρίζουμε τα στοιχεία της $(U(\mathbb{Z}_n), \cdot)$;

Θεώρημα (Απάντηση στο 2)

$$[a]_n \in U(\mathbb{Z}_n) \iff (a,n) = 1$$

Απόδειξη

"$\Longleftarrow$" Έστω $(a,n) = 1$. Από θεώρημα Bezout υπάρχουν $x, y \in \mathbb{Z}$ ώστε $ax + ny = 1$. Τότε:

$$[1]_n = [ax+ny]_n = [ax]_n + [ny]_n = [a]_n[x]_n + [n]_n[y]_n$$

$$= [a]_n[x]_n, \text{ αφού } [n]_n = [0]_n$$

$[a]_n[x]_n = [1]_n$, που σημαίνει ότι $[a]_n \in U(\mathbb{Z}_n)$.

"$\Longrightarrow$" Έστω $[a]_n \in U(\mathbb{Z}_n)$. Επομένως, υπάρχει $[x]_n \in \mathbb{Z}_n$ ώστε $[a]_n[x]_n = [1]_n$, δηλαδή

$[ax]_n = [1]_n \Rightarrow ax \equiv 1 \pmod n \Rightarrow$

$n \mid ax-1 \Rightarrow \exists y \in \mathbb{Z}: ax-1 = ny$, άρα:

$ax + n(-y) = 1$ (*). Έστω $d = (a,n)$.

Διαδοχικά έχουμε: $\begin{matrix} d \mid a \\ d \mid n \end{matrix} \Rightarrow \begin{matrix} d \mid ax \\ d \mid n(-y) \end{matrix}$

$\Rightarrow d \mid ax + n(-y) \overset{(*)}{\Longrightarrow} d \mid 1 \Rightarrow d = 1 = (a,n)$ ∎

Ορισμός: (Απάντηση στο 1) Η συνάρτηση φ του Euler ορίζεται ως $\varphi: \mathbb{N} \to \mathbb{N}$ με $\varphi(n) := |\{a \in \mathbb{N} \mid 1 \le a \le n \text{ και } (a,n) = 1\}|$.

Πχ: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$, ...

Τι παρατηρείτε;

Ο ορισμός της φ και το προηγούμενο θεώρημα συνδυαστικά δίνουν:

$$|U(\mathbb{Z}_n)| = \varphi(n), \quad \forall n \in \mathbb{N}.$$

Παραδείγματα

- $n=1$: $\mathbb{Z}_1 = \{[0]_1\} = \{[1]_1\}$

  $U(\mathbb{Z}_1) = \{[1]_1\}$

- $n=2$: $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$

  $U(\mathbb{Z}_2) = \{[1]_2\}$

- $n=3$: $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$

  $U(\mathbb{Z}_3) = \{[1]_3, [2]_3\}$. $[2]_3^{-1} = [2]_3$

- $n=4$: $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$

  $U(\mathbb{Z}_4) = \{[1]_4, [3]_4\}$, $[3]_4^{-1} = [3]_4$

- $n=5$: $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$

  $U(\mathbb{Z}_5) = \{[1]_5, [2]_5, [3]_5, [4]_5\}$

  $[2]_5^{-1} = [3]_5$, $[3]_5^{-1} = [2]_5$, $[4]_5^{-1} = [4]_5$

Άσκηση: Να προσδιορίσετε την ομάδα $U(\mathbb{Z}_8)$.
Με ποια γνωστή ομάδα "μοιάζει";

Θεώρημα

Έστω $n \in \mathbb{N}$. Η ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική.

Απόδειξη: Πράγματι, για κάθε $[a]_n \in \mathbb{Z}_n$ ισχύει

$$[a]_n = [a \cdot 1]_n = a[1]_n \in \langle [1]_n \rangle, \text{ οπότε:}$$

$$\mathbb{Z}_n = \langle [1]_n \rangle$$

το $[1]_n$ είναι γεννήτορας της $(\mathbb{Z}_n, +)$

Ερώτημα: Είναι οι $(U(\mathbb{Z}_n), \cdot)$ κυκλικές;

Θεώρημα (Gauss): Οι $(U(\mathbb{Z}_n), \cdot)$ είναι κυκλικές μόνο για $n = 2, 4, p^k, 2p^k$, p: πρώτος, $p \geq 3$, $k \in \mathbb{N}$.

Παρατήρηση - SOS: Έστω p: πρώτος, $p \geq 3$.

Τότε: $\varphi(p) = |\{\alpha \in \mathbb{N} \mid 1 \leq \alpha \leq p, (\alpha, p) = 1\}|$

$= |\{1, 2, \ldots, p-1\}| = p - 1 = |U(\mathbb{Z}_p)|$

Άρα: $U(\mathbb{Z}_p) = \{[1]_p, [2]_p, \ldots, [p-1]_p\}$

$= \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$

Πρόταση: (Ιδιότητες και τύπος της φ)

(i) $\varphi(p^k) = p^k - p^{k-1}$, p: πρώτος, $p \geq 3$, $k \in \mathbb{N}$

(ii) - SOS: $(m, n) = 1 \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$

(iii) $\forall n \in \mathbb{N}$, $\varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right)$

! Στη συνέχεια, αφού εισαχθεί η έννοια της τάξης στοιχείων μιας ομάδας και το Θεώρημα Lagrange θα δούμε διάφορες εφαρμογές των ομάδων στη θεωρία Αριθμών.

Ομάδες Μεταθέσεων

Υπενθυμίζουμε ότι αν X είναι ένα μη-κενό σύνολο, τότε το σύνολο

$$S(X) = \{ f : X \to X \mid f : 1\text{-}1 \text{ και επί απεικόνιση} \}$$

εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων είναι ομάδα με ουδέτερο στοιχείο την ταυτοτική απεικόνιση Id_X και αν $f \in S(X)$ τότε το αντίστροφο του f είναι η αντίστροφη απεικόνιση f^{-1}.

▶ Σε αυτή την ενότητα θα ασχοληθούμε με την περίπτωση όπου $X = \{1, 2, \dots, n\}$ με $n \in \mathbb{N}$ και γράφουμε $S(X) = S(\{1, 2, \dots, n\}) =: S_n$.

Τα στοιχεία της S_n είναι 1-1 και επί απεικονίσεις $\sigma : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$

$$i \longmapsto \sigma(i)$$

Παριστώντας, χάριν ευκολίας, ως εξής:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(i) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix} \in S_n.$$

Πχ: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \in S_4$

• Η ταυτοτική απεικόνιση Id_n τη συμβολίζουμε

Id ή $1 = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$

ενώ αν $\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \end{pmatrix} \in S_n$ τότε

$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n-1) & \sigma(n) \\ 1 & 2 & \dots & n-1 & n \end{pmatrix} \in S_n$

Παράδειγμα

Στη συμμετρική ομάδα $(S_6, \circ)$ θεωρούμε

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 6 & 2 & 4 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

Να βρείτε, $\sigma\circ\tau$, $\tau\circ\sigma$, σ^{-1}, τ^{-1}.

Λύση

$$\sigma\circ\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}$$

$$\tau\circ\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 5 & 4 & 2 & 6 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 1 & 3 & 5 & 4 & 2 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 3 & 6 \end{pmatrix}$$

$$\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 6 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$$

• $n=1$: $S_1 = \{Id\}$ ← κυκλική $\quad |S_1| = 1$

• $n=2$: $S_2 = \{Id, \sigma\}$, $\quad Id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ $\quad |S_2| = 2$

$= \langle \sigma \rangle \quad \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$

↑
κυκλική

• $n=3$: $Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\quad |S_3| = 6$

Πρόταση

$$|S_n| = n!$$

Απόδειξη: Για τυχούσα $\sigma \in S_n$ έχουμε:

n τρόπους για το $\sigma(1)$

$n-1$ τρόπους για το $\sigma(2)$

⋮ ⋮

1 τρόπο για το $\sigma(n)$

Η πολλαπλασιαστική αρχή μας λέει ότι συνολικά έχουμε: $n \cdot (n-1) \cdots 1 = n!$ τρόπους.

Κύκλοι της S_n

Έστω $x_1, \ldots, x_k \in \{1, \ldots, n\}$ με $k \leq n$. Μια μετάθεση $\sigma \in S_n$ λέγεται **k-κύκλος** ή **κύκλος μήκους k** αν

$\sigma(x_1) = x_2$, $\sigma(x_2) = x_3$, $\ldots$, $\sigma(x_{k-1}) = x_k$, $\sigma(x_k) = x_1$ και

$\sigma(x) = x$, $\forall x \in \{1, \ldots, n\} \setminus \{x_1, \ldots, x_k\}$.

Συμβολισμός: $\sigma = (x_1\ x_2\ \ldots\ x_k)$

Αν $k = 2$ τότε η σ λέγεται **αντιμετάθεση**.

Παραδείγματα

Για την $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix} \in S_8$

Ισχύει $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$

↳ κύκλος μήκους 8

Για την $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 7 & 4 & 5 & 6 & 3 & 8 \end{pmatrix} \in S_8$

ισχύει $\sigma = (3\ 7)$ ← αντιμετάθεση.

Ομοίως, η $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 8 \end{pmatrix} \in S_8$

δεν είναι κύκλος της S_8 (είναι γινόμενο κύκλων)

• Επίσης, σε κάθε S_n, η ταυτοτική απεικόνιση είναι κύκλος μήκους 1.

Ορισμός: Δύο κύκλοι $\sigma = (x_1, \dots, x_k)$ και $\tau = (y_1, \dots, y_r)$ της $(S_n, \circ)$, με $2 \le k, r \le n$ λέγονται **ξένοι κύκλοι**, αν

$$\{x_1, \dots, x_k\} \cap \{y_1, \dots, y_r\} = \emptyset.$$

ΠΧ: Στην $(S_{12}, \circ)$ οι κύκλοι $\sigma = (1\ 9\ 8)$ και $\tau = (11\ 1\ 12)$ δεν είναι ξένοι διότι

$$\{1, 9, 8\} \cap \{11, 1, 12\} = \{1\} \neq \emptyset$$

Αντίθετα οι $\sigma' = (1\ 9\ 8)$ και $\tau' = (3\ 7)$ είναι ξένοι αφού $\{1, 9, 8\} \cap \{3, 7\} = \emptyset$.

! Θα αποδείξουμε ότι κάθε μετάθεση της S_n ή είναι ένας κύκλος ή γράφεται σαν σύνθεση κύκλων ξένων ανά δύο, όπου κάθε ένας έχει μήκος ≥ 2.

Για να το αποδείξουμε αυτό θα χρειαστούμε κάποια προαπαιτούμενα!!

Προαπαιτούμενα

Έστω $n \in \mathbb{N}$ και έστω $\sigma \in S_n$. Με βάση τη σ, ορίζουμε μια σχέση "$\sim_\sigma$" επί του $X_n = \{1, 2, \dots, n\}$ ως εξής:

$$\forall i, j \in X_n: \quad i \sim_\sigma j \iff \exists m \in \mathbb{Z}: \sigma^m(i) = j$$

[Υπενθύμιση: $\sim_\sigma \subseteq X_n \times X_n$ ώστε: $(i,j) \in \sim_\sigma \iff \exists m \in \mathbb{Z}: \sigma^m(i) = j$]

Λήμμα: Έστω $\sigma \in S_n$. Η $\sim_\sigma$ είναι σχέση ισοδυναμίας επί του X_n.

Απόδειξη

- **ανακλαστική:** $i \sim_\sigma i$, $\forall i \in X_n$.

Πράγματι, αν $i \in X_n$ τότε: $\sigma^0(i) = Id(i) = i$,

άρα $i \sim_\sigma i$

▶ συμμετρική: Έστω $i, j \in X_n$ με $i \underset{\sigma}{\sim} j$.

Υπάρχει $m \in \mathbb{Z}$ ώστε $\sigma^m(i) = j$. Τότε $-m \in \mathbb{Z}$

και $\sigma^{-m}(j) = \sigma^{-m}(\sigma^m(i)) = (\sigma^{-m} \circ \sigma^m)(i) =$

$\sigma^{-m+m}(i) = \sigma^0(i) = Id(i) = i$, άρα $j \underset{\sigma}{\sim} i$

▶ μεταβατική: Έστω $i, j, k \in X_n$ με $i \underset{\sigma}{\sim} j$

και $j \underset{\sigma}{\sim} k$. Τότε υπάρχουν $m, m' \in \mathbb{Z}$ ώστε

$\sigma^m(i) = j$ και $\sigma^{m'}(j) = k$. Έχουμε:

$\sigma^{m'+m}(i) = (\sigma^{m'} \circ \sigma^m)(i) = \sigma^{m'}(\sigma^m(i)) = \sigma^{m'}(j) = k$,

οπότε $i \underset{\sigma}{\sim} k$.

■

Ορισμός: Η σ-τροχιά του $i \in X_n$ είναι η κλάση ισοδυναμίας του i ως προς τη σχέση ισοδυναμίας $\underset{\sigma}{\sim}$, δηλαδή

$$\mathcal{O}(\sigma) = [i]_\sigma = \{j \in X_n \mid j \underset{\sigma}{\sim} i\} = \{j \in X_n \mid \exists m \in \mathbb{Z} : \sigma^m(i) = j\}$$

$$= \{\sigma^m(i) \in X_n \mid m \in \mathbb{Z}\}$$

Παράδειγμα

Στην $(S_9, \circ)$ θεωρούμε τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 5 & 7 & 6 & 1 & 4 & 8 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 3 & 2 & 1 & 4 & 5 & 6 & 9 & 7 \end{pmatrix}$$

Θα βρούμε την τροχιά κάθε στοιχείου $i \in \{1, 2, \ldots, 9\}$ ως προς τις σ και τ.

▶ $1 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 7$, $\quad 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2$, $\quad 6 \xrightarrow{\sigma} 6$

$O_\sigma(1) = \{1, 9, 8, 4, 5, 7\}$, $O_\sigma(2) = \{2, 3\}$, $O_\sigma(6) = \{6\}$

$= O_\sigma(9) = O_\sigma(8) = O_\sigma(4) = O_\sigma(5) = O_\sigma(7)$ $\quad = O_\sigma(3)$

▶ $1 \xrightarrow{\tau} 8 \xrightarrow{\tau} 9 \xrightarrow{\tau} 7 \xrightarrow{\tau} 6 \xrightarrow{\tau} 5 \xrightarrow{\tau} 4$, $\quad 2 \xrightarrow{\tau} 3 \xrightarrow{\tau} 2$

$O_\tau(1) = \{1, 8, 9, 7, 6, 5, 4\}$, $O_\tau(2) = \{2, 3\}$.

▶ Έστω $\sigma \in S_n$. Για κάθε $i \in X_n$ ορίζει

$\mathcal{O}_\sigma(i) = \{\sigma^m(i) \in X_n \mid m \in \mathbb{Z}\} \subseteq X_n$. Εφόσον το X_n είναι πεπερασμένο, έπεται ότι $\mathcal{O}_\sigma(i)$: πεπερασμένο

άρα υπάρχουν $m, m' \in \mathbb{Z}$ με $m > m'$, ώστε:

$\sigma^m(i) = \sigma^{m'}(i) \Rightarrow \sigma^{m-m'}(i) = i$. Συνεπώς

το σύνολο $M_\sigma(i) = \{t \in \mathbb{N} \mid \sigma^t(i) = i\}$ είναι

μη-κενό υποσύνολο του $\mathbb{N}$, οπότε έχει

ελάχιστο στοιχείο, έστω $s = \min M_\sigma(i)$, που

σημαίνει ότι το s είναι ο ελάχιστος φυσικός

αριθμός με την ιδιότητα $\sigma^s(i) = i$.

Τότε: $\mathcal{O}_\sigma(i) = \{i, \sigma(i), \ldots, \sigma^{s-1}(i)\}$ / Η/W/

Παρατήρηση: Αν $i, j \in X_n$ τότε είτε

$\mathcal{O}_\sigma(i) = \mathcal{O}_\sigma(j)$ ή $\mathcal{O}_\sigma(i) \cap \mathcal{O}_\sigma(j) = \emptyset$.

Ορισμός (κύκλος στην S_n): Έστω $\sigma \in S_n$.

(I) Η σ λέγεται **κύκλος** στην S_n, αν διαθέτει το πολύ μία τροχιά με περισσότερα των ενός στοιχεία.

(II) Μήκος ενός κύκλου σ λέμε το πλήθος των στοιχείων εκείνης της τροχιάς του, που έχει το μεγαλύτερο πλήθος στοιχείων.

(III) Ένας κύκλος μήκους 2 λέγεται **αντιμετάθεση**.

Πρόταση

Έστω $n \in \mathbb{N}$ και έστω $\sigma \in S_n$. Τότε η σ ή είναι κύκλος ή είναι σύνθεση κύκλων ξένων ανά δύο, όπου το μήκος καθενός είναι ≥ 2.

Απόδειξη: Αν η σ είναι κύκλος δε χρειάζεται να αποδειχθεί τίποτα. Ας υποθέσουμε ότι η σ δεν είναι κύκλος. Εξ' ορισμού, η σ διαθέτει τουλάχιστον δύο τροχιές με περισσότερα του ενός στοιχεία. Έστω

$$\mathcal{O}_1 = \mathcal{O}_\sigma(a_{11}) = \{a_{11}, a_{12}, \dots, a_{1t_1}\}$$

$$\mathcal{O}_2 = \mathcal{O}_\sigma(a_{21}) = \{a_{21}, a_{22}, \dots, a_{2t_2}\}$$

$$\vdots$$

$$\mathcal{O}_s = \mathcal{O}_\sigma(a_{s1}) = \{a_{s1}, a_{s2}, \dots, a_{st_s}\}$$

οι τροχιές αυτές.

Για κάθε $1 \le i \le s$, ορίζουμε μετάθεση σ_i ως

$$\sigma_i(a) = \begin{cases} \sigma(a), & a \in \Theta_i \\ a, & a \notin \Theta_i \end{cases}$$

Τότε, $\sigma_i = (a_{i1}\ a_{i2} \dots a_{it_i})$ κύκλος μήκους $|\Theta_i| = t_i \ge 2$.

Ισχυρισμός: $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_s$

- Έστω $a \in X_n = \{1, 2, \dots, n\}$. Αν $a \in X_n \setminus (\Theta_1 \cup \Theta_2 \cup \dots \cup \Theta_s)$, τότε προφανώς $\sigma(a) = a = (\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_s)(a)$ διότι το a δεν εμφανίζεται σε κανέναν από τους κύκλους σ_i.

Έστω $a \in \Theta_1 \cup \Theta_2 \cup \dots \cup \Theta_s$. Τότε το a ανήκει σε ακριβώς μια τροχιά, έστω $a \in \Theta_i$, διότι $\Theta_\kappa \cap \Theta_\lambda = \emptyset$ για $\kappa, \lambda = 1, 2, \dots, s$ με $\kappa \neq \lambda$.

Τότε: $\sigma_{i+1}(a) = \dots = \sigma_{s-1}(a) = \sigma_s(a) = a$ και

$$(\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-1} \circ \sigma_i \circ \dots \sigma_s)(a) = (\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-1} \circ \sigma_i)(a)$$

Όμως $\sigma_i(a) = \sigma(a) \in O_i$ και γι' αυτό το $\sigma(a)$ δεν ανήκει σε καμία από τις τροχιές $O_1, O_2, \dots, O_{i-1}$, άρα $\sigma_k(\sigma(a)) = \sigma(a)$

για $k = 1, 2, \dots, i-1$

Επομένως,

$$(\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-1} \circ \sigma_i)(a) = (\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-1})(\sigma(a)) =$$

$$(\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-2})(\sigma(a)) = \dots = \sigma_1(\sigma(a)) = \sigma(a),$$

οπότε: $(\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_{i-1} \circ \sigma_i \circ \dots \circ \sigma_s)(a) = \sigma(a)$.

Αποδείχθηκε ότι $\sigma(a) = (\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_s)(a)$ για κάθε $a \in X_n$ και άρα $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_s$ με το μήκος κάθε κύκλου σ_i να είναι ≥ 2.

■

Πρόταση: Η ανάλυση μιας μετάθεσης σε γινόμενο ξένων κύκλων, καθένας εκ των οποίων έχει μήκος ≥ 2, είναι μοναδική. Δηλαδή, αν $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_s = \delta_1 \circ \delta_2 \circ \dots \circ \delta_r$, τότε $r = s$ και υπάρχει μια αναδιάταξη $i_1, i_2, \dots, i_s$ των δεικτών $1, 2, \dots, s$ έτσι ώστε

$$\gamma_k = \delta_{ik} \text{ για κάθε } 1 \leq k \leq s.$$

Βλέπε απόδειξη Ηλεκτρονικό βιβλίο σελ. 254

Πρόταση 5.1.16.

Λήμμα: Έστω $n \in \mathbb{N}$ και γ, δ δύο ξένοι κύκλοι της $(S_n, \circ)$. Τότε $\gamma \circ \delta = \delta \circ \gamma$

Απόδειξη: Έστω $\gamma = (c_1\ c_2 \dots c_r)$ και $\delta = (d_1\ d_2 \dots d_t)$, όπου $r, t \geq 2$ και

$$\{c_1, c_2, \dots, c_r\} \cap \{d_1, d_2, \dots, d_t\} = \emptyset.$$

Έστω $a \in X_n = \{1, 2, \dots, n\}$. Διακρίνουμε 3 περιπτώσεις

(i) $a \in X_n \setminus (\{c_1, c_2, \dots, c_r\} \cup \{d_1, d_2, \dots, d_t\})$. Τότε

$$\left.\begin{aligned}(\gamma \circ \delta)(a) &= \gamma(\delta(a)) = \gamma(a) = a \\ (\delta \circ \gamma)(a) &= \delta(\gamma(a)) = \delta(a) = a\end{aligned}\right\} \Rightarrow (\gamma \circ \delta)(a) = (\delta \circ \gamma)(a)$$

(ii) $a \in \{c_1, \dots, c_r\}$. Τότε $\gamma(a) \in \{c_1, c_2, \dots, c_r\}$ και συνεπώς $\delta(\gamma(a)) = \gamma(a)$, οπότε:

$$(\gamma \circ \delta)(a) = \gamma(\delta(a)) = \gamma(a) = \delta(\gamma(a)) = (\delta \circ \gamma)(a)$$

(iii) $a \in \{d_1, d_2, \dots, d_t\}$. Τότε $\delta(a) \in \{d_1, d_2, \dots, d_t\}$, άρα $\gamma(\delta(a)) = \delta(a)$ και έτσι έχουμε:

$(\gamma\circ\delta)(a) = \gamma(\delta(a)) = \delta(a) = \delta(\gamma(a)) = (\delta\circ\gamma)(a)$.

Σε κάθε περίπτωση, $(\gamma\circ\delta)(a) = (\delta\circ\gamma)(a)$.

Αυτό ισχύει στο τυχόν $a \in X_n$ και συνεπώς

$$\gamma\circ\delta = \delta\circ\gamma$$

■

Με χρήση Μαθηματικής Επαγωγής εύκολα προκύπτει το ακόλουθο πόρισμα:

Πόρισμα: Αν $\gamma_1, \gamma_2, \dots, \gamma_s$ είναι κύκλοι της $(S_n, \circ)$ ανά δύο ξένοι, τότε

$$\gamma_1\circ\gamma_2\circ\dots\circ\gamma_s = \gamma_{i_1}\circ\gamma_{i_2}\circ\dots\circ\gamma_{i_s},$$

όπου $i_1, i_2, \dots, i_s$ είναι μια οποιαδήποτε αναδιάταξη των $1, 2, \dots, s$.

Άσκηση 1: Έστω ένας κ-κύκλος $\gamma = (a_1\ a_2 \dots a_k) \in S_n$. Τότε $\gamma^{-1} = (a_k\ a_{k-1} \dots a_2\ a_1)$.

Λύση: Θέτουμε $\delta = (a_k\ a_{k-1} \dots a_2\ a_1)$ και θα δείξουμε ότι $\gamma\circ\delta = \delta\circ\gamma = Id_n$.

▶ $\gamma\circ\delta = Id_n$: Έστω $x \in X_n = \{1, 2, \dots, n\}$. Αν $x \in X_n \setminus \{a_1, a_2, \dots, a_k\}$ τότε

$$(\gamma\circ\delta)(x) = \gamma(\delta(x)) = \gamma(x) = x = Id_n(x)$$

Αν $x \in \{a_1, a_2, \dots, a_k\}$ τότε:

$$(\gamma\circ\delta)(x) = \begin{cases} (a_1\ a_2 \dots a_k)\circ(a_k\ a_{k-1} \dots a_1)(a_i), & i \neq 1 \\ (a_1\ a_2 \dots a_k)\circ(a_k\ a_{k-1} \dots a_1)(a_1), & i = 1 \end{cases}$$

$$= \begin{cases} (a_1\ a_2 \dots a_k)(a_{i-1}), & i \neq 1 \\ (a_1\ a_2 \dots a_k)(a_k), & i = 1 \end{cases} = \begin{cases} a_i, & i \neq 1 \\ a_1, & i = 1 \end{cases}$$

Τελικά, $(\gamma\circ\delta)(x) = x,\ \forall x \in X_n \Rightarrow \gamma\circ\delta = Id_n$.

▶ $\delta\circ\gamma = Id_n$: Πράγματι, αν $\delta\circ\gamma = \sigma$ τότε:

$(\delta\circ\gamma)\circ\delta = \sigma\circ\delta \Rightarrow \delta\circ(\gamma\circ\delta) = \sigma\circ\delta \Rightarrow \delta\circ Id_n = \sigma\circ\delta$

$\Rightarrow Id_n\circ\delta = \sigma\circ\delta \xrightarrow[\text{Διαγραφής}]{\text{Νόμος}} \sigma = Id_n = \delta\circ\gamma$

□

Άσκηση 2: Για κάθε $\sigma \in S_n$ και για κάθε κύκλο $\gamma = (a_1\, a_2 \dots a_k) \in S_n$, μήκους k, ισχύει:

$$\sigma \circ \gamma \circ \sigma^{-1} = \sigma \circ (a_1\, a_2 \dots a_k) \sigma^{-1} = (\sigma(a_1)\, \sigma(a_2) \dots \sigma(a_k)).$$

Λύση: Θέτουμε $\delta = (\sigma(a_1)\, \sigma(a_2) \dots \sigma(a_k))$ και θα αποδείξουμε ότι $\sigma\gamma\sigma^{-1} = \delta$ ή ισοδύναμα $\sigma\gamma = \delta\sigma$. Έστω $x \in X_n = \{1, 2, \dots, n\}$. Αν $x \notin \{a_1, a_2, \dots, a_k\}$ τότε επειδή σ: 1-1 έχουμε $\sigma(x) \notin \{\sigma(a_1), \dots, \sigma(a_k)\}$ και άρα

$$\left.\begin{aligned} (\sigma\gamma)(x) &= \sigma(\gamma(x)) = \sigma(x) \\ (\delta\sigma)(x) &= \delta(\sigma(x)) = \sigma(x) \end{aligned}\right\} \Rightarrow (\sigma\gamma)(x) = (\delta\sigma)(x)$$

Αν $x \in \{a_1, a_2, \dots, a_k\}$ τότε $x = a_i$ για κάποιο $i = 1, 2, \dots, k$, το οποίο είναι ισοδύναμο με το $\sigma(x) = \sigma(a_i)$ διότι σ: 1-1, οπότε έχουμε:

$$(\sigma\gamma)(x) = (\sigma\gamma)(a_i) = \begin{cases} \sigma(a_{i+1}), & i = 1, 2, \dots, k-1 \\ \sigma(a_1), & i = k \end{cases}$$

Και $(\delta \circ \sigma)(x) = \delta(\sigma(a_i)) = \begin{cases} \sigma(a_{i+1}), & i = 1, 2, \dots, k-1 \\ \sigma(a_1), & i = k \end{cases}$

άρα $(\sigma \circ \gamma)(x) = (\delta \circ \sigma)(x)$.

Όμως, $\left.\begin{array}{l} (\sigma \circ \gamma)(x) = (\delta \circ \sigma)(x) \\ \forall x \in X_n \end{array}\right\} \Rightarrow \sigma \circ \gamma = \delta \circ \sigma$ ∎

Λήμμα: Έστω $n \in \mathbb{N}$, $n \geq 2$. Κάθε κύκλος $\gamma = (a_1, a_2 \dots a_k) \in S_n$ είναι γινόμενο αντιμεταθέσεων. Αν $k \geq 2$ τότε ο κύκλος γ είναι γινόμενο $k-1$ το πλήθος αντιμεταθέσεων.

Απόδειξη: Αν ο κύκλος γ έχει μήκος $k=1$ τότε $\gamma = Id_n$ και εφ' όσον $n \geq 2$ γράφουμε $\gamma = (1\ 2) \circ (2\ 1)$ ← γινόμενο αντιμεταθέσεων.

Έστω $k \geq 2$. Τότε:

$$\gamma = (a_1\ a_2 \dots a_k) = \underbrace{(a_1\ a_k) \circ (a_1\ a_{k-1}) \circ \dots \circ (a_1\ a_2)}_{k-1 \text{ το πλήθος}} \quad (*)$$

απόδειξη (*): Πράγματι, αν $x \in X_n \setminus \{a_1, a_2, \dots, a_k\}$, τότε $\gamma(x) = x$ και

$$((a_1\ a_k) \circ (a_1\ a_{k-1}) \circ \dots \circ (a_1\ a_2))(x) = x = \gamma(x) \quad \checkmark$$

Έστω τώρα $x \in \{a_1, a_2, \dots, a_{k-1}\}$, δηλαδή $x = a_i$ για κάποιο $i \in \{1, 2 \dots, k-1\}$. Τότε $\gamma(x) = \gamma(a_i) = a_{i+1}$

και $((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots\circ(a_1\ a_2))(x) =$

$((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots\circ(a_1\ a_i)\circ\dots\circ(a_1\ a_2))(x) =$

$= ((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots\circ(a_1\ a_{i+1})\circ(a_1\ a_i))(a_i) =$

$= ((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots\circ(a_1\ a_{i+1}))(a_1) =$

$= ((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots(a_1\ a_{i+2}))(a_{i+1}) = a_{i+1} = f(a_i)$

Τέλος, αν $x = a_k$ τότε $f(x) = f(a_k) = a_1$

και $((a_1\ a_k)\circ(a_1\ a_{k-1})\circ\dots\circ(a_1\ a_2))(a_k) =$

$(a_1\ a_k)(a_k) = a_1 = f(a_k)$.

Επομένως, $f(x) = ((a_1\ a_k)\circ\dots\circ(a_1\ a_2))(x),\ \forall x\in X_4$

και άρα $f = (a_1\ a_k)\circ\dots\circ(a_1\ a_2)$

∎

Πρόταση: Κάθε μετάθεση $\sigma \in S_n$, $n \geq 2$, είναι γινόμενο αντιμεταθέσεων.

Απόδειξη: Κάθε μετάθεση είναι γινόμενο (ξένων) κύκλων και κάθε κύκλος είναι γινόμενο αντιμεταθέσεων. Επομένως, κάθε μετάθεση είναι γινόμενο αντιμεταθέσεων. ∎

Πχ: Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 6 & 4 & 3 & 1 & 5 \end{pmatrix} \in S_7$.

Γράφω $\sigma = (1\ 7\ 5\ 3\ 6) \leftarrow$ 5-κύκλος

$= \underbrace{(1\ 6) \circ (1\ 3) \circ (1\ 5) \circ (1\ 7)}$

4 αντιμεταθέσεις

σχόλιο: Εύκολα υπολογίζουμε ότι:

$\sigma = \underbrace{(1\ 5) \circ (1\ 2) \circ (1\ 7) \circ (3\ 5) \circ (3\ 6) \circ (3\ 7) \circ (2\ 7) \circ (2\ 3)}$

8 αντιμεταθέσεις

Θεώρημα (Χωρίς απόδειξη): Δεν υπάρχει μετάθεση σε S_n, $n \geq 2$, η οποία να είναι ταυτόχρονα γινόμενο και άρτιου και περιττού πλήθους αντιμεταθέσεων.

Ορισμός: Μια μετάθεση σε S_n, $n \geq 2$, καλείται **άρτια**, αντίστοιχα **περιττή**, αν είναι γινόμενο άρτιου, αντίστοιχα περιττού, πλήθους αντιμεταθέσεων.

Παραδείγματα

(i) Θεωρούμε τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 4 & 5 & 3 & 7 & 6 & 10 & 2 & 8 \end{pmatrix} \in S_{10}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 7 & 4 & 5 & 3 & 10 & 1 & 8 & 9 & 6 \end{pmatrix} \in S_{10}$$

- $\sigma = (1\ 9\ 2) \circ (3\ 4\ 5) \circ (6\ 7) \circ (8\ 10)$

$= (1\ 2) \circ (1\ 9) \circ (3\ 5) \circ (3\ 4) \circ (6\ 7) \circ (8\ 10)$

σ: άρτια

$$\tau = (1\ 2\ 7)\circ(3\ 4\ 5)\circ(6\ 10)\circ(1\ 7)$$
$$= (1\ 7)\circ(1\ 2)\circ(3\ 5)\circ(3\ 4)\circ(6\ 10)\circ(1\ 7)$$
$$= (1\ 7)\circ(1\ 2)\circ(3\ 5)\circ(3\ 4)\circ(6\ 10)$$

τ: περιττή

(ii) Κάθε κύκλος $\gamma = (a_1\ a_2 \dots a_k) \in S_n$, $n \geq 2$, $k \geq 2$ είναι άρτια (αντ. περιττή) αν k: περιττό (αντ. άρτιο)

(iii) $\forall n \geq 2$, $Id_n = (1\ 2)\circ(2\ 1)$ ← άρτια

Πρόταση

Έστω $n \in \mathbb{N}$, $n \geq 2$. Το υποσύνολο

$$A_n = \{\sigma \in S_n \mid \sigma: \text{άρτια μετάθεση}\} \subseteq S_n$$

είναι υποομάδα της $(S_n, \circ)$.