20/3/19

Ορισμός: Έστω G ομάδα και $a \in G$. **Τάξη** ενός στοιχείου a ονομάζεται η τάξη της κυκλικής υποομάδας της G που παράγεται από το a. Η τάξη συμβολίζεται με $o(a)$ δηλ. $o(a) = |\langle a \rangle|$

Παραδείγματα 1) Βρείτε την τάξη του $[3]_9 \in \mathbb{Z}_9$.

Λύση: $\langle [3]_9 \rangle = \{[0]_9, [3]_9, [6]_9\}$

$o([3]_9) = 3$

2) Βρείτε την τάξη του $\sigma = (1,2,4,3) \in S_5$

$\langle \sigma \rangle = \{\sigma^n \mid n \in \mathbb{Z}\} = \{I, (1,2,4,3), (1,4)(2,3), (1,3,4,2)\}$

$\sigma^2 = \sigma \cdot \sigma = \underset{f}{(1,2,4,3)} \circ \underset{g(1)}{(1,2,4,3)} = (1,4)(2,3)(5)$

$f(g(1))$

$f(2)$

Date. No.

$\sigma^3 = \sigma^2 \cdot \sigma = (1,4)(2,3) \cdot (1,2,4,3) = (1,3,4,2)$

$\sigma^4 = \sigma^3 \cdot \sigma = (1,3,4,2)(1,2,4,3) = (1)(2)(4)(3) = I$

$\sigma^5 = \sigma^4 \cdot \sigma = I \cdot \sigma = \sigma$

$\sigma^6 = \sigma^4 \cdot \sigma^2 = I \cdot \sigma^2 = \sigma^2$

$\sigma^7 = \ldots = \sigma^3$

$\sigma^8 = \sigma^4 \cdot \sigma^4 = I \cdot I = I$

$O(\sigma) = 4$

Φυλλάδιο 2

$(GL_2(\mathbb{R}), \circ)$

② Βρείτε την τάξη του $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ → αντιστρέψιμοι πίνακες

Λύση:

$$\langle A \rangle = \{ A^n \mid n \in \mathbb{Z} \} = \{ \underset{I_2}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}, \underset{A^1}{\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}}, \underset{A^2}{\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}}, \underset{A^3 = -I_2}{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}, \underset{A^4}{\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}}, \underset{A^5}{\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}}, \underset{A^6 = I_2}{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} \}$$

$O(A) = 6$

3) Βρείτε την τάξη του $0 \in \mathbb{Z}$

Λύση: $\langle 0 \rangle = \{0\}$ $\quad O(0) = 1$

4) Βρείτε την τάξη του $1 \in \mathbb{Z}$

Λύση: $\langle 1 \rangle = \{ \ldots -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots \} = \mathbb{Z}$

$O(1) = \infty$

$O(a) < \infty \Rightarrow$ το a έχει πεπερασμένη τάξη

$O(a) = \infty \Rightarrow$ το a δεν έχει -״- -״-

$\dots, a^{-4}, a^{j}, a^{-2}, a^{-1}, 1, a, a^{2}, a^{i}, a^{4}, \dots$

1η περίπτωση: Όλα τα παραπάνω στοιχεία είναι διαφορετικά μεταξύ τους. $\boxed{o(a)=\infty}$

2η περίπτωση: Τουλάχιστον δύο από τα παραπάνω στοιχεία είναι ίσα.

$a^{i} = a^{j} \Rightarrow a^{i} \cdot a^{-j} = a^{j} a^{-j} \Rightarrow a^{i-j} = 1$

$\left.\begin{array}{l} i>j \\ i-j>0 \end{array}\right\} \Rightarrow i-j$ φυσικός

Έστω s ο μικρότερος φυσικός αριθμός τέτοιος ώστε $a^{s}=1$. Ισχυριζόμαστε ότι:

$\langle a \rangle \underset{\supseteq}{\overset{\subseteq}{=}} \{1, a, a^{2}, \dots, a^{s-2}, a^{s-1}\}$

* Τα στοιχεία $a^{0}, a^{1}, a^{2}, \dots, a^{s-1}$ είναι διαφορετικά μεταξύ τους.

(Αποδ: Έστω όχι. Τότε $a^{k} = a^{\lambda} \Rightarrow a^{k} \cdot a^{-\lambda} = a^{\lambda} \cdot a^{-\lambda} \Rightarrow a^{k-\lambda} = 1$

$s-1 \geq k > \lambda \geq 0$

$k-\lambda$ φυσικός

$k-\lambda < k < s$ (*) Άτοπο

(*) Έχω ορίσει τον s ως τον μικρότερο φυσικό αριθμό τ.ω. $a^{s}=1$ και βρήκα έναν αριθμό (τον $k-\lambda$) μικρότερο του s γι' αυτό κατέληξα σε ↑

αποδ: $(\supseteq)$ $1=a^{0}, a=a^{1}, \dots, a^{s-1}=a^{s-1}$ Όλα τα στοιχεία είναι δυνάμεις του a. Άρα:

$\{1, a, \dots, a^{s-1}\} \subseteq \langle a \rangle$

$(\subseteq)$ Έστω $b \in \langle a \rangle \Rightarrow b = a^{n}$ όπου $n \in \mathbb{Z}$

$n = qs + r$, $0 \leq r < s$

$a^{n} = a^{qs+r} = a^{qs} a^{r} = (a^{s})^{q} a^{r} = 1 \cdot a^{r} = a^{r}$, $0 \leq r \leq s-1$, $0 \leq r \leq s-1 \Rightarrow$

$\Rightarrow a^{n} \in \{a^{0}=1, a^{1}=a, a^{2}, \dots, a^{s-1}\}$

$o(a) = s$

Date. No.

Θεώρημα: Αν $ord(a) < \infty$ τότε η τάξη του a είναι ο μικρότερος φυσικός αριθμός s τέτοιος ώστε $\underset{\text{πολλ/σμος}}{a^s = 1}$ (ή $\underset{\text{πρόσθεση}}{s \cdot a = 0}$)

(Π.χ.)$_1$ Βρείτε την τάξη του $[3]_7 \in \mathbb{Z}_7$

Λύση:

$1 \cdot [3]_7 = [3]_7 \neq [0]_7$

$2 \cdot [3]_7 = [6]_7 \neq [0]_7$

$3 \cdot [3]_7 = [9]_7 = [2]_7 \neq [0]_7$

$4 \cdot [3]_7 = [5]_7 \neq [0]_7$

$5 \cdot [3]_7 = [1]_7 \neq [0]_7$

$6 \cdot [3]_7 = [4]_7 \neq [0]_7$

$7 \cdot [3]_7 = [21]_7 = [0]_7$

Άρα $o([3]_7) = 7$

(Π.χ.)$_2$ Βρείτε την τάξη του $[3]_7 \in U(\mathbb{Z}_7)$

Λύση:

$[3]_7 \neq [1]_7$

$[3]^2_7 = [2]_7 \neq [1]_7$

$[3]^3_7 = [6]_7 \neq [1]_7$

$[3]^4_7 = [4]_7 \neq [1]_7$

$[3]^5_7 = [5]_7 \neq [1]_7$

$[3]^6_7 = [1]_7$

Άρα $o([3]_7) = 6$

• Είναι η $U(\mathbb{Z}_7)$ κυκλική?

$\underset{6}{\langle [3]_7 \rangle} \subseteq \underset{\varphi(7) = 6}{U(\mathbb{Z}_7)} \Rightarrow U(\mathbb{Z}_7) = \langle [3]_7 \rangle$

δηλ. $U(\mathbb{Z}_7)$: κυκλική

Date. No.

Θεώρημα: Έστω G μία πεπερασμένη ομάδα H, G είναι κυκλική αν και μόνο αν υπάρχει στοιχείο $a \in G$ με τάξη ίση με την τάξη της ομάδας, δηλ. $o(a) = |G|$

Αποδ. ($\Rightarrow$) G κυκλική $\overset{ορσ.}{\Rightarrow}$ υπάρχει $a \in G$ τέτοιο ώστε: $G = \langle a \rangle \Rightarrow o(a) = |G|$

($\Leftarrow$) υπάρχει $a \in G$ με $\langle a \rangle = |G|$
$a \in G \Rightarrow a^n \in G \Rightarrow \underset{|G|}{\langle a \rangle} \le \underset{|G|}{G} \Rightarrow G = \langle a \rangle \Rightarrow G$: κυκλική

Άσκηση: Δείξτε ότι η ομάδα $U(\mathbb{Z}_8)$ δεν είναι κυκλική.
Λύση: $|U(\mathbb{Z}_8)| = \overset{\varphi(8)}{4}$. Έστω $U(\mathbb{Z}_8)$ κυκλική $\overset{προηγ.θ.}{\Rightarrow}$ υπάρχει $a \in U(\mathbb{Z}_8)$ τέτοιο ώστε $o(a) = |U(\mathbb{Z}_8)| = 4$

$o([1]_8) = 1$ $\quad o([5]_8) = 2$
$o([3]_8) = 2$ $\quad o([7]_8) = 2$ $\quad$ Άτοπο, άρα G όχι κυκλική

$[1]_8^1 = [1]_8$ $\quad [5]_8^1 = 5$ $\quad [7]_8^2 = [1]_8$
$[3]_8^1 = [3]_8$ $\quad [5]_8^2 = [1]_8$
$[3]_8^2 = [1]_8$ $\quad [7]_8^1 = [7]_8 = [1]_8$

Άσκηση για το σπίτι: Δείξτε ότι η ομάδα $U(\mathbb{Z}_{15})$ δεν είναι κυκλική.

Πρόταση: Έστω G ομάδα και $a \in G$ με $o(a) < \infty$. Ισχύει $a^n = 1$ αν και μόνο αν $o(a) \mid n$
Αποδ. ($\Rightarrow$) $a^n = 1$. Έστω $o(a) = s$, $n = q \cdot s + r$, $0 \le r < s$
i) $0 < r < s$, r: θετικός
$a^n = 1 \Rightarrow a^{qs+r} = 1 \Rightarrow (a^s)^q \cdot a^r = 1 \Rightarrow 1^q a^r = 1 \Rightarrow a^r = 1$
r: θετικός $\boxed{r < s}$ άτοπο

Date. No.

ii) $r = 0 \Rightarrow n = qs \Rightarrow \boxed{s \mid n}$

($\Leftarrow$) $s = o(a) \mid n \Rightarrow n = q \cdot s \Rightarrow a^n = a^{qs} = (a^s)^q = 1^q = 1$