09/03/2020

Ερώτηση: Έστω $(G,*)$ ομάδα και H υποσύνολο G, ώστε $e_G \in H$ και αν $a,b \in H$ τότε $a*b \in H$. Είναι η H υποομάδα της G;

Απάντηση: ΟΧΙ. Αν $G=(\mathbb{Z},+)$ και $H=\{k \in \mathbb{Z},\ k \geq 0\}$ τότε $e_G = 0 \in H$, $a,b \in H \Rightarrow a+b \in H$. Αλλά H όχι υποομάδα, γιατί το $-1 \notin H$, ενώ $1 \in H$.

Υπενθύμιση: Έστω $X \neq \emptyset$ πεπερασμένο σύνολο και $f: X \to X$, 1-1 συνάρτηση. Τότε f επί

Πρόταση: Έστω $(G,*)$ ομάδα και H υποσύνολο της G πεπερασμένο, ώστε $e_G \in H$ και αν $a,b \in H$ τότε $a*b$ ανήκει στο H. Τότε H υποομάδα της G.

Απόδειξη: Έστω $a \in H$ και $a^{-1} \in G$, ο αντίστροφος. Θα δείξουμε ότι $a^{-1} \in H$. Ορίζουμε $f: H \to H$ με $f(b) = a*b \in H$. Από κανόνα διαγραφής στην G η f είναι 1-1. Αφού H πεπερασμένο σύνολο, έχουμε f επί. Αφού $e_G \in H$, υπάρχει $b \in H$ με $f(b) = e_G \Rightarrow a*b = e_G \Rightarrow$
$\Rightarrow a^{-1}*(a*b) = a^{-1}*e_G \Rightarrow (a^{-1}*a)*b = a^{-1} \Rightarrow e_G*b = a^{-1}$
$\Rightarrow a^{-1} = b \in H$.

ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ ΟΜΑΔΑΣ

Ερώτημα: Έστω $(G,*)$ ομάδα, $a \in G$. Θεωρούμε τις θετικές δυνάμεις του a στην G $a, a^2, a^3, \dots, a^4$.
Θα φθάσουμε κάποτε στο e_G ή όχι, δηλαδή υπάρχει $k>0$ με $a^k = e_G$;

Απάντηση: Μπορεί ναι. Παράδειγμα: $2([1]_2) = [0]_2 = e_G$ για $G = (\mathbb{Z}_2, +)$.
Μπορεί όχι. Παράδειγμα: $1 \in \mathbb{Z}$, τότε $k \cdot 1 \neq 0$ για κάθε $k \in \mathbb{Z}$ με $k>0$.
Ενώ για το $0 \in \mathbb{Z}$, ισχύει $1 \cdot 0 = 0 \in G$.

Ορισμός: Έστω $(G,*)$ ομάδα και $a \in G$. Αν υπάρχει $k \in \mathbb{Z}$ με $k>0$ ώστε $a^k = e_G$, λέμε ότι το a έχει πεπερασμένη τάξη σαν στοιχείο της G. Ορίζουμε $ord(a)$ (τάξη του a), τον ελάχιστο θετικό ακέραιο k_0 με $a^{k_0} = e_G$.
Αν $a^k \neq e_G$ για κάθε $k \in \mathbb{Z}$ με $k>0$ λέμε ότι ο a έχει άπειρη τάξη και γράφουμε $ord(a) = +\infty$

Παράδειγμα: Αν $(G,*)$ ομάδα, τότε $ord(e_G)=1$

Παράδειγμα: Αν $G=(\mathbb{Z},+)$ και $a \in \mathbb{Z} \setminus \{0\}$ τότε $\underbrace{a+\dots+a}_{k\text{-φορές}} \neq 0$ για κάθε $k>0$, άρα $ord(a)=+\infty$

Παράδειγμα: $G=(\mathbb{R}\setminus\{0\},\cdot)$ και $a \in G$. Αν $a=-1$, τότε $ord(a)=2$

Ισχυρισμός: Αν $a \in G \setminus \{1,-1\}$ τότε $ord(a) = +\infty$

Απόδειξη: Αφού $a \in \mathbb{R}\setminus\{0,1,-1\}$, έχουμε $|a|>1$
$0<|a|<1$

$-1 \quad 0 \quad 1$

Έστω ότι υπάρχει $k>0$ με $a^k=1$.
Άρα $|a^k|=1 \Rightarrow |a|^k = 1 \underset{a\in\mathbb{R}}{\Rightarrow} |a|=1$, αντίφαση.

Ερώτημα: $G=(\mathbb{C}\setminus\{0\},\cdot)$. Ποια είναι η τάξη του i;

Απάντηση: 4, γιατί $i^1=i$, $i^2=-1$, $i^3=-1$, $i^4=1$

Παράδειγμα: $G=GL_2(\mathbb{R})$ = αντίστροφοι 2×2 πίνακες

$$A=\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \quad B=\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Υπολογίστε $ord_G(A)$, $ord_G(B)$.

Για τον A

$$A^2 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

$$A^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ -1 & 0 \end{bmatrix}$$

$$A^4 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e_G$$

Συνεπώς $ord_G(A) = 4$

$$B^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$B^3 = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ και για $k \in \mathbb{Z}$ έχουμε δει ότι

$B^k = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix}$. Άρα αν $k \in \mathbb{Z}$ με $k \neq 0$.

Τότε $B^k \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e_G$. Άρα $ord_G(B) = +\infty$

<u>Πρόταση</u>: Έστω $(G, *)$ ομάδα και $a \in G$ στοιχείο με πεπερασμένη τάξη d. Τότε:

i) $\# \langle a \rangle = d$ και $\langle a \rangle = \{a, a^2, \dots, a^d\}$

↑ ΚΥΚΛΙΚΗ ΥΠΟΟΜΑΔΑ ΠΟΥ ΠΑΡΑΓΕΙ ΤΟ a.

ii) Έστω $k \in \mathbb{Z}$ και r το υπόλοιπο της Ευκλ. Διαίρεσης του k με το d. Τότε $a^k = a^r$

iii) Για $k \in \mathbb{Z}$, $a^k = e_G$ αν και μόνο αν $d \mid k$

iv) $a^{-1} = a^{d-1}$

v) Για $k_1, k_2 \in \mathbb{Z}$, $a^{k_1} = a^{k_2}$ αν και μόνο αν $d \mid k_2 - k_1$

Απόδειξη: ii) Υπάρχει $q \in \mathbb{Z}$ με $k = qd + r$

Συνεπώς $a^k = a^{qd+r} = a^{qd} \cdot a^r = (a^d)^q \cdot a^r = (e_G)^q \cdot a^r = a^r$

iii) Έστω $k \in \mathbb{Z}$ με $a^k = e_G$ και r με $0 \leq r \leq d-1$ το υπόλοιπο της Ευκλ. Διαίρεσης του k με το d. Από ii) $a^r = a^k = e_G$. Αν $r \neq 0$, αντίφαση στο ότι $ord_G(a) = d$.

Άρα $r = 0 \Rightarrow d \mid k$.

v) Έστω $a^{k_1} = a^{k_2} \Rightarrow a^{-k_1} * a^{k_1} = a^{-k_1} * a^{k_2}$

$$\Rightarrow (a^{k_1})^{-1} * a^{k_1} = a^{k_2 - k_1} \Rightarrow a^{k_2 - k_1} = e_G$$

$$\overset{iii)}{\Rightarrow} d \mid k_2 - k_1$$

iv) $a^d = e_G \Rightarrow a * a^{d-1} = e_G$ και $a^{d-1} * a = e_G$

άρα $(a^{-1}) = a^{d-1}$

i) Έστω $0 \leq r_1 < r_2 \leq d-1$. Τότε από v) $a^{r_1} \neq a^{r_2}$

Συνεπώς τα στοιχεία $a, a^2, a^3, \dots, a^d$ είναι διαφορετικά ανά δύο και από ii) $\langle a \rangle = \{a, a^2, a^3, \dots, a^d\}$

<u>Παράδειγμα:</u> $G = (\mathbb{C}^* \setminus \{0\}, \cdot)$, $a = i$

Υπολογίστε την $\langle a \rangle$, το a^{-213} και το a^{-1}.

<u>Λύση:</u> Είδαμε $ord_G(a) = 4$. Συνεπώς από την Πρόταση $\# \langle a \rangle = 4$

και $\langle a \rangle = \{a = i, a^2 = -1, a^3 = -i, a^4 = 1\}$

Υπολογίζουμε το υπόλοιπο Ευκλ. Διαίρεσης του -213 με το 4

Έχουμε $213 = 53 \cdot 4 + 1$

$\Rightarrow -213 = (-53) \cdot 4 - 1 = (-54) \cdot 4 + 3$

$$\begin{array}{r|l} 213 & 4 \\ \hline 13 & 53 \\ 1 & \end{array}$$

Συνεπώς $a^{-213} = a^3 = -i$. Επίσης $a^{-1} = a^{4-1} = a^3 = -i$.

Παρατηρούμε ότι ο πίνακας δυνάμεων του i είναι:

k	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
i^k		i	-1	$-i$	1	i	-1	i	1	i	-1	$-i$	1	i

Αυτό εξηγεί το όριο $\langle a \rangle$ η "κυκλική" υποομάδα που παράγεται από το a.

Πρόταση: Έστω $(G,*)$ ομάδα και $a \in G$ με $ord_G(a) = +\infty$
Τότε:
i) Για $k_1, k_2 \in \mathbb{Z}$ $a^{k_1} = a^{k_2}$ αν και μόνο αν $k_1 = k_2$
ii) $\# \langle a \rangle = \infty$

Απόδειξη:
i) Έστω $k_1, k_2 \in \mathbb{Z}$ με $a^{k_1} = a^{k_2}$.
Υποθέτουμε $k_1 \leq k_2$. Τότε $a^{k_1} = a^{k_2} \Rightarrow a^{-k_1} * a^{k_1} = a^{-k_1} * a^{k_2}$
$\Rightarrow e_G = a^{k_2 - k_1} \underset{ord(a)=\infty}{\Longrightarrow} k_1 = k_2$

Αν $k_1 > k_2$ παρόμοιο επιχείρημα δουλεύει.
ii) Άμεσο από το i)

~~Παρατήρηση~~ Πόρισμα: Έστω G πεπερ. ομάδα και $a \in G$. Τότε η $ord_G(a)$ είναι πεπερασμένη.
Απόδειξη: Αν όχι, δηλαδή $ord(a) = +\infty$ έπεται $\# \langle a \rangle = +\infty$ αντίφαση γιατί $\langle a \rangle$ υποσύνολο της G και G πεπερασμένη ομάδα.

Ερώτημα: Έστω $(G, *)$ ομάδα $k \in \mathbb{Z}$, $a \in G$ με τάξη $ord_G(a) = d \in \mathbb{Z}$. Ποιά είναι η τάξη του a^k;

Πρόταση: Έστω $(G, *)$ ομάδα και $a \in G$ με $ord_G(a) = d \in \mathbb{Z}$. Έστω $k \in \mathbb{Z}$. Τότε $ord(a^k) = \dfrac{d}{\text{ΜΚΔ}(d,k)}$

Απόδειξη: Θέτουμε $s = \dfrac{d}{\text{ΜΚΔ}(d,k)}$

Τότε $s \in \mathbb{Z}$ με $s \geq 1$. Θα δείξουμε $s = ord_G(a^k)$

Ισχυρισμός 1: $(a^k)^s = e_G$

Απόδειξη: $(a^k)^s = a^{ks} = a^{k \cdot \frac{d}{\text{ΜΚΔ}(k,d)}} = a^{d \cdot \left(\frac{k}{\text{ΜΚΔ}(k,d)}\right)} = (a^d)^{\frac{k}{\text{ΜΚΔ}(k,d)}} =$

$= (e_G)^{\frac{k}{\text{ΜΚΔ}(k,d)}} = e_G$

Ισχυρισμός 2: Έστω $l \in \mathbb{Z}$ με $l \geq 1$ και $(a^k)^l = e_G$. Τότε $s \leq l$

Απόδειξη: $(a^k)^l = e_G \Rightarrow a^{k \cdot l} = e_G \Rightarrow d \mid k \cdot l$

$\Rightarrow \dfrac{d}{\text{ΜΚΔ}(d,k)} \Big| \dfrac{k}{\text{ΜΚΔ}(d,k)} l \Rightarrow s \Big| \dfrac{k}{\text{ΜΚΔ}(d,k)} \cdot l$

(Από Θ. Αριθμών $d = \text{ΜΚΔ}(a,b) \Rightarrow \text{ΜΚΔ}\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$)

Άρα ~~από~~ $\text{ΜΚΔ}\left(s, \dfrac{k}{\text{ΜΚΔ}(d,k)}\right) = 1$

Συνεπώς $s \Big| \dfrac{k}{\text{ΜΚΔ}(d,k)} \cdot l \Rightarrow s \mid l \Rightarrow s \leq l$

Παράδειγμα:
Έστω $ord(a) = d$

1) Αν $d=3$, $ord(a^2) = \frac{3}{ΜΚΔ(2,3)} = \frac{3}{1} = 3$

2) Έστω $d=4$, $ord(a^2) = \frac{d}{ΜΚΔ(2,d)} = \frac{4}{ΜΚΔ(2,4)} = \frac{4}{2} = 2$

$ord(a^3) = \frac{d}{ΜΚΔ(3,d)} = \frac{4}{ΜΚΔ(3,4)} = \frac{4}{1} = 4$

$d=5$, Έστω k με $1 \leq k \leq 4$. Αφού 5 πρώτος,
$ΜΚΔ(d,k) = ΜΚΔ(5,k) = 1$
Άρα $ord(a^k) = 5$. Συνεπώς $ord(a) = ord(a^2) = ord(a^3) = ord(a^4) = 5$

$d=6$, $ord(a^2) = \frac{6}{ΜΚΔ(2,6)} = \frac{6}{2} = 3$

$ord(a^3) = \frac{6}{ΜΚΔ(3,6)} = 2$

$ord(a^4) = \frac{6}{ΜΚΔ(4,6)} = 3$ $\quad ord(a^5) = \frac{6}{ΜΚΔ(5,6)} = 6$

Παρατήρηση: Έστω $n \geq 2$ και $G = (\mathbb{Z}_n, +)$
↑ ΑΚΕΡΑΙΟΙ MODULO n

Φανερά $ord_G([1]_n) = n$
Έστω $k \in \mathbb{Z}$. Τότε $[k]_n = k[1]_n$
Συνεπώς από την Πρόταση: $ord_{(\mathbb{Z}_n, +)}([k]_n) = \frac{n}{ΜΚΔ(n,k)}$

(ΓΝΩΣΤΟ ΑΠΟ Θ. ΑΡΙΘΜΩΝ)

Πρόταση: Έστω $(G, *)$ ομάδα και $a \in G$. Τότε $ord_G(a^{-1}) = ord_G(a)$

Απόδειξη:

Ισχυρισμός 1: Έστω $k \in \mathbb{Z}$ με $k \geq 1$ και $a^k = e_G$
Τότε $(a^{-1})^k = e_G$
Απόδειξη: $(a^{-1})^k = a^{-1k} = a^{-k} = a^{k(-1)} = (a^k)^{-1} = e_G^{-1} = e_G$
(Ιδιότητες δυνάμεων $(a^{m_1})^{m_2} = a^{m_1 m_2}$ για κάθε $m_1, m_2 \in \mathbb{Z}$).

Ισχυρισμός 2: Έστω $k \in \mathbb{Z}$ με $k \geq 1$ και $(a^{-1})^k = e_G$. Τότε $a^k = e_G$.
Απόδειξη: $a^k = a^{(-k)(-1)} = (a^{-k})^{-1} = ((a^{-1})^{k})^{-1} = e_G^{-1} = e_G$

Προσοχή: Σε μια αβελιανή ομάδα μπορεί $a, b \in G$, $ord_G(a) < \infty$, $ord_G(b) < \infty$ και $ord_G(a*b) = +\infty$. Δηλαδή μπορεί το γινόμενο δύο στοιχείων πεπερασμένης τάξης να έχει άπειρη τάξη.

Πρόταση: Έστω G αβελιανή ομάδα και $a, b \in G$ με $ord(a) = d_1 \in \mathbb{Z}$, $ord(b) = d_2 \in \mathbb{Z}$. Τότε το $a*b$ έχει πεπερασμένη τάξη και η τάξη του $a*b \mid d_1 d_2$

Απόδειξη: $(a*b)^{d_1 d_2} = \underbrace{(a*b)*(a*b)*(a*b)*\dots*(a*b)}_{d_1 d_2 \text{ φορές}} =$
$= a^{d_1 d_2} b^{d_1 d_2} = (a^{d_1})^{d_2} \cdot (b^{d_2})^{d_1} =$
$= (e_G)^{d_2} (e_G)^{d_1} = e_G$