21/3/2019

Τάξη $a \in G$ $\quad ord(a) = \#\langle a \rangle$

$= \{a^k : k \in \mathbb{Z}\}$

Π.χ. $ord(e) = 1$, γιατί $\langle e \rangle = \{e\}$

$G = (\mathbb{R}, \cdot)$ $\quad ord(-1) = 2$ $\quad$ γιατί $\langle -1 \rangle = \{1, -1\}$

$G = (\mathbb{Z}, +)$ $\quad ord(a) = +\infty$ για κάθε $a \neq 0$ γιατί $\langle a \rangle = a\mathbb{Z}$

$= \{ka : k \in \mathbb{Z}\}$

ΣΗΜΑΝΤΙΚΟ ΕΡΩΤΗΜΑ : Είναι $ord(a) = +\infty$ ή $ord(a) \in \{1, 2, 3, \dots\}$;

ΠΡΟΤΑΣΗ: Έστω G ομάδα και $a \in G$ Τ.Α.Ε.Ι

(i) $ord(a) < \infty$ (δηλ. $ord(a) \neq +\infty$)
(ii) Υπάρχουν $k_1, k_2 \in \mathbb{Z}$ με $k_1 \neq k_2$ ώστε $a^{k_1} = a^{k_2}$

ΑΠΟΔΕΙΞΗ

(i) $\Rightarrow$ (ii) Υποθέτουμε $ord(a) < \infty$ και αν $k_1, k_2 \in \mathbb{Z}$ με $k_1 \neq k_2$ έχουμε $a^{k_1} \neq a^{k_2}$. Θα βρούμε αντίφαση. Ορίζουμε $\Phi: \mathbb{Z} \longrightarrow \langle a \rangle$, $\Phi(k) = a^k$
Αφού $k_1 \neq k_2 \Rightarrow a^{k_1} \neq a^{k_2}$ η Φ είναι 1-1. Φανερά Φ επί. Άρα τα σύνολα $\mathbb{Z}$ και $\langle a \rangle$ έχουν το ίδιο πλήθος στοιχεία. Άρα $\langle a \rangle$ άπειρο σύνολο, αντίφαση.

(ii) $\Rightarrow$ (i) Υποθέτουμε ότι υπάρχουν $k_1, k_2 \in \mathbb{Z}$ με $k_1 \neq k_2$ και $a^{k_1} = a^{k_2}$. Αφού $k_1 \neq k_2$ θα έχουμε $k_1 < k_2$ ή $k_2 < k_1$. Ενδεχομένως, με εναλλαγή των k_1, k_2 υποθέτουμε $k_1 < k_2$. Θέτουμε $m = k_2 - k_1$.

ΙΣΧΥΡΙΣΜΟΣ: Α $l \in \mathbb{Z}$ το a^l είναι κάποιο από τα $a, a^2, \dots, a^m$ (αυτά δεν είναι απαραίτητα διαφορετικά ανά δύο)

ΑΠΟΔΕΙΞΗ

ΙΣΧΥΡΙΣΜΟΣ: $a^{k_1} = a^{k_2} \Rightarrow a^{k_1} \cdot a^{-k_1} = a^{k_2} \cdot a^{-k_2}$

$\Rightarrow a^0 = a^m \Rightarrow a^m = e$

Αφού $m \in \mathbb{Z}$ με $m \neq 0$ κάνουμε Ευκλείδεια διαίρεση του l με το m.

Επομένως, υπάρχουν $q, r \in \mathbb{Z}$ με $0 \leq r < m$ ώστε $l = q \cdot m + r$
Τότε $a^l = a^{qm+r} = a^{mq+r} = a^{mq} \cdot a^r = (a^m)^q \cdot a^r \overset{(*)}{=}$
$e^q \cdot a^r = a^r$ και το αποτέλεσμα έπεται, διότι

$a^0 = e = a^m$

ΠΟΡΙΣΜΑ: Έστω G ομάδα $a \in G$ Τ.Α.Ε.Ι.

1) $\text{ord}(a) = +\infty$
2) Για κάθε $m \in \mathbb{Z}$ με $m > 0$, $a^m \neq e$
3) Αν $k_1, k_2 \in \mathbb{Z}$ και $k_1 \neq k_2$ τότε $a^{k_1} \neq a^{k_2}$

Με άλλα λόγια το $a \in G$ έχει άπειρη τάξη αν και μόνο αν διαφορετικές δυνάμεις του είναι διαφορετικά στοιχεία της G, αν και μόνο αν καμία δύναμη a^m με $m \in \mathbb{Z}$ και $m > 0$ δεν είναι το ταυτοτικό στοιχείο της G.

ΠΑΡΑΔΕΙΓΜΑ Δείξτε ότι στο $(\mathbb{R} \setminus \{0\}, \cdot)$ το στοιχείο $\frac{1}{2}$ έχει $\text{ord}\left(\frac{1}{2}\right) = +\infty$

ΑΠΟΔΕΙΞΗ Έστω $m > 0$ ακέραιος. Φανερά $\left(\frac{1}{2}\right)^m = \frac{1}{2^m} \leq \frac{1}{2} < 1$. Άρα $\left(\frac{1}{2}\right)^m \neq 1$. Άρα από ΠΟΡΙΣΜΑ

$\text{ord}\left(\frac{1}{2}\right) = +\infty$

Δείξτε ότι στο $(\mathbb{R} \setminus \{0\}, \cdot)$ το στοιχείο -1 έχει $\text{ord}(-1) < \infty$

ΑΠΟΔΕΙΞΗ Για $m = 2$ $(-1)^m = (-1)^2 = 1$. Άρα από Πόρισμα $\text{ord}(-1) < \infty$

ΠΑΡΑΔΕΙΓΜΑ Έστω $z = a + bi \in \mathbb{C}$ με $a, b \in \mathbb{R}$ και $|z| > 1$ ή $0 < |z| < 1$

Δείξτε ότι το z σαν στοιχείο της ομάδας $(\mathbb{C} \setminus \{0\}, \cdot)$ έχει άπειρη τάξη. (Υπενθ. $|z| = \sqrt{a^2 + b^2}$)

ΑΠΟΔΕΙΞΗ Αφού $|z| > 1$ ή $0 < |z| < 1$ έχουμε $z \neq 0$. Άρα $z \in \mathbb{C} \setminus \{0\}$. Από Πόρισμα, αρκεί να δείξουμε ότι αν $m \in \mathbb{Z}$ με $m > 0$ τότε

$z^m \neq 1$

ΠΕΡΙΠΤΩΣΗ 1 $|z| > 1$. Τότε $|z^m| = \underbrace{|z| \cdot |z| \cdot \ldots |z|}_{m\text{-φορές}} > |z| > 1 = |1|$

Άρα $z^m \neq 1$.

ΠΕΡΙΠΤΩΣΗ 2. $0 < |z| < 1$. Τότε $|z^m| = \underbrace{|z| \cdot |z| \cdot \ldots |z|}_{m\text{-φορές}} < 1 = |1|$

Άρα $z^m \neq 1$.

ΠΑΡΑΔΕΙΓΜΑ Θεωρούμε τον πίνακα

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in (GL_2(\mathbb{R}), \cdot)$$

Έχουμε $A \neq I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$$A^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2$$. Άρα $ord(A) < \infty$.

ΠΡΟΤΑΣΗ Έστω G ομάδα και $a \in G$. Αν G πεπερασμένο σύνολο τότε $ord(a) < \infty$

ΑΠΟΔΕΙΞΗ Έχουμε $\langle a \rangle \subseteq G$ Αφού G πεπερασμένο σύνολο. Έχουμε $\langle a \rangle$ πεπερασμένο σύνολο. Άρα $ord(a) < \infty$

ΠΑΡΑΔΕΙΓΜΑ Στα ακόλουθα G πεπερασμένο σύνολο, άρα κάθε $a \in G$ έχει πεπερασμένη τάξη.

$G = (\mathbb{Z}_n, +)$ όπου $n \geq 2$ $G = S_n$ όπου $n \geq 2$

$G = (U(\mathbb{Z}_n), \cdot)$ όπου $n \geq 2$ ↑ Δείξαμε $|S_n| = n! = 1 \cdot 2 \cdot 3 \cdots n$

ΠΡΟΤΑΣΗ Έστω G ομάδα και $a \in G$ με $ord(a) < \infty$ Από πόρισμα υπάρχει θετικός ακέραιος m με $a^m = e$. Έστω m_0 ο ελάχιστος τέτοιος θετικός ακέραιος. Τότε:

1) $\langle a \rangle = \{a, a^2, \ldots, a^{m_0}\}$ και τα στοιχεία $a, a^2, \ldots, a^{m_0}$

Είναι διαφορετικά από δύο

2) $ord(a) = m_0$

3) Αν $k_1, k_2 \in \mathbb{Z}$ τότε $a^{k_1} = a^{k_2}$ αν και μόνο αν $ord(a) \mid k_1 - k_2$, δηλ. αν και μόνο αν $k_1 \equiv k_2 \bmod m_0$

4) Αν $k \in \mathbb{Z}$, $a^k = e$ αν και μόνο αν $ord(a) \mid k$.

ΑΠΟΔΕΙΞΗ

1) Έστω $l \in \mathbb{Z}$. Υπάρχουν $q, r \in \mathbb{Z}$ με $0 \le r \le m_0$ ώστε $l = qm_0 + r$, όπως προηγουμένως

$a^l = a^{qm_0+r} = a^{qm_0} \cdot a^r = (a^{m_0})^q \cdot a^r = e^q \cdot a^r = a^r$, και αφού $a^0 = a^{m_0} = e$, έχουμε $\langle a \rangle = \{a, a^2, \dots, a^{m_0}\}$

Έστω $1 \le k_1 \le k_2 \le m_0$. Θ.Δ.Ο. $a^{k_1} \neq a^{k_2}$. Πράγματι αν $a^{k_1} = a^{k_2} \Rightarrow a^{k_1} \cdot a^{-k_1} = a^{k_2} \cdot a^{-k_1} \Rightarrow a^{(k_2 - k_1)} = e$

Αλλά $0 < k_2 - k_1 < m_0$ αντίφαση στον ορισμό του m_0

2) Άμεσο από το 1) και τον ορισμό του $ord(a)$

ΑΠΟΔΕΙΞΗ 3) Έστω $m_0 \mid k_1 - k_2 \Rightarrow$ υπάρχει $q \in \mathbb{Z}$ με $k_1 - k_2 = qm_0 \Rightarrow k_1 = qm_0 + k_2 \Rightarrow a^{k_1} = a^{qm_0 + k_2} =$

$(a^{m_0})^q * a^{k_2} = e * a^{k_2} = a^{k_2}$

Αντίστροφα, υποθέτουμε $a^{k_1} = a^{k_2}$. Τότε υπάρχουν $q \in \mathbb{Z}$ και $r \in \mathbb{Z}$ με $0 \le r < m_0$ ώστε $k_2 - k_1 = qm_0 + r \Rightarrow k_2 = k_1 + qm_0 + r$

$\Rightarrow a^{k_2} = a^{k_1 + qm_0 + r} = a^{k_1} * a^{qm_0} * a^r =$

$a^{k_1} * (a^{m_0})^q * a^r \Rightarrow a^{k_2} = a^{k_1} * a^r$

Άρα από υπόθεση $a^{k_1} = a^{k_2} \Rightarrow a^r = e$

Αν $r \neq 0$ έχουμε αντίφαση στον ορισμό του m_0.

Άρα $r = 0 \Rightarrow m_0 \mid k_1 - k_2$.

ΠΑΡΑΔΕΙΓΜΑ Έστω $ord(a) = 2$ Τότε $a^2 = e$ και $\langle a \rangle = \{a, a^2 = e\}$

Ποιο στοιχείο είναι το a^{2018};

ΑΠΑΝΤΗΣΗ $2013 = 1009 \cdot ord(a) + r$, με $r = 0$

Άρα $a^{2013} = a^r = a^0 = e = a^2$

ΠΑΡΑΔΕΙΓΜΑ Έστω $ord(a) = 3$ Τότε $a^3 = e$ και

$\langle a \rangle = \{a, a^2, a^3 = e\}$

Ποιο στοιχείο είναι το a^{2013};

Έχουμε $2018 = 672 \cdot ord(a) + 2$.

Άρα $ord(a) \mid 2013 - 2$

Συνεπώς $a^{2013} = a^2$ από την Πρόταση.

Πιο γενικά αν $ord(a) = m_0$, τότε $a^{m_0} = e$

$\langle a \rangle = \{a, a^2, \dots, a^{m_0} = e\}$ και όλα υπολογίσιμα

Το a^{2013} κάναμε Ευκλείδια Διαίρεση του 2013 με το m_0, δηλαδή υπολογίζαμε q, r με

$2013 = q m_0 + r$ και $0 \le r < m_0$

Τότε από την πρόταση $a^{2013} = a^r$

ΠΑΡΑΔΕΙΓΜΑ Έστω $G = (S_5, \circ)$ όπου $S_5 = \{\sigma : \{1, \dots, 5\} \to \{1, \dots, 5\}$ με σ 1-1 και επί$\}$

και $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ Υπολογίστε

$ord(\sigma)$, $\langle \sigma \rangle$ και το σ^{2013}

ΛΥΣΗ: Το σ είναι εξ' ορισμού η απεικόνιση $\sigma(1) = 3$, $\sigma(2) = 2$ $\sigma(3) = 5$ $\sigma(4) = 4$ $\sigma(5) = 1$

Έστω $e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ το ταυτοτικό της

ομάδας S_5 $\sigma \neq e$

$$\sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} \neq e$$

$$\sigma \circ \sigma \circ \sigma = \sigma \circ (\sigma \circ \sigma) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = e$$

Συνεπώς από την πρόταση $ord(\sigma) = 3$

$$\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3 = e\}$$

Όπως προηγουμένως $2018 \equiv 2 \bmod 3$ Άρα $\sigma^{2018} = \sigma^2$