26/02/20

Φυλλάδιο 1 άσκηση 4

Έστω $(G,*)$ ομάδα με την ιδιότητα $x*x=e_G$ για κάθε $x\in G$.
Δείξτε ότι είναι αβελιανή η G.

Απόδειξη

Έστω $a,b\in G$. Τότε $a*a=e_G$ (1)

και $b*b=e_G$ (2)

και $(a*b)*(a*b)=$ (3)

Άρα από την 1 και 2: $a*a*b*b=e_G*e_G=e_G=a*b*a*b$

Άρα $a*a*b*b=a*b*a*b$

(Κανόνας Διαγραφής)

$a*b*b=b*a*b \Rightarrow a*b=b*a$ άρα G αβελιανή.

Φυλλάδιο 1 άσκηση 5

Έστω $(G,*)$ ομάδα, $a,b,c\in G$. Δείξτε ότι τα ακόλουθα
είναι ισοδύναμα: α) $a*b*c=e_G$

β) $b*c*a=e_G$

γ) $c*a*b=e_G$

Απόδειξη

(α) ⇒ (β)

$a*b*c=e_G \Rightarrow a^{-1}*(a*b*c)=a^{-1}*e_G$

$\Rightarrow (a^{-1}*a)*b*c=a^{-1}$

$\Rightarrow e_G*b*c=a^{-1}$

$\Rightarrow b*c=a^{-1} \Rightarrow (b*c)*a=a^{-1}*a$

$\Rightarrow b*c*a=e_G$

Το ίδιο επιχείρημα δίνει (β) ⇒ (γ) και (γ) ⇒ (α)

Άσκηση: Έστω S το σύνολο των 2×2 πινάκων A με στοιχεία στο $\mathbb{Z}$ και $\det(A) \neq 0$.

1) Δείξτε ότι ο πολλαπλασιασμός πινάκων ορίζει πράξη στο S.

2) Είναι το S ομάδα με αυτή την πράξη;

Λύση

$$S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad a,b,c,d \in \mathbb{Z} \text{ και } a\cdot d - bc \neq 0 \right\}$$

1) Έστω $A, B \in S$. Από τον ορισμό του πολλαπλασιασμού πινάκων, ο AB έχει ακέραιους συντελεστές.

Επιπλέον $\det(AB) = (\det(A)\cdot\det(B)) \neq 0$

Αποδείξαμε το 1).

Για το 2): Η πράξη στο S είναι προσεταιριστική (από Γραμμ. Άλγ.)

Υπάρχει ουδέτερο, ο πίνακας $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S$.

Ισχυρισμός: Ο πίνακας $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \in S$ αλλά δεν αντιστρέφεται στο S.

Απόδειξη ισχυρισμού: Αφού ο A έχει ακέραιους συντελεστές και ορίζουσα $\det(A) = 2 \neq 0$.

Έχουμε $A \in S$. Έστω ότι $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in S$, αντίστροφος του A.

Τότε $A\cdot B = B\cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Συνεπώς $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 2a & 2b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow$

$\Rightarrow 2a = 1$ και αφού $B \in S$, $a \in \mathbb{Z}$.

Δηλαδή 1 αριθμός → αντίφαση.
Άρα ο A δεν αντιστρέφεται στο S.
Συμπέρασμα S όχι ομάδα.

Συμβολισμός: Για κάποιες αβελιανές ομάδες συμβολίζουμε την πράξη με + (αντί για $*$), το ουδέτερο με 0 (αντί για e_G), "το αντίστροφο ως προς + του $a \in G$" το συμβολίζουμε $-a$ και το λέμε αντίθετο και για από το $\underbrace{a+a+\dots+a}_{n\text{-φορές}}$ το συμβολίζουμε na και παρόμοια για $a<0$.

Παραδείγματα τέτοιων ομάδων:
$(\mathbb{R},+)$, $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{C},+)$, $n \times n$ πίνακας με πράξη πρόσθεση και άλλα.

Παράδειγμα: Αν $a=2$, $n=3$ στο $\mathbb{R}$ με $3a=a+a+a$, $a^3=a \cdot a \cdot a$
Ως προς την πρόσθεση τον αντίστροφο του a είναι το $-a=-2$
και ως προς τον πολλαπλασιασμό τον αντίστροφο του a είναι το $1/2$.

Πρόταση: Έστω $n \geq 1$ και $U(\mathbb{Z}_n)=\{[a]_n \ a \in \mathbb{Z}$ με $\text{ΜΚΔ}(a,n)=1\}$
Τότε με πράξη $[a]_n \cdot [b]_n = [a \cdot b]_n$ για $a,b \in \mathbb{Z}$
το $U(\mathbb{Z}_n)$ είναι αβελιανή ομάδα.
Απόδειξη:
Πράξη καλά ορισμένη, προσεταιριστική, ουδέτερο το $[1]_n$ από Θ. Αριθμών

Παρατήρηση: Καλά ορισμένη πράξη σημαίνει εδώ δύο πράγματα
1) Αν $[a]_n=[a']_n$, $[b]_n=[b']_n$ τότε $[a \cdot b]_n=[a' b']_n$
2) Αν $\text{ΜΚΔ}(a,n)=1$ και $\text{ΜΚΔ}(b,n)=1$, τότε και $\text{ΜΚΔ}(a \cdot b,n)=1$

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

Από Θ. Αριθμών ΜΚΔ$(a,n)=1 \Rightarrow$ υπάρχουν $z_1, z_2 \in \mathbb{Z}$ με $1 = z_1 a + z_2 n$ και το αντίστροφο στο $U(\mathbb{Z}_n)$ του $[a]_n$ είναι το $[z_1]_n$

Πόσα στοιχεία του $U(\mathbb{Z}_n)$;

Απάντηση: $\varphi(n)$ όπου φ η συνάρτηση του Euler

Υπενθύμιση: Αν $n \geq 2$ και $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ όπου p_i πρώτοι $p_i \neq p_j$ για $i \neq j$ και $a_i > 0$ της $\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$

ΥΠΟΟΜΑΔΕΣ

Ορισμός: Έστω $(G,*)$ ομάδα και H υποσύνολο του G. Το H λέγεται υποομάδα αν είναι κλειστό ως προς την πράξη, το ουδέτερο στοιχείο $e_G \in H$ και αν $a \in H$, τότε και το αντίστροφο του στην G a^{-1} είναι στοιχείο του H.

Παράδειγμα 1: Είναι το $S = \{k \in \mathbb{Z}, k \geq 0\}$ υποομάδα του $(\mathbb{Z},+)$;

Απάντηση: Το S είναι κλειστό ως προς την πρόσθεση. Το ουδέτερο του $(\mathbb{Z},+)$ είναι το 0 και $0 \in S$. Αλλά το S δεν λέγεται υποομάδα του $(\mathbb{Z},+)$ γιατί $1 \in S$, το αντίστροφο του στο $(\mathbb{Z},+)$ είναι το -1 και $-1 \notin S$.

Παράδειγμα 2: Έστω $G = (\mathbb{R} \setminus \{0\}$, πολλαπλασιασμό$)$ και $S_1 = \{1,-1\}$, $S_2 = \{a \in \mathbb{R} \mid a > 0\}$. Είναι τα S_1, S_2 υποομάδες του G;

Απάντηση: Το S_1 είναι υποομάδα, γιατί $1 \cdot 1 = 1$, $1(-1) = -1$ άρα είναι κλειστό. Επίσης το ουδέτερο της G είναι το 1 και $1 \in S_1$.

Επιπλέον, το αντίστροφο στην G του 1 είναι το 1 και $1 \in S_1$.
Το αντίστροφο στην G του -1 είναι το -1 και $-1 \in S_1$.

Επίσης το S_2 είναι υποομάδα της G γιατί $1 \in S_2$.
Το γινόμενο δύο θετικών πραγματικών αριθμών είναι θετικός και αν $\alpha \in \mathbb{R}$ θετικός τότε και το α^{-1} θετικός.

Παράδειγμα: Έστω $G = (\mathbb{R}, +)$ και $S = \mathbb{Q}$. Το S είναι υποομάδα της G, γιατί το $0 \in \mathbb{Q}$, το άθροισμα δύο ρητών είναι ρητός και αν $\alpha \in \mathbb{Q}$ τότε και $-\alpha \in \mathbb{Q}$.

Παράδειγμα: Έστω $G = (GL_2(\mathbb{R}), \cdot)$ και $S_1 = \{A \in G \mid \det A = 1\}$, $S_2 = \{A \in G \mid \det A \in \mathbb{Q} \setminus \{0\}\}$, $S_3 = \{A \in G \mid \det A \geq 1\}$
Είναι τα S_1, S_2, S_3 υποομάδες της G;

Λύση

Για το S_1: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S_1$, γιατί $\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1$.

Έστω $A, B \in S_1$. Τότε $\det A = \det B = 1$, συνεπώς
$\det(A \cdot B) = \det A \cdot \det B = 1 \cdot 1 = 1$ άρα $AB \in S_1$
Έχουμε $A \cdot A^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow \det(A \cdot A^{-1}) = \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1$

$$\Rightarrow \det A \cdot \det A^{-1} = 1 \Rightarrow \det A^{-1} = \frac{1}{\det A}$$

άρα αν $\det A = 1$ τότε και $\det A^{-1} = \frac{1}{1} = 1$
Συνεπώς S_1 υποομάδα της G.

Για το S_2: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S_2$ γιατί $1 \in \mathbb{Q}$.

Αν $\det(A) \in \mathbb{Q} \setminus \{0\}$, $\det B \in \mathbb{Q} \setminus \{0\}$, τότε
$\det(A \cdot B) = \det A \cdot \det B \in \mathbb{Q} \setminus \{0\}$

Επιπλέον, αν $\det(A) \in \mathbb{Q} \setminus \{0\}$, αφού $\det(A^{-1}) = \dfrac{1}{\det(A)} \in \mathbb{Q} \setminus \{0\}$.

Συνεπώς S_2 είναι υποομάδα της G.

Για το S_3: $\det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1 \geq 1$ άρα $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S_3$

Αν $A, B \in S_3$ τότε $\det A \geq 1$, $\det B \geq 1$
Συνεπώς $\det(A \cdot B) = \det A \cdot \det B \geq 1$ άρα $A \cdot B \in S_3$
Αλλά για $A = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ έχουμε $A \in S_3$, γιατί $\det A = 2$.

αλλά $\det A^{-1} = \dfrac{1}{\det A} = \dfrac{1}{2} < 1$.

Συνεπώς $A^{-1} \notin S_3$ άρα S_3 <u>όχι</u> υποομάδα του G.

$S_4 = \left\{ A \in GL_2(\mathbb{R}) : A^t A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}$

<u>Ισχυρισμός</u>: Το S_4 είναι υποομάδα της G η υποομάδα των ορθογωνίων πινάκων.

<u>Απόδειξη ισχυρισμού</u>:
Το S_4 είναι υποσύνολο της G, γιατί $A^t \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\Rightarrow \det(A^t A) = 1 \Rightarrow \det(A^t)\det(A) = 1 \Rightarrow \det(A) \neq 0 \Rightarrow A \in G$.

Φανερά $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}^t \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

άρα $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in S_4$.

Έστω $A, B \in S_4$. Τότε $(A \cdot B)^t A B = B^t \cdot A^t \cdot A B = B^t \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} B$

$= B^t \cdot B \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Συνεπώς $A \cdot B \in S_4$

Έστω $A \in S_4$. Τότε $A^t A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Άρα $A^{-1} = (A^t)$. Συνεπώς αρκεί να δείξουμε ότι $(A^{-1})^t A^{-1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

δηλαδή ότι $(A^t)^t A^t = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. δηλαδή ότι $A A^t = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Αυτό ισχύει γιατί $A^{-1} = A^t \Rightarrow A^t \cdot A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

και $A \cdot A^t = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$