ΑΣΚΗΣΕΙΣ

Άσκηση 2 σελ 34:

$o(a) = \nu$, $o(b) = \mu$

$(ab)^{\mu\nu} = a^{\mu\nu} \cdot b^{\mu\nu} = (a^\nu)^\mu \cdot (b^\mu)^\nu \xRightarrow[o(b)=\mu]{o(a)=\nu} e^\mu \cdot e^\nu = e \cdot e = e$

$\Rightarrow o(ab) \mid \mu\nu$.

ενώ $(ab)^k = e \Rightarrow a^k \cdot b^k = e \Rightarrow a^k = b^{-k} \Rightarrow (a^k)^\nu = (b^{-k})^\nu \Rightarrow$

$\Rightarrow (a^\nu)^k = b^{-k\nu} \Rightarrow e^k = e^{-k\nu} \Rightarrow b^{-k\nu} = e \xRightarrow{o(b)=\mu} \mu \mid k\nu \xRightarrow{(k,\nu)=1}$

$\Rightarrow \mu \mid k$ και άρα $\nu \mid k \xRightarrow{(\mu,\nu)=1} \nu\mu \mid k \xRightarrow{k \mid \nu\mu} k = \nu\cdot\mu$

$\Rightarrow \nu\cdot\mu \mid o(a\beta)$

Άσκηση 8 σελ. 34:

$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle/ a, b, c \in \mathbb{Z}_p \quad p: \text{πρώτος} \right\}$

$GL(3, \mathbb{Z}_p)$ ομάδα $\geq G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle/ a, b, c \in \mathbb{Z}_p \right\}$

$|G| = p \cdot p \cdot p = p^3$ πεπερασμένο με πράξη κ.ο $\Rightarrow$

$\Rightarrow G$ ομάδα

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2a & 2b+ac \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3a & 3b+3ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix}$$

Με επαγωγή στο n μπορώ νάο μέσω επαγωγής

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & na & nb+\frac{n(n-1)}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

$$n=p \Rightarrow pa \equiv pc \equiv pb + \frac{p(p-1)}{2}ac \equiv 0 \bmod p$$

Άρα, $\mathrm{Ord}\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = p$

Για $p=2$ δυνατές περιπτώσεις:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Άσκηση 3 σελ 34:

$x * x = 2x - 1$

$x * x * x = (2x-1) * x = 3x - 2$

$x^k = kx - (k-1)$ επαγωγικά

$a = kx - (k-1)$ $\forall a$ να υπάρχει k ώστε

$a = 0 \Rightarrow kx = k-1$ αδύνατο

ΥΠΟΟΜΑΔΕΣ

$W \leq V$ διανυσμ. χωρου τοτε W καλειται υπόχωρος

ΟΡΙΣΜΟΣ

$Y \leq O$ υποομάδα $\Leftrightarrow$ $Y \subseteq O$ και Y με την πράξη της O θα είναι ομάδα

Σύνηθεις υποομάδες

$(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

$(\mathbb{Q}^*,\cdot) \leq (\mathbb{R}^*,\cdot) \leq (\mathbb{C}^*,\cdot)$

ΠΡΟΤΑΣΗ:

Το $Y \leq O$ για $Y \subseteq O$:

αν.ν ισχυουν

α) Η πραξη καλά ορισμενη

β) $\forall a \in Y \Rightarrow a^{-1} \in Y$

ΑΠΟΔΕΙΞΗ

$(\Leftarrow)$: 1) Προσεταιριστική

$a,b,\gamma \in Y \Rightarrow (a*b)*\gamma = a*(b*\gamma)$

2) μοναδιαιο-ουδετερο ($\in Y$ επειδή καλά ορισμενη)

$Y \neq \phi \Rightarrow \exists a \in Y \Rightarrow \exists a^{-1}: a*a^{-1} = e \in Y$

3) Εξ ορισμου για το αντιθετο

Πχ

$(\mathbb{Z},+)$ ομάδα

$(\mathbb{N},+)$ έχει καλά ορισμένη πράξη αλλά δεν είναι ομάδα

Πχ

$GL(2,\mathbb{R}) \geq \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} / \, ac \neq 0 \right\}$

$GL(n,\mathbb{R}) \geq \left\{ \begin{pmatrix} \alpha_1 & & * \\ & \alpha_2 & \\ 0 & & \ddots \; \alpha_n \end{pmatrix} / \, \Pi a_i \neq 0 \right\}$

$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & * \\ 0 & c'c \end{pmatrix} \neq 0$ καθε τετοιος πινακας έχει αντιστρέψιμο. Είναι ομάδα

- As είναι $|O|=8$, $O=D_4=\{1, f, f^2, f^3, g, fg, f^2g, f^3g\}$
  $f^4=1=g^2= gf^ig^{-1}=f^{-i}$

- Q_8 τετραγονια $i^2=-1$

$I=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $J=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$

$K=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $L=\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

Η ομάδα που γενναται απο τα στοιχεία παραπάνω

$J^2=\begin{pmatrix} i^2 & 0 \\ 0 & i^2 \end{pmatrix}=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$J^4=I=K^4=L^4$

$JK=L$, $KJ=-L$, $KL=J$ και $LK=-J$
$LJ=K$, $JL=-K$

$JK=\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = L$

$KJ=-L$

$Q_8=\{\pm I, \pm J, \pm K, \pm L\}$
ομάδα 8 στοιχείων οχι αβελιανη
Η D4 έχει μονο ενα στοιχειο τάξης 4 το f
Η Q8 έχει τρία στοιχεία ταξης 4: J, K, L

ΠΡΟΤΑΣΗ Όλες οι υποομάδες $(\mathbb{Z},+)$ είναι της μορφής $k\mathbb{Z}$, $k\in\mathbb{N}$

Απόδειξη

Έστω $Y\neq\{0\}$ υποομάδα της $\mathbb{Z}$

Έστω $k\in Y$ ώστε να είναι θετικό και μικρότερο

ΘΔΟ κάθε στοιχείο $a\in Y$ είναι της μορφής $a=k\lambda$. Y υποομάδα και περιέχει το k, θα περιέχει όλα τα πολλαπλάσια του.

Υποθέτουμε ότι έχουμε $b\in Y$ με b όχι πολλαπλάσιο του k: $b=kn+u$, $0<u<k$

$$\left.\begin{array}{l} b\in Y \\ kn\in Y \end{array}\right\} \Rightarrow b-kn\in Y \Rightarrow u\in Y \text{ αδύνατο}$$

ΠΡΟΤΑΣΗ: Κάθε υποομάδα κυκλικής είναι κυκλική.

ΟΡΙΣΜΟΣ: Έστω O ομάδα. Το υποσύνολο της $Z(O)=\{a \mid a\in O \text{ και } ab=ba \ \forall b\in O\}$ κέντρο της O

Πχ

$GL(2,\mathbb{R})$ όχι αβελιανή

Υπάρχει $A\in GL(2,\mathbb{R})$ με $AB=BA$ $\forall B\in GL(2,\mathbb{R})$

Για $A=I$ ισχύει

$Z(O)\ni 1 \Rightarrow Z(O)\neq\emptyset$ $\forall O$ ομάδα

$Z(O)=O \Leftrightarrow O$ αβελιανή

Πχ

Να βρούμε το κέντρο της $GL(2,\mathbb{R})$

Έστω a,b,γ,δ ώστε:

$$\begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix}\in Z(O) \Rightarrow \begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\cdot\begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix} \Rightarrow$$

$$\begin{pmatrix} b & a \\ \delta & \gamma \end{pmatrix} = \begin{pmatrix} \gamma & \delta \\ a & b \end{pmatrix}, \quad b=\gamma \text{ και } a=\delta$$

Αρα, $\begin{pmatrix} a & b \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$

Ετσι

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ b & a \end{pmatrix}$$

$$\begin{pmatrix} a+b & a \\ a+b & b \end{pmatrix} = \begin{pmatrix} a+b & a+b \\ a & b \end{pmatrix}, \quad b=0$$

άρα $\begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI \Rightarrow$

$\Rightarrow Z(0) = \{ aI / \alpha \in \mathbb{R}^* \}$

ΠΡΟΤΑΣΗ $Z(0) \leq 0$

ΑΠΟΔΕΙΞΗ

1) πράξη κλειστή

2) $\forall a \in Z(0) \Rightarrow a^{-1} \in Z(0)$

1) Αν a, b εν $Z(0) \Rightarrow a \cdot b \in Z(0) \Leftrightarrow$

2) $(a \cdot b)\gamma = \gamma(ab)$, $\forall \gamma \in 0$

$(ab)\gamma = a(b\gamma) = a(\gamma b) = (a\gamma)b = (\gamma a)b = \gamma(ab)$

πχ

Στο $\mathbb{Z}$ και $k\mathbb{Z}$ και $\lambda\mathbb{Z}$ υποομάδες και $k \neq k_1 \cdot \lambda$ (δηλ. όχι πολλαπλάσιο του λ) έτσι $k\mathbb{Z} \cap \lambda\mathbb{Z} = \mu\mathbb{Z} \Rightarrow$

$$\Rightarrow \left.\begin{cases} k \mid \mu \\ \lambda \mid \mu \end{cases}\right\} \Rightarrow [k,\lambda] \mid \mu \Rightarrow \mu = [k,\lambda]$$

πρακτικά $3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$

Όσο για την ένωση περιγράφεται στην ακόλουθη πρόταση

ΠΡΟΤΑΣΗ Αν Y, Y' υποομάδες της O τότε

1) $Y \cap Y' \leq O$ και 2) $Y \cup Y' \leq O \Leftrightarrow Y \leq Y'$

ΘΕΩΡΗΜΑ: Έστω $O\langle a \rangle$ κυκλική τάξης n

1) Η O έχει υποομάδα τάξης $\mu \Leftrightarrow$ ο μ διαιρεί το n

2) Αν $n = k\mu$, τότε η O έχει μοναδική υποομάδα τάξης μ

3) $\langle a^{\tau} \rangle = \langle a^{u} \rangle \Leftrightarrow (\tau, n) = (u, n)$

πχ

$\mathbb{Z}_{12}$ υποομάδες $\rightarrow$ 1, 2, 3, 4, 6, 12 : τάξεις

$$\{\bar{0}\} \quad \{\bar{0}, \bar{6}\} \quad \{\bar{0}, \bar{4}, \bar{8}\}$$

$$\langle \bar{0} \rangle, \ \langle \bar{6} \rangle, \ \langle \bar{4} \rangle$$

$$\frac{12}{1}\mathbb{Z}_{12} = \{12 \cdot \bar{0}, \ldots, 12 \cdot \bar{11}\} = \{\bar{0}\}$$

$$\frac{12}{2}\mathbb{Z}_{12} = \{6 \cdot \bar{0}, 6 \cdot \bar{1}, \ldots 6 \cdot \bar{11}\} = \{\bar{0}, \bar{6}\}$$

$$\frac{12}{3}\mathbb{Z}_{12} = \{\bar{0}, \bar{4}, \bar{8}\}$$

Απόδειξη:

"$\Rightarrow$": Έστω $Y \leq O = \langle a \rangle$, $o(a) = n$

$Y \subseteq \{a^0, a^1, \ldots, a^{n-1}\}$

Ας παρουμε το α με την μικρότερη δύναμη εντός απο το a^0 στο Y.

$a^\lambda \in Y$ με $0<\lambda<n-1$

$(a^\lambda)^k \in Y \Rightarrow a^{\lambda k} \in Y \quad \forall k \in \mathbb{N}$

$|Y| = m \Leftrightarrow (a^\lambda)^m = 1$ και $\forall (a^{\lambda k})^m = 1$, $a^\lambda \in Y \Rightarrow a^{-\lambda \pi} \in Y$

$(a^\lambda)^m = a^{\lambda m} = a^0 = 1 \Rightarrow n$ διαιρεί το λm

Αν ο $\lambda \nmid n \Rightarrow$ με την ευκλ. διαίρεση:

$n = \pi\lambda + \upsilon, \quad 0 < \upsilon \leq \lambda - 1$

$1 = a^n = a^{\pi\lambda+\upsilon} = (a^\lambda)^\upsilon \cdot a^\upsilon \Rightarrow 1 = a^{\lambda\pi} a^\upsilon \Rightarrow a^\upsilon = a^{-\lambda\pi} = (a^\lambda)^{-\pi}$

$\Rightarrow$ Το $a^\upsilon \in Y \Rightarrow \boxed{\upsilon < \lambda}$ άτοπο. Άρα ο $\lambda | n$

Με ίδιο τρόπο το m διαιρεί τον n

$|Y| = m \Rightarrow m | n$.

"$\Leftarrow$", $n = mk \Rightarrow$ βρες υποομάδα Y τάξης m

$Y = \langle a^k \rangle \Rightarrow |Y| = m = \frac{n}{(n,k)} = \frac{n}{k} = m$

2) Y και Y' υποομάδες τάξης m και το m/n

Άρα $Y = \langle a^\tau \rangle$ και $Y' = \langle a^\upsilon \rangle$ $\tau = \upsilon$

$|Y| = |Y'| = m \qquad o(a^\tau) = o(a^\upsilon)$

$o(a^\tau) = \frac{n}{(n,\tau)} = o(a^\upsilon) = \frac{n}{(n,\upsilon)} \Rightarrow (n,\tau) = (n,\upsilon)$

Άρα, επειδή $0<\tau, \upsilon<n-1$ έχουμε

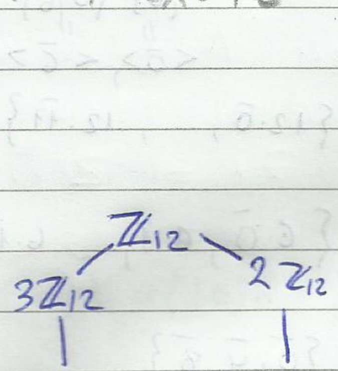
$\tau \equiv \upsilon \mod n$

ΠΧ

$1\mathbb{Z}_{12} = \mathbb{Z}_{12}$

$2\mathbb{Z}_{12} = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\}$

$3\mathbb{Z}_{12} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}\}$



Ασκήσεις (εργασία) σελίδα 43 (1, 3, 4, 7, 9, 11, 12, 15, 16, 17)

ΕΥΘΕΑ ΓΙΝΟΜΕΝΑ ΟΜΑΔΩΝ

$\mathbb{Z}_2 \times \mathbb{Z}_4 = \{ (a,b) \mid a \in \mathbb{Z}_3 \wedge b \in \mathbb{Z}_4 \}$

$(a,b) \oplus (a',b') = (a+a', b+b')$

$\Sigma_3 \times D_4 = \{ (a,b) \mid a \in \Sigma_3 , b \in D_4 \}$

$6 \times 8 = 48$ στοιχεία

ΟΡΙΣΜΟΣ: Έστω $O_1, \dots, O_k$ ομάδες (όχι πάντα αβελιανές) Ορίζουμε ευθύ γινόμενο να είναι το σύνολο $O_1 \times \dots \times O_k = \{ (a_1, \dots, a_k) \mid a_i \in O_i \}$ με πράξη κατά συντεταγμένες:

$(a_1, \dots, a_k) \oplus (a_1', \dots, a_k') = (a_1 + a_1', \dots, a_k + a_k')$

ΠΡΟΤΑΣΗ Το $O_1 \times \dots \times O_k$ όπως πριν αποτελεί ομάδα.

ΙΔΙΟΤΗΤΕΣ:

- Αν O_i αβελιανές $\forall i$ τότε και το ευθύ γινόμενο τους είναι αβελιανή. Ισχύει και το αντίστροφο γιατί η πράξη έχει οριστεί κατά συντεταγμένες.
- Αν οι O_i είναι κυκλικές είναι και το γινόμενο τους κυκλική;; ΟΧΙ ($\mathbb{Z}_2 \times \mathbb{Z}_2$ όχι) ΠΟΤΕ ΕΙΝΑΙ;;

ΘΕΩΡΗΜΑ: Έστω $O = O_1 \times \dots \times O_k$ ευθύ γινόμενο ομάδων

1) Αν $a_i \in O_i$ και έχει πεπερασμένη τάξη τότε η τάξη του $(a_1, \dots a_k)$ ισούται με το ΕΚΠ των τάξεων $o(a_1), \dots, o(a_k)$

2) Υποθέτουμε ότι $O_i = \langle a_i \rangle$ είναι κυκλικές για όλα τα $i \in \{1, \dots, k\}$ πεπερασμένης τάξης. Τότε η O είναι κυκλική $\Leftrightarrow$

$\Leftrightarrow (o(a_i), o(a_j)) = 1 \ \forall i \neq j \Leftrightarrow$

$\text{εκπ}(o(a_1), \dots, o(a_k)) = o(a_1) \cdots o(a_k)$