28/3/2019

Θεώρημα Lagrace: i) Αν G πεπερασμένη ομάδα και H υποομάδα της G τότε $\#H \mid \#G$

ΠΟΡΙΣΜΑ Αν G πεπερασμένη ομάδα και $a \in G$ τότε $ord(a) \mid \#G$

ΕΦΑΡΜΟΓΗ 1 Έστω G ομάδα με $|G| = 11$. Έστω H υποομάδα της G. Απο Θ. Lagrace $\#H \mid \#G = 11$. Άρα $\#H = 1 \Rightarrow H = \{e\}$ ή $\#H = 11 \Rightarrow H = G$
Πιο γενικά, αν $\#G = p$, p πρώτος οι μόνες υποομάδες της είναι η $\{e\}$ και η G.

ΕΦΑΡΜΟΓΗ 2 Η ομάδα $(S_3, \circ)$ έχει $|S_3| = 6$. Άρα αν H υποομάδα της G, $\#H \mid 6$. Άρα $\#H \neq 4$ και $\#H \neq 5$

ΕΦΑΡΜΟΓΗ 3 Έστω $a \in (S_6, \circ)$. Τότε $ord(a) \mid \#S_6 =$

$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 2^4 \cdot 3^2 \cdot 5$

Άρα υπάρχουν $a, b, c \in \mathbb{Z}$ με $0 \leq a \leq 4$, $0 \leq b \leq 2$, $0 \leq c \leq 1$ ώστε $ord(a) = 2^a \cdot 3^b \cdot 5^c$
π.χ. Αδύνατον η τάξη του a να είναι 7, αδύνατον $ord(a) = 25$, αδύνατον $ord(a) = 2^5$

ΟΡΙΣΜΟΣ Έστω $(G, *)$ ομάδα, H υποομάδα της G και $a \in G$.
1) Το $a * H = \{a * h \mid h \in H\}$ λέγεται μία αριστερή πλευρική κλάση της H στην G που περιέχει το a.
2) Το $H * a = \{h * a \mid h \in H\}$ λέγεται η δεξία πλευρική κλάση της G που περιέχει το a.

ΠΑΡΑΤΗΡΗΣΗ Η πλευρική κλάση λέγεται και σύμπλοκο

ΠΑΡΑΔΕΙΓΜΑ $G = (\mathbb{Z}, +)$, $H = \langle 4 \rangle = 4\mathbb{Z} = \{4k : k \in \mathbb{Z}\}$
Για $a = 0$ $a + H = \{0 + h : h \in H\} = H =$ τα πολλαπλάσια του 4.

$a=1$ $\quad a+H = \{1+h : h\in H\} = \{1+4k : k\in \mathbb{Z}\} =$

{οι ακέραιοι που είναι ισότιμοι 1 modulo 4}

Για $a=2$ $\quad a+H = \{2+h : h\in H\} = \{2+4k : k\in \mathbb{Z}\} =$

{οι ακέραιοι που είναι ισότιμοι 2 modulo 4}

$a=3$ $\quad a+H = \{3+h : h\in H\} = \{3+4k : k\in \mathbb{Z}\} =$

{οι ακέραιοι που είναι ισότιμοι 3 modulo 4}

Βλέπουμε: 1) Αν $a,b \in \{0,1,2,3\}$ με $a\neq b$ τότε
$a+H \cap b+H = \emptyset$

2) $\mathbb{Z} = \bigcup_{a\in\{0,1,2,3\}} (a+H)$. Άρα τα αριστερά σύμπλοκα

$H, 1+H, 2+H, 3+H$ είναι <u>διαμέριση</u> του $\mathbb{Z}$.

<u>Διαμέριση</u>: ανά δύο κενή τομή, και η ένωση τους όλο το $\mathbb{Z}$.

<u>ΠΡΟΤΑΣΗ</u> Αν G ομάδα, H υποομάδα και $a\in G$. Η απεικόνιση $\phi : H \longrightarrow a*H$
$\phi(h) = a*h$ είναι καλά ορισμένη 1-1 και επί.

<u>ΑΠΟΔΕΙΞΗ</u> Καλά ορισμένο άμεσο απ' τον ορισμό του $a*H$. Επί « « « « « « $a*H$

1-1: Έστω $\phi(h) = \phi(h') \Rightarrow a*h = a*h'$ στην G.
$\Rightarrow h=h'$ αφού G ομάδα.

<u>Θεώρημα Lagrace</u>. Έστω G πεπερασμένη ομάδα και H υποομάδα της G. Τότε $\#H \mid \#G$

ΑΠΟΔΕΙΞΗ

ΙΣΧΥΡΙΣΜΟΣ 1 Έστω $a, b \in G$. Αν $a*H \cap b*H \neq \emptyset$ τότε $a*H = b*H$.

Δηλαδή δύο αριστερές πλευρικές κλάσεις ή ταυτίζονται ή έχουν τομή το κενό.

ΑΠΟΔΕΙΞΗ Έστω $c \in a*H \cap b*H$. Τότε $c \in a*H$. Άρα υπάρχει $h \in H$ με $c = ah$ (*), άρα αν $h_1 \in H$ $ch_1 = ahh_1 = a(hh_1) \in a*H$, αφού H υποομάδα. Άρα $c*H \subseteq a*H$

Η (*) $\Rightarrow$ $a = c*h^{-1}$ (**) και $h^{-1} \in H$ γιατί H υποομάδα.
Η (**) $\Rightarrow$ $a*H \subseteq c*H$ (2)
Άρα (1)+(2) $\Rightarrow$ $a*H = c*H$
Από συμμετρία έχουμε και $b*H = c*H$. Άρα $a*H = b*H$.

ΙΣΧΥΡΙΣΜΟΣ 2 Αν $a \in G \Rightarrow a \in a*H$.

ΑΠΟΔΕΙΞΗ Αφού H υποομάδα, $e_G \in H$. Άρα $a = a*e_G \in a*H$

Από Ισχυρ. 1 και Ισχυρ. 2, αφού G πεπερασμένη, υπάρχουν $a_1, \dots, a_r \in G$ ώστε G = ξένη ένωση $a_1*H, a_2*H, \dots, a_r*H$.

Άρα $|G| = |a_1*H| + |a_2*H| + \dots + |a_r*H| \overset{\text{ΠΡΟΤΑΣΗ}}{=} |H| + |H| + \dots + |H| \Rightarrow |G| = r|H| \Rightarrow |H| \mid |G|$

ΠΡΟΣΟΧΗ Γενικά δεν ισχύει αν G πεπερασμένη ομάδα και $d \mid \#G$, τότε υπάρχει υποομάδα H της G τάξης d.
(Το παράδειγμα είναι η "ομάδα A_4" που έχει τάξη 12 και δεν έχει υποομάδα τάξης 6.)

ΠΟΡΙΣΜΑ Αν G πεπερασμένη ομάδα και $a \in G$, τότε $\mathrm{ord}(a) \mid |G|$

ΑΠΟΔΕΙΞΗ Από ορισμό $\mathrm{ord}\, a = \# \langle a \rangle$. Άρα από Θ. Lagrance $\mathrm{ord}(a) = \# \langle a \rangle \mid |G|$

ΠΡΟΣΟΧΗ Γενικά δεν ισχύει αν G πεπερασμένη ομάδα και $d \mid |G|$ τότε υπάρχει $a \in G$ με $\mathrm{ord}(a) = d$

ΑΠΟΔΕΙΞΗ 1 Έστω G πεπερασμένη μη αβελιανή ομάδα π.χ. $G = (S_3, \circ)$

ΙΣΧΥΡΙΣΜΟΣ Δεν υπάρχει $a \in G$ με $\mathrm{ord}(a) = |G|$

ΑΠΟΔ. Αν υπήρχε $a \in G$ με $\mathrm{ord}(a) = |G| \Rightarrow G = \langle a \rangle$ άρα G κυκλική συνεπώς G αβελιανή αντίφαση.

ΑΠΟΔΕΙΞΗ 2 ΙΣΧΥΡΙΣΜΟΣ Έστω $G = (U(\mathbb{Z}_8), \cdot)$

Τότε G αβελιανή, $|G| = 4$ και δεν υπάρχει $a \in G$ με $\mathrm{ord}(a) = 4$.

ΑΠΟΔΕΙΞΗ $U(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$

έχουμε $\mathrm{ord}[1]_8 = 1$

$$([3]_8)^2 = [3]_8 \cdot [3]_8 = [9]_8 = [1]_8$$

άρα $\mathrm{ord}([3]_8) = 2$

$([5]_8)^2 = [5]_8 \cdot [5]_8 = [25]_8 = [1]_8$ άρα $\mathrm{ord}([5]_8) = 2$

$([7]_8)^2 = [49]_8 = [1]_8$ άρα $\mathrm{ord}([7]_8) = 2$

ΠΟΡΙΣΜΑ Έστω G πεπερασμένη ομάδα με $|G| = p =$ πρώτος. Τότε G κυκλική (Δηλ. υπάρχει $a \in G$ με $G = \langle a \rangle$)

ΑΠΟΔΕΙΞΗ Αφού p πρώτος $\Rightarrow p \geq 2$. Άρα υπάρχει $a \in G \setminus \{e\}$

ΙΣΧΥΡΙΣΜΟΣ $\langle a \rangle = G$.

ΑΠΟΔΕΙΞΗ Έχουμε $e, a \in \langle a \rangle \Rightarrow \# \langle a \rangle \geq 2$
Από Θ. Lagrange $\# \langle a \rangle \mid \# G = p$ πρώτος
Αφού p πρώτος, $\# \langle a \rangle \geq 2$ και $\# \langle a \rangle \mid p \Rightarrow$
$\langle a \rangle = p$. Άρα $\langle a \rangle = G$.

ΠΡΟΤΑΣΗ Έστω G πεπερασμένη ομάδα και $a \in G$.
Τότε $a^{\# G} = e$

ΑΠΟΔΕΙΞΗ
Έστω $d = ord(a)$. Από πόρισμα $d \mid \# G$
άρα υπάρχει και θετικό ακέραιος με $\# G = d \cdot k$.
Τότε $a^{\# G} = (a^{d \cdot k}) = (a^d)^k = e^k = e$

ΕΦΑΡΜΟΓΗ Αν $|G| = 22$, τότε $a^{22} = e$ για κάθε $a \in G$.

ΘΕΩΡΗΜΑ FERMAT Έστω p πρώτος και $a \in \mathbb{Z}$
με $ΜΚΔ(a,p) = 1$ Τότε
$a^{p-1} \equiv 1 \mod p$.

ΑΠΟΔΕΙΞΗ Έστω $G = (U(\mathbb{Z}_p), \cdot)$. Άρα

$ΜΚΔ(a,p) = 1$. Έχουμε $[a]_p \in U(\mathbb{Z}_p)$ Αφού p
πρώτος $\# U(\mathbb{Z}_p) = p - 1$
Από πρόταση στην G $([a]_p)^{\# U(\mathbb{Z}_p)} = [1]_p$
$\Rightarrow ([a]_p)^{p-1} = [1]_p \Rightarrow [a^{p-1}]_p = [1]_p \Rightarrow$
$a^{p-1} \equiv 1 \mod p$.

ΘΕΩΡΗΜΑ EULER Έστω $n \geq 2$ ακέραιος και

$a \in \mathbb{Z}$ με $ΜΚΔ(a,n) = 1$. Τότε $a^{\phi(n)} \equiv 1 \mod n$.
(ϕ του Euler)

ΑΠΟΔΕΙΞΗ Έστω $G = (U(\mathbb{Z}_n), \cdot)$. Αφού $ΜΚΔ(a,n) = 1$
έχουμε $[a]_n \in G$. Έχουμε ότι $\# U(\mathbb{Z}_n) = \phi(n)$

Από πρόταση στην G $([a]_n)^{\# U(\mathbb{Z}_n)} = [1]_n$.

$\Rightarrow ([a]_n)^{\phi(n)} = [1]_n \Rightarrow [a^{\phi(n)}]_n = [1]_n \Rightarrow$

$a^{\phi(n)} \equiv 1 \mod n$.

ΕΦΑΡΜΟΓΗ: Εύρεση <u>όλων</u> των υποομάδων της $(S_3, \circ)$

ΛΥΣΗ

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Έχουμε δείξει

$ord(\sigma_1) = ord(\sigma_2) = ord(\sigma_3) = 2$, $ord(\sigma_4) = ord(\sigma_5) = 3$

και $\sigma_4^2 = \sigma_5$ $\sigma_5^2 = \sigma_4$.

<u>ΙΣΧΥΡΙΣΜΟΣ</u> Υποομάδες της G είναι <u>ακριβώς</u> οι εξής

τάξη 1	$\{e\}$	ΜΙΑ
τάξη 2	$\langle\sigma_1\rangle = \{\sigma_1, e\}, \langle\sigma_2\rangle = \{\sigma_2, e\}, \langle\sigma_3\rangle = \{\sigma_3, e\}$	ΤΡΕΙΣ
τάξη 3	$\langle\sigma_4\rangle = \langle\sigma_5\rangle = \{\sigma_4, \sigma_5, e\}$	ΜΙΑ
τάξη 6	S_3	ΜΙΑ

<u>ΑΠΟΔΕΙΞΗ</u> Έχουμε δει οι παραπάνω είναι υποομάδες με τις τάξεις που αναφέρουμε. Έστω H υποομάδα της S_3 θα δείξουμε ότι είναι μια από τις παραπάνω.

<u>ΒΗΜΑ 1</u> Από Θ. Lagrange $|H| \mid |G|$ άρα $|H| \in \{1, 2, 3, 6\}$

ΒΗΜΑ 2 Αν $\#H = 1 \Rightarrow H = \{e\}$

ΒΗΜΑ 3 Αν $\#H = 6$ Αφού $\#G = 6$ και $H \subseteq G$

$\Rightarrow H = G = S_3$

ΒΗΜΑ 4 Αν $\#H = 2$ αναγκαστικά $H = \{e, \sigma\}$ με

$ord(\sigma) = 2$ (γιατί $ord(\sigma) \mid \#H = 2$, άρα $\sigma = \sigma_1$
ή σ_2 ή σ_3 γιατί αυτά είναι τα μόνα
στοιχεία τάξης 2 της G

ΒΗΜΑ 5 Έστω $\#H = 3$ Αφού 3 πρώτος, από

Πρόταση H κυκλική άρα υπάρχει $\sigma \in G$ με
$ord(\sigma) = 3$ ώστε $H = \langle \sigma \rangle$. Τα μόνα στοιχεία
της S_3 με τάξη 3 είναι τα σ_4 και σ_5 και
γέρατα $\langle \sigma_4 \rangle = \langle \sigma_5 \rangle = \{\sigma_4, \sigma_5, e\}$

ΤΕΛΟΣ ΑΠΟΔΕΙΞΗΣ

ΠΑΡΑΤΗΡΗΣΗ S_3 όχι κυκλική ούτε και αβελιανή
αλλά κάθε γνήσια υποομάδα ΚΥΚΛΙΚΗ.