24-03-2016

Αν $(G,\cdot)$ είναι ομάδα, τότε: η G πεπ/νη ομάδα ή ομάδα πεπερασμένης τάξης $\Leftrightarrow |G|<\infty$

Αν $|G|=\infty$, τότε η G: άπειρη ομάδα ή ομάδα άπειρης τάξης

Αν $a\in G$, τότε η τάξη του a, ορίζεται να είναι:

$$o(a)=|\langle a\rangle|$$

Ιδιότητες

① $o(a)=\infty \Leftrightarrow \nexists\, n\in\mathbb{N} : a^n=e$

② $o(a)<\infty \Leftrightarrow \exists\, n\in\mathbb{N} : a^n=e$, κ' τότε:
$o(a)=\min\{\kappa\in\mathbb{N} \mid a^\kappa=e\}$

Παρατήρηση

① Αν $|G|<\infty$, τότε $o(a)<\infty,\ \forall a\in G$
Το αντίστροφο δεν ισχύει.

② $\forall a\in G : o(a)=o(a^{-1})$, διότι:
$\langle a\rangle=\{a^n\in G \mid n\in\mathbb{Z}\}=\{a^{-n}\in G\mid n\in\mathbb{Z}\}$
$=\{(a^{-1})^n\in G\mid n\in\mathbb{Z}\}=\langle a^{-1}\rangle$ κ' άρα:
$o(a)=|\langle a\rangle|=|\langle a^{-1}\rangle|=o(a^{-1})$

③ $o(a)=1 \Leftrightarrow a=e$

Θεώρημα:

Έστω $(G,\cdot)$ ομάδα κ' $a \in G$

① Αν $o(a)<\infty$, τότε $\forall\ k \geq 1 : a^k = e \Leftrightarrow o(a) \mid k$

② Αν $o(a)<\infty$ και $k \geq 1$, τότε:

$$o(a^k) = \frac{o(a)}{(o(a),k)}$$

Πιο σημαντικά: (1), (2)

③ Αν $o(a)<\infty$ και $k \mid o(a)$, τότε: $o(a^k) = \frac{o(a)}{k}$

④ $o(a) = o(a^k) \Leftrightarrow (o(a),k)=1$

Απόδειξη

① "$\Leftarrow$" Έστω ότι: $o(a) \mid k \Rightarrow \exists\ m \in \mathbb{N}$: $k = o(a)m$. Τότε:

$$a^k = a^{o(a)m} = (a^{o(a)})^m = e^m = e$$

"$\Rightarrow$" Έστω ότι: $a^k = e$

Από την Ευκλείδεια διαίρεση του k με την $o(a)$, θα έχουμε:

$k = o(a)\cdot q + r$, όπου είτε $r=0$ είτε $0<r<o(a)$

Τότε: $e = a^k = a^{o(a)\cdot q + r} = a^{o(a)\cdot q} a^r = (a^{o(a)})^q \cdot a^r$
$= e^q \cdot a^r = e \cdot a^r$

Αν $r>0$, τότε καταλήγουμε σε άτοπο, διότι έχουμε: $a^r = e$ κ' $r<o(a)$ και

$o(a) = \min\{m \in \mathbb{N} \mid a^m = e\}$

Άρα: $r = 0 \Rightarrow o(a) \mid k$

$a^{\kappa} \in \langle a \rangle \Rightarrow \langle a^{\kappa} \rangle \subseteq \langle a \rangle$

$\xRightarrow{|\langle a \rangle| < \infty} o(a^{\kappa}) = |\langle a^{\kappa} \rangle| \leq |\langle a \rangle| = o(a) < \infty$

β' τρόπος

$o(a) = n < \infty \Rightarrow a^n = e \Rightarrow a^m = e$

$\Rightarrow (a^{\kappa})^n = e \Rightarrow o(a^{\kappa}) < \infty$

② Έστω $o(a) = n$ και $r = o(a^{\kappa})$

Θέτουμε : $d = (o(a), \kappa) = (n, \kappa)$

Θ.δ.ο. $\boxed{r = \frac{n}{d}}$

$o(a^{\kappa}) = r \Rightarrow (a^{\kappa})^r = e \Rightarrow a^{\kappa r} = e$

$\Rightarrow o(a) = n \mid \kappa r \Rightarrow \exists\, m \in \mathbb{N} : \boxed{\kappa \cdot r = n \cdot m}$

$d = (n, \kappa) \Rightarrow \begin{cases} d \mid n \\ d \mid \kappa \end{cases} \Rightarrow \boxed{\begin{matrix} n = d \cdot n' \\ \kappa = d \cdot \kappa' \end{matrix}}$ όπου

$n', \kappa' \in \mathbb{N}$ και $\underline{(n', \kappa') = 1}$

Τότε: $\kappa \cdot r = n \cdot m \Rightarrow \cancel{d} \cdot \kappa' \cdot r = \cancel{d} \cdot n' m \Rightarrow \kappa' \cdot r = n' \cdot m$

$\left.\begin{matrix} \Rightarrow n' \mid \kappa' \cdot r \\ (n', \kappa') = 1 \end{matrix}\right\} \Rightarrow \boxed{n' \mid r}$ ①

Τότε: $(a^{\kappa})^{n'} = a^{\kappa n'}$ Όμως $\kappa = d\kappa'$ κ' τότε:

$\kappa \cdot n' = d \cdot \kappa' \cdot n' = n \cdot \kappa'$

Τότε: $a^{\kappa \cdot n'} = a^{n \cdot \kappa'} = (a^n)^{\kappa'} = e^{\kappa'} = e$

Άρα: $(a^{\kappa})^{n'} = e \xRightarrow{①} \boxed{o(a^{\kappa}) = r \mid n'}$ ②

Από τις ①, ② $\Rightarrow r = n' = \frac{n}{d} = \frac{o(a)}{(o(a), \kappa)}$

③ Αν $o(a) < \infty$ κ' $\kappa \geq 1$ με $\kappa \mid n$, τότε: $(o(a), \kappa) = \kappa$

κ' τότε από ② $\Rightarrow o(a^{\kappa}) = \frac{o(a)}{\kappa}$

④ $o(a)=o(a^{\kappa}) \overset{②}{\Longleftrightarrow} o(a)=\frac{o(a)}{(o(a),\kappa)}$

$\Leftrightarrow (o(a),\kappa)=1$

Παρατήρηση

Στο ② μπορεί το κ να είναι και αρνητικός κ' τότε: $o(a^{\kappa})=\frac{o(a)}{(o(a),|\kappa|)}$

- $\forall\ \kappa\geq 1$: $o(a^{-\kappa})=o((a^{\kappa})^{-1})=o(a^{\kappa})=\frac{o(a)}{(o(a),\kappa)}$

Πότε: $\langle b\rangle=\langle a\rangle$???

Πόρισμα

Έστω $(G,\cdot)$ μια ομάδα και $a\in G$. Έστω $\langle a\rangle$ η κυκλική υποομάδα που παράγεται από το a. Έστω $b\in\langle a\rangle$. Τότε:

① Αν $o(a)=\infty$, τότε: $\langle b\rangle=\langle a\rangle \Leftrightarrow b=a$ ή a^{-1}

② Αν $o(a)<\infty$, και $b=a^{\kappa}$, όπου $\kappa\in\mathbb{Z}$, τότε:
$\langle b\rangle=\langle a^{\kappa}\rangle=\langle a\rangle \Leftrightarrow (\kappa,o(a))=1$

Απόδειξη

① Αν $b=a$ ή $b=a^{-1}$, τότε προφανώς:
$\langle b\rangle=\langle a\rangle$

Αντίστροφα: έστω $\langle a\rangle=\langle b\rangle \Rightarrow b\in\langle b\rangle=\langle a\rangle$
$\Rightarrow b=a^{\kappa}$, για κάποιο $\kappa\in\mathbb{Z}$

- $a\in\langle a\rangle=\langle b\rangle \Rightarrow a=b^{\lambda}$ για κάποιο $\lambda\in\mathbb{Z}$. Τότε:

$a=b^{\lambda}=(a^{\kappa})^{\lambda}=a^{\kappa\lambda} \Rightarrow a^{\kappa\lambda}\cdot a^{-1}=e \Rightarrow a^{\kappa\lambda-1}=e$

$\Rightarrow \kappa\lambda-1=0 \Rightarrow \kappa=\pm1 \Rightarrow b=a$ ή a^{-1}.

$\Rightarrow \kappa\lambda-1>0 \Rightarrow o(a)<\infty$ άτοπο

$\Rightarrow \kappa\lambda-1<0 \Rightarrow a^{1-\kappa\lambda}=e$ κ' $1-\kappa\lambda>0$ κ' τότε
$o(a)<\infty$ άτοπο

Άρα: $b=a$ ή a^{-1}

② Έστω $o(a) < \infty$ και $b = a^k \in \langle a \rangle$ κ' τότε:
$\langle b \rangle = \langle a \rangle \Leftrightarrow \langle a^k \rangle \subseteq \langle a \rangle \Leftrightarrow o(a^k) = o(a)$

<u>Υπενθύμιση</u> $H \leq G$ και $|G| < \infty$
$|H| = |G| \Leftrightarrow H = G$

$\Leftrightarrow \dfrac{\cancel{o(a)}}{(k, o(a))} = \cancel{o(a)} \Leftrightarrow (|k|, o(a)) = 1$

<u>Ορισμός</u>:

Η ομάδα $(G, \cdot)$ καλείται <u>κυκλική ομάδα</u>
$\Leftrightarrow \exists\, a \in G : G = \langle a \rangle$
Κάθε στοιχείο $a \in G : G = \langle a \rangle$ καλείται
<u>γεννήτορας</u> της G

Αν $(G, \cdot)$ είναι μια κυκλική ομάδα, με γεννήτορα το $a \in G$, τότε: $G = \langle a \rangle$

① Αν $|G| = \infty$ τότε $G = \langle a \rangle = \{a^n \in G \mid n \in \mathbb{Z}\}$
και $a^k = a^\lambda \Leftrightarrow k = \lambda$

② Αν $|G| = n < \infty$, τότε: $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$

<u>Πρόταση</u>: Έστω $(G, \cdot)$ είναι μια κυκλική ομάδα με γεννήτορα το $a \in G$. Τότε
① Αν $|G| = \infty$, τότε οι μόνοι γεννήτορες της G, είναι οι: a, a^{-1}
② Αν $|G| = n < \infty$, τότε: οι γεννήτορες της G είναι a^k, όπου $1 \leq k \leq n$ $(k, n) = 1$

Το πλήθος των γεννητόρων είναι:

$$\varphi(n) = \left| \left\{ \kappa \in \mathbb{N} \;\middle|\; \begin{array}{c} 1 \le \kappa \le n \\ (\kappa, n) = 1 \end{array} \right\} \right|$$

φ: συνάρτηση του Euler

Παρατήρηση

Κάθε κυκλική ομάδα είναι αβελιανή. Το αντίστροφο γενικά δεν ισχύει.

Έστω $G = \langle a \rangle$ και $x, y \in G$. Τότε:
$x = a^{\kappa}$, $y = a^{\lambda}$, όπου $\kappa, \lambda \in \mathbb{Z}$. Τότε: $x \cdot y = a^{\kappa} a^{\lambda}$
$= a^{\kappa+\lambda} = a^{\lambda+\kappa} = a^{\lambda} a^{\kappa} = y \cdot x$
Άρα: $xy = yx$, $\forall\, x, y \in G \Rightarrow G$: αβελιανή

Η ομάδα του Klein $V_4 = \{e, a, b, c\}$ ΔΕΝ είναι κυκλική, διότι: $a^2 = b^2 = c^2 = e^2 = e$
$\Rightarrow o(e) = 1$, $o(a) = o(b) = o(c) = 2$ κ' άρα $\nexists\, x \in V_4$: $V_4 = \langle x \rangle$. Αν υπήρχε $x \in V_4$: $V_4 = \langle x \rangle$ θα έπρεπε: $o(x) = |V_4| = 4$ Άτοπο

Παράδειγμα ① Η προσθετική ομάδα $(\mathbb{Z}, +)$ είναι κυκλική με γεννήτορα το 1
$\mathbb{Z} = \langle 1 \rangle$, διότι: $\langle 1 \rangle = \{ n \cdot 1 \in \mathbb{Z} \mid n \in \mathbb{Z} \}$
$= \{ n \in \mathbb{Z} \mid n \in \mathbb{Z} \} = \mathbb{Z}$
Οι μόνοι γεννήτορες της $(\mathbb{Z}, +)$ είναι οι: $1, -1$

- $\langle a \rangle = \{ na \in G \mid n \in \mathbb{Z} \}$
- Αν $o(a) = \infty$, τότε γεννήτορες της $\langle a \rangle$ είναι: $a, -a$
- $o(\kappa a) = \dfrac{o(a)}{(o(a), |\kappa|)}$

② Για κάθε $n \geq 1$, υπάρχει τουλάχιστον μια κυκλική ομάδα με τάξη ίση με n: η προσθετική ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική με γεννήτορα: $[1]_n$

Διότι: $\langle [1]_n \rangle = \{ k[1]_n \in \mathbb{Z}_n \mid k \in \mathbb{Z} \}$
$= \{ [k]_n \in \mathbb{Z}_n \mid k \in \mathbb{Z} \}$
$= \{ [0]_n, [1]_n, \dots, [n-1]_n \} = \mathbb{Z}_n$

Οι γεννήτορες της $(\mathbb{Z}_n, +)$ είναι οι κλάσεις υπολοίπων $[k]_n$, όπου $1 \leq k \leq n$, $(k,n) = 1$ και το πλήθος τους είναι $\varphi(n)$.

③ Έστω $U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$, όπου $n \geq 1$

$U_n = \{ \cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right) \in \mathbb{C} \mid 0 \leq k \leq n-1 \}$

- $z \in \mathbb{C}$

Τύπος De Moivre

$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta)$

Τύπος του Euler

$e^{i\theta} = \cos\theta + i\sin\theta$

Η U_n είναι κυκλική με τάξη ίση με n, με γεννήτορα:

$\omega = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right)$

Τότε $U_n = \langle \omega \rangle = \{ 1, \omega, \omega^2, \dots, \omega^{n-1} \}$

Οι γεννήτορες της U_n είναι:

$\cos\left(\frac{2k\pi}{n}\right) + i\sin\left(\frac{2k\pi}{n}\right)$

$1 \leq k \leq n \qquad (k,n) = 1$