6° online μάθημα 15/04/2020

Σημειώσεις από αρχείο pdf του καθηγητή:

ΠΡΟΤΑΣΕΙΣ ΓΙΑ ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ

Πρόταση 1:
Έστω $G = \langle a \rangle$ πεπερασμένη κυκλική ομάδα της τάξης $n \geq 2$ και H υποομάδα της G με $H \neq \{e_G\}$.
Συμβολίζουμε με k τον ελάχιστο θετικό ακέραιο με την ιδιότητα $a^k \in H$. Τότε ο k διαιρεί το n και $H = \langle a^k \rangle$.

Απόδειξη
Ευκλείδεια Διαίρεση: $n = qk + r$ με $q, r \in \mathbb{Z}$ και $0 \leq r \leq k-1$
Έχουμε $a^n = e_G \in H$, επιπλέον $a^k \in H$, άρα $(a^k)^q \in H$.
Συνεπώς $a^{kq} \in H$.
Επομένως $a^r = a^n \cdot (a^{qk})^{-1} \in H$, γιατί H υποομάδα.
Αν $r > 0$ αντίφαση, γιατί $r < k$ και k ο ελάχιστος θετικός ακέραιος με $a^k \in H$. Συνεπώς $r = 0$, άρα ο k διαιρεί n.
Έστω τώρα $b \in H$.
Θα δείξουμε $b \in \langle a^k \rangle$.
Αφού $b \in G = \langle a \rangle$, υπάρχει $l \in \mathbb{Z}$ με $b = a^l$.
Ευκλείδεια Διαίρεση: $l = q_1 k + r_1$ με $q_1, r_1 \in \mathbb{Z}$ και
$0 \leq r_1 \leq k-1$
Αφού $a^l \in H$, $a^k \in H$, έπεται
$$a^{r_1} = (a^l) \cdot ((a^k)^{q_1})^{-1} \in H.$$
Αν $r_1 > 0$ αντίφαση, γιατί $r_1 < k$ και k ο ελάχιστος θετικός ακέραιος με $a^k \in H$.
Συνεπώς $r_1 = 0$ άρα $b = a^{q_1 k} = (a^k)^{q_1} \in \langle a^k \rangle$
Δείξαμε $H \leq \langle a^k \rangle$. Αφού $a^k \in H$ έπεται $\langle a^k \rangle \leq H$.
Σαν συνέπεια $H = \langle a^k \rangle$.

Πρόταση 2: Έστω $G = \langle a \rangle$ άπειρη κυκλική και $H \neq \{e_G\}$ υποομάδα της G. Τότε υπάρχει ακέραιος $m > 0$ με $a^m \in H$ και έστω $k > 0$ ο ελάχιστος τέτοιος ακέραιος. Τότε $H = \langle a^k \rangle$

Απόδειξη: Αφού $H \neq \{e_G\}$, υπάρχει $m_1 \in \mathbb{Z}$ με $m_1 \neq 0$ ώστε $a^{m_1} \in H$.
Αφού H υποομάδα, έπεται $(a^{m_1})^{-1} \in H$, άρα $a^{-m_1} \in H$.
Θέτουμε $m = \max(m_1, -m_1)$
Τότε $m > 0$ και $a^m \in H$.
Έστω $b \in H$. Θα δείξουμε $b \in \langle a^k \rangle$
Αφού $b \in H$, υπάρχει $l \in \mathbb{Z}$ με $b = a^l$.
Ευκλείδεια Διαίρεση: $l = qk + r$ με $q, r \in \mathbb{Z}$ και $0 \leq r \leq k-1$.
Έχουμε $a^r = a^l \cdot (a^{qk})^{-1} = a^l \cdot (a^k)^{-q} \in H$.
Αφού $r < k$, έπεται $r = 0$, γιατί k ο ελάχιστος θετικός ακέραιος ώστε $a^k \in H$. Συνεπώς, $b = a^l = (a^k)^q \in \langle a^k \rangle$
Άρα $H \subseteq \langle a^k \rangle$. Αφού $a^k \in H$ έχουμε $\langle a^k \rangle \subseteq H$.
Σαν συνέπεια $H = \langle a^k \rangle$

Πρόταση 3: Έστω $n \geq 2$ ακέραιος, $d \geq 1$ θετικός διαιρέτης του n και $l \geq 1$ ακέραιος
Τότε $\text{ΜΚΔ}\left(l\frac{n}{d}, n\right) = \frac{n}{d}$ αν-ν $\text{ΜΚΔ}(l, d) = 1$

Απόδειξη:
Από Θ. Αριθμών $\text{ΜΚΔ}(ab, ac) = a\,\text{ΜΚΔ}(b, c)$ όπου $a, b, c \in \mathbb{Z}$.
Συνεπώς $\text{ΜΚΔ}\left(l\frac{n}{d}, n\right) = \text{ΜΚΔ}\left(l \cdot \frac{n}{d}, d \cdot \frac{n}{d}\right) = \frac{n}{d}\,\text{ΜΚΔ}(l, d)$

Άρα $\text{ΜΚΔ}\left(l\frac{n}{d}, n\right) = \frac{n}{d} \Leftrightarrow \text{ΜΚΔ}(l, d) = 1$

Πρόταση 4:

Έστω $G = \langle a \rangle$ πεπερασμένη κυκλική τάξη $n \geq 2$ και d θετικός διαιρέτης του n. Το σύνολο των στοιχείων της G τάξης d είναι το εξής:

$$\{a^{n/d \cdot l} : 1 \leq l \leq d \text{ και } ΜΚΔ(l,d) = 1\}$$

και έχει πλήθος στοιχείων $\varphi(d)$, όπου φ η συνάρτηση Euler.

Απόδειξη

Ξέρουμε $G = \{a, a^2, \dots, a^n\}$

Έστω k με $1 \leq k \leq n$

Ξέρουμε $ord(a^k) = \dfrac{n}{ΜΚΔ(k,n)}$

Συνεπώς $ord(a^k) = d \Leftrightarrow \dfrac{n}{ΜΚΔ(k,n)} = d \Leftrightarrow \dfrac{n}{d} = ΜΚΔ(k,n)$

Άρα υπάρχει l με $1 \leq l \leq d$ (γιατί $1 \leq k \leq n$) ώστε $k = l\dfrac{n}{d}$. Επιπλέον από Πρόταση 3

$ΜΚΔ(l\frac{n}{d}, n) = \frac{n}{d}$ αν-ν $ΜΚΔ(l,d) = 1$

Το αποτέλεσμα έπεται.

Επίσης από Βιβλίο: «Θεωρία Ομάδων» του Νίκου Μαρμαρίδη

Σελίδες: 84-86: Από Πρόταση 1.5.12 μέχρι την Πρόταση 1.5.16.

ΟΧΙ: το παράδειγμα 1.5.15.