14/3/2019

ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ

ΥΠΕΝΘΥΜΙΣΗ: Η ομάδα $(G,*)$ λέγεται κυκλική αν υπάρχει $a \in G$ με $G = \langle a \rangle$.

Με άλλα λόγια, αν υπάρχει $a \in G$ ώστε αν $b \in G$ τότε υπάρχει $k \in \mathbb{Z}$ με $b = a^k$.

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

Ισοδύναμα αν για κάθε $b \in G$ με $b \neq e$ υπάρχει $k \in \mathbb{Z}$ με $k > 0$ ώστε $b = \underbrace{a * a * \ldots * a}_{k\text{-φορές}}$ ή $b = \underbrace{a^{-1} * a^{-1} * \ldots * a^{-1}}_{k\text{-φορές}}$

ΠΑΡΑΔΕΙΓΜΑ 1 $(\mathbb{Z},+)$ είναι κυκλική με γεννήτορα $a=1$ γιατί αν $b\in\mathbb{Z}$ με $b\neq 0$, έχουμε

ΠΕΡΙΠΤΩΣΗ 1 $b>0$, άρα $b=\underbrace{1+1+1+\dots+1}_{b\text{-φορές}}$

ΠΕΡΙΠΤΩΣΗ 2 $b<0$, άρα $b=\underbrace{(-1)+(-1)+\dots+(-1)}_{|b|\text{-φορές}}$

Υπάρχει άλλος γεννήτορας $a\in\mathbb{Z}$ με $a'\neq a=1$

Ναι, το -1 είναι επίσης γεννήτορας του $(\mathbb{Z},+)$.

ΠΑΡΑΔΕΙΓΜΑ 2 Έστω $G=\{e\}$ η ομάδα με ένα στοιχείο. Είναι η G κυκλική;

Ναι, με γεννήτορα το e.

ΠΑΡΑΔΕΙΓΜΑ 3 Έστω $n\geq 2$ ακέραιος και η

$G=(\mathbb{Z}_n,+)$. Είναι η G κυκλική;

Έχουμε $\mathbb{Z}_n=\{[0]_n,[1]_n,\dots,[n-1]_n\}$

Φανερά η $\mathbb{Z}_n$ είναι κυκλική με γεννήτορα το

$[1]_n$. Γιατί αν $k\in\mathbb{Z}$ με $0<k\leq n-1$ έχουμε

$$[n]_n=\underbrace{[1]_n+[1]_n+\dots+[1]_n}_{k\text{-φορές}}$$

ΠΡΟΤΑΣΗ Υποθέτουμε G κυκλική ομάδα. Τότε η G είναι αβελιανή.

ΑΠΟΔΕΙΞΗ Έστω $a\in G$ γεννήτορας της G και $b,c\in G$. Τότε υπάρχει $k_1,k_2\in\mathbb{Z}$ ώστε $b=a^{k_1}$, $c=a^{k_2}$

Έχουμε $b*c=a^{k_1}*a^{k_2}=a^{k_1+k_2}=a^{k_2+k_1}=a^{k_2}*a^{k_1}=c*b$, άρα G αβελιανή.

ΠΡΟΣΟΧΗ Το αντίστροφο δεν ισχύει! Δηλαδή, υπάρχουν αβελιανές ομάδες που δεν είναι κυκλικές.

<u>ΠΑΡΑΔΕΙΓΜΑ 4</u> Φανερά $G=(\mathbb{R},+)$ είναι αβελιανή ομάδα.

(Για παράδειγμα αν $a=\frac{1}{2}\in\mathbb{Q}$.

$$\langle a\rangle=\left\{\frac{k}{2}:k\in\mathbb{Z}\right\}=\left\{\dots,-1,-\frac{1}{2},0,\frac{1}{2},1,\dots\right\}\neq\mathbb{Q}$$

άρα a όχι γεννήτορας της G.

<u>ΙΣΧΥΡΙΣΜΟΣ</u> Η G δεν είναι κυκλική ομάδα.

<u>ΑΠΟΔΕΙΞΗ</u> Έστω $a\in\mathbb{Q}$. Θα δείξουμε ότι $\langle a\rangle\neq\mathbb{Q}$.

Βήμα 1ο: Αφού $a\in\mathbb{Q}$ υπάρχουν $b,c\in\mathbb{Z}$ με $c>0$ ώστε $a=\frac{b}{c}$. Άρα $c\cdot a=b\in\mathbb{Z}$ (*)

Βήμα 2ο: Έστω $d\in\langle a\rangle$. Τότε $c\cdot d$ είναι ακέραιος.

<u>ΑΠΟΔΕΙΞΗ</u>: Αφού $d\in\langle a\rangle$ έχουμε 3 περιπτώσεις

1) $d=0$. Τότε (*) ισχύει

2) $d=\underbrace{a+a+\dots+a}_{k\text{-φορές } k>0}$. Τότε $cd=c(a+a+\dots+a)=$
$ca+ca+\dots+ca$, αφού $ca\in\mathbb{Z}$

3) $d=\underbrace{-a-a-\dots-a}_{k\text{-φορές } k>0}$. Τότε $cd=c(-a-a-\dots-a)=$
$-(ca)-(ca)\dots-(ca)\in\mathbb{Z}$, γιατί $ca\in\mathbb{Z}$.

Βήμα 3ο: $\langle a\rangle\neq\mathbb{Q}$

Πράγματι $\frac{1}{c+1}\notin\langle a\rangle$, γιατί αν $\frac{1}{c+1}\in\langle a\rangle$

Βήμα 2ο: $c\cdot\frac{1}{c+1}\in\mathbb{Z}\Rightarrow\frac{c}{c+1}\in\mathbb{Z}$ αντίφαση.

αφού $0<\frac{c}{c+1}<1$

ΠΑΡΑΔΕΙΓΜΑ 5 Είναι η $(S_3, \circ)$ κυκλική;

α' τρόπος: Όχι, γιατί από πρόταση κάθε κυκλική ομάδα είναι αβελιανή, ενώ S_3 όχι αβελιανή.

Πιο γενικά αν G όχι αβελιανή τότε G ΔΕΝ είναι κυκλική. (από την πρόταση)

β' τρόπος: Για κάθε $a \in S_3$ υπολογίσαμε την υποομάδα $\langle a \rangle$ και είδαμε ότι σε κάθε περίπτωση $\langle a \rangle \neq S_3$

ΟΡΙΣΜΟΣ: Έστω G ομάδα. Αν G πεπερασμένο σύνολο συμβολίζουμε με $|G|$ ή $\#G$ τον αριθμό των στοιχείων της G. Αν G άπειρο σύνολο, γράφουμε

$|G| = +\infty$ (ή $\#G = +\infty$).

ΠΑΡΑΔΕΙΓΜΑ · Αν $G = \{e\}$ τότε $\#G = 1$

· Αν $G = (\mathbb{Z}_n, +)$ τότε $\#\mathbb{Z}_n = n$.

· Αν $G = (U(\mathbb{Z}_n), \cdot)$ δηλ. τα αναστρέψιμα στοιχεία του $(\mathbb{Z}_n, \cdot)$ τότε $|G| = \phi(n)$ όπου ϕ η συνάρτηση ϕ του Euler.

· Έχουμε $|(\mathbb{Z}, +)| = +\infty$, $|(\mathbb{Q}, +)| = +\infty$ $|(\mathbb{R}, +)| = +\infty$

$\#|(\mathbb{Q} \setminus \{0\}, \cdot)| = +\infty$, $|(\mathbb{R} \setminus \{0\}, \cdot)| = +\infty$.

· Επίσης, $\# S_3 = 6$.

Πιο γενικά ορίζουμε για $n \geq 1$ αναδρομικά:

$1! = 1$ και $(n+1)! = (n+1) \cdot n!$

(π.χ. $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$ $5! = 4! \cdot 5 = 120$)

Τότε για $n \geq 1$ έχουμε $\#(S_n, \circ) = n!$ όπου

S_n η ομάδα μεταθέσεων σε n στοιχεία, δηλ.

$S_n = \{f : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ με f 1-1 και επί$\}$

γιατί αν $f \in S_n$ $f = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}$

και έχουμε n επιλογές για το $f(1)$, μετά $(n-1)$ επιλογές για το $f(2)$ κτλ. και ισχύει $n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n$

ΤΑΞΗ ΣΤΟΙΧΕΙΟΥ ΟΜΑΔΑΣ.

<u>ΟΡΙΣΜΟΣ</u>: Έστω G ομάδα, $a \in G$. Ορίζουμε τάξη του a και συμβολίζουμε $\mathrm{ord}(a)$ (ή $O(a)$) ως εξής $\mathrm{ord}(a) = \# \langle a \rangle$

<u>ΠΑΡΑΔΕΙΓΜΑ 1</u> Αν $e \in G$ ουδέτερο, τότε $\langle e \rangle = \{e\}$

Άρα $\mathrm{ord}(e) = 1$.

<u>ΠΑΡΑΔΕΙΓΜΑ 2</u> Στο $(\mathbb{Z}_n, +)$ και $a = [1]_n$. Είδαμε $\mathbb{Z}_n = \langle a \rangle$. Συνεπώς $\mathrm{ord}(a) = \# \mathbb{Z}_n = n$

<u>ΠΑΡΑΔΕΙΓΜΑ 3</u> $G = (S_3, \circ)$ $\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$.

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Είδαμε $\langle \sigma_1 \rangle = \{\sigma_0, \sigma_1\}$

Άρα $\mathrm{ord}(\sigma_1) = 2$.

$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Είδαμε $\langle \sigma_4 \rangle = \{\sigma_0, \sigma_4, \sigma_5\}$

Συνεπώς $\mathrm{ord}(\sigma_4) = 3$

<u>ΠΑΡΑΔΕΙΓΜΑ 4</u> $(\mathbb{Z}_6, +)$ $\quad a = [4]_6$

$a + a = [2]_6$, $a + a + a = [12]_6 = [0]_6$

Θέταμε $H = \{[0]_6, [2]_6, [4]_6\}$

<u>ΙΣΧΥΡΙΣΜΟΣ</u> Η υποομάδα της G και $H < [4]_6 >$

Συνεπώς $\mathrm{ord}([4]_6) = \# H = 3$.

<u>ΑΠΟΔΕΙΞΗ</u> Αφού $H \neq \emptyset$ υποσύνολο της G και Η πεπερασμένο, για να είναι το Η υποομάδα της G αρκεί Η κλειστό ως προς + που ισχύει. Αφού $[4]_6 \in H \implies \langle [4]_6 \rangle \subseteq H$. (1)

Αφού $[0]_6 = [4]_6 + [4]_6 + [4]_6$
$[4]_6 = [4]_6$
$[2]_6 = [4]_6 + [4]_6$ Έχαμε $H \subseteq \langle [4]_6 \rangle$ (2)

Άρα από την (1) και (2) $H = \langle [4]_6 \rangle$

<u>ΠΑΡΑΔΕΙΓΜΑ 5</u> $G = (\mathbb{Z}, +)$. Αφού $\langle 1 \rangle = \mathbb{Z}$,

$\mathrm{ord}(1) = \# \mathbb{Z} = +\infty$.

Πιο γενικά, έστω $a \in \mathbb{Z}$. Συμβολίζουμε

$a\mathbb{Z} = \{ k \cdot a \mid k \in \mathbb{Z} \}$

Για παράδειγμα, $2\mathbb{Z}$ = άρτιοι ακέραιοι

$6\mathbb{Z} = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$

$0\mathbb{Z} = \{0\}$

<u>ΙΣΧΥΡΙΣΜΟΣ</u>. Έστω $a \in \mathbb{Z}$. Τότε $\langle a \rangle = a\mathbb{Z}$.

δηλ. αν $a \in \mathbb{Z}$ η ελάχιστη ομάδα του $(\mathbb{Z}, +)$ που περιέχει το a είναι η $a\mathbb{Z}$.

<u>ΑΠΟΔΕΙΞΗ</u> $a\mathbb{Z} = \{ka : k \in \mathbb{Z}\}$ εξ ορισμού

Αν $k = 0$ $k \cdot a = 0$

Αν $k > 0$ $k \cdot a = \underbrace{a + a + \ldots + a}_{k\text{-φορές}}$

Αν $k < 0$ $ka = \underbrace{(-a) + (-a) + \ldots + (-a)}_{|k|\text{-φορές}}$ Άρα $\langle a \rangle = a\mathbb{Z}$

Σαν συνέπεια: Για $a \in (\mathbb{Z}, +)$

- Αν $a = 0$ $\operatorname{ord}(a) = \# 0 \cdot \mathbb{Z} = \# \{0\} = 1$
- Αν $a \neq 0$ $a\mathbb{Z}$ είναι άπειρο σύνολο. Συνεπώς $\operatorname{ord}(a) = +\infty$.

<u>ΠΑΡΑΔΕΙΓΜΑ</u> Έστω $G = (\mathbb{Q} \setminus \{0\}, \cdot)$ και $a \in G$.

Υπολογίστε $\operatorname{ord}(a)$

Αν $a = 1 =$ το ουδέτερο της G, $\operatorname{ord}(a) = 1$.

Έστω $a = -1$ ισχυρισμός: $\langle 1 \rangle = \{-1, 1\}$

<u>ΑΠΟΔΕΙΞΗ</u> Άμεση, αφού $(-1)^2 = 1$, $(-1)^{-1} = -1$

Άρα $\operatorname{ord}(-1) = 2$.

ΙΣΧΥΡΙΣΜΟΣ Έστω $\alpha \in G \setminus \{1,-1\}$. Τότε

$ord(a) = +\infty$

ΑΠΟΔΕΙΞΗ
Υποθέτουμε για αντίφαση ότι δεν ισχύει. Άρα $\langle \alpha \rangle$ πεπερασμένο υποσύνολο του $\mathbb{Q}$.

Άρα υπάρχει $N > 0$ ώστε $|\alpha|^{\kappa} < n$ για κάθε $\kappa \in \mathbb{Z}$.

Αφού $\alpha \in \mathbb{Q} \setminus \{0, 1, -1\}$ έχουμε δυο περιπτώσεις

1) $|\alpha| > 1$. Τότε για κ θετικό αρκετά μεγάλο $|\alpha|^{\kappa_0} > N$ αντίφαση.

2) $0 < |\alpha| < 1 \Rightarrow \frac{1}{|\alpha|} > 1$. Άρα για κ_0 αρνητικό με κ_0 πολύ μεγάλο

$$|\alpha^{\kappa_0}| = \left|\frac{1}{\alpha^{\kappa_0}}\right| = \left(\frac{1}{|\alpha|}\right)^{\kappa_0} > N$$, αντίφαση.

Άρα, δεν μπορεί $\langle \alpha \rangle$ πεπερασμένο.

ΠΑΡΑΔΕΙΓΜΑ $G = GL_2(\mathbb{R})$ = 2×2 αντιστρέψιμοι πίνακες με στοιχεία στο $\mathbb{R}$.
με πράξη πολλαπλ. πινάκων και $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$

Τι τάξη έχει;

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

$$A^3 = A^2 \cdot A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

ΙΣΧΥΡΙΣΜΟΣ Αν $\kappa \in \mathbb{Z}$ με $\kappa \geq 1$, τότε $A^{\kappa} = \begin{bmatrix} 1 & \kappa \\ 0 & 1 \end{bmatrix}$

ΑΠΟΔΕΙΞΗ Επαγωγή στο n. Για $n=1$ ισχύει.

Υποθέτουμε ότι ισχύει για $n=k$. Τότε

$$A^{k+1} = A^k \cdot A = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k+1 \\ 0 & 1 \end{bmatrix}$$

Επομένως, από την αρχή της μαθηματικής επαγωγής ο ισχυρισμός ισχύει.

Αφού για $k_1, k_2 \in \mathbb{Z}$ θετικούς $k_1 \neq k_2$ από τον ισχυρισμό έχουμε: $A^{k_1} = \begin{bmatrix} 1 & k_1 \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & k_2 \\ 0 & 1 \end{bmatrix} = A^{k_2}$

προκύπτει ότι το σύνολο $\{A^k : k \in \mathbb{Z}, k>0\}$ άπειρο.
Άρα $\langle A \rangle$ άπειρο σύνολο, συνεπώς $\operatorname{ord}(A) = +\infty$.