NO: 08-04-16
Date:

Previously on Beligiannis

Θεώρημα Lagrange: Έστω G πεπερασμένη ομάδα. Τότε για κάθε υποομάδα H της G θα έχουμε $|H| \mid |G|$

Πόρισμα: Αν G είναι μια ομάδα και $|G| < \infty$, τότε $\forall x \in G$: $o(x) \mid |G|$ κι επιπλέον: $x^{|G|} = e$, $\forall x \in G$

Απόδειξη: $\forall x \in G$, θεωρούμε την κυκλική υποομάδα $\langle x \rangle \leq G$ και τότε $|\langle x \rangle| = o(x)$. Από το Θ. Lagrange έχουμε το ζητούμενο.

$\forall x \in G$: $|G| = o(x) \cdot k$. Τότε: $x^{|G|} = x^{o(x)k} = (x^{o(x)})^k = e^k = e$

- Πόρισμα: Αν G: ομάδα και η τάξη της, $|G| = p$: πρώτος τότε η G είναι κυκλική.

Απόδειξη: Προφανώς, $G \neq \{e\}$. Άρα, $\exists x \in G$, $x \neq e$.

Θεωρούμε την $\langle x \rangle \leq G$. Από το Θεώρημα Lagrange

$\Rightarrow o(x) = |\langle x \rangle| \mid |G| = p$. Άρα, $o(x) = 1$ ή $o(x) = p$

Αν $o(x) = 1 \Rightarrow \langle x \rangle = \{e\}$: άτοπο, διότι $x \neq e$.

Άρα, $o(x) = p$ και άρα $|\langle x \rangle| = p = |G| \Rightarrow$

$\Rightarrow \langle x \rangle = G \Rightarrow$ G: κυκλική

NO:
Date:

• Πόρισμα: Έστω G: πεπερασμένη ομάδα και $H \leq G$, $K \leq G$

Αν $(|H|, |K|) = 1$, τότε $H \cap K = \{e\}$

Απόδειξη: $H \cap K \subseteq H$, $H \cap K \subseteq K$ } Απ' το Θεώρημα του Lagrange προκύπτει:

$|H \cap K| \,|\, |H|$
$|H \cap K| \,|\, |K|$ } $\Rightarrow |H \cap K| \,|\, (|H|, |K|) = 1$

Άρα, $|H \cap K| = 1 \Rightarrow H \cap K = \{e\}$

• Πόρισμα: Έστω G: πεπερασμένη ομάδα και η τάξη της $|G| = pq$, p, q: πρώτοι αριθμοί.

Τότε: Κάθε γνήσια υποομάδα της G είναι κυκλική.

Απόδειξη: Έστω $H \leq G$ και $H \neq G$. Από το Θεώρημα του Lagrange προκύπτει:

$|H| \,|\, |G| = pq \Rightarrow |H| = 1$ ή p ή q

Τότε αν $|H| = 1 \Rightarrow |H| = \{e\} = \langle e \rangle$

αν $|H| = p$ ή q, τότε: προκύπτει η κυκλική από το προηγούμενο πόρισμα

NO:
Date:

• Πόρισμα: Έστω G: πεπερασμένη ομάδα και $K \leq G$, $H \leq G$ έτσι ώστε $K \leq H \leq G$

Τότε: $[G:K] = [G:H] = [H:K]$

Απόδειξη: Απ' το Θεώρημα Lagrange $\Longrightarrow$

$\Rightarrow$ • $|G| = |H|\,[G:H]$ $\Big\{$ $|G| = |H|\,[G:H] =$

• $|G| = |K|\,[G:K]$ $\Big/$ $= |K|\,[H:K]\,[G:H]$ $\Big\{$

• $|H| = |K|\,[H:K]$ $\Big/$ $|G| = |K|\,[G:K]$ $\Big/$

Άρα, $[G:K] = [H:K]\,[G:H]$

Υποομάδες και Διάγραμμα Hasse της S_3

$$S_3 = \left\{ i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right.$$

$$\left. \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

• $o(i) = 1$, $o(\sigma_1) = o(\sigma_2) = o(\sigma_3) = 2$, $o(\rho_1) = o(\rho_2) = 3$ $\Big|$ $\rho_1^2 = \rho_2$

• $\langle i \rangle = \{i\}$, $\sigma_1 = \{i, \sigma_1\}$, $\langle \sigma_2 \rangle = \{i, \sigma_2\}$, $\sigma_3 = \{i, \sigma_3\}$

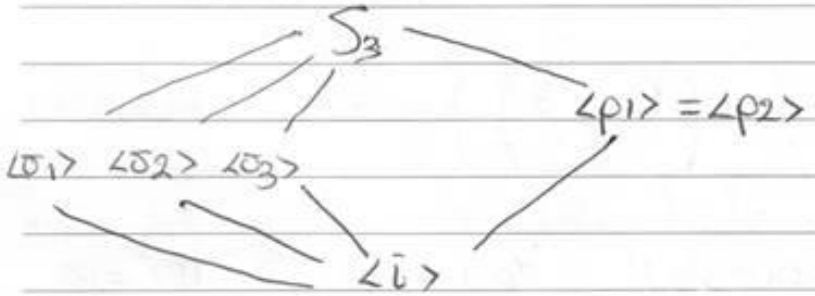
$\langle \rho_1 \rangle = \{i, \rho_1, \rho_2\} = \langle \rho_2 \rangle$, S_3

NO:
Date:

Έστω Η τυχούσα υποομάδα της S_3, $H \leq S_3$. Από το Θεώρημα Lagrange $\Rightarrow$ $|H| = 1$ ή 2 ή 3 ή 6

- $|H| = 1 \Rightarrow H = \{i\} = \langle i \rangle$
- $|H| = G \Rightarrow H = S_3$
- $|H| = 2 \Rightarrow$ Η κυκλική τάξης 2, θα παράγεται από ένα στοιχείο της S_3, τάξης 2.
Τα μόνα στοιχεία τάξης 2 της S_3 είναι τα $\sigma_1, \sigma_2, \sigma_3$.
Άρα, η Η θα είναι μία εκ των $\langle \sigma i \rangle$, $i = 1,2,3$
- $|H| = 3 \Rightarrow$ Η κυκλική τάξης 3, θα παράγεται από ένα στοιχείο της S_3, τάξης 2.
Τα μόνα στοιχεία τάξης 3 της S_3 είναι τα ρ_1, ρ_2.
Άρα, η Η θα είναι μία εκ των $\langle \rho i \rangle$, $i = 1,2$

Διάγραμμα Hasse



NO:
Date:

• Έστω $H = \langle \sigma_3 \rangle = \{i, \sigma_3\} \leq S_3 \parallel [S_3 : H] = \frac{|S_3|}{|H|} = \frac{6}{2} = 3$

Αριστερά Σύμπλοκα της H στην S_3:

- $iH = H = \{i, \sigma_3\}$
- $\sigma_1 H = \{\sigma_1 \cdot i, \sigma_1 \sigma_3\} = \{\sigma_1, \rho_2\}$
- $\sigma_2 H = \{\sigma_2 i, \sigma_2 \sigma_3\} = \{\sigma_2, \rho_1\}$

Δεξιά Σύμπλοκα της H στην S_3:

- $Hi = \{i, \sigma_3\}$
- $H\sigma_1 = \{i\sigma_1, \sigma_3 \cdot \sigma_1\} = \{\sigma_1, \rho_1\}$
- $H\sigma_2 = \{i\sigma_2, \sigma_3\sigma_2\} = \{\sigma_2, \rho_2\}$

Παρατηρούμε ότι: $\sigma_1 H \neq H\sigma_1$

• Διάγραμμα Hasse της ομάδας των τετρανίων του Hamilton

$Q = \{\pm I_2, \pm I, \pm J, \pm K\}$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$Q \leq GL(2, \mathbb{C})$, $I^2 = J^2 = K^2 = IJK = -I_2$

$o(I_2) = 1$, $o(-I_2) = 2$, $o(\pm I) = o(\pm J) = o(\pm K) = 4$

Άρα, δεν υπάρχει στοιχείο τάξης 8.

Συνεπώς, η Q δεν είναι κυκλική!

NO:
Date:

- $\langle I_2 \rangle = \{I_2\}$ → τάξης 1
- $\langle -I_2 \rangle = \{I_2, -I_2\}$ → τάξης 2
- $\langle I \rangle = \langle -I \rangle = \{I_2, I, -I, -I_2\}$ → τάξης 4 $(= \langle -I \rangle)$
- $\langle J \rangle = \{I_2, +J, -J, -I_2\}$ → τάξης 4 $(= \langle -J \rangle)$
- $\langle K \rangle = \{I_2, K, -K, -I_2\}$ → τάξης 4 $(= \langle -K \rangle)$
- $Q = \{\pm I_2, \pm I, \pm J, \pm K\}$ → τάξης 8

Έστω $H \leq Q$. Απ' το Θεώρημα Lagrange

$\Rightarrow |H|\,|Q| = 8 \Rightarrow |H| = 1$ ή 2 ή 4 ή 8

① Αν $|H| = 1$, τότε $H = \langle I_2 \rangle$

② Αν $|H| = 2$, τότε H: κυκλική τάξης 2 $\Rightarrow H = \langle x \rangle$, $o(x) = 2 \Rightarrow x = -I_2 \Rightarrow H = \langle -I_2 \rangle$

③ $|H| = 4$, τότε: H: κυκλική, διότι διαφορετικά θα ήταν ισόμορφη με την ομάδα του Klein κι άρα κάθε στοιχείο της εκτός του ουδετέρου θα είχε τάξη 2.

Άτοπο: Μόνο το $-I_2$ έχει τάξη 2. Άρα H: κυκλική.

Τα μόνα στοιχεία της Q, με τάξη 4 είναι $\pm I, \pm J, \pm K$

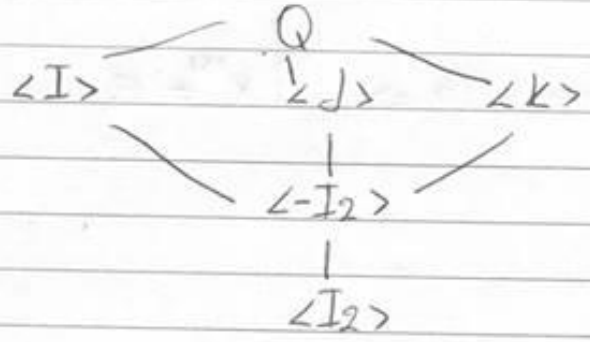
Επειδή όμως $\langle I \rangle = \langle -I \rangle$, $\langle J \rangle = \langle -J \rangle$ $\langle K \rangle = \langle -K \rangle$, έπεται $H = \langle I \rangle$ ή $H = \langle J \rangle$ ή $H = \langle K \rangle$

NO:
Date:

④ Αν $|H| = 8 \Rightarrow \boxed{H = Q}$

Άρα, οι: $\langle I_2 \rangle, \langle -I_2 \rangle, \langle I \rangle, \langle J \rangle, \langle K \rangle, Q$ είναι όλες οι υποομάδες της Q.

Διάγραμμα Hasse



Παρατήρηση: Το αντίστροφο του Θεωρήματος Lagrange:

Αν $d \mid |G|$, τότε: $\exists\, H \leq G : |H| = d$, γενικά δεν ισχύει

Ισχύει ειδικά για τις κυκλικές ομάδες.

• Εφαρμογές του Θ. Lagrange στη Θεωρία Αριθμών

Για κάθε θετικό ακέραιο $n \geq 1$, θεωρούμε την ομάδα $(U(Z_n), \cdot)$, όπου $U(Z_n) = \{[k]_n \in Z_n \mid \substack{1 \leq k \leq n \\ (k,n)=1}\}$

↓ αβελιανή τάξης $\varphi(n)$

NO:
Date:

• Θεώρημα Euler: Αν $n \geq 1$ και $a \in \mathbb{Z}$: $(a,n)=1$. Τότε: $a^{\varphi(n)} \equiv 1 \bmod n$

Απόδειξη: Επειδή, $(a,n)=1 \Rightarrow [a]_n \in U(\mathbb{Z}_n)$

Τότε, επειδή $|U(\mathbb{Z}_n)| = \varphi(n)$ θα έχουμε: $[a]_n^{\varphi(n)} = [1]_n \Rightarrow [a^{\varphi(n)}]_n = [1]_n \Rightarrow$

$\Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$

| $|G|<\infty$ και $x \in G$. $x^{|G|} = e$

• Πόρισμα Fermat

Αν p: πρώτος και $a \in \mathbb{Z}$ με $p \nmid a$, τότε: $a^{p-1} \equiv 1 \bmod p$

• Θεώρημα Wilson: $p \geq 2$, p: πρώτος $\Leftrightarrow (p-1)! \equiv -1 \bmod p$

Απόδειξη: ($\Rightarrow$) Υποθέτουμε ότι p: πρώτος

Αν $p=2$, τότε $(2-1)! = 1 \equiv -1 \bmod 2$, ισχύει

Υποθέτουμε ότι $p \geq 3$. Θεωρούμε την $U(\mathbb{Z}_p)$, αβελιανή ομάδα, $\varphi(p) = p-1$ και $U(\mathbb{Z}_p) = \{[1]_p, [2]_p, \dots, [p-1]_p\}$

Έστω $[x]_p \in U(\mathbb{Z}_p)$ τάξης 2. Τότε $[x]_p \neq [1]$ και

$[x]_p^2 = [1]_p \Rightarrow [x^2]_p = [1]_p \Rightarrow p \mid x^2-1 \Rightarrow p \mid (x-1)(x+1) \Rightarrow$

p: πρώτος $\Longrightarrow$ $p \mid x-1$ ή $p \mid x+1$

NO:
Date:

• Αν $p|x-1 \Rightarrow x-1 \equiv 0 (\mathrm{mod} p) \Rightarrow x \equiv 1 \mathrm{mod} p \Rightarrow$

$\Rightarrow [x]_p = [1]_p$, άτοπο διότι $[x]_p \neq [1]_p$

Άρα, $p|x+1 \Rightarrow x+1 \equiv 0 (\mathrm{mod} p) \Rightarrow x \equiv -1 (\mathrm{mod} p) \Rightarrow$

$\Rightarrow [x]_p = [-1]_p$

Άρα, το μόνο στοιχείο τάξης 2 στη $U(Z_p)$ είναι το $[-1]_p = [p-1]_p$

Οπότε, το μόνο στοιχείο εκτός του αυξετέρου $[1]_p$ για το οποίο $[x]_p = [x]^{-1}_p$ είναι το $[p-1]_p$

$[1]_p [2]_p \dots [p-2]_p [p-1]_p = [2]_p [3]_p \dots [p-2]_p [p-1]_p$

$\| \quad ([(p-1)!]_p)$ Στο παραπάνω γινόμενο, τα στοιχεία

$[2]_p, [3]_p, \dots, [p-2]_p$ εμφανίζονται κατά ζεύγη όπου $[x]_p \neq [x]^{-1}_p$.

Θα έχαμε: $[x]_p \cdot [x]^{-1}_p = [1]_p$

Τότε: $[(p-1)!]_p = \underbrace{[2]_p [3]_p \dots [p-2]_p}_{[1]_p} [p-1]_p =$

$= [p-1]_p = [-1]_p \Rightarrow (p-1)! \equiv 1 (\mathrm{mod} p)$

NO:
Date:

Θεώρημα Gauss: $n = \sum_{d|n} \varphi(d)$

$|G| < \infty \Rightarrow \forall x \in G : o(x) < \infty$ {Το αντίστροφο γενικά δεν ισχύει}
$\not\Leftarrow$

Έστω $(G_1, \cdot)$, $(G_2, \cdot)$ δύο ομάδες. Στο καρτεσιανό γινόμενο $G_1 \times G_2$ ορίζουμε πράξη $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$

- Τότε, το ζεύγος $(G_1 \times G_2, \cdot)$ είναι ομάδα με ουδέτερο στοιχείο $e = (e_1, e_2)$, όπου e_i = ουδέτερο στοιχείο της G_i, $i = 1, 2$
- Το αντίστροφο στοιχείο είναι $(x, y)^{-1} = (x^{-1}, y^{-1})$

! Η ομάδα $(G_1 \times G_2, \cdot)$ καλείται ευθύ γινόμενο των G_1, G_2

$|G_1 \times G_2| < \infty \Leftrightarrow |G_1| < \infty$ και $|G_2| < \infty$ και τότε:

$|G_1 \times G_2| = |G_1| |G_2|$

Η $G_1 \times G_2$ είναι αβελιανή $\Leftrightarrow$ G_1, G_2: αβελιανές

Γενικότερα, αν $(G_i, \cdot)$, $i = 1, 2, \ldots, n$ είναι μια αριθμήσιμη συλλογή ομάδων τότε η ομάδα ευθύ γινόμενο $(G_1 \times G_2 \times \ldots) = \underset{i \geq 1}{\times} G_i$, όπου

$\underset{i \geq 1}{\times} G_i = \{(x_i)_{i \geq 1} \mid x_i \in G_i \ \forall i \geq 1\}$ και

NO:
Date:

$(X_i)_{i\geq 1} \cdot (Y_i)_{i\geq 1} = (X_i Y_i)_{i\geq 1}$

Τότε: ουδέτερο στοιχείο $e=(e_i)_{i\geq 1}$, e_i: ουδέτερο της G_i

$(X_i)^{-1}_{i\geq 1} = (X_i^{-1})_{i\geq 1}$

Θεωρούμε μια κυκλική ομάδα: H, $|H|=2$, πχ

$H=U_2=\{1,-1\}$ κι έστω η ομάδα αυθ' γινόμενο

$G = H \times H \times \ldots = U_2 \times U_2 \times \ldots$

$\forall\, x=(X_i)_{i\geq 1} \in G : X^2 = (X_i)_{i\geq 1} \cdot (X_i)_{i\geq 1} =$

$= (X_i \cdot X_i)_{i\geq 1} = (X_i^2)_{i\geq 1}$

$= (e_i)_{i\geq 1} = e \Rightarrow o(x) = 1 \text{ ή } 2 \;\forall x \in G$ και $|G|=\infty$