Αλγεβρικές Δομές (1) 31.03.2016

Θεώρημα: Κάθε υποομάδα μιας κυκλικής ομάδας, είναι κυκλική.

Απόδειξη: Έστω $G=\langle a\rangle$ μια κυκλική ομάδα με γεννήτορα το $a\in G$. Έστω $H\leq G$, τυχούσα υποομάδα της G. Αν $H=\{e\}$, τότε προφανώς $H=\langle e\rangle$ και άρα η H είναι κυκλική με γεννήτορα το $e=a^0$. Υποθέτουμε ότι $H\neq\{e\}$. Τότε $\exists\, x\in H$ με $x\neq e$. Τότε $x\in G=\{a^n\in G\mid n\in\mathbb{Z}\}$ και άρα $x=a^k$ για κάποιο $k\in\mathbb{Z}$. Τότε $k\neq 0$, διότι διαφορετικά θα είχαμε $x=a^0=e$: άτοπο. Αν $k<0$, τότε $x=a^k \underset{a^k\in H}{\overset{H\leq G}{\Longrightarrow}} x^{-1}=a^{-k}\in H$ και $-k>0$. Επομένως η H περιέχει θετικές δυνάμεις του a.

Έστω $n=\min\{k\in\mathbb{N}\mid a^k\in H\}$

Το n υπάρχει από την Αρχή Καλής διάταξης, αν αυτή εφαρμοσθεί στο σύνολο.

Θ.δ.ο.: $H=\langle a^n\rangle$. Επειδή εκ κατασκευής $a^n\in H\Rightarrow \langle a^n\rangle\subseteq H$ (1)

Έστω $x\in H$. Τότε $x=a^m$ για κάποιο $m\in\mathbb{Z}$. Από την Ευκλείδεια διαίρεση του m, με το n θα έχουμε:

$m=n\cdot q+r$, $r=0$ ή $0<r<n$.

$a^m=a^{n\cdot q+r}=a^{n\cdot q}a^r=(a^n)^q\cdot a^r\Rightarrow a^r=a^m\cdot a^{-nq}\Rightarrow a^r=a^{m-nq}\in H$, διότι $a^m\in H$ και $a^n\in H$ $[a^{-n}\in H\Rightarrow a^{-nq}\in H\Rightarrow a^m a^{-n\cdot q}\in H]$. Άρα

$a^r \in H$. Αν $r \neq 0$, τότε θα έχουμε ότι $a^r \in H$ και $n = \min\{k \in \mathbb{N} \mid a^k \in H\}$ το οποίο είναι άτοπο, διότι $r < n$. Άρα $r = 0 \Rightarrow m = nq$. Τότε $x = a^m = a^{n \cdot q} = (a^n)^q \in \langle a^n \rangle$.

Άρα $H \subseteq \langle a^n \rangle$ (2). Από τις (1) κ' (2) $\Rightarrow H = \langle a^n \rangle$.

Υποθέτουμε ότι $G = \langle a \rangle$ είναι μια άπειρη κυκλική ομάδα.

Έστω ότι $H \leq G$. Από το Θεώρημα $\Rightarrow H = \langle a^n \rangle$: όπου $n \geq 0$

Έστω $\langle a^n \rangle \subseteq \langle a^m \rangle$. Τότε: $a^n \in \langle a^n \rangle \subseteq \langle a^m \rangle \Rightarrow a^n \in \langle a^m \rangle$.

$\Rightarrow a^n = (a^m)^k$, για κάποιο $k \in \mathbb{Z}$. Τότε $a^n = a^{mk} \Rightarrow a^n \cdot a^{-mk} = e \Rightarrow$

$\Rightarrow a^{n-mk} = e \Rightarrow n - mk = 0$, διότι διαφορετικά:

- αν $n - mk > 0 \Rightarrow o(a)$ ... άτοπ
- αν $n - mk < 0 \Rightarrow$ $\Rightarrow a^{mk-n} = e \Rightarrow$ $\Rightarrow o(a) = o(a^{-1}) < \infty$ άτοπο

Άρα $\langle a^n \rangle \subseteq \langle a^m \rangle \Rightarrow m \mid n$

Αντίστροφα αν $m \mid n \Rightarrow n = m \cdot k$, για κάποιο $k \in \mathbb{Z}$, και τότε

$a^n = a^{mk} = (a^m)^k \in \langle a^m \rangle \Rightarrow \langle a^n \rangle \subseteq \langle a^m \rangle$. Άρα

$\langle a^n \rangle \subseteq \langle a^m \rangle \Leftrightarrow m \mid n$, $\forall m, n \geq 1$

3

<u>Ιδιαίτερα</u>: $\forall\, n,m \geq 1$: $\langle a^n \rangle = \langle a^m \rangle \Leftrightarrow n=m$

<u>Θεώρημα</u>: Οι υποομάδες μιας άπειρης κυκλικής ομάδας $G=\langle a \rangle$, είναι: $\langle a^n \rangle$: $n \geq 0$, δηλαδή: $\langle a^0 \rangle, \langle a^1 \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \dots$

Με άλλα λόγια η απεικόνιση:

$\Phi: \mathbb{N} \cup \{0\} \longrightarrow \{\text{Υποομάδες της } G\}$ είναι 1-1 κ' επί

$n \longmapsto \langle a^n \rangle = \Phi(n)$

Επιπλέον $\Phi(n) \subseteq \Phi(m) \Leftrightarrow m \mid n$

Τέλος η απεικόνιση $\Psi: \{1,-1\} \longrightarrow \{\text{Γεννήτορες της } G\}$

$n \longmapsto \Psi(n) = a^n$

είναι 1-1 κ' επί

Από τώρα και στο εξής υποθέτουμε ότι:

$G=\langle a \rangle$ είναι μια πεπερασμένη κυκλική ομάδα τάξης n

Τότε $G = \{e, a, a^2, \dots, a^{n-1}\}$

Πρόταση

1

Έστω $H \leq G$. Τότε: $H = \langle a^m \rangle$, όπου $m \geq 1$ και:

$$H = \langle a^m \rangle = \langle a^{(n,m)} \rangle \text{ και } |H| = \frac{n}{(n,m)}$$

Απόδειξη: Από το Θεώρημα $\Rightarrow \exists\, m \geq 0$, έτσι ώστε $H = \langle a^m \rangle$ $m \geq 0$ και αν $H \neq \{e\}$, τότε $m \geq 1$.

Θέτουμε $d = (n,m)$. Τότε: $d \mid m \Rightarrow \exists\, \kappa \in \mathbb{Z} : m = d \cdot \kappa$. Τότε $a^m = a^{d\cdot\kappa} = (a^d)^\kappa \in \langle a^d \rangle$. Άρα: $H \leq \langle a^d \rangle$ (1)

Επειδή $d = (n,m) \Rightarrow \exists\, x, y \in \mathbb{Z} : d = n \cdot x + my$. Τότε $a^d = a^{nx+my} = a^{nx} \cdot a^{my} = (a^n)^x \cdot (a^m)^y = e^x (a^m)^y = (a^m)^y \in \langle a^m \rangle$. Άρα: $\langle a^d \rangle \leq H$ (2)

Από τις (1) κ' (2) $\Rightarrow H = \langle a^m \rangle = \langle a^d \rangle = \langle a^{(n,m)} \rangle$

Τέλος $|H| = |\langle a^{(n,m)} \rangle| = o(a^{(n,m)}) = \dfrac{o(a)}{(o(a),(n,m))} = \dfrac{n}{(n,(n,m))} = \dfrac{n}{(n,m)}$

Πόρισμα: Αν $H \leq G$, όπου G: κυκλική τάξης $n < \infty$, τότε $|H| \mid |G|$

Απόδειξη: $G=\langle a\rangle$, όπου $o(a)=|G|=n$. Αν $H\leq G$, τότε:

1) Α $H=\{e\}\Rightarrow |H|=1 \,|\, |G|=n$

2) Αν $H\neq\{e\}\Rightarrow H=\langle a^m\rangle$, όπου $m\geq 1$. Από την ΠΡΟΤΑΣΗ $H=\langle a^{(n,m)}\rangle$ και $|H|=\dfrac{n}{(n,m)}\Rightarrow n=|H|\cdot(n,m)\Rightarrow |H|\,/\,n=|G|$

Πρόταση: Με τους παραπάνω συμβολισμούς:

$\forall\, r,s\geq 1: \langle a^r\rangle=\langle a^s\rangle \Leftrightarrow (r,n)=(s,n)$

ΑΠΟΔΕΙΞΗ: "$\Rightarrow$" Έστω $\langle a^r\rangle=\langle a^s\rangle \overset{\text{ΠΡΟΤΑΣΗ}}{\Longrightarrow}$

$\langle a^r\rangle=\langle a^{(r,n)}\rangle$,

$\langle a^s\rangle=\langle a^{(s,n)}\rangle$.

Άρα θα έχουμε $\langle a^{(r,n)}\rangle=\langle a^{(s,n)}\rangle\Rightarrow o(a^{(r,n)})=o(a^{(s,n)})\Rightarrow$

$\Rightarrow \dfrac{n}{(r,n)}=\dfrac{n}{(s,n)}\Rightarrow (r,n)=(s,n)$.

"$\Leftarrow$" Έστω ότι: $(r,n)=(s,n)\Rightarrow a^{(r,n)}=a^{(s,n)} \overset{\text{ΠΡΟΤΑΣΗ}}{\Longrightarrow} \langle a^r\rangle=\langle a^{(r,n)}\rangle$

$=\langle a^{(s,n)}\rangle=\langle a^s\rangle$

6

<u>Θεώρημα</u>: Έστω $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ μια κυκλική ομάδα τάξης n.

① $\forall m \geq 1$: η G έχει μια υποομάδα τάξης $m \iff m / n$

② Αν m/n, τότε η G έχει μοναδική υποομάδα H τάξης $H = m$, την $H = \langle a^{\frac{n}{m}} \rangle$

③ Η απεικόνιση

$$\phi : \{d \in \mathbb{N} \mid d / n = |G|\} \longrightarrow \{\text{Υποομάδες της } G\} \quad \text{είναι 1-1 και επί.}$$
$$d \longmapsto \phi(d) = \langle a^{\frac{n}{d}} \rangle$$

Επιπλέον αν d_1, d_2 είναι διαιρέτες του n, και $\langle a^{n/d_1} \rangle, \langle a^{n/d_2} \rangle$, οι αντίστοιχες κυκλικές υποομάδες της G, τότε $\langle a^{n/d_1} \rangle \leq \langle a^{n/d_2} \rangle \iff d_1 \mid d_2$.

④ Η απεικόνιση $\psi : \{k \in \mathbb{N} \mid 1 \leq k \leq n, (k,n) = 1\} \to \{\text{Γεννήτορες της } G\}$ είναι 1-1 κ' επί και άρα πλήθος γεννητόρων της G είναι $\phi(n)$

<u>Απόδειξη</u>: ① "$\Rightarrow$" Προκύπτει από το προηγούμενο πόρισμα.

"$\Leftarrow$" Έστω ~~m~~ m/n, τότε το $\frac{n}{m} \in \mathbb{N}$ και έστω $H = \langle a^{\frac{n}{m}} \rangle \leq G$. Τότε:

7

$$|H| = o\left(a^{\frac{n}{m}}\right) = \frac{o(a)}{\left(o(a), \frac{n}{m}\right)} = \frac{n}{\left(n, \frac{n}{m}\right)} = \frac{n}{\frac{n}{m}} = m$$ Άρα η

G περιέχει μια υποομάδα τάξης m.

(2) Έστω m/n και έστω $H = \langle a^r \rangle$ και $K = \langle a^s \rangle$ υποομάδες της G με $|H| = |K| = m$.

Τότε: $H = \langle a^r \rangle = \langle a^{(r,n)} \rangle$ και $K = \langle a^s \rangle = \langle a^{(s,n)} \rangle$.

Τότε $|H| = |K| \Rightarrow \frac{n}{(r,n)} = \frac{n}{(s,n)} \Rightarrow (r,n) = (s,n) \Rightarrow$

$\Rightarrow \langle a^r \rangle = \langle a^s \rangle \Rightarrow H = K$

(3): Προκύπτει άμεσα, καθώς είναι άμεσο συμπέρασμα του (2)

Επιπλέον, αν: d_1/n κι d_2/n, θα έχουμε: Έστω ότι:

$\langle a^{n/d_1} \rangle \subseteq \langle a^{n/d_2} \rangle \Leftrightarrow n/d_2 \mid n/d_1 \Leftrightarrow d_1/d_2$

(4) Έχουμε δείξει ότι: $\langle a^k \rangle = \langle a \rangle = G$, όπου $k \geq 1 \Leftrightarrow (k,n) = 1$.

Τότε προφανώς η Ψ είναι 1-1 και επί...

Διάγραμμα Hasse Υποομάδων

Πεπερασμένης κυκλικής ομάδας

Έστω $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$: κυκλική ομάδα τάξης n

① Βρίσκουμε τους θετικούς διαιρέτες του n: $d_1, d_2, \dots, d_{\tau(n)}$

② Θεωρούμε τις κυκλικές υποομάδες:

Διαιρέτες (θετικοί) του n: $d_1, d_2, d_3, \dots, d_{\tau(n)}$

Υποομάδες της G

$H_1 = \langle a^{n/d_1} \rangle$, $H_2 = \langle a^{n/d_2} \rangle$ … $H_{\tau(n)} = \langle a^{\frac{n}{d_{\tau(n)}}} \rangle$

③ Εξετάζουμε $H_i \subseteq H_j$ όπου: $H_i = \langle a^{n/d_i} \rangle$, $H_j = \langle a^{n/d_j} \rangle$ και

τότε Αυτό σημαίνει αν-ν d_i / d_j.