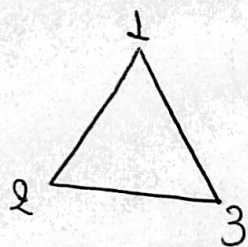


Ισομετρίες του ισοπλεύρου τριγώνου



$$\{f: \{1,2,3\} \xrightarrow[\text{επι}]{1-2} \{1,2,3\}\} = \mathcal{I}_3$$

\mathcal{I}_3 γεννιέται από τα 2 στοιχεία

1) Μια στροφή κατά 120° $f(1,2,3) \rightarrow (2,3,1)$

2) Μια εστιασμένη ως προς τη μεσοκάθετο από την κορυφή 1: g

$$f^2 = f \cdot f : (1,2,3) \xrightarrow{f} (2,3,1) \xrightarrow{f} (3,1,2)$$

$$\boxed{f^3 = 1 \text{ ταυτοτική}} \text{ (1)}$$

$$g: (1,2,3) \rightarrow (1,3,2)$$

$$\boxed{g^2 = 1 \text{ ταυτοτική}} \text{ (2) αφού } (1,2,3) \xrightarrow{g} (1,3,2) \xrightarrow{g} (1,2,3)$$

$$gfg: (1,3,2) \xrightarrow{g} (1,2,3) \xrightarrow{f} (2,3,1) \xrightarrow{g} (3,1,2)$$

$$\boxed{gfg = f^2} \text{ (3)}$$

$$\mathcal{I}_3 = \{1, f, f^2, g, fg, f^2g\} \text{ μαζί με τις σχέσεις (1), (2), (3)}$$

$$D_4 = \{ \text{ισομετρίες του τετραγώνου} \}$$

(ο δείκτης που δείχνει το σχήμα)

8 στοιχεία

$$f: (1, 2, 3, 4) \xrightarrow[90^\circ]{\text{εστροφή}} (2, 3, 4, 1)$$

$$f^2: (1, 2, 3, 4) \longrightarrow (3, 4, 1, 2)$$

$$f^3: (1, 2, 3, 4) \longrightarrow (4, 1, 2, 3)$$

$$f^4 = \text{I} \quad \textcircled{1}$$

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

$$g^2 = \text{I} \quad \textcircled{2}$$

$$gfg: (1, 2, 3, 4) \xrightarrow{g} (4, 3, 2, 1) \xrightarrow{f} (1, 4, 3, 2) \xrightarrow{g} (4, 1, 2, 3)$$

$$gfg = f^3 \quad \textcircled{3}$$

$$f^{-1} = f^3 \quad \text{αφού} \quad f \cdot f^3 = \text{I}$$

$$gf^2g = f^{-2} = f^2 \quad \textcircled{4}$$

$$gf^3g = f^{-3} = f \quad \textcircled{5}$$

$$D_4 = \{1, f, f^2, f^3, g, fg, f^2g, f^3g\} \text{ μαζί με τις σχέσεις}$$

①, ②, ③, ④, ⑤

Ονομάζεται διεδρική ομάδα με 4 στοιχεία

ΠΡΟΣΟΧΗ

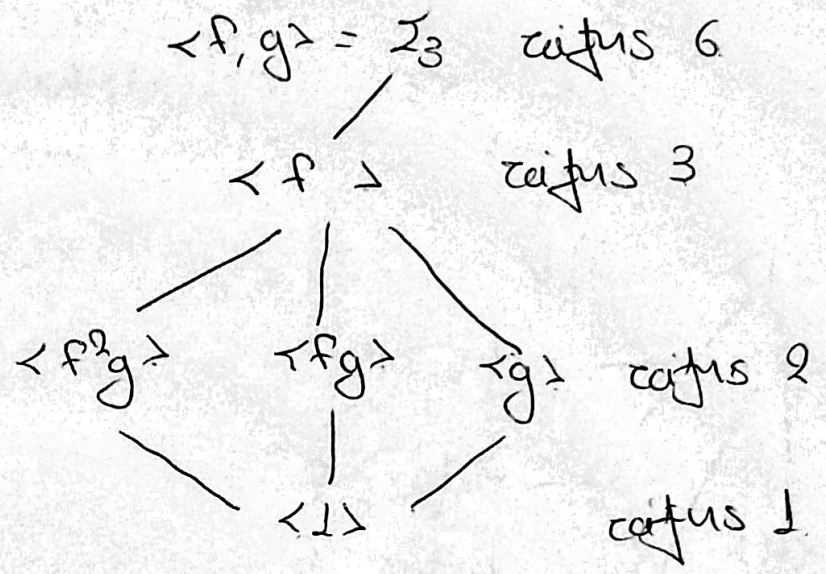
$$D_4 \not\cong \mathbb{Z}_4$$

$$|D_4| = 8 < |\mathbb{Z}_4| = 24$$

\mathbb{Z}_3 όχι κυκλική αφού δεν είναι αβελιανή ή αφού δεν υπάρχει στοιχείο που να γεννάει όλα.

$|Z_3| = 6$ και όχι κυκλική $\Rightarrow \nexists a \in Z_3$ με $o(a) = 6$
 $o(f) = 3$ και $o(g) = 2$

Υποομάδες της Z_3 :



$f g f g = f f^2 = 1$
 $f^2 g f^2 g = f^2 f = 1$
 $g g f g g = g f^2 g \Rightarrow$
 $\Rightarrow f = g f^2 g$

$\langle f, fg \rangle = \langle f, fg, f^2g, f f^2g = g \rangle$

(Παρατηρώ ότι όλες οι υποομάδες είναι κυκλικές εκτός της Z_3 .

ΠΡΟΤΑΣΗ

Με D_n θα συμβολίζαμε το σύνολο των συμμετρίων ενός κανονικού n -γώνου. Το σύνολο με πράξη τη σύνθεση αποτελεί ομάδα. Έχει $2n$ στοιχεία, δεν είναι αβελιανή και γεννιέται από δύο στοιχεία με μια στροφή f και μια συμμετρία g . Η ομάδα αυτή καλείται διευδρική τάξης $2n$.

Παράδειγμα

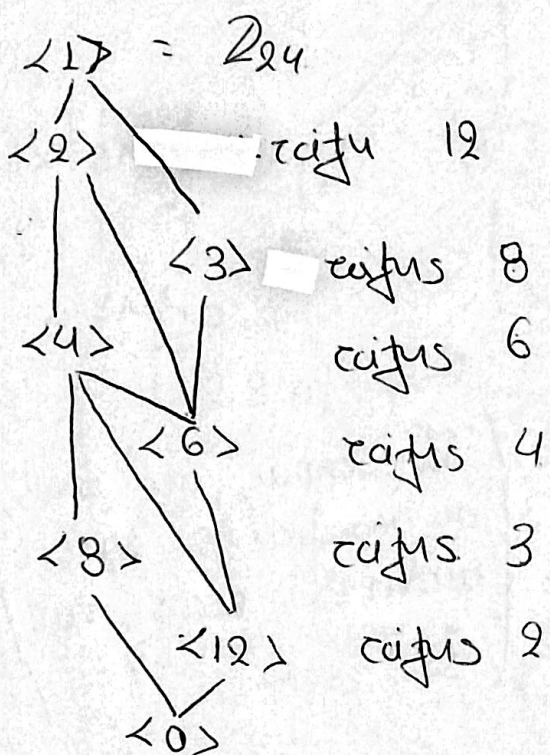
Να βρεθούν όλες οι υποομάδες της Z_{24}

Λύση

$Z_{24} = \langle [1] \rangle$ κυκλική τάξης 24.

Οι διατεταγμένες υποομάδες της ισοπλάσιας είναι όλοι οι διατεταγμένοι διαιρέτες του 24

1	2	3	4	6	8	12	24
$\langle 1 \rangle$	$\langle 2 \rangle$	$\langle 3 \rangle$	$\langle 4 \rangle$	$\langle 6 \rangle$	$\langle 8 \rangle$	$\langle 12 \rangle$	$\langle 24 \rangle$



ΕΥΘΕΑ ΓΙΝΟΜΕΝΑ

π.χ. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$

$$(a_1, a_2) + (a'_1, a'_2) = (a_1 + a'_1, a_2 + a'_2)$$

ΟΡΙΣΜΟΣ

Το καρτεσιανό ή ευθύ γινόμενο των (A, \oplus) και (B, \otimes) δίνεται από το $A \times B$ με πράξη $(a, b) \boxplus (a', b') = (a \oplus a', b \otimes b')$

Η νέα πράξη καθορίζεται από τις επιμέρους

Η νέα πράξη λέγεται πράξη κατά βυτισταγμένους $A \times B = \{a, b \mid a \in A, b \in B\}$

1) $\mathbb{Z} \times \mathbb{Z} = \{(r, v) \mid r, v \in \mathbb{Z}\}$

$(r, v) + (r', v') = (r + r', v + v')$

2) $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$
 $(1,0) + (1,0) = (1+1, 0+0) = (0,0)$

$0(1,0) = 2$

$(0,1) + (0,1) = (0,0)$

$0(0,1) = 2$

$(1,1) + (1,1) = (0,0)$

$0(1,1) = 2$

Άρα $\mathbb{Z}_2 \times \mathbb{Z}_2$ όχι κυκλική (δεν υπάρχει στοιχείο που να έχει τάξη 4)

3) Φάχου $|A \times B| = 12$ όχι αβελιανή

D_6 έχει 12 στοιχεία αλλά δεν είναι καρτεσιανό γινόμενο

$|S_3 \times \mathbb{Z}_2| = 12$ και όχι αβελιανή αφού S_3 όχι αβελιανή

ΟΡΙΣΜΟΣ

Έστω $(A_1, \cdot), \dots, (A_k, \cdot)$ ομάδες. Το καρτεσιανό γινόμενο τους είναι το σύνολο $A_1 \times A_2 \times \dots \times A_k$ με πράξη κατά συστατικά $(a_1, \dots, a_k) \cdot (a_1', \dots, a_k') = (a_1 a_1', \dots, a_k a_k')$

Μοναδικό : $(\perp_{A_1}, \perp_{A_2}, \dots, \perp_{A_k})$

$(a_1, \dots, a_k)^{-1} = (a_1^{-1}, \dots, a_k^{-1})$

Η $A_1 \times \dots \times A_k$ είναι αβελιανή αυτ όταν είναι αβελιανές

$$(a_1, a_2, \dots, a_k)(a'_1, \dots, a'_k) = (a'_1 a'_2, \dots, a'_k)(a_1, \dots, a_k)$$

$$\Leftrightarrow (a_1 a'_1, \dots, a_k a'_k) = (a'_1 a_1, \dots, a'_k a_k)$$

$$\Leftrightarrow a_1 a'_1 = a'_1 a_1, \dots, a_k a'_k = a'_k a_k$$

Δείξτε το αντίστροφο για κωδικία

Παράδειγμα

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{ (0,0), (0,1), (0,2), (1,0), (1,1), (1,2) \}$$

$$(0,1) + (0,2) = (0,2)$$

$$(0,2) + (0,1) = (0,0)$$

$$\text{Άρα } 0(0,1) = 3$$

$$0(1,0) = 2$$

$$(1,1) + (1,1) = (0,2)$$

$$(0,2) + (1,1) = (1,0)$$

$$(1,0) + (1,1) = (0,1)$$

$$(0,1) + (1,1) = (1,2)$$

$$(1,2) + (1,1) = (0,0)$$

$$\Rightarrow \left. \begin{array}{l} 0(1,1) = 6 \\ |\mathbb{Z}_2 \times \mathbb{Z}_3| = 6 \end{array} \right\} \Rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1,1) \rangle$$

κωδικία

ΠΡΟΤΑΣΗ

Έστω A_1, A_2, \dots, A_k ομάδες και (a_1, a_2, \dots, a_k) στοιχείο της $A_1 \times A_2 \times \dots \times A_k$. Αν $O(a_i) = u_i \quad i=1, \dots, k$ τότε

$$O(a_1, \dots, a_k) = \text{ΕΚΠ}(O(a_1), \dots, O(a_k))$$

Απόδειξη

Έστω $O(a_1, a_2, \dots, a_k) = u \implies (a_1, a_2, \dots, a_k)^u = (\perp_{A_1}, \dots, \perp_{A_k}) \implies$
 $\implies (a_1^u, \dots, a_k^u) = (\perp_{A_1}, \dots, \perp_{A_k})$

$$a_i^u = \perp_{A_i} \implies O(a_i) = u_i \mid u \quad \forall i=1, \dots, k$$

Άρα $\text{ΕΚΠ}(u_1, u_2, \dots, u_k) \mid u$

Αρκεί να $u \mid \text{ΕΚΠ}(u_1, \dots, u_k) \iff$

$$(a_1, \dots, a_k)^{\text{ΕΚΠ}(u_1, \dots, u_k)} = (\perp_{A_1}, \perp_{A_2}, \dots, \perp_{A_k})$$

$$a_i^{\text{ΕΚΠ}(u_1, u_2, \dots, u_k)} = \perp_{A_i} \text{ αφού}$$

$\text{ΕΚΠ}(u_1, u_2, \dots, u_k)$ είναι πολλαπλάσιο του u_i

$$|\mathbb{Z}_3 \times \mathbb{Z}_6| = |\mathbb{Z}_3| \cdot |\mathbb{Z}_6| = 3 \cdot 6 = 36$$

$$O(\mathbb{F}, 1) = \text{ΕΚΠ}(O(\mathbb{F}), O(1)) = \text{ΕΚΠ}(3, 6) = 6$$

$$O(\mathbb{F}, 2) = \text{ΕΚΠ}(3, 3) = 3$$

ΘΕΩΡΗΜΑ

Έστω $0 = A_1 \times \dots \times A_k$ με A_1, \dots, A_k ιδεώδη. Αν οι A_1, \dots, A_k είναι κωδικές τάξεις u_1, \dots, u_k τότε η 0 είναι κωδική

$$\underline{\text{αυν}} \quad \underbrace{(u_i, u_j)}_{\text{υ.κ.δ.}} = 1 \quad i \neq j$$

Απόδειξη

(\Rightarrow) $|0| = |A_1| \dots |A_k| = u_1 \cdot u_2 \dots u_k$. Για να είναι η 0 κωδική

πρέπει να υπάρχει στοιχείο τάξης $u_1 \cdot u_2 \dots u_k$

Έστω ότι $A_1 = \langle a_1 \rangle, A_2 = \langle a_2 \rangle, \dots, A_k = \langle a_k \rangle$

$$0(a_1, a_2, \dots, a_k) = \text{ε.κ.π.}(u_1, \dots, u_k)$$

Έστω 0 κωδική. Άρα υπάρχει $(a_1, a_2, \dots, a_k) \in 0$ με τάξη $u_1 \cdot u_2 \dots u_k = \text{ε.κ.π.}(u_1, \dots, u_k)$

Θεωρία τριθλιών $\rightarrow (u_i, u_j) = 1$ είναι πρώτοι μεταξύ τους.

(\Leftarrow) έχουμε $(u_i, u_j) = 1 \Rightarrow u_1 \cdot u_2 \dots u_k = \text{ε.κ.π.}(u_1, \dots, u_k)$

Αλλά $u_1 \cdot u_2 \dots u_k = |0|$ και $\text{ε.κ.π.}(u_1, u_2, \dots, u_k) = 0(a_1, \dots, a_k)$

Άρα υπάρχει στοιχείο (a_1, \dots, a_k) ώστε να έχει τάξη ίση με την τάξη της $0 \Rightarrow 0$ κωδική.

Παράδειγμα.

$\mathbb{Z}_4 \times \mathbb{Z}_{15}$ κυκλική

$\mathbb{Z}_4 \times \mathbb{Z}_{15} \times \mathbb{Z}_{53}$ κυκλική

$\mathbb{Z}_3 \times \mathbb{Z}_5$ όχι κυκλική