

$O_1 \times O_2 \times \dots \times O_k$ ορίζεται όταν O_1, \dots, O_k ορίζονται

Αν O_1, \dots, O_k κυκλικές τότε $O_1 \times \dots \times O_k$ κυκλική \Leftrightarrow

$$\Leftrightarrow (10;1, 10;1) = 1 \quad \forall i \neq j$$

Παράδειγμα

$Z_6 \times Z_{25}$ κυκλική

$Z_3 \times Z_{35}$ όχι κυκλική

$a \in O$ με $o(a) = k$

$$o(a^u) = \frac{k}{(k, u)}$$

$O(a) = k, \quad o(b) = l \quad O(ab) = ?$

• Αν $ab \neq ba$ δεν συμπιέζονται

• Αν $ab = ba \Rightarrow o(a, b) = u, \quad \text{εκπ}(k, l) = u$

$$(ab)^u = a^u b^u = 1 \Rightarrow a^u = 1 \quad \text{και} \quad b^u = 1 \Rightarrow$$

$ab = ba$

$\Rightarrow o(a) | u$ και $o(b) | u \Rightarrow k | u$ και $l | u \Rightarrow$

$$\Rightarrow \text{εκπ}(k, l) | u \quad \textcircled{1}$$

$$(a, b)^m = a^m \cdot b^m = 1 \Rightarrow \text{ord}(a, b) / m = \text{EK}(\kappa, \ell) \quad (2)$$

$$ab = ba$$

m πολλαπλασίου του κ (1), (2) $\Rightarrow \text{EK}(\kappa, \ell) = \text{ord}(a, b)$
 m πολλαπλασίου του ℓ

Συμμετρικές ομάδες S_n

$$S_n = \{ f: \{1, 2, \dots, n\} \xrightarrow{1-1} \{1, 2, \dots, n\} \}$$

$$f: (1, 2, \dots, n)$$

↓

$$(f(1), f(2), \dots, f(n))$$

Παράδειγμα

$$f: (1, 2, 3, 4)$$

↓

$$(4, 2, 1, 3)$$

$$g: (1, 2, 3, 4)$$

↓

$$(4, 3, 2, 1)$$

f, g		1	2	3	4
	g	4	3	2	1
	f	3	1	2	4

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

≠

gf		1	2	3	4
	f	4	2	1	3
	g	1	3	4	2

$$gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

Το Z_n με την κώδεση αποτελεί ομάδα με τάξη n

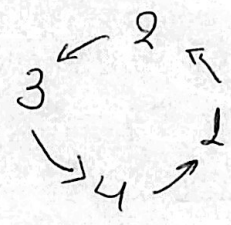
$n > 2 \Rightarrow Z_n$ όχι αβελιανή

Τα στοιχεία ονομάζονται μεταθέσεις

Παράδειγμα

1)

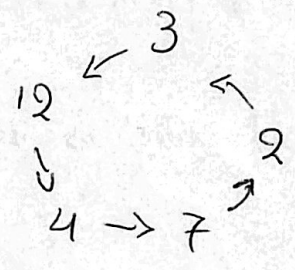
1	2	3	4
2	3	4	1



κύκλος μήκους 4

2)

3	12	4	7	2
12	4	7	2	3



θα το γράψουμε : $(12, 4, 7, 2, 3) = (7, 2, 3, 12, 4)$

ΟΡΙΣΜΟΣ

Μια μεταθέση $(a_1 \ a_2 \ a_3 \ \dots \ a_k)$ με την ιδιότητα

$a_1 \rightarrow a_2 \rightarrow a_3 \rightarrow \dots \rightarrow a_k \rightarrow a_1$, $(a_i \neq a_j)$ ονομάζεται κύκλος

μήκους k . Εδώ $\{a_1, a_2, \dots, a_k\} \subseteq \{1, 2, \dots, n\}$

Σημειώνεται (a_1, a_2, \dots, a_k)

ΟΡΟΙΣΜΟΣ

Δύο σύνολα (a_1, \dots, a_n) και (b_1, \dots, b_m) θα είναι ξένοι μεταξύ τους αν $\{a_1, a_2, \dots, a_n\} \cap \{b_1, b_2, \dots, b_m\} = \emptyset$

Παραδείγματα

$(2, 7, 4)$ $(1, 3, 5, 12)$ ξένοι.

Ιδιότητες σύνολων

$$1) (2, 7, 4)(2, 7, 4) = (2, 7, 4)^2$$

$$\begin{array}{c} 2 \rightarrow 7 \rightarrow 4 \\ \underbrace{\hspace{2cm}} \end{array}$$

$$\begin{array}{c} 7 \rightarrow 4 \rightarrow 2 \\ \underbrace{\hspace{2cm}} \end{array}$$

$$\begin{array}{c} 4 \rightarrow 2 \rightarrow 7 \\ \underbrace{\hspace{2cm}} \end{array}$$

Άρα $(2, 7, 4)^2 = (2, 4, 7)$

$$(2, 7, 4)(2, 7, 4)^2 = (2, 7, 4)^3 = (2, 7, 4)(2, 4, 7)$$

$$\begin{array}{c} 2 \rightarrow 4 \rightarrow 2 \\ \underbrace{\hspace{2cm}} \end{array}$$

$$\begin{array}{c} 4 \rightarrow 7 \rightarrow 4 \\ \underbrace{\hspace{2cm}} \end{array}$$

$$\begin{array}{c} 7 \rightarrow 2 \rightarrow 7 \\ \underbrace{\hspace{2cm}} \end{array}$$

Άρα $(2, 7, 4)^3 = 1$ ταυτοτική

$$o(2, 7, 4) = 3$$

ΠΡΟΤΑΣΗ

Κάθε κύκλος μήκους k έχει τμήμα k

2) $(2, 7, 4) (1, 3, 5, 12) \oplus$

- 1 \rightarrow 3 \rightarrow 3
- 2 \rightarrow 2 \rightarrow 7
- 3 \rightarrow 5 \rightarrow 5
- 4 \rightarrow 4 \rightarrow 2
- 5 \rightarrow 12 \rightarrow 12
- 6 \rightarrow 6 \rightarrow 6
- 7 \rightarrow 7 \rightarrow 4
- 8 \rightarrow 8 \rightarrow 8
- 9 \rightarrow 9 \rightarrow 9
- 10 \rightarrow 10 \rightarrow 10
- 11 \rightarrow 11 \rightarrow 11
- 12 \rightarrow 1 \rightarrow 1

Άρα μπορούμε να γράψω -

$$\oplus \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 3 & 7 & 5 & 2 & 12 & 6 & 4 & 8 & 9 & 10 & 11 & 1 \end{pmatrix}$$

$(0, \oplus, \oplus)$ είναι οι ίδιες μεταθέσεις "f"

$1 \rightarrow 3 \rightarrow 5 \rightarrow 12 \rightarrow 1 = (1, 3, 5, 12) = g$
 $2 \rightarrow 7 \rightarrow 4 \rightarrow 2 = (2, 7, 4) = h$
 $6 \rightarrow 6, 8 \rightarrow 8, 9 \rightarrow 9, 10 \rightarrow 10, 11 \rightarrow 11$

$(1, 3, 5, 12) (2, 7, 4)$

- 1 \rightarrow 1 \rightarrow 3
- 2 \rightarrow 7 \rightarrow 7
- 3 \rightarrow 3 + 5
- 4 \rightarrow 2 + 2
- 5 \rightarrow 5 \rightarrow 12
- 12 \rightarrow 12 \rightarrow 1

Παρατηρώ ότι είναι ίδια με πριν
Άρα αναμετατίθεται

Άρα όπως $o(f) = \text{ε.κ.η} (o(g), o(h))$
 $o(f) = 12$

ΠΡΟΤΑΣΗ

α) Δύο κώδοι f και g μετατίθενται αντιστρέφοντας $fg = gf$

β) Αν f και g είναι κώδοι f και g μετατίθενται τότε

$$o(fg) = \langle \text{ΚΠ} / o(f), o(g) \rangle$$

Απόδειξη

α. Έστω $f(a_1, a_2, \dots, a_n)$ και $g = (b_1, \dots, b_n)$

$$fg = gf?$$

$$b_i \rightarrow b_{i+1}$$

$$a_i \rightarrow a_{i+1}$$

Παρατηρώ ότι fg : $b_i \xrightarrow{g} b_{i+1} \xrightarrow{f} b_{i+1}$
 $a_i \xrightarrow{g} a_i \xrightarrow{f} a_{i+1}$

$$gf: b_i \xrightarrow{f} b_i \xrightarrow{g} b_{i+1}$$

$$a_i \xrightarrow{f} a_{i+1} \xrightarrow{g} a_{i+1}$$

Άρα $fg = gf$

Παράδειγμα

Έστω $H = \{ I, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \}$

και $H \leq S_4$ ΝΔΟ $H \leq S_4$ αβελιανή

Λύση

Επειδή $|H| = 4$ πεπερασμένη, αν η πράξη είναι κλειστή τότε $H \leq S_4$

$g_2 = (1,2)(3,4) \Rightarrow O(g_2) = \text{Eκπ}(O(1,2), O(3,4)) = \text{Eκπ}(2,2) = 2$

$g_2 = (1,3)(2,4) \Rightarrow O(g_2) = 2$

$g_3 = (1,4)(2,3) \Rightarrow O(g_3) = 2$

$g_1, g_2 \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix} = g_3$

(Να δείξω ως ισότιμες ομάδες)

$g_1 g_3 = g_2$

$g_2 g_3 = g_1$

$g_2 g_1 = g_3$

$g_3 g_1 = g_2$

$g_3 g_2 = g_1$

Άρα η ομάδα είναι αβελιανή $\Rightarrow H \cong \mathbb{Z}_4$

$H = \langle g_1, g_3 \rangle \left(\cup H = \langle g_1, g_2 \rangle \cup H = \langle g_2, g_3 \rangle \right)$

ΜΕ ΤΙΣ ΧΑΡΑΚΤΗΡΙΣΤΙΚΕΣ $O(g_1) = O(g_3) = 2$ και $g_1 g_3 = g_3 g_1$

Άρα $H = \{ 1, g_1, g_2, \underbrace{g_1 g_3 = g_3 g_1}_{= g_2} \}$

Αυτή μοιάζει με ως $\mathbb{Z}_2 \times \mathbb{Z}_2$ και την ομάδα του κλείν

||
υπάρχει αντιστοιχία
που ως ομαδοει \rightsquigarrow ισομορφικώς

ΘΕΩΡΗΜΑ

Έστω $f \in \mathbb{Z}_n$ μεταθέσει. Τότε η f γράφεται σαν γινόμενο κύκλων
γένων μεταθέσι τους.

$f = g_1 g_2 \dots g_k$ όπου g_1, \dots, g_k κύκλοι γένων n_i με
διαφορετική μήκη.

ΟΡΙΣΜΟΣ

Ένας κύκλος μήκους 2 καλείται αυτομεταθετός: $(a_1, a_2) = (a_2, a_1)$

Παράδειγμα

$$(1, 3, 7, 4) = (1, 4)(1, 7)(1, 3)$$

$$(1, 3, 7, 4) = (4, 7)(4, 3)(4, 1)$$

ΠΡΟΤΑΣΗ

Κάθε κύκλος (a_1, a_2, \dots, a_k) μήκους k γράφεται σαν γινόμενο $k-1$ αυτομεταθετών: $(a_1, a_2, \dots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \dots (a_1, a_2)$

ΘΕΩΡΗΜΑ

Έστω $f \in \Sigma_n$ μεταθετός. Α f θα γράφεται πάντα σαν γινόμενο περιττού ή άρτιου πλήθους αυτομεταθετών αποκλειστικά (χωρίς αποδείξη)

ΟΡΙΣΜΟΣ

Μια μεταθετός $f \in \Sigma_n$ καλείται άρτια αν γράφεται σαν άρτιο πλήθος αυτομεταθετών. Διαφορετικά καλείται περιττή.

Παράδειγμα

$$(1, 3, 7) = (1, 7)(1, 3) = (4, 7)(1, 7)(1, 4)(1, 3)$$

ΟΡΙΣΜΟΣ

Με A_n θα συμβολίζουμε το υποόμοιο της Z_n το οποίο θα περιέχει όλες τις άρτιες μεταθέσεις. Αυτό ονομάζεται η εναλλάξιμοτητα υποομάδα της Z_n .

ΠΡΟΤΑΣΗ

$$A_n \leq Z_n$$

Απόδειξη

Από την παραπάνω υποομάδα αρχει $n/2$ η οποία είναι κλειστή. Έστω $f, g \in A_n$. Πρέπει $fg \in A_n$

$$fg = \underbrace{(\) (\) \dots (\)}_{\substack{\text{άρτιο αριθμός} \\ \text{αλλαγών της } f}} \underbrace{(\) (\) \dots (\)}_{\substack{\text{άρτιο αριθμός} \\ \text{αλλαγών της } g}} \text{ άρτιο}$$

Παράδειγμα

$$Z_3 = \{ 1, \underbrace{(1,2,3)}_f, \underbrace{(1,2)}_g, \underbrace{(1,3,2)}_{f^2}, \underbrace{(1,3,2)(1,2)}_{fg} = (2,3), \underbrace{(1,3)}_{f^2g} \}$$

$$o(f) = 3, \quad o(g) = 2, \quad fg = gf^2$$

$$A_3 \leq Z_3 \quad \mu\epsilon \quad A_3 = \{ 1, f, f^2 \}$$

Παρατηρώ ότι $|A_3| = \frac{|Z_3|}{2} = \frac{6}{2} = 3$