Τάξη στοιχείου Ομάδας

Ορισμός: Έστω $(G,\cdot)$ μια ομάδα και έστω $\alpha\in G$. Η τάξη του στοιχείου α, συμβολίζεται με $o(\alpha)$ και ορίζεται να είναι η τάξη $|\langle\alpha\rangle|$ της κυκλικής υποομάδας $\langle\alpha\rangle$ που παράγεται από το α.

$$o(\alpha) = |\langle\alpha\rangle|.$$

Πρόταση: Έστω $(G,\cdot)$ μια ομάδα και έστω $\alpha\in G$. Τότε:

(1) $o(\alpha)=\infty \iff \alpha^m \neq e, \ \forall m\in\mathbb{N}$

(2) $o(\alpha)<\infty \iff \exists m\in\mathbb{N},\ \alpha^m=e$

(3) Αν $o(\alpha)<\infty$, τότε

$$o(\alpha) = \min \Theta(\alpha) = \min\{n\in\mathbb{N} \mid \alpha^n = e\}$$

Απόδειξη

(1) "$\Rightarrow$" Έστω $o(a)=\infty$ και υποθέτουμε προς άτοπο, ότι υπάρχει $m \in \mathbb{N}$ ώστε $a^m = e$. Θα δείξουμε ότι $\langle a \rangle = \{e, a, \dots, a^{m-1}\}$.

Επειδή $\{e, a, \dots, a^{m-1}\} \subseteq \langle a \rangle$, αρκεί να δείξουμε ότι $\langle a \rangle \subseteq \{e, a, \dots, a^{m-1}\}$. Έστω $x \in \langle a \rangle$. Τότε, υπάρχει $n \in \mathbb{Z}$ ώστε $x = a^n$. Από Ευκλείδεια Διαίρεση του n με το m, υπάρχουν $q, r \in \mathbb{Z}$ ώστε $n = qm + r$, όπου $0 \leq r < m-1$

Τότε, $x = a^n = a^{qm+r} = a^{qm} \cdot a^r = (a^m)^q \cdot a^r = e^q \cdot a^r = e \cdot a^r = a^r \in \{e, a, \dots, a^{m-1}\}$. Επομένως, $\langle a \rangle = \{e, a, \dots, a^{m-1}\}$, άτοπο διότι το $\{e, a, \dots, a^{m-1}\}$ είναι πεπερασμένο ενώ η $\langle a \rangle$ άπειρη.

Ώστε, $a^m \neq e$, $\forall m \in \mathbb{N}$.

"$\Leftarrow$" Έστω $a^m \neq e$, $\forall m \in \mathbb{N}$. Θα αποδείξουμε ότι η $\langle a \rangle$ έχει άπειρο πλήθος στοιχείων.

Επειδή $X=\{a^n \in G \mid n \in \mathbb{N}\} \subseteq \langle a \rangle$, αν αποδείξουμε ότι το X είναι άπειρο τότε θα έχουμε το ζητούμενο. Πράγματι, αν το X ήταν πεπερασμένο, θα υπήρχαν $i, j \in \mathbb{N}$, $i \neq j$ ώστε $a^i = a^j$. Χωρίς βλάβη της γενικότητας, $i>j$.

Επομένως, $a^{i-j} = e$, όπου $i-j \in \mathbb{N}$, το οποίο αντίκειται στην υπόθεση $a^m \neq e, \forall m \in \mathbb{N}$.

Άρα, $|X| = \infty \Rightarrow |\langle a \rangle| = \infty \Rightarrow o(a) = \infty$.

(2) Είναι ισοδύναμο του (1)

(3) Υποθέτουμε ότι $o(a) < \infty$. Από το (2), υπάρχει $m \in \mathbb{N}$ ώστε $a^m = e$, άρα $m \in O(a) = \{n \in \mathbb{N} \mid a^n = e\}$ και συνεπώς το $O(a)$ ως μη-κενό υποσύνολο του $\mathbb{N}$ έχει ελάχιστο στοιχείο n, δηλαδή $n = \min O(a)$, που σημαίνει ότι ο n είναι ο μικρότερος

φυσικός αριθμός με την ιδιότητα $\alpha^n = e$.

Έστω $B = \{e, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$. Αν υπήρχαν $i, j \in \mathbb{N}$ με $i > j$ και $0 \leq j < i \leq n-1$, ώστε $\alpha^i = \alpha^j$, τότε $\alpha^{i-j} = e$, όπου $i-j < n$, άτοπο. Άρα, $\alpha^i \neq \alpha^j$, $\forall i, j \in \{0, 1, \dots, n-1\}$, δηλαδή $|B| = n$. Θα δείξουμε $B = \langle \alpha \rangle$.

Εφ' όσον $B \subseteq \langle \alpha \rangle$, αρκεί να δείξουμε ότι $\langle \alpha \rangle \subseteq B$. Έστω $x \in \langle \alpha \rangle$. Τότε $x = \alpha^k$ για κάποιο $k \in \mathbb{Z}$. Από Ευκλείδεια Διαίρεση του k με το n, υπάρχουν $\tilde{q}, \tilde{r} \in \mathbb{Z}$ ώστε $k = \tilde{q}n + \tilde{r}$, με $0 \leq \tilde{r} < n-1$. Τότε:

$x = \alpha^k = (\alpha^n)^{\tilde{q}} \cdot \alpha^{\tilde{r}} = e^{\tilde{q}} \alpha^{\tilde{r}} = \alpha^{\tilde{r}} \in B$. Συνεπώς,

$$\langle \alpha \rangle = B \Rightarrow |\langle \alpha \rangle| = |B|$$

$$\Rightarrow o(\alpha) = n = \min\{k \in \mathbb{N} \mid \alpha^k = e\}$$

∎

Παραδείγματα

(I) $G=\{e,a\}$, $o(e)=1$, $o(a)=2=|G|$. $((\mathbb{Z}_2,+))$

(II) $G=\{e,a,b\}$

$((\mathbb{Z}_3,+))$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$$o(e)=1, \quad \begin{cases} a\neq e \\ a^2=b \\ a^3=a^2a=ba=e \end{cases} \Rightarrow o(a)=3$$

$$\begin{cases} b\neq e \\ b^2=a \\ b^3=b^2b=ab=e \end{cases} \Rightarrow o(b)=3$$

- $\langle a\rangle=\{e,a,a^2\}=\{e,a,b\}=G$
- $\langle b\rangle=\{e,b,b^2\}=\{e,b,a\}=G$

(III) $|G|=4$, $G=\{e,a,b,c\}$

(A') $\leftarrow (\mathbb{Z}_4,+)$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$o(e) = 1$

- $\begin{cases} a \neq e \\ a^2 = b \\ a^3 = c \\ a^4 = e \end{cases} \Longrightarrow$ $o(a) = 4$ (σκέψου $[1]_4$)

$4 \cdot [1]_4 = [0]_4$

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

- $\begin{cases} b \neq e \\ b^2 = e \end{cases} \Longrightarrow o(b) = 2$, $\langle b \rangle = \{e, b\}$

(σκέψου $[2]_4$)

$2 \cdot [2]_4 = [4]_4 = [0]_4$

- $\begin{cases} c \neq e \\ c^2 = b \\ c^3 = a \\ c^4 = e \end{cases} \Longrightarrow o(c) = 4$ (σκέψου $[3]_4 = -[1]_4$)

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

$c = a^{-1}$

(Β') V_4 : $\forall x \in V_4 : x^2 = e \Rightarrow o(x) = 2, \forall x \in V_4 \setminus \{e\}$

$\{e\}$

Σκέψου $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$

$+$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$
$([0]_2,[0]_2)$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$
$([0]_2,[1]_2)$	$([0]_2,[1]_2)$	$([0]_2,[0]_2)$	$([1]_2,[1]_2)$	$([1]_2,[0]_2)$
$([1]_2,[0]_2)$	$([1]_2,[0]_2)$	$([1]_2,[1]_2)$	$([0]_2,[0]_2)$	$([0]_2,[1]_2)$
$([1]_2,[1]_2)$	$([1]_2,[1]_2)$	$([1]_2,[0]_2)$	$([0]_2,[1]_2)$	$([0]_2,[0]_2)$

- $o(([0]_2,[0]_2)) = 1$
- $2([0]_2,[1]_2) = ([0]_2,[1]_2)+([0]_2,[1]_2) = ([0]_2,[0]_2)$

άρα $o(([0]_2,[1]_2)) = 2$

αντίστοιχα, $o(([1]_2,[0]_2)) = o(([1]_2,[1]_2)) = 2$

(IV) $S_3 = \{ Id_3, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$

• $o(Id_3) = 1$

$$\left.\begin{array}{l} \cdot\ (1\ 2) \neq Id_3 \\ \cdot\ (1\ 2)^2 = Id_3 \end{array}\right\} \Longrightarrow \begin{array}{l} o((1\ 2)) = 2 \\ \langle (1\ 2) \rangle = \{ Id_3, (1\ 2) \} \end{array}$$

Εύκολα $(1\ 3)^2 = (2\ 3)^2 = Id_3$ και

$(1\ 2\ 3)^3 = (1\ 3\ 2)^3 = Id_3$

• $\langle (1\ 2\ 3) \rangle = \{ Id_3, (1\ 2\ 3), (1\ 2\ 3)^2 \}$
$= \{ Id_3, (1\ 2\ 3), (1\ 3\ 2) \}$

• $\langle (1\ 3\ 2) \rangle = \{ Id_3, (1\ 3\ 2), (1\ 3\ 2)^2 \}$
$= \{ Id_3, (1\ 3\ 2), (1\ 2\ 3) \}$

(V) Στην ομάδα $(\mathbb{Z}, +)$ το μόνο στοιχείο με πεπερασμένη τάξη είναι το ουδέτερο στοιχείο $0 \in \mathbb{Z}$, $o(0) = 1$.

Πράγματι, αν $k \in \mathbb{Z}$ με $o(k) = m < \infty$, τότε:

$$mk = 0 \underset{m \in \mathbb{N}}{\Longrightarrow} k = 0.$$

(VI) Στην πολλαπλασιαστική ομάδα $GL(2, \mathbb{R})$ θεωρούμε το στοιχείο $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

<u>Ισχυρισμός</u>: $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \forall n \in \mathbb{N}$

<u>απόδειξη</u>: <u>$n = 1$</u>: $A^1 = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ✓

- Έστω $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ για κάποιο $n \in \mathbb{N}$.
- $A^{n+1} = A^n A = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$

Επαγωγικά, $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \forall n \in \mathbb{N}$

Αφού $A^n \neq I_2$, $\forall n \in \mathbb{N}$ προκύπτει ότι

$$o(A) = \infty.$$

Πορίσματα

(i) Μια πεπερασμένη ομάδα $(G, \cdot)$ είναι κυκλική αν-ν υπάρχει $a \in G$ με $o(a) = |G|$.

(ii) Αν μια ομάδα είναι πεπερασμένη τότε κάθε στοιχείο της έχει πεπερασμένη τάξη.

! Το αντίστροφο του (ii) δεν ισχύει.
Δηλαδή υπάρχει άπειρη ομάδα της οποίας κάθε στοιχείο έχει πεπερασμένη τάξη.

Έστω $\prod_{n=1}^{\infty} \mathbb{Z}_2 := \{ x = (x_n)_{n \in \mathbb{N}} \mid x_n \in \mathbb{Z}_2, \forall n \in \mathbb{N} \}$

Προφανώς το $\prod_{n=1}^{\infty} \mathbb{Z}_2$ είναι ένα άπειρο σύνολο.

Στο $\prod_{n=1}^{\infty} \mathbb{Z}_2$ ορίζουμε πράξη πρόσθεσης ως εξής: Αν $x = (x_n)_{n \in \mathbb{N}}, y = (y_n)_{n \in \mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$

τότε: $x + y := \underbrace{(x_n + y_n)}_{\text{πρόσθεση στο } \mathbb{Z}_2}{}_{n \in \mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$

Εύκολα (H/W), το ζεύγος $\left(\prod_{n=1}^{\infty} \mathbb{Z}_2, +\right)$

είναι αβελιανή άπειρη ομάδα με ουδέτερο

στοιχείο το $\mathbb{0} = ([0]_2, [0]_2, \dots, [0]_2, \dots)$

και για κάθε $x = (x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$ είναι

$-x = (-x_n)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$.

Επειδή $2[x]_2 = [x]_2 + [x]_2 = [2x]_2 = [0]_2, \ \forall [x]_2 \in \mathbb{Z}_2$

προκύπτει ότι: $\forall \tilde{x} = ([x_n]_2)_{n\in\mathbb{N}} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$ ισχύει:

$$2\tilde{x} = \tilde{x} + \tilde{x} = ([x_n]_2 + [x_n]_2)_{n\in\mathbb{N}} = ([0]_2)_{n\in\mathbb{N}} = \mathbb{0}$$

άρα: $o(\tilde{x}) = 2, \ \forall \tilde{x} \in \prod_{n=1}^{\infty} \mathbb{Z}_2 \setminus \{\mathbb{0}\}$.

$\blacksquare$

Ιδιότητες Τάξης Στοιχείου

Πρόταση 1: Έστω $(G,\cdot)$ μια ομάδα και έστω $\alpha \in G$ με $o(a)<\infty$. Τότε:

$$\forall \kappa \in \mathbb{N}: \quad \alpha^{\kappa}=e \iff o(\alpha) \mid \kappa.$$

Απόδειξη

Θέτουμε $o(\alpha)=n<\infty$ και έστω $\kappa \in \mathbb{N}$.

"$\Leftarrow$" Αν $n \mid \kappa$, τότε $\kappa = tn$ για κάποιο $t \in \mathbb{N}$, οπότε: $\alpha^{\kappa} = \alpha^{tn} = (\alpha^{n})^{t} = e^{t} = e$

"$\Rightarrow$" Έστω $\alpha^{\kappa}=e$. Από Ευκλείδεια Διαίρεση του κ με το n, υπάρχουν $q,r \in \mathbb{Z}$ με $\kappa = qn+r$, όπου $0 \leq r \leq n-1$. Τότε:

$\alpha^{\kappa}=e \Rightarrow \alpha^{qn+r} = e \Rightarrow (\alpha^{n})^{q} \cdot \alpha^{r} = e \Rightarrow e^{q}\cdot\alpha^{r} = e \Rightarrow e\cdot \alpha^{r}=e \Rightarrow \alpha^{r}=e$. Αν $r>0$, τότε $\alpha^{r}=e$ με $r \in \mathbb{N}$, $r \leq n-1<n$, άτοπο διότι $n=o(\alpha)$ είναι ο μικρότερος φυσικός με την ιδιότητα $\alpha^{n}=e$.

Ώστε, $r=0 \Rightarrow k = qn \Rightarrow n = o(a) | k$. ∎

Βασικό Θεώρημα

$(G,\cdot)$ ομάδα, $a \in G$, $k \in \mathbb{N}$. Τότε

(i) $o(a) = \infty \Rightarrow o(a^k) = \infty$

(ii) $o(a) < \infty \Rightarrow o(a^k) = \dfrac{o(a)}{(o(a), k)} = o(a^{-k})$

Ιδιαίτερα, $o(a) = o(a^{-1})$.

(iii) Αν $o(a) < \infty$, τότε: $k \mid o(a) \Leftrightarrow o(a^k) = \dfrac{o(a)}{k}$

(iv) Αν $o(a) < \infty$, τότε: $(k, o(a)) = 1 \Leftrightarrow o(a^k) = o(a)$.

<u>Απόδειξη</u>: Ηλεκτρονικό βιβλίο σελ. 182

Προκύπτει τώρα το ακόλουθο σημαντικό πόρισμα.

Πόρισμα: Έστω $(G, \cdot)$ μια κυκλική ομάδα πεπερασμένης τάξης με γεννήτορα το $a \in G$. Τότε, $\forall k \in \mathbb{N}$: $G = \langle a^k \rangle \iff (k, o(a)) = 1$.

Δηλαδή, ένα στοιχείο a^k της G είναι γεννήτοράς της αν-ν $(k, o(a)) = 1$.

Απόδειξη

Έστω $k \in \mathbb{N}$. Έχουμε: $G = \langle a \rangle$.

"$\Longrightarrow$" Υποθέτουμε ότι $G = \langle a^k \rangle$. Τότε:

$$o(a^k) = |\langle a^k \rangle| = |G| = o(a) \xRightarrow[\text{Θεώρημα}]{\text{Βασικό}} \frac{o(a)}{(o(a), k)} = o(a) \Longrightarrow (o(a), k) = 1.$$

"$\Longleftarrow$" Έστω $(k, o(a)) = 1$. Τότε:

$$o(a^k) = \frac{o(a)}{(o(a), k)} = o(a) \Longrightarrow |\langle a^k \rangle| = |\langle a \rangle| = |G|$$

και εφ' όσον $\langle a^k \rangle \subseteq G$ προκύπτει

$$G = \langle a^k \rangle.$$

$\blacksquare$

Παρατήρηση: Έστω $G=\langle a\rangle$ μια κυκλική ομάδα τάξης $n\in\mathbb{N}$. Τότε το σύνολο γεννητόρων της G είναι το

$$\{\alpha^k\in G \mid 1\leq k\leq n \text{ και } (k,n)=1\}$$

οπότε το πλήθος των γεννητόρων της G είναι

$$\left|\{\alpha^k\in G \mid 1\leq k\leq n \text{ και } (k,n)=1\}\right| = \varphi(n)$$

Τάξη Γινομένου Στοιχείων μιας Ομάδος

Η ακόλουθη σειρά παραδειγμάτων δείχνει ότι, γενικά, δεν είναι δυνατόν να περιμένουμε να υπάρχει κάποια σχέση μεταξύ των τάξεων $o(x)$, $o(y)$ και $o(xy)$ για $x,y\in G$.

Παραδείγματα

(I) Στην $(S_4, \circ)$ θεωρούμε τα στοιχεία

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \text{και} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

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

- $\sigma \neq Id_4$
- $\sigma^2 = \sigma\circ\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \neq Id_4$
- $\sigma^3 = \sigma^2\circ\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = Id_4$

άρα $o(\sigma) = 3$. Όμοια, $\tau^3 = Id_4$ $\therefore$
$o(\tau) = 3$

Επίσης, $(\sigma\circ\tau)^2 = (\sigma\circ\tau)\circ(\sigma\circ\tau) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = Id_4$, οπότε

$o(\sigma\circ\tau) = 2 \neq 9 = o(\sigma)o(\tau)$

(II) Θεωρούμε την (άπειρη μη αβελιανή) ομάδα $GL(2,\mathbb{R}) = \{A \in \mathbb{M}_2(\mathbb{R}) \mid \det(A) \neq 0\}$

και έστω $A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

Τότε προφανώς $A, B, \underset{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}{\underset{\parallel}{AB}} \in GL(2,\mathbb{R})$

- $A \neq I_2$
- $A^2 = A \cdot A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

  $o(A) = 2$

- $B \neq I_2$, $B^2 = B \cdot B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$

  $o(B) = 2$

Ωστόσο, επαγωγικά, $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2, \forall n \in \mathbb{N}$

και άρα $o(AB) = \infty$.

Πρόταση

Έστω $(G,\cdot)$ μια ομάδα και $a,b,x \in G$.

Τότε: i) $o(x^{-1}ax) = o(a) = o(xax^{-1})$

ii) $o(ab) = o(ba)$

Απόδειξη

i) Για κάθε $n \in \mathbb{N}$ ισχύει:

$$(x^{-1}ax)^n = \underbrace{(x^{-1}ax)(x^{-1}ax)\cdots(x^{-1}ax)}_{n-\text{φορές}}$$

$$= x^{-1}a^n x$$

οπότε για κάθε $n \in \mathbb{N}$ ισχύει:

$(x^{-1}ax)^n = e \iff x^{-1}a^n x = e \iff a^n x = xe$

$\iff a^n = xex^{-1} \iff a^n = e$, που συνεπάγεται

$$o(x^{-1}ax) = \min\{n \in \mathbb{N} \mid (x^{-1}ax)^n = e\}$$

$$= \min\{n \in \mathbb{N} \mid a^n = e\}$$

$$= o(a)$$

Πρόταση

Έστω $(G, \cdot)$ μια ομάδα και $a, b, x \in G$.

Τότε: i) $o(x^{-1}ax) = o(a) = o(xax^{-1})$

ii) $o(ab) = o(ba)$

Απόδειξη

i) Για κάθε $n \in \mathbb{N}$ ισχύει:

$$(x^{-1}ax)^n = \underbrace{(x^{-1}ax)(x^{-1}ax)\cdots(x^{-1}ax)}_{n-\text{φορές}}$$

$$= x^{-1}a^n x$$

οπότε για κάθε $n \in \mathbb{N}$ ισχύει:

$$(x^{-1}ax)^n = e \iff x^{-1}a^n x = e \iff a^n x = xe$$

$$\iff a^n = xex^{-1} \iff a^n = e,$$ που συνεπάγεται

$$o(x^{-1}ax) = \min\{n \in \mathbb{N} \mid (x^{-1}ax)^n = e\}$$

$$= \min\{n \in \mathbb{N} \mid a^n = e\}$$

$$= o(a)$$

Επίσης, $o(xax^{-1}) = o((x^{-1})^{-1} a x^{-1}) = o(a)$

ii) Έχουμε,

$o(ba) = o(a^{-1}(ab)a) = o(ab)$ λόγω του (i) $\blacksquare$

<u>Πρόταση</u> (χωρίς απόδειξη) Έστω $(G, \cdot)$ μια ομάδα και $a, b \in G$ με $ab = ba$. Αν $o(a), o(b) < \infty$ και $(o(a), o(b)) = 1$ τότε:

$$o(ab) = o(a)o(b)$$

Πρόταση

Έστω G_1 και G_2 δύο ομάδες και έστω η ομάδα γινόμενο $G = G_1 \times G_2$.

Για ένα στοιχείο $x = (x_1, x_2) \in G$, τα ακόλουθα είναι ισοδύναμα:

(1) Το στοιχείο x έχει πεπερασμένη τάξη

(2) Τα $x_1 \in G_1$ και $x_2 \in G_2$ έχουν πεπερασμένη τάξη.

► Αν $o(x) < \infty$, τότε:

$$o(x) = o((x_1, x_2)) = [o(x_1), o(x_2)]$$

Απόδειξη

Για κάθε $n \in \mathbb{N}$ έχουμε:

$x^n = (x_1, x_2)^n = (x_1^n, x_2^n)$ και συνεπώς:

$$x^n = e \iff (x_1^n, x_2^n) = (e_1, e_2)$$

$$\iff x_1^n = e_1 \text{ και } x_2^n = e_2$$

Άρα, $o(x) < \infty \iff o(x_1) < \infty$ και $o(x_2) < \infty$.

Υποθέτουμε τώρα ότι $o(x) = m$ και $o(x_k) = m_k$, $k = 1, 2$, και θα δείξουμε $m = [m_1, m_2]$.

Θέτουμε $\lambda = [m_1, m_2]$ και θα δείξουμε $m = \lambda$.

Υπάρχουν $\lambda_1, \lambda_2 \in \mathbb{N}$ ώστε: $\begin{array}{l} \lambda = \lambda_1 m_1 \\ \lambda = \lambda_2 m_2 \end{array}$

Άρα, $x^\lambda = (x_1, x_2)^\lambda = (x_1^\lambda, x_2^\lambda) = (x_1^{\lambda_1 m_1}, x_2^{\lambda_2 m_2})$
$= ((x^{m_1})^{\lambda_1}, (x^{m_2})^{\lambda_2}) = (e_1^{\lambda_1}, e_2^{\lambda_2}) = (e_1, e_2) = e$,

δηλαδή $o(x) = m | \lambda$. Απ' την άλλη,

$o(x) = m \Rightarrow x^m = (e_1, e_2) = e \Rightarrow (x_1^m, x_2^m) = (e_1, e_2)$

$\Rightarrow \begin{cases} x_1^m = e_1 \\ x_2^m = e_2 \end{cases} \Rightarrow \begin{array}{l} m | o(x_1) \\ m | o(x_2) \end{array} \Rightarrow m | m_1, m | m_2$

$\Rightarrow \lambda | m$. Τελικά, $\lambda = m$, όπως θέλαμε. ⊠

Πρόταση

Έστω $n \in \mathbb{N}$, $n \geq 2$ και έστω $\sigma \in S_n$.

(1) Αν η σ είναι κύκλος μήκους κ τότε $o(\sigma) = \kappa$

(2) Αν η σ είναι σύνθεση ξένων ανά δύο κύκλων, $\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \circ \gamma_s$, όπου ο καθένας έχει μήκος $\underset{t_i,\ i=1,2,\ldots,s}{\geq 2}$, τότε

$$o(\sigma) = [t_1, t_2, \ldots, t_s]$$

Παράδειγμα

Στην $(S_{10}, \circ)$ θεωρούμε τις μεταθέσεις

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 3 & 4 & 5 & 1 & 10 & 9 & 2 & 8 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 4 & 5 & 3 & 7 & 6 & 10 & 2 & 8 \end{pmatrix}$$

Γράφω $\sigma = (1\ 7\ 10\ 8\ 9\ 2\ 6)$,

οπότε $o(\sigma) = 7$.

Γράφω $\tau = (1\ 9\ 2) \circ (3\ 4\ 5) \circ (6\ 7) \circ (8\ 10)$

Άρα, $o(\tau) = [3, 3, 2, 2] = 6$

. Θα βρούμε την τάξη της $\sigma \circ \tau$.

Αρχικά,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 7 & 4 & 5 & 3 & 10 & 1 & 8 & 6 & 9 \end{pmatrix}$$

$$= (1\ 2\ 7) \circ (3\ 4\ 5) \circ (6\ 10\ 9)$$

οπότε: $o(\sigma \circ \tau) = [3, 3, 3] = 3$

▶ (Ομο) μορφισμοί Ομάδων

Ορισμός: Έστω $(G_1, \cdot)$ και $(G_2, *)$ δύο ομάδες. Μια απεικόνιση $f: G_1 \to G_2$ λέγεται **μορφισμός** αν

$$f(x \cdot y) = f(x) * f(y), \quad \forall x, y \in G_1$$

Πρόταση

(1) Έστω $f: (G_1, \cdot) \to (G_2, *)$ μορφισμός ομάδων. Τότε

(i) $f(e_1) = e_2$ (ii) $f(x^{-1}) = (f(x))^{-1}, \forall x \in G_1$

(iii) $\forall x_1, x_2, \dots, x_n \in G_1, \ f(x_1 \cdot x_2 \cdots x_n) = f(x_1) * f(x_2) * \dots * f(x_n)$

(iv) $\forall x \in G_1, \forall n \in \mathbb{Z}, \ f(x^n) = (f(x))^n$

Ακολουθεί η απόδειξη

Απόδειξη

(i) $f(e_1) = f(e_1 \cdot e_1) = f(e_1) * f(e_1)$, άρα:

$$f(e_1) * e_2 = f(e_1) * f(e_1) \xRightarrow[\text{στην } G_2]{\text{Νόμος Διαγραφής}} f(e_1) = e_2$$

(ii) Έστω $x \in G_1$. Τότε:

$$f(x^{-1}) * f(x) = f(x^{-1} \cdot x) = f(e_1) \overset{(i)}{=\!=} e_2$$

$$f(x) * f(x^{-1}) = f(x \cdot x^{-1}) = f(e_1) \overset{(i)}{=\!=} e_2$$

Λόγω μοναδικότητας του αντιστρόφου,

προκύπτει: $(f(x))^{-1} = f(x^{-1})$

(iii) Επαγωγή στο πλήθος $n \in \mathbb{N}$.

(iv) Έστω $x \in G_1$ και έστω $n \in \mathbb{Z}$.

▶ $\underline{\underline{n = 0}}$: $f(x^0) = f(e_1) = e_2 = (f(x))^0$ ✓

▶ $\underline{\underline{n \in \mathbb{N}}}$: $f(x^n) = f(\underbrace{x \cdot x \cdots x}_{n\text{-φορές}}) \overset{iii)}{=\!=} \underbrace{f(x) * f(x) * \cdots * f(x)}_{n\text{-φορές}}$

$$= (f(x))^n$$

▲ $\underline{\underline{n<0}}$: $f(x^n) = f((x^{-1})^{-n}) \overset{-n\in\mathbb{N}}{=\!=} (f(x^{-1}))^{-n} =$

$\overset{ii)}{=\!=} ((f(x))^{-1})^{-n} = (f(x))^n$.

■

$\underline{\underline{\text{Σχόλιο}}}$: Αν $f: G_1 \to G_2$ και $g: G_2 \to G_3$ είναι μορφισμοί ομάδων τότε και η $g\circ f: G_1 \to G_3$ είναι μορφισμός ομάδων.

Πράγματι, για κάθε $x, y \in G_1$ έχουμε:

$$(g\circ f)(xy) = g(f(xy)) \underset{\text{μορφισμός}}{\overset{f:}{=\!=}} g(f(x)f(y))$$

$$\underset{\text{μορφισμός}}{\overset{g:}{=\!=}} g(f(x))g(f(y))$$

$$= (g\circ f)(x)(g\circ f)(y)$$

■

Ορισμοί: Ένας μορφισμός ομάδων $f: G_1 \to G_2$ λέγεται:

(α) **μονομορφισμός**, αν η f είναι 1-1

(β) **επιμορφισμός**, αν η f είναι επί

(γ) **ισομορφισμός**, αν η f είναι 1-1 και επί.

Σχόλιο: Αν $f: G_1 \to G_2$ είναι ισομορφισμός τότε και η $f^{-1}: G_2 \to G_1$ είναι επίσης ισομορφισμός.

Πράγματι, αρχικά ορίζεται καλώς η $f^{-1}: G_2 \to G_1$ διότι f: 1-1 και επί, και επιπλέον και η f^{-1} είναι 1-1 και επί.

Τέλος, για κάθε $a, b \in G_2$ θα δείξουμε ότι $f^{-1}(ab) = f^{-1}(a) f^{-1}(b)$. Θέτουμε $x = f^{-1}(ab)$, $y = f^{-1}(a)$ και $z = f^{-1}(b)$ και θα δείξουμε ότι $x = yz$. Πράγματι,

$$f(x) = f(f^{-1}(ab)) = ab = f(y)f(z) \overset{f:\ \text{μορφισμός}}{=} f(y \cdot z)$$

αφού f: 1-1 έπεται: $x = yz$ ∎

__Ορισμός__: Αν υπάρχει ισομορφισμός ομάδων $f: G_1 \to G_2$ τότε οι ομάδες G_1 και G_2 λέγονται __ισόμορφες__ και γράφουμε

$$G_1 \cong G_2.$$

<u>Παρατήρηση</u>: Σύμφωνα με τα προηγούμενα σχόλια συμπεραίνουμε ότι η σχέση $\cong$ είναι σχέση ισοδυναμίας στην κλάση των ομάδων: Δηλαδή, αν G_1, G_2 και G_3 είναι ομάδες, τότε:

(1) $G_1 \cong G_1$ (2) $G_1 \cong G_2 \to G_2 \cong G_1$

(3) $G_1 \cong G_2$ και $G_2 \cong G_3 \Longrightarrow G_1 \cong G_3$.

<u>Απόδειξη</u>

(1) Η $Id: G_1 \to G_1$ με $Id(x) = x$ είναι ισομορφισμός.

(2) Αν $G_1 \cong G_2$ τότε υπάρχει ισομορφισμός $f: G_1 \to G_2$. Άρα $f^{-1}: G_2 \to G_1$ είναι ισομορφισμός και συνεπώς $G_2 \cong G_1$.

(3) Αν $G_1 \cong G_2$ και $G_2 \cong G_3$ τότε υπάρχουν ισομορφισμοί $f: G_1 \to G_2$ και $g: G_2 \to G_3$. Η $g \circ f: G_1 \to G_3$ είναι επίσης ισομορφισμός, οπότε: $G_1 \cong G_3$ ■

<u>Άσκηση</u>: Έστω $f: G_1 \to G_2$ μορφισμός ομάδων και $x \in G_1$ με $o(x) < \infty$. Τότε $o(f(x)) < \infty$ και $o(f(x)) \mid o(x)$.

<u>Λύση</u>: Έστω $o(x) = n < \infty$, άρα $x^n = e_1$.

Τότε: $f(x^n) = f(e_1) \Rightarrow (f(x))^n = e_2 \xRightarrow[\text{Πρόταση}]{\text{Γνωστή}} o(f(x)) < \infty$. Επίσης: αν $o(f(x)) = m < \infty$

τότε: $(f(x))^n = f(x^n) = f(e_1) = e_2$, οπότε:

$$m \mid n \Rightarrow o(f(x)) \mid o(x)$$

■

Παραδείγματα

(1) Αν G_1, G_2 είναι δύο ομάδες τότε η $f: G_1 \rightarrow G_2$ με $f(x) = e_2$ είναι μορφισμός (τετριμμένος μορφισμός). Πράγματι, $\forall x, y \in G_1 : f(xy) = e_2 = e_2 \cdot e_2 = f(x) f(y)$.

(2) Αν G: ομάδα τότε η ταυτοτική απεικόνιση $Id: G \rightarrow G$ είναι ισομορφισμός.

(3) Η απεικόνιση πρόσημο $\varepsilon: (S_n, \circ) \rightarrow (\mathbb{Z}_2, +)$ με $\varepsilon(\sigma) = \begin{cases} [0]_2, & \sigma: \text{άρτια} \\ [1]_2, & \sigma: \text{περιττή} \end{cases}$

είναι μορφισμός (έχει αποδειχθεί)

(4) Η απεικόνιση $\pi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}_n, +)$ με $\pi(x) = [x]_n$ είναι επιμορφισμός διότι:

$$\pi(x+y) = [x+y]_n = [x]_n + [y]_n, \quad \forall x,y \in \mathbb{Z}$$
$$= \pi(x) + \pi(y)$$

Το επί είναι προφανές.

$$\left(\forall [x]_n \in \mathbb{Z}_n,\ x \in \mathbb{Z}, \text{ και } \pi(x) = [x]_n \right).$$

(5) Η $f: (\mathbb{R}^*, \cdot) \to (GL(2,\mathbb{R}), \cdot)$

$$x \mapsto f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

είναι καλά ορισμένη διότι: για κάθε $x \in \mathbb{R}^*$: $\det(f(x)) = \det\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = x^2 \neq 0$, άρα $f(x) \in GL(2,\mathbb{R})$.

Επίσης, για κάθε $x, y \in \mathbb{R}^*$ έχουμε:

$$f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x)f(y)$$

οπότε f: μορφισμός ομάδων.

Επιπλέον, f: 1-1: Αν $x, y \in \mathbb{R}^*$ τότε

$f(x) = f(y) \Rightarrow \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} = \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} \rightarrow x = y$

Συνεπώς, f: μονομορφισμός ομάδων.

<u>Σχόλιο</u>: Λέμε ότι μια ιδιότητα P διατηρείται υπό ισομορφισμούς αν ισχύει το εξής: Αν η G έχει την ιδιότητα P και $G \cong H$ τότε και η H έχει την ιδιότητα P.

Θα αποδείξαμε στο μάθημα της Παρασκευής 26/4/2024 ότι οι ακόλουθες ιδιότητες διατηρούνται υπό ισομορφισμούς:

P_1: Η ομάδα G είναι αβελιανή

P_2: Η ομάδα G είναι κυκλική

P_3: Η ομάδα G είναι άπειρη

P_4: Η ομάδα G είναι πεπερασμένη

P_5: Το κέντρο της G είναι τετριμμένο.

▶ Σύμφωνα με αυτά έχουμε:

(1) $(\mathbb{Z},+) \ncong (\mathbb{Q},+)$ διότι $(\mathbb{Z},+)$ κυκλική ενώ η $(\mathbb{Q},+)$ όχι.

(2) $\underbrace{(\mathbb{Z},+)}_{\text{άπειρη}} \ncong \underbrace{(\mathbb{Z}_n,+)}_{\text{πεπερασμένη}}$, $\forall n \in \mathbb{N}$

(3) $(S_3,\circ) \ncong (\mathbb{Z}_6,+)$ διότι $(\mathbb{Z}_6,+)$ αβελιανή ενώ η $(S_3,\circ)$ όχι αβελιανή

(4) $\underbrace{(\mathbb{Z}_4,+)}_{\text{κυκλική}} \ncong \underbrace{(\mathbb{Z}_2\times\mathbb{Z}_2,+)}_{\text{μη-κυκλική}}$

Πρόταση

Έστω $f: G_1 \to G_2$ ομορφισμός ομάδων.

(i) $H \leq G_1 \Longrightarrow f(H) \leq G_2$

(ii) $K \leq G_2 \Longrightarrow f^{-1}(K) \leq G_1$

Απόδειξη

(i) Έστω $H \leq G_1$ και θα αποδείξουμε ότι $f(H) = \{ f(x) \in G_2 \mid x \in H \} \leq G_2$

Επειδή $e_1 \in H$ και $e_2 = f(e_1)$ έπεται $e_2 \in f(H)$.

Επίσης, αν $f(x), f(y) \in f(H)$ $(x, y \in H)$ τότε:

$f(x)(f(y))^{-1} = f(x) f(y^{-1}) = f(xy^{-1}) \in f(H)$ διότι:

$xy^{-1} \in H$ (αφού $x, y \in H$ και $H \leq G_1$).

Συνεπώς, $f(H) \leq G_2$.

(ii) Έστω $K \leq G_2$ και θα αποδείξουμε

$$f^{-1}(K) = \{x \in G_1 \mid f(x) \in K\} \leq G_1.$$

Επειδή $K \leq G_2$ ισχύει $e_2 \in K$, άρα

$$f(e_1) = e_2 \in K \Rightarrow e_1 \in f^{-1}(K).$$

Έστω τώρα $x, y \in f^{-1}(K)$ και θα αποδείξουμε

$xy^{-1} \in f^{-1}(K)$. Πράγματι,

$$\left.\begin{array}{l} \cdot\ x \in f^{-1}(K) \\ \cdot\ y \in f^{-1}(K) \end{array}\right\} \Rightarrow f(x), f(y) \in K. \text{ Τότε:}$$

$f(xy^{-1}) = f(x)f(y^{-1}) = f(x)(f(y))^{-1} \in K$, διότι:

$f(x), f(y) \in K$ και $K \leq G_2$.

Συνεπώς: $f(xy^{-1}) \in K \Rightarrow xy^{-1} \in f^{-1}(K)$,

όπως θέλαμε. Άρα, $f^{-1}(K) \leq G_1$.

$\blacksquare$

Ορισμός: Έστω $f: G_1 \to G_2$ μορφισμός ομάδων. Επειδή $G_1 \leq G_1$, η προηγούμενη πρόταση μας δίνει ότι η

$$\mathrm{Im}(f) = f(G_1) = \{ f(x) \in G_2 \mid x \in G_1 \} \leq G_2 .$$

↑ εικόνα της f.

Απ' την άλλη, επειδή $\{e_2\} \leq G_2$, η προηγούμενη πρόταση μας δίνει ότι η

$$\mathrm{Ker}(f) := f^{-1}(\{e_2\}) = \{ x \in G_1 \mid f(x) = e_2 \} \leq G_1$$

↑ πυρήνας της f.

Πόρισμα

Έστω $f: G_1 \to G_2$ μορφισμός ομάδων.

(α) f: μονομορφισμός $\Longleftrightarrow Ker(f) = \{e_1\}$

(β) f: επιμορφισμός $\Longleftrightarrow Im(f) = G_2$

Απόδειξη

(α) "$\Longrightarrow$" Έστω f: μονομορφισμός. Τότε η f είναι 1-1. Επειδή $\{e_1\} \subseteq Ker(f)$, αρκεί να δείξουμε ότι $Ker(f) \subseteq \{e_1\}$.

Έστω $x \in Ker(f)$. Τότε: $f(x) = e_2 \Longrightarrow$

$$f(x) = f(e_1) \xrightarrow[1-1]{f} x = e_1 \in \{e_1\}.$$

Άρα, $Ker(f) = \{e_1\}$.

"$\Longleftarrow$" Έστω $Ker(f) = \{e_1\}$ και θα δείξουμε ότι f: 1-1. Πράγματι, για κάθε $x, y \in G_1$ έχουμε:

$$f(x) = f(y) \Rightarrow f(x)(f(y))^{-1} = f(y)(f(y))^{-1}$$

$$\Rightarrow f(x)f(y^{-1}) = e_2 \Rightarrow f(xy^{-1}) = e_2 \Rightarrow$$

$$xy^{-1} \in Ker(f) \Rightarrow xy^{-1} \in \{e_1\} \Rightarrow xy^{-1} = e_1$$

$$\Rightarrow xy^{-1}y = e_1 y \Rightarrow x e_1 = y \Rightarrow x = y.$$

(β) f: επιμορφισμός $\Longleftrightarrow f(G_1) = G_2$

$$\Longleftrightarrow Im(f) = G_2$$

■

<u>Σχόλιο</u>: Οι ιδιότητες των μορφισμών ομάδων θα μας φανούν ιδιαίτερα χρήσιμες αργότερα στις έννοιες της κανονικής υποομάδας μιας ομάδας και του πρώτου Θεωρήματος Ισομορφισμών.

Ακολουθεί η ταξινόμηση των κυκλικών ομάδων.

Ταξινόμηση Κυκλικών Ομάδων

Το ακόλουθο θεώρημα μας δίνει την ταξινόμηση των κυκλικών ομάδων·

ΘΕΩΡΗΜΑ (sos): Έστω $G = \langle a \rangle$ μια κυκλική ομάδα. Τότε:

1. Αν η G είναι άπειρη, τότε
$$G \cong (\mathbb{Z}, +)$$

2. Αν η G είναι πεπερασμένη τάξης $n \in \mathbb{N}$ τότε: $G \cong (\mathbb{Z}_n, +)$

3. Δύο κυκλικές ομάδες είναι ισόμορφες αν-ν έχουν την ίδια τάξη.

Δηλαδή: $G_1 \cong G_2 \iff |G_1| = |G_2|$.

Απόδειξη

1. Θεωρούμε την απεικόνιση

$$f : (\mathbb{Z}, +) \to (G, \cdot) \text{ με } f(m) = a^m$$

Για κάθε $m, m' \in \mathbb{Z}$ έχουμε:

$f(m+m') = a^{m+m'} = a^m \cdot a^{m'} = f(m) f(m')$, οπότε

f: μορφισμός ομάδων.

▸ **f: επί**: Αν $x \in G$, τότε $x \in \langle a \rangle$, άρα υπάρχει $m \in \mathbb{Z}$ ώστε $x = a^m$ και τότε:

$$f(m) = a^m = x.$$

▸ **f: 1-1**: Έστω $m, m' \in \mathbb{Z}$ με $f(m) = f(m')$.

Τότε: $a^m = a^{m'} \Rightarrow a^{m-m'} = e$. Αν $m > m'$ τότε $m - m' \in \mathbb{N}$ και $a^{m-m'} = e$, άρα $o(a) < \infty \Rightarrow |\langle a \rangle| < \infty \Rightarrow |G| < \infty$, άτοπο.

Ομοίως καταλήγουμε σε άτοπο αν $m < m'$.

Τελικά $m = m'$. Άρα $(G, \cdot) \cong (\mathbb{Z}, +)$

2. Αφού $G = \langle a \rangle$ και $|G| = n < \infty$, έχουμε $G = \langle a \rangle = \{e, a, \ldots, a^{n-1}\}$. Ορίζουμε $\varphi : (G, \cdot) \to (\mathbb{Z}_n, +)$ με $\varphi(e) = [0]_n$, $\varphi(a) = [1]_n, \ldots, \varphi(a^{n-1}) = [n-1]_n$. Πιο γενικά, $\varphi(a^k) = [k]_n$ για $k = 0, 1, \ldots, n-1$

▶ $\underline{\underline{\varphi : \text{επί}}}$: Προφανές

▶ $\underline{\underline{\varphi : \text{μορφισμός}}}$: Για κάθε $k, \lambda \in \{0, 1, \ldots, n-1\}$ ισχύει: $\varphi(a^k \cdot a^\lambda) = \varphi(a^{k+\lambda}) = [k+\lambda]_n = [k]_n + [\lambda]_n = \varphi(a^k) + \varphi(a^\lambda)$

▶ $\underline{\underline{\varphi : 1\text{-}1}}$: Έστω $a^k, a^\lambda \in G$ με $\varphi(a^k) = \varphi(a^\lambda)$. Τότε: $[k]_n = [\lambda]_n \Rightarrow n \mid k - \lambda$, άτοπο εκτός αν $k - \lambda = 0$, δηλαδή $k = \lambda$.

Πράγματι, αν $k - \lambda \neq 0$ τότε:

$\Rightarrow a^{k-\lambda} = e \Rightarrow$

$$\left.\begin{array}{l} 0 \le k \le n-1 \\ 0 \le \lambda \le n-1 \end{array}\right\} \Rightarrow \begin{array}{r} 0 \le k \le n-1 \\ 1-n \le -\lambda \le 0 \\ \hline 1-n \le k-\lambda \le n-1 \end{array} \; (+)$$

άρα $|k-\lambda| \le n-1 < n$, δεν μπορεί να ισχύει $n \mid k-\lambda$.

Συνεπώς, $(G, \cdot) \cong (\mathbb{Z}_n, +)$.

3. Έστω G_1, G_2 δύο κυκλικές ομάδες.
Από 1. και 2. υπάρχουν οι εξής περιπτώσεις:

(α) $(G_1, \cdot) \cong (\mathbb{Z}, +) \cong (G_2, \cdot) \rightarrow |G_1| = |G_2|$

(β) $\left.\begin{array}{l} (G_1, \cdot) \cong (\mathbb{Z}, +) \\ (G_2, \cdot) \cong (\mathbb{Z}_k, +) \end{array}\right. \Rightarrow \begin{array}{l} |G_1| \neq |G_2| \\ G_1 \not\cong G_2 \end{array}$

(γ) $(G_1, \cdot) \cong (\mathbb{Z}_k, +)$, $(G_2, \cdot) \cong (\mathbb{Z}, +)$
$G_1 \not\cong G_2$, $|G_1| = |G_2|$

(δ) $(G_1, \cdot) \cong (\mathbb{Z}_\lambda, +)$, $(G_2, \cdot) \cong (\mathbb{Z}_n, +)$
$G_1 \cong G_2 \Leftrightarrow n = \lambda$.

$\blacksquare$