16/4/2018

Υπενθύμιση: Αν G ομάδα, $a \in G$ με $ord(a) = n < \infty$ και $s \in \mathbb{Z}$, δείξαμε $ord(a^s) = \dfrac{n}{ΜΚΔ(n, s)}$

ΥΠΟΟΜΑΔΕΣ ΚΥΚΛΙΚΗΣ ΟΜΑΔΟΣ

ΕΡΩΤΗΜΑ: Έστω G ομάδα. Περιγράψτε όλες τις υποομάδες της G.

ΠΑΡΑΤΗΡΗΣΗ: Γενικά δύσκολο ερώτημα.

Για την $(S_3, \circ)$ το κάναμε. Τώρα θα κάνουμε για G κυκλική.

ΠΕΡΙΠΤΩΣΗ 1 Πεπερασμένη κυκλική.

ΠΡΟΤΑΣΗ Έστω G πεπερασμένη κυκλική με τάξη $|G| = n < \infty$ και $a \in G$ με $G = \langle a \rangle$.

Ορίζουμε ψ: Θετικούς διαιρέτες του n $\longrightarrow$ υποομάδες της G

με $\psi(d) = \langle a^d \rangle$.

Τότε η ψ είναι 1-1 και επί.

Άρα,

1) Κάθε υποομάδα της G είναι κυκλική

2) Για κάθε διαιρέτη h του n υπάρχει ακριβώς μια υποομάδα της G τάξης h, η υποομάδα $\langle a^{\frac{n}{h}} \rangle$

ΠΑΡΑΔΕΙΓΜΑ 1

$G = \langle a \rangle$, $ord(a) = 2$ Θετικοί διαιρέτες του 2 είναι οι 1, 2. Άρα η G έχει δύο υποομάδες την $\langle a^1 \rangle = \langle a \rangle = G$ και την $\langle a^2 \rangle = \langle e \rangle = \{e\}$

2. $G = \langle a \rangle$, $ord(a) = 3$ Θετικοί διαιρέτες του 3 είναι οι 1, 3. Άρα η G έχει 2 υποομάδες την $\langle a^1 \rangle = \langle a \rangle = G$ και την $\langle a^3 \rangle = \langle e \rangle = \{e\}$

3. Γενικά αν $G = \langle a \rangle$ και $ord(a) = p$ πρώτος οι μόνοι θετικοί διαιρέτες του p είναι $1, p$ και η G έχει ακριβώς δύο υποομάδες την $G = \langle a^1 \rangle = \langle a \rangle$ και την $\{e\} = \langle a^p \rangle$

4. Έστω $G = \langle a \rangle$ και $\#G = 4$.

(Άρα $ord(a) = 4$) Αφού οι θετικοί διαιρέτες του 4 είναι $1, 2, 4$ η G έχει ακριβώς 3 υποομάδες τις εξής:

$H_1 = \langle a^1 \rangle = \langle a \rangle = G$ $\quad$ $H_2 = \langle a^2 \rangle$

$H_3 = \langle a^4 \rangle = \langle e \rangle = \{e\}$

Η H_1 έχει τάξη 4, η H_2 έχει τάξη $\frac{4}{2} = 2$, η H_3 έχει τάξη 1.

5) Έστω $G = \langle a \rangle$ και $\#G = 30$ (Άρα $ord(a) = 30 = 2 \cdot 3 \cdot 5$) Τότε οι θετικοί διαιρέτες του 30 είναι $2^a \cdot 3^b \cdot 5^c$ με $0 \leq a, b, c \leq 1$.

ΠΙΝΑΚΑΣ ΥΠΟΟΜΑΔΩΝ

d	ΥΠΟΟΜΑΔΑ	ΤΑΞΗ ΥΠΟΟΜΑΔΑΣ
1	$\langle a^1 \rangle = G$	$30 = \frac{30}{d}$
2	$\langle a^2 \rangle$	15
3	$\langle a^3 \rangle$	10
5	$\langle a^5 \rangle$	6
6	$\langle a^6 \rangle$	5
10	$\langle a^{10} \rangle$	3
15	$\langle a^{15} \rangle$	2
30	$\langle a^{30} \rangle = \{e\}$	1

ΑΠΟΔΕΙΞΗ ΠΡΟΤΑΣΗΣ

ΒΗΜΑ 1 Έστω $d|n$, $d \geq 1$. Τότε $ord(a^d) = \frac{n}{ΜΚΔ(d,n)} = \frac{n}{d}$

ΒΗΜΑ 2 Έστω H υποομάδα της G. Θέτουμε $s = \#G$. Από Θ. Lagrange $s|n$. Θα δείξουμε ότι $H = \langle a^{n/s} \rangle$

Ξέρουμε ότι αφού $G = \langle a \rangle$ και $|G| = n$, έχουμε $G = \{a^1, a^2, \ldots, a^n = e\}$

Έστω r ο ελάχιστος θετικός ακέραιος με $a^r \in H$.

ΙΣΧΥΡΙΣΜΟΣ 1. $H = \langle a^r \rangle$

ΑΠΟΔΕΙΞΗ Αν δεν ισχύει,

τότε υπάρχει l με $1 \le l \le n$ ώστε
$a^l \in H$ και $a^l \notin \langle a^r \rangle$. Άρα $r \nmid l$.
Κάνουμε Ευκλείδια Διαίρεση του l με το r.
Άρα υπάρχουν $q_1, q_2 \in \mathbb{Z}$ με $0 < q_2 < r$ ώστε

$$l = q_1 r + q_2 \implies l + (-q_1) \cdot r = q_2$$

$$\implies a^{q_2} = a^{l + (-q_1) r} = a^l \cdot (a^r)^{(-q_1)} \in H.$$

αντίφαση του ορισμού του r αφού $q_2 < r$

ΙΣΧΥΡΙΣΜΟΣ 2 $H = \langle a^{n/s} \rangle$

ΑΠΟΔΕΙΞΗ Έχουμε $H = \langle a^r \rangle$ από Ισχυρ. 1. Άρα
$ord(a^r) = \# H = s \implies \frac{n}{ΜΚΔ(n,r)} = s \implies$

$ΜΚΔ(n,r) = \frac{n}{s}$

Συνεπώς $\frac{n}{s} \mid r$. Άρα υπάρχει $l \in \mathbb{Z}$ με

$$r = \frac{n}{s} \cdot l \implies a^r = a^{\frac{n}{s} \cdot l} = (a^{\frac{n}{s}})^l \implies$$

$$a^r \in \langle a^{n/s} \rangle \implies H \subseteq \langle a^{n/s} \rangle \; (*)$$

Αλλά $\# H = s = \# \langle a^{n/s} \rangle$
Συνεπώς $(*) \implies H = \langle a^{n/s} \rangle$

ΟΡΙΣΜΟΣ Έστω H υποομάδα της ομάδας G.
Ορίζουμε ΔΕΙΚΤΗ της H στην G, και συμβολίζουμε $[G:H]$ τον αριθμό των αριστερών πλευρικών κλάσεων της H στην G. Αυτός ο αριθμός μπορεί να είναι θετικός ακέραιος ή ∞.

ΠΡΟΤΑΣΗ Έστω πεπερασμένη ομάδα και H υποομάδα της G. Τότε ο δείκτης $[G:H]$ της H στην G είναι ίσος με $\frac{|G|}{|H|}$, δηλ. $[G:H] = \frac{|G|}{|H|}$

ΑΠΟΔΕΙΞΗ Έχουμε δει (στην απόδειξη του Θ. Lagrace) ότι η G είναι η ξένη ένωση των αριστερών πλευρικών κλάσεων της H στην G και ότι κάθε αριστερή πλευρική κλάση της H στην G έχει αριθμό στοιχείων ίσων με $|H|$. Το αποτέλεσμα έπεται.

ΠΑΡΑΔΕΙΓΜΑ Αν $|G|=75$ και $|H|=5$ τότε από την Πρόταση $[G:H] = \frac{|G|}{|H|} = \frac{75}{5} = 15$

ΠΑΡΑΤΗΡΗΣΗ Έστω $G=(\mathbb{Z},+)$, $n \geq 1$ ακέραιος και $H = n\mathbb{Z} = \langle n \rangle = \{kn : k \in \mathbb{Z}\} \leq G$

Φανερά, G άπειρη ομάδα, άρα η Πρόταση δεν εφαρμόζεται

$\hookrightarrow [G:H] = \frac{|G|}{|H|}$

Εύκολα βλέπουμε ότι το σύνολο των αριστερών πλευρικών κλάσεων της H στην G είναι {κλάση του 1, κλάση του 2, ..., κλάση του n}

Άρα $[G:H] = n$

ΠΡΟΤΑΣΗ (ΥΠΟΟΜΑΔΕΣ ΑΠΕΙΡΗΣ ΚΥΚΛΙΚΗΣ)

Έστω $G = \langle a \rangle$ άπειρη κυκλική. (Άρα $ord(a) = +\infty$) Ορίζουμε

Φ: Μη αρνητικούς ακέραιους

$\longrightarrow$ Υποομάδες της G. με $\Phi(d) = \langle a^d \rangle$

Τότε Φ είναι 1-1 και επί. Επίσης, για $d \geq 0$ ακέραιο. $[G : \langle a^d \rangle] = \begin{cases} \infty, & \text{αν } d=0 \\ d, & \text{αν } d \geq 1. \end{cases}$

Άρα: 1 Κάθε υποομάδα της G είναι κυκλική.

2. Αν $d=0$ $\langle a^d \rangle = \langle a^0 \rangle = \langle e \rangle = \{e\}$ που έχει άπειρο δείκτη στην G. Αν $d \geq 1$ υπάρχει μοναδική ΥΠΟΟΜΑΔΑ H της G με δείκτη d, η εξής $H = \langle a^d \rangle$

3. Αν $d \geq 1$ $|\langle a^d \rangle| = +\infty$ (Γιατί αν $k>0$ αφού $|\langle a \rangle| = \infty$, $(a^d)^k = a^{dk} \neq e_G$

ΠΟΡΙΣΜΑ Για $G=(\mathbb{Z},+)$ έχουμε:

1) Αν H υποομάδα του G τότε υπάρχει $d \in \mathbb{Z}$ $d \geq 0$ με $H = \langle d \rangle = d\mathbb{Z} = \{k \cdot d : k \geq 0\}$

2) Αν $d_1, d_2 \geq 0$ και $d_1 \neq d_2$ τότε $d_1\mathbb{Z} \neq d_2\mathbb{Z}$

Απόδειξη ΠΟΡΙΣΜΑΤΟΣ Άμεσο από την πρόταση γιατί $(\mathbb{Z},+)$ άπειρη κυκλική με γεννήτορα το $1_\mathbb{Z}$.

Απόδειξη ΠΡΟΤΑΣΗΣ. Έστω $G = \langle a \rangle$ άπειρη κυκλική και H υποομάδα της G. Αν $H=\{e\}$, τότε $H = \langle a^0 \rangle = \Phi(0)$. Υποθέτουμε $H \neq \{e\}$. Άρα υπάρχει $s \in \mathbb{Z} \setminus \{0\}$ με $a^s \in H$. Αφού H υποομάδα $(a^s)^{-1} = a^{-s} \in H$. Άρα υπάρχει $s>0$ με $a^s \in H$.
Θέτουμε $r =$ ο ελάχιστος θετικός ακέραιος s με $a^s \in H$

ΙΣΧΥΡΙΣΜΟΣ. $H = \langle a^r \rangle$

ΑΠΟΔΕΙΞΗ ΙΣΧΥΡΙΣΜΟΥ Αφού $a^r \in H \Longrightarrow$

$\langle a^r \rangle \subseteq H$

Υποθέτουμε ότι $H \setminus \langle a^r \rangle \neq \emptyset$. Άρα υπάρχει $l \in \mathbb{Z}$ με $r \nmid l$ ώστε $a^l \in H$. Εφαρμόζουμε Ευκλείδια διαίρεση του l με το r. Άρα υπάρχουν $q_1, q_2 \in \mathbb{Z}$ με $0 < q_2 < l$ ώστε $l = q_1 r + q_2 \Rightarrow l + (-q_1) r = q_2$
Άρα $a^{q_2} = a^{l+(-q_1)r} = a^l * (a^r)^{-q_1} \in H$

αντίφαση στον ορισμό του r αφού $0 < q_2 < r$

<u>ΙΣΧΥΡΙΣΜΟΣ 2</u> Έστω $d > 0$. Τότε $[G : \langle a^d \rangle] = d$

<u>ΑΠΟΔΕΙΞΗ</u> Θέτουμε $H = \langle a^d \rangle$ Θεωρούμε το σύνολο

$\{a * H, a^2 * H, \ldots, a^d * H = H\}$

Τότε $G =$ ξένη ένωση $a * H \cup a^2 * H \cup \ldots \cup a^d * H$.
γιατί αν $a^r \in G$ και κάνουμε διαίρεση:
$r = q_1 d + q_2$ με $0 \leq q_2 < d$ τότε $a^r = a^{q_2 + q_1 d} =$

$a^{q_2} \cdot (a^d)^{q_1} \in a^{q_2} * H$ και αν $1 \leq d_1, d_2 \leq d$ με $d_1 \neq d_2$
έστω $d_1 < d_2$, έχουμε $a^{d_1} * H \neq a^{d_2} * H$, γιατί
αλλιώς $a^{d_2 - d_1} \in H$ αντίφαση στο $H = \langle a^d \rangle$)

Επομένως $[G : \langle a^d \rangle] = d$
Άρα για $d_1 \neq d_2$ με $d_1, d_2 \geq 0$ $\langle a^{d_1} \rangle \neq \langle a^{d_2} \rangle$,
γιατί έχουν διαφορετικό δείκτη στην G. Συνεπώς
Φ 1-1 και επί.

<u>ΣΥΜΠΕΡΑΣΜΑ</u> Τώρα ξέρουμε όλες τις υποομάδες μιας (πεπερασμένης ή άπειρης) κυκλικής ομάδος.

ΕΥΘΥ ΓΙΝΟΜΕΝΟ ΟΜΑΔΩΝ

Έστω $n \geq 2$ ακέραιος και $(G_1, *_1), (G_2, *_2), \ldots, (G_n, *_n)$
n ομάδας Θεωρούμε το καρτεσιανό γινόμενο
$G = G_1 * G_2 * \ldots * G_n = \{(a_1, a_2, \ldots, a_n) : a_i \in G_i\}$
Ορίζουμε πράξη $*$ στον G ως εξής:

$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) =$

$(a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n)$

<u>ΛΗΜΜΑ</u> Η $(G, *)$ είναι ομάδα που λέγεται ευθύ γινόμενο των ομάδων $G_1, G_2, \ldots, G_n$. Επιπλέον έχει ουδέτερο στοιχείο το $e_G = (e_{G_1}, e_{G_2}, \ldots, e_{G_n})$ και ισχύει

$(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$

όπου a_i^{-1} είναι το αντίστροφο του a_i στην ομάδα G

<u>ΑΠΟΔΕΙΞΗ</u> Προσεταιριστικότητα

$$((a_1, \ldots, a_n) * (b_1, \ldots, b_n)) * (c_1, \ldots, c_n) =$$

$$(a_1 *_1 b_1, a_2 *_2 b_2, \ldots, a_n *_n b_n) * (c_1, \ldots, c_n) =$$

Αφού κάθε $(G_i, *_i)$ προσ.

$$((a_1 *_1 b_1) *_1 c_1, (a_2 *_2 b_2) *_2 c_2, \ldots, (a_n *_n b_n) *_n c_n) =$$

$$(a_1 *_1 (b_1 *_1 c_1), a_2 *_2 (b_2 *_2 c_2), \ldots, a_n *_n (b_n *_n c_n)) =$$

$$(a_1, a_2, \ldots, a_n) * ((b_1, \ldots, b_n) * (c_1, \ldots, c_n))$$

<u>ΙΣΧΥΡΙΣΜΟΣ</u> $e_G = (e_{G_1}, e_{G_2}, \ldots, e_{G_n}) \in G$ ουδέτερο.

<u>ΑΠΟΔΕΙΞΗ</u> $e_G * (a_1, \ldots, a_n) = (e_{G_1} *_1 a_1, e_{G_2} *_2 a_2, \ldots, e_{G_n} *_n a_n)$
$= (a_1, a_2, \ldots, a_n)$ και

$(a_1, \ldots, a_n) * e_G = (a_1 *_1 e_{G_1}, \ldots, a_n *_n e_{G_n}) = (a_1, \ldots, a_n)$

<u>ΙΣΧΥΡΙΣΜΟΣ</u> Έστω $(a_1, \ldots, a_n) \in G$. Τότε έχει αντίστροφο το $(a_1^{-1}, \ldots, a_n^{-1})$

<u>ΑΠΟΔΕΙΞΗ</u> $(a_1, \ldots, a_n) *_1 (a_1^{-1}, \ldots, a_n^{-1}) =$

$(a_1 *_1 a_1^{-1}, a_2 *_2 a_2^{-1}, \ldots, a_n *_n a_n^{-1}) = (e_{G_1}, e_{G_2}, \ldots, e_{G_n}) = e_G$

και $(a_1^{-1}, \ldots, a_n^{-1}) * (a_1, \ldots, a_n) =$

$(a_1^{-1} *_1 a_1, \ldots, a_n^{-1} *_n a_n) = (e_{G_1}, e_{G_2}, \ldots, e_{G_n}) = e_G$

Άρα $(G, *)$ ομάδα.

υποθέτοντας ότι κάθε G_i πεπερασμένη ομάδα;

<u>ΑΠΑΝΤΗΣΗ</u> Από Θ. Συνόλων $|G| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$

<u>ΠΑΡΑΤΗΡΗΣΗ</u> Αν κάθε $G_1, \ldots, G_n$ αβελιανή, τότε

$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 * b_1, a_2 * b_2, \ldots, a_n * b_n) =$

Αφού G_i αβελ.

$(b_1 *_1 a_1, b_2 *_2 a_2, \ldots, b_n *_n a_n) = (b_1, \ldots, b_n) * (a_1, \ldots, a_n)$

Άρα $G = G_1 * \ldots * G_n$ αβελιανή

Αντίστροφα, αν $G = G_1 * G_2 * \ldots * G_n$ αβελιανή τότε κάθε $(G_i, *_i)$ είναι αβελιανή.

<u>ΑΠΟΔΕΙΞΗ</u> Έστω G αβελιανή. Έστω $i \geq 1$ και $a_i, b_i \in G_i$ τότε $(e_{a_1}, \ldots, e_{a_{i-1}}, a_i, e_{a_{i+1}}, \ldots, e_{a_n}) *$

$(e_{a_1}, \ldots, e_{a_{i-1}}, b_i, e_{a_{i+1}}, \ldots, e_{a_n}) =$

$(e_{a_1}, \ldots, e_{a_{i-1}}, b_i, e_{a_{i+1}}, \ldots, e_{a_n}) * (e_{a_1}, \ldots, e_{a_{i-1}}, a_i, e_{a_{i+1}}, \ldots, e_{a_n})$

$\Leftrightarrow (e_{a_1}, \ldots, e_{a_{i-1}}, a_i * b_i, e_{a_{i+1}}, \ldots, e_{a_n}) = (e_{a_1}, \ldots, e_{a_{i-1}}, b_i *_i a_i,$

$e_{a_{i+1}}, \ldots, e_{a_n}) \Rightarrow a_i *_i b_i = b_i *_i a_i \Rightarrow G_i$ αβελιανή.

<u>ΣΥΜΠΕΡΑΣΜΑ</u> Δείξαμε $G_1 * G_2 * \ldots * G_n$ αβελιάνη ομάδα αν και μόνο αν κάθε G_i, $i = 1, 2, \ldots, n$ είναι αβελιανή ομάδα.

<u>ΕΡΩΤΗΜΑ</u> Έστω G_1, G_2 πεπερασμένες ομάδες και $(a,b) \in G_1 * G_2$. Τι τάξη έχει το (a,b);

<u>ΠΡΟΤΑΣΗ</u> Έστω G_1, G_2 πεπερασμένες ομάδες και $(a,b) \in G_1 * G_2$. Τότε $ord(a,b) =$ Ε.Κ.Π. $(ord(a), ord(b))$

όπου Ε.Κ.Π. συμβολίζει το ελάχιστο κοινό πολλαπλάσιο.

ΑΠΟΔΕΙΞΗ Θέτουμε $d_1 = ord(a,b)$,

$d_2 = Ε.Κ.Π.(ord(a), ord(b))$

ΙΣΧΥΡΙΣΜΟΣ 1 $d_2 | d_1$

ΑΠΟΔΕΙΞΗ $(a,b)^{d_1} = e_G \Rightarrow (a^{d_1}, b^{d_1}) = (e_{G_1}, e_{G_2}) \Rightarrow$

$\begin{cases} a^{d_1} = e_{G_1} \\ \text{και} \\ a^{d_2} = e_{G_2} \end{cases} \Rightarrow ord(a) | d_1$ και $ord(b) | d_1 \Rightarrow$

d_1 κοινό πολλαπλάσιο των $ord(a)$ και $ord(b) \Rightarrow d_2 | d_1$

ΙΣΧΥΡΙΣΜΟΣ 2 $d_1 | d_2$

ΑΠΟΔΕΙΞΗ ΙΣΧΥΡΙΣΜΟΥ 2 Υπάρχουν $l_1, l_2 \in \mathbb{Z}$

με $d_2 = l_1 \cdot ord(a)$

Άρα $(a,b)^{d_2} = (a^{d_2}, b^{d_2}) = (a^{l_1 \cdot ord(a)}, b^{l_2 ord(b)})$

$= ((a^{ord(a)})^{l_1}, (b^{ord(b)})^{l_2}) = (e_{G_1}, e_{G_2}) = e_G$

Άρα $d_1 | d_2$

Από Ισχυρ. 1 και 2 $\Rightarrow d_1 = d_2$

ΠΑΡΑΔΕΙΓΜΑ Έστω $G_1 = \langle a \rangle$ με $ord(a) = 2$

$G_2 = \langle b \rangle$ με $ord(b) = 3$

ΕΡΩΤΗΜΑ 1 Πόσα στοιχεία έχει η $G = G_1 * G_2$

ΑΠΑΝΤΗΣΗ $|G| = |G_1 * G_2| = |G_1| \cdot |G_2| = 2 \cdot 3 = 6$

ΕΡΩΤΗΜΑ 2 $ord((a,b)) = ;$

ΑΠΑΝΤΗΣΗ $ord((a,b)) = Ε.Κ.Π.(ord(a), ord(b)) =$

$Ε.Κ.Π.(2,3) = 6$. Άρα G κυκλική τάξης 6, γιατί βρήκαμε στοιχείο (a,b) με τάξη ίση με την τάξη της G.

ΠΑΡΑΔΕΙΓΜΑ 2 Έστω $G_1 = \langle a \rangle$, $G_2 = \langle b \rangle$ με

$ord(a) = ord(b) = 2$ και $G = G_1 * G_2$

ΙΣΧΥΡΙΣΜΟΣ 1 $|G| = |G_1 * G_2| = |G_1| \cdot |G_2| = 4$

Έχουμε $G_1 = \{e_{G_1}, a\}$ $G_2 = \{e_{G_2}, b\}$

Άρα $G = \{(e_{G_1}, e_{G_2}), (e_{G_1}, b), (a, e_{G_2}), (a,b)\}$

Έχουμε $ord((e_{G_1}, e_{G_2})) = ΕΚΠ(1,1) = 1$.

$ord((e_{G_1}, b)) = ΕΚΠ(1,2) = 2$.

$ord((a, e_{G_2})) = ΕΚΠ(2,1) = 2$

$ord((a,b)) = ΕΚΠ(2,2) = 2$

ΣΥΜΠΕΡΑΣΜΑ Η $G = G_1 * G_2$ είναι αβελιανή τάξης 4 αλλά δεν είναι κυκλική, γιατί δεν έχει στοιχείο τάξης 4.