

-1-

μαθημα 05: (15/10/24)

Παρατήρηση: Μία ομάδα τάξης p^2q δεν είναι αβελική, όπου p, q πρώτοι

Απόδειξη: Έστω $|G| = p^2q$. Αν $p=q$, τότε $|G| = p^2 \cdot p = p^3$
Έχουμε ήδη δείξει σ' αυτήν την περίπτωση ότι
η G δεν είναι αβελική.

Αν $p \neq q$: Εάν $n_p = 1$ ή $n_q = 1$, τότε η αντίστοιχη Sylow είναι κανονική (ως μοναδική) κι άρα η G δεν είναι αβελική.

Υποθέτουμε $n_p > 1, n_q > 1$.

$$\begin{aligned} & \bullet n_p | q \Rightarrow n_p \in \{1, q\} \Rightarrow n_p = q \\ & \bullet n_p \equiv 1 \pmod{p} \Rightarrow p | n_p - 1 \neq 0 \Rightarrow p \leq n_p - 1 < n_p = q \end{aligned} \quad \left. \vphantom{\begin{aligned} & \bullet n_p | q \Rightarrow n_p \in \{1, q\} \Rightarrow n_p = q \\ & \bullet n_p \equiv 1 \pmod{p} \Rightarrow p | n_p - 1 \neq 0 \Rightarrow p \leq n_p - 1 < n_p = q \end{aligned}} \right\} \Rightarrow q > p$$

$$\begin{aligned} & \bullet n_q | p^2 \Rightarrow n_q \in \{1, p, p^2\} \Rightarrow n_q \in \{p, p^2\} \\ & \bullet n_q \equiv 1 \pmod{q} \Rightarrow p < q \leq n_q \end{aligned} \quad \left. \vphantom{\begin{aligned} & \bullet n_q | p^2 \Rightarrow n_q \in \{1, p, p^2\} \Rightarrow n_q \in \{p, p^2\} \\ & \bullet n_q \equiv 1 \pmod{q} \Rightarrow p < q \leq n_q \end{aligned}} \right\} \Rightarrow n_q = p^2$$

Κάθε Sylow q -υποομάδα έχει τάξη q (άρα είναι κυκλική)

Έστω ότι η τάξη κάθε ~~γείωσης~~ διαφορ. Sylow q -υποομ.
εν G είναι τετραπλήτη.

Συνεπώς οι $n_q = p^2$ Sylow q -υποομάδες μας δίνουν

$$n_q(q-1) = p^2(q-1) \text{ πολλαπλά τάξης } q.$$

Μέσω p^2 ω ηγίνας στοιχεία, άρα γινάχων μόνο 1 Sylow p -υποομάδα, δηλαδή $n_p=1$. Άρα $\square$

Παρασέρναι: Μία ομάδα τάξης pqr δέν είναι αβή, άνου p, q, r άρρώοι.

Απόδειξη: Αν $p=q \neq r$, $p \neq q=r$, $p=r \neq q$, $p=q=r$, ή παρασέρναι νάβει, άνου τα προηώφα.

Υποθέτω $p \neq q \neq r$ και αραερίτω $p < q < r$.

• Αν $n_p=1$ ή $n_q=1$ ή $n_r=1$, ή αντίστοιχη Sylow υποομάδα είναι κανονική και η G άν είναι αβή.

• Αν $n_p > 1$, $n_q > 1$, $n_r > 1$:

$$\left. \begin{array}{l} n_r \mid pq \Rightarrow n_r \in \{1, p, q, pq\} \\ n_r = 1 \pmod r \Rightarrow r < n_r \Rightarrow p < q < r < n_r \end{array} \right\} \Rightarrow n_r = pq$$

$$\left. \begin{array}{l} n_q \mid pr \Rightarrow n_q \in \{1, p, r, pr\} \\ n_q = 1 \pmod q \Rightarrow p < q < n_q \end{array} \right\} \Rightarrow n_q \geq r$$

Κάθε Sylow r -υποομάδα είναι κυρία τάξης r , άρα ανα 2 διαδορικές έχου τετρ τομή.

Συνέως, οι n_r Sylow r -υποομάδες με G δίνου $n_r(r-1) = pq(r-1)$ στοιχεία τάξης r . Οποίως, οι n_q Sylow q -υποο. δίνου ταυράχισών

$r(q-1)$ στοιχεία τάξης q

οι h_p Sylow p -υποομάδες. Σίγουρα περιλαμβάνουν $q(p-1)$ στοιχεία τάξης p .

Συνεπώς:

$$|G| \geq pq(r-1) + r(q-1) + q(p-1) + 1$$

$$= pqr - pq + rq - r + qp - q + 1$$

$$> pqr \quad (\text{απόρροια})$$

□

Λήμμα 1: Έστω $H \leq G$, G πεπερασμένη, p πρώτος, $p \mid |G|$, $p \mid |H|$ και

$$P \in \text{Syl}_p(H), Q \in \text{Syl}_p(G).$$

$$\text{Αν } P \leq Q, \text{ τότε } P = Q \cap H$$

(Αποκρίνεται με Sylow)

Απόδειξη: $Q \cap H \leq P \Rightarrow Q \cap H$ p -υποομάδα της H

$$\text{Επίσης } P \leq Q \cap H$$

□

$$\text{Syl}_p(H).$$

$$\text{Από } \text{Syl}_p(H) \ni P \text{ (πρώτη } p\text{-υποομάδα), } P = Q \cap H \quad \square$$

Παρατήρηση: Εφόσον κάθε p -υποομάδα της G περιέχεται σε κάποια Sylow υποομάδα της G , έχουμε ότι:

$$\text{Syl}_p(H) = \{ Q \cap H \mid Q \in \text{Syl}_p(G) \}$$

Συνέπεια: $n_p(H) \leq n_p(G)$.

Λήμμα 2: Έστω G πεπερημένη ομάδα, p πρώτος, $p \mid |G|$.

Εάν H p -υποομάδα της G , $p \mid [G:H]$. Τότε $H \leq N_G(H)$.

Απόδειξη: Θεωρούμε τον πομπό της φυσικής δράσης της G ως προς την αριστερή επίρροή της H και τον πομπό της H .

$$H \curvearrowright G/H, \quad \text{ht}_G H = \text{ht}_H H$$

Παρατηρούμε ότι: $\mathcal{O}(H) = \{H\}$. Αν $1 \neq \mathcal{O}(xH)$ δεν είναι πομπό, $p \mid |\mathcal{O}(xH)|$ ($1 \neq \mathcal{O}(xH)$)

Εφόσον το G/H είναι γνήσια ομάδα, προκύπτει ότι το p διαιρεί το πλήθος των πομπών που είναι πομπό.

Εξαιτίας, το πλήθος των πομπών που είναι πομπό είναι $\geq p$.

Υπάρχει $\exists g \in G$, $gH \neq H \Leftrightarrow g \notin H$ και $\mathcal{O}(gH) = \{gH\} \Rightarrow$

$\text{ht}_G H = gH \notin H$. Δηλαδή: $g \in N_G(H) \setminus H \Rightarrow$

$$H < N_G(H).$$

□

Πρόταση 1: Αν G πεπερημένη p -ομάδα και $H \leq G$, τότε $H \leq N_G(H)$.

Πρόταση 2: Αν $|G| = p^n$ και $H \leq G$ με $|H| = p^{n-1}$, τότε $H \trianglelefteq G$.

Υπόθεση 3: Έστω G πεπερασμένη, $|G| = 2n$, n περιττός.
Τότε $\exists N \leq G$ με $|N| = n$. Ίδιαίτερα, η G δεν είναι εναρτή.

Απόδειξη: Η G δρα στο $X = G$ με πολλαπλούς από τα αριστερά.

Έστω $\rho: G \rightarrow S_{2n}$ ο αντίστοιχος ομομορφισμός.

Είναι άμεσο ότι $\rho \neq 1$. (αλλιώς δεν είναι αριστερά)

Άρα $\rho: G \hookrightarrow S_{2n}$.

Θεωρούμε στοιχεία $g \in G$ τάξης 2. Τέτοιο υπάρχει, αφού $g = g^{-1}$ αντιστοιχεί τάξη 2 και αν τέτοιο δεν υπάρχει, τότε

$$G = \{g, g^{-1}\} \cup \{1\} \text{ ή αν θα είχε άρτια τάξη.}$$

Πράγματι $\rho(g) = \pi_1 \dots \pi_n$ με πολλαπλούς άρτιους 2 κύκλους.

$$2 = \varphi(\rho(g)) = \text{lcm}(\varphi(\pi_1), \dots, \varphi(\pi_n)) \Rightarrow \varphi(\pi_i) = 2 \quad \forall i.$$

Κύκλος μήκους k δεν υπάρχει, διότι διαδορειακά $k \leq \varphi(\pi_i) = 2$ σε κάθε i .

Αντικαθιστώντας π_i είναι αντικαταστάση,

Επιπλέον: $2n = 2 \cdot n \Rightarrow n = n$ περιττός.

Έχουμε λοιπόν:

$$\begin{array}{c} G \hookrightarrow S_n \xrightarrow{\pi} S_{2n}/A_{2n} \cong \mathbb{Z}_2 \quad \left(\begin{array}{l} \pi: \\ \text{quasiregular} \end{array} \right) \\ \quad \quad \quad \uparrow \rho \\ \quad \quad \quad G \end{array}$$

Εφόσον $\rho(g) \notin A_{2n}$ (περιττός), $\rho(g) \notin \ker \pi$ και έτσι

— 6 —

φ επιμορφισμός. Αν $N = \ker \varphi$, τότε $N \trianglelefteq G$ και $G/N \cong \mathbb{Z}_2$,
 συνεπώς: $|G/N| = 2$, $|N| = n$. □

Τέλος μαθημάτων 5



-1-

ΜΑΘΗΜΑ 06 : (27/10/24)

Υπόθεση 1 : Κάθε πεπερ/μ υπομ. της μορ/κής
οφάδας έως αψάτος Π είναι κυκλική.

Απόδειξη : Για F * μορ/κή οφάδα, έστω $G \leq F^*$,
ε πεπερ/μ., $|G| = p_1^{n_1} \cdots p_k^{n_k}$, με p_i πρώτος, διαδοχ.
ανά 2, $n_i > 0$.

Εφόσον $G = \text{αβεβίαση}$, θα είναι $\exists$ υπάρχει μοναδική

$P_i \in \text{Syl}_{p_i}(G)$ ($\hookrightarrow P_i \leq G$) και $G = P_1 \times \cdots \times P_k$, Εφόσον
 $\gcd(|P_i|, |P_j|) = 1 \ \forall i \neq j$, αρκεί νδο κάθε P_i είναι
κυκλική.

Ας υποθέσουμε ότι P_i δεν είναι κυκλική για κάποιο i , με
 $|P_i| = p_i^{n_i}$. Τότε η τάξη κάθε υποομάδας της θα 'είναι
μικρότερη από $p_i^{n_i}$ (αφού αν ήταν ίση, θα ήταν το στοιχείο
αυτό γεννήτορας της κυκλικής).

Έτσι, θα $g \in P_i$, $\text{ord}(g) \leq p_i^{n_i-1}$ και $\text{ord}(g) \mid p_i^{n_i}$.

Συνεπώς $g^{p_i^{n_i-1}} = 1 \ \forall g \in P_i$. Αντιστ. η εξίσωση $x^{p_i^{n_i-1}} = 1$
έχει τουλάχιστον $p_i^{n_i}$ ρίζες ως Π , πράγμα άτοπο,

Άρα κάθε P_i κυκλική. □

Υπόθεση 2 : Έστω G πεπερ/μ οφάδα, $H \leq G$ με $p \mid |H|$,
 p πρώτος, $p \mid |G|$.

(i) Αν $P \in \text{Syl}_p(G)$, τότε $\exists g \in G$ τω. $gPg^{-1} \cap H \in \text{Syl}_p(H)$.

Απόδειξη (i) :

Έστω $Q \in \text{Syl}_p(H)$. Εφόσον η Q p -υποομάδα της H , υπάρχει p -Sylow υποομάδα της G που την περιέχει. Όπως οι Sylow p -υποομάδες της G είναι συζυγείς. Άρα, $\exists g \in G$ τέτοια ώστε $Q \leq gPg^{-1}$.

$$Q \leq gPg^{-1} \cap H \leq H \xrightarrow{Q \in \text{Syl}_p(H)} gPg^{-1} \cap H = Q \in \text{Syl}_p(H). \quad \square$$

(ii) Για $P \in \text{Syl}_p(G)$ και αν $K \trianglelefteq G$, τότε $K \cap P \in \text{Syl}_p(K)$ και $PK/K \in \text{Syl}_p(G/K)$.

Απόδειξη (ii): Από το προηγούμενο, $\exists g \in G$ τέτοια ώστε $gPg^{-1} \cap K \in \text{Syl}_p(K)$.

$$\begin{aligned} \text{Λόγω κανονικότητας } g(K \cap P)g^{-1} &= K \cap gPg^{-1} \in \text{Syl}_p(K) \Rightarrow \\ &\Rightarrow K \cap P \in \text{Syl}_p(K). \end{aligned}$$

$$\bullet |G| = p^n m, \gcd(p, m) = 1, |K| = p^v t, \gcd(p, t) = 1:$$

$$|PK/P| = \left| \underbrace{P/K \cap P}_{\in \text{Syl}_p(K)} \right| \stackrel{\text{v. Isomorf.}}{=} \frac{p^n}{p^v} = p^{n-v}$$

$$\bullet |G/K| = p^{n-v} \cdot m, \gcd(p, m) = 1, \text{ άρα } PK/P \in \text{Syl}_p(G/K). \quad \square$$

(iii) Με τις παραπάνω υποθέσεις, κάθε Sylow p -υποομάδα της G/K είναι η εικόνα της PK/P , $P \in \text{Syl}_p(G)$.

Αν $Q \in \text{Syl}_p(G/K)$, τότε από το 2. τις παραπάνω, $Q = N/K$, $K \leq N \leq G$.

$$|N| = |Q| \cdot |K| = p^{n-v} \cdot p^v \cdot t = p^n t, \gcd(p, t) = 1$$

$$\text{Άρα, } \text{Syl}_p(N) \leq \text{Syl}_p(G).$$

Έστω $P_1 \in \text{Syl}_p(N)$. Τότε $P_1 \in \text{Syl}_p(G)$ και από το
 πρῶτο $P_1 K/K \in \text{Syl}_p(G/K)$.

$P_1 \leq N$. Από $P_1 K/K \leq N/K \in \text{Syl}_p(G/K) \Rightarrow R = P_1 K/K$,
 $P_1 \in \text{Syl}_p(G)$.

Από τα προηγούμενα, $\gamma: \text{Syl}_p(G) \rightarrow \text{Syl}_p(G/K)$
 $p \mapsto P_1 K/K$

Είναι επί, άρα:

$$n_p(G/K) \leq n_p(G).$$

D

Άσκηση 3: Μια ομάδα τάξης 144 δεν είναι απλή.

Απόδειξη: Ας υποθέσουμε ότι υπάρχει ομάδα G , $|G| = 144$.

$$|G| = 144 = 2^4 \cdot 3^2$$

Έστω $H < G$, $[G:H] = n > 1$. Η G είναι S -πλάγια ως προς G
 και σύμφωνα με το πρώτο H είναι το αντιστοιχεί ομοιομορφία.
 $\varphi: G \rightarrow S_n$, $\ker \varphi \leq H < G$.

Εφόσον G απλή, $\ker \varphi = \{1\}$ & $\gamma: G \rightarrow S_n$ είναι έμφαντος.
 $G \hookrightarrow S_n$.

$$\text{Έτσι, } |G| \mid n! \Rightarrow 2^4 \cdot 3^2 \mid n! \Rightarrow n \geq 6.$$

Επίσης, $n_3 \geq 6$ και $n_2 \geq 6$, αφού για να είναι
 $n_p = [G : \mathcal{O}_p(G)]$

- $n_3 \mid 2^4 \Rightarrow n_3 \in \underbrace{\{1, 2, 4, 8, 16\}}_{\text{αποδεκτά}} \Rightarrow n_3 = 16.$
- $n_3 \equiv 1 \pmod{3}.$

Έστω $P, Q \in \text{Syl}_3(G)$, $P \neq Q$, $P \cap Q \neq \{1\}$.

Έστω $\mathcal{N}_G(P \cap Q)$. Εφόσον P, Q αβελιανές (έχουν τάξη τετρ. αριθμ.), κανονικοποιούν την τάξη $P \cap Q$, κι έτσι $P \cap Q \leq \mathcal{N}_G(P \cap Q)$ ως γνήσιος υποομάδα.

$$[\text{Αν } P = \mathcal{N}_G(P \cap Q), \text{ τότε } Q \leq P \xrightarrow{|P| = |Q|} Q = P, \text{ άτοπος}]$$

Έτσι, $3^2 \mid |G| \Rightarrow |G| \geq 9 \text{ \& } |G| \mid 19!$

Ύρα: $|G| \in \{3^2 \cdot 2, 3^2 \cdot 2^2, 3^2 \cdot 2^3, 3^2 \cdot 2^4\}$

$\downarrow$
 διίκτης 4
 (αριθμ. ≥ 6)

$\swarrow$
 διίκτης 2

$\searrow$
 $G = \mathcal{N}_G(P \cap Q)$
 (άτοπος).

Έστω: $|G| = 3^2 \cdot 2 = 18$. Τότε:

$$[G:P] = [G:Q] = 2 \Rightarrow P \triangleleft G, Q \triangleleft G$$

Από παραδικατομότητα $P = Q$ (άτοπος)

Συνεπώς η τάξη κάθε γνήσιου διαμορφωτή ανά 2 Sylow 3-υποομάδα, n_3 είναι τετράπληξη από αριθμ. $n_3 = 2^4$, το άθροισμα των 3-Sylow, μας δίνει:

$$n_3(3^2 - 1) = 2^4(3^2 - 1)$$

απαιτείται τάξη διίκτης του 3.

Τα 24 στοιχεία που απεικονίζονται προπούν ως χαρακτηριστικά 1 Sylow 2-υποομάδα.

$$n_5 \mid 2^2 \cdot 3^2 \Rightarrow n_5 \in \left\{ \overbrace{1, 2, 2^2, 3, 3 \cdot 2, 3^2 \cdot 2}^{\text{απορ.}}, 3^2 \cdot 2^2 \right\} \Rightarrow n_5 = 3^2 \cdot 2^2$$

$$n_5 = 1 \pmod{5}$$

$$\begin{array}{l} n_3 \mid 2^2 \cdot 5 \\ n_3 = 1 \pmod{5} \end{array} \quad \left\{ \begin{array}{l} n_3 \neq 7 \\ \Rightarrow n_3 = 10 \quad (\text{απορ.}) \end{array} \right.$$

$$\text{Έστω } P, Q \leq \text{Syl}_p(G), P \neq Q, P \cap Q \neq \{1\}, N = N_G(P \cap Q),$$

$$|P| = |Q| = 3^2 \Rightarrow P, Q \text{ αβελιανές} \Rightarrow P, Q \leq N' \text{ \& } P, Q \leq N', P \neq Q$$

$$\text{Άρα } 3^2 \mid |N'|, |N'| > 9 \text{ \& } |N'| \mid |G|$$

$$\text{Οπότε πάλι, } |N'| = 3^2 \cdot 2$$

$$[N':P] = [N':Q] = 2 \Rightarrow P, Q \triangleleft N' \xrightarrow{\text{Sylow}} P = Q \quad (\text{απορ.})$$

$$\text{Συνεπώς, αν } P, Q \leq \text{Syl}_3(G), \text{ τότε } P \cap Q = \{1\}, P \neq Q$$

$$\text{Syl}_3(G) \text{ έχει } n_3(3^2-1) = 10 \cdot 8 \text{ στοιχεία } \overset{\text{ταίρια}}{\text{δίνοντας}} \text{ που 3}$$

$$\text{Syl}_5(G) \text{ έχει } n_5(5-1) = 2^2 \cdot 3^2 \cdot 4 \text{ στοιχεία ταίρια 5}$$

οι 5-σβλω και 2 έχουν ταίρια. Τελική γιατί έχουν ταίρια μεταξύ τους.

$$\text{Τελικά } |G| \geq 10 \cdot 8 + 36 \cdot 4 > 180 = |G| \quad (\text{απορ.}) \quad \text{D.}$$

ΠΕΤΕΡΑΣΜΕΝΑ ΠΑΡΑΘΕΜΕΝΕΣ ΑΒΕΛΙΑΝΕΣ ΟΜΑΔΕΣ

Υποβάλλεται προσθετικός υπολογισμός από πολ/κό.

Τεχνικές λήψης: Έστω G αβελιανή ομάδα με πεπερασμένο σύνολο γεννητόρων $\{x_1, \dots, x_k\}$.

Έστω $\lambda_1, \dots, \lambda_k$ ακέραιοι με $\gcd(\lambda_1, \dots, \lambda_k) = 1$.

Τότε: Υπάρχει σύνολο γεννητόρων $\{y_1, \dots, y_k\}$ της G με:

$$y_i = \lambda_1 x_1 + \dots + \lambda_k x_k$$

Απόδειξη: Μπορούμε να υπολ. $\lambda_i \geq 0$, αφού αλλιώς τα αρνητικά των x_i μπορούν να αλλαχθούν.

Θα το αποδείξουμε με επαγωγή ως $\lambda_1 + \dots + \lambda_k = \lambda$,

- $\lambda = 1$: Τότε $\lambda_i = 1$ για κάποιον i και $\lambda_j = 0$, $j \neq i$

Τα $\{y_1, \dots, y_k\}$ είναι αναδιάταξη των $\{x_1, \dots, x_k\}$.

- $\lambda > 1$: Δεν έχουμε μονάχα ένα $\lambda_i \neq 0$, αφού τότε $\gcd(\lambda_1, \dots, \lambda_k) \neq 1$. Τουλάχιστον 2 λ_i άντικαν 0.

Έστω, χωρίς βλάβη της γενικότητας, $\lambda_1 \geq \lambda_2 > 0$.

Παρατηρούμε:

- $\{x_1, x_2 + x_1, x_3, \dots, x_k\}$ είναι σύνολο γεννητόρων της G ,

- $\gcd(\lambda_1 - \lambda_2, \lambda_2, \dots, \lambda_k) = 1$

- 6 -

$$\bullet (\lambda_1 - \lambda_2) + \lambda_2 + \dots + \lambda_k \leq \lambda = \lambda_1 + \dots + \lambda_k$$

Από την παραπάνω υπόθεση, υπάρχει αλγόριθμος που βρίσκει
 $\{y_1, \dots, y_k\}$ μη $\emptyset$ τέτοιο ώστε:

$$\begin{aligned} y_1 &= (\lambda_1 - \lambda_2)x_1 + \lambda_2(x_2 + x_1) + \lambda_3x_3 + \dots + \lambda_kx_k \\ &= \lambda_1x_1 + \lambda_2x_2 + \dots + \lambda_kx_k. \end{aligned} \quad \square$$

Τέλος μαθήματος ☺

