

ΜΕΤΑΠΤΥΧΙΑΚΗ ΑΛΓΕΒΡΑ Ι

Δευτέρα 06/10/2025

Διάλεξη 1

Βιβλιογραφία:

Hungerford Algebra

Διμερείς πράξεις στο σύνολο G :

$$\circ : G \times G \rightarrow G$$

$$(g_1, g_2) \mapsto g_1 \circ g_2$$

1. « Προσεταιριστική ιδιότητα » [ημιομάδα]

$$(g_1 \circ g_2) \circ g_3 = g_1 \circ (g_2 \circ g_3)$$

2. « Μοναδιαίο στοιχείο » [μονοειδές]

$$\exists e \in G : g \circ e = e \circ g = g, \forall g \in G$$

3. « Ύπαρξη αντιστράφου στοιχείου » [ομάδα]

$$\forall g \in G \exists g^{-1} \in G : g \circ g^{-1} = g^{-1} \circ g = e$$

4. « Αντιμεταθετική ιδιότητα » [αβελιανή ομάδα]

$$g_1 \circ g_2 = g_2 \circ g_1, \forall g_1, g_2 \in G$$

★ Συνήθως θα μιλάμε για G αβελιανή ομάδα.

Ορισμός:

1. Έστω G αβελιανή ομάδα, $X \subseteq G$ η υποομάδα που παράγεται απ' το X . Τότε: $\langle X \rangle = \{n_1x_1 + \dots + n_kx_k \mid n_i \in \mathbb{Z}\}$

2. Το X είναι « βάση της G », αν :

i. $\langle X \rangle = G$

ii. $n_1x_1 + \dots + n_kx_k = 0 \Rightarrow n_1 = \dots = n_k = 0$

(Το $\mathbb{Z}_2$ δεν έχει βάση!) $2 \cdot 1 = 0$ (εξωτερικά)

Θεώρημα:

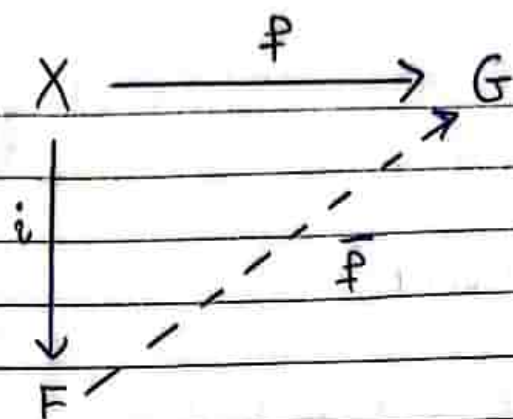
Έστω αβελιανή ομάδα F . ΤΑΕΙ

1. Η F έχει μη μηδενική βάση X .

2. Η F είναι ενθύ άθροισμα απείρων κυκλικών ομάδων.

3. Η F είναι ισόμορφη με ενθύ άθροισμα των $\mathbb{Z}$.

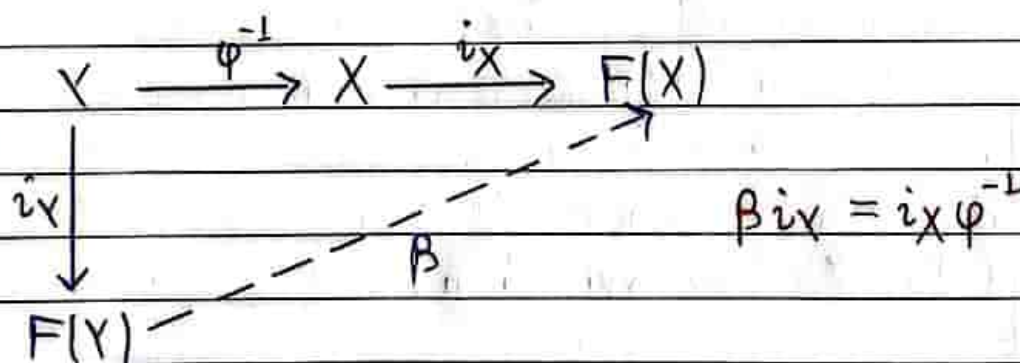
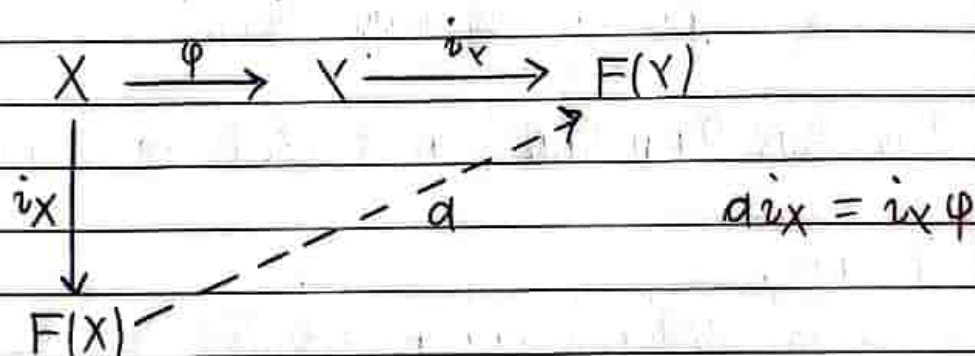
4. $\exists$ εμφύτευση $\iota : X \rightarrow F$ έτσι, ώστε:



- G αβελιανή
- $\exists$ ισομορφισμός $\bar{f}: F \rightarrow G$ ώστε $\bar{f} \circ i = f$
 (Το τελευταίο εκφράζει στους διανυσματικούς χώρους ότι για να γνωρίσουμε τα στοιχεία του χώρου, αρκεί να γνωρίσουμε τα στοιχεία της βάσης.)

Σχόλιο:

Έστω ότι $|X| = |Y|$ (δηλαδή $\exists \varphi: X \rightarrow Y$ 1-1 και επί).
 Τότε παίρνουμε ότι $F(X) \cong F(Y)$.



$\beta \circ \alpha \circ i_X = \beta \circ i_Y \circ \varphi = i_X \circ \varphi^{-1} \circ \varphi = i_X \Rightarrow \beta \alpha = 1_{F(X)}$
 Όμοια $\alpha \beta = 1_{F(Y)}$. Άρα α, β ισομορφισμοί.

Απόδειξη θεωρήματος:

κανονική
υποομάδα

$$(1) \Rightarrow (2) \quad X \text{ βάση: } \forall x \in X; nx = 0 \Rightarrow n = 0$$

Άρα η $\langle X \rangle$ είναι απείρη κυκλική. Επίσης $\langle X \rangle \trianglelefteq F$,
γιατί F αβελιανή.

$$F = \langle X \rangle \Rightarrow F = \left\langle \bigcup_{x \in X} \langle x \rangle \right\rangle \quad (a)$$

$$\text{Έστω } z \in X, \langle z \rangle \cap \left\langle \bigcup_{x \in X \setminus \{z\}} \langle x \rangle \right\rangle \neq 0.$$

$$nz = n_1 x_1 + \dots + n_k x_k \Rightarrow n_1 x_1 + \dots + n_k x_k - nz = 0 \Rightarrow \\ \Rightarrow n_1 = \dots = n_k = n = 0, \text{ άτοπο!}$$

$$\text{Άρα } \langle z \rangle \cap \left\langle \bigcup_{x \in X \setminus \{z\}} \langle x \rangle \right\rangle = 0, \quad (b)$$

$$\text{Άρα } F = \sum_{x \in X} \langle x \rangle, \text{ απ' τις (a) και (b).}$$

$$(2) \Rightarrow (3) \quad \text{Τετριμμένο!}$$

$$(3) \Rightarrow (1) \quad F \xrightarrow{\varphi} \sum_{x \in X} \mathbb{Z}, \quad \forall x \in X, \vartheta_x = (u_i)_{i \in X}, u_i = \begin{cases} 0, & i \neq x \\ 1, & i = x \end{cases}$$

Τότε $\{\vartheta_x\}$ βάση του $\sum \mathbb{Z}$ (παραφάνες!).

Επίσης $\{\varphi^{-1}(\vartheta_x)\}$ βάση της F .

$$(1) \Rightarrow (4) \quad \text{Έστω } u \in F, u = n_1 x_1 + \dots + n_r x_r \text{ (μοναδικό!)}$$

$$\left. \begin{aligned} u &= n_1 x_1 + \dots + n_r x_r \\ u &= m_1 x_1 + \dots + m_r x_r \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow n_1 x_1 + \dots + n_r x_r = m_1 x_1 + \dots + m_r x_r \Rightarrow$$

$$\Rightarrow (n_1 - m_1) x_1 + \dots + (n_r - m_r) x_r = 0 \Rightarrow$$

$$\Rightarrow n_1 - m_1 = \dots = n_r - m_r = 0 \Rightarrow$$

$$\Rightarrow n_1 = m_1 \text{ και } \dots \text{ και } n_r = m_r$$

Ορίσουμε $\bar{f}(u) = n_1 f(x_1) + \dots + n_k f(x_k)$ και $\bar{f} \circ i = f$.

Αν υπήρχε $g: F \rightarrow G$ ώστε $g \circ i = f$, τότε $\forall x \in X$:

$$g(x) = g(i(x)) = f(x) = \bar{f}(x), \text{ άρα } g = \bar{f}.$$

$$(4) \Rightarrow (3) \quad Y = \{\vartheta_x \mid x \in X\} \text{ βάση του } \sum \mathbb{Z}$$

$$Y \xrightarrow{\bar{f}} G$$

$$i \downarrow \quad \nearrow \bar{f} \\ \sum \mathbb{Z} \quad \quad \quad$$

«βαθμός της F »

Θεώρημα :

Κάθε δύο βάσεις της F έχουν την ίδια πληθικότητα.

Απόδειξη θεωρήματος :

$$F \cong \underbrace{\mathbb{Z} \oplus \mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n \text{ όροι}}$$

υπομάδα
↑

Για κάθε αβελιανή ομάδα $G : 2G = \{2g \mid g \in G\} < G$.

Ο ισομορφισμός περιορίζεται σε ισομορφισμό :

$$2F \cong 2\mathbb{Z} \oplus 2\mathbb{Z} \oplus \dots \oplus 2\mathbb{Z}.$$

$$F/2F \cong (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus \dots \oplus (\mathbb{Z}/2\mathbb{Z})$$

Παίρνουμε ότι $|F/2F| = 2^n$.

Για μία άλλη βάση με m στοιχεία : $|F/2F| = 2^m$.

Άρα $2^n = 2^m \Rightarrow n = m$. ■

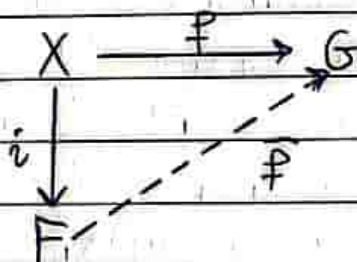
Θεώρημα :

Κάθε αβελιανή ομάδα είναι ομομορφική εικόνα μιας ελεύθερης αβελιανής ομάδας βαθμού $|X|$, όπου X ένα σύνολο γεννητόρων της ομάδας.

Απόδειξη θεωρήματος :

$$F \cong \sum_{x \in X} \mathbb{Z}$$

Τότε $\text{Im } \bar{f} = G$, γιατί
το X παράγει την G . ■



Λήμμα :

Ελεύθερη αβελιανή ομάδα $F = \langle x_1, \dots, x_n \rangle$, $a \in \mathbb{Z}$

Τότε $\forall i \neq j$ το $\{x_1, \dots, x_{j-1}, x_j + ax_i, x_{j+1}, \dots, x_n\}$ βάση της F
 $\cong X'$

Απόδειξη λήμματος :

Είναι $x_j = -ax_i + (x_j + ax_i)$, άρα $x_j \in F(X')$ και όλα τα άλλα στοιχεία του X ανήκουν. Άρα X' παράγει την F .
Τώρα ελέγχουμε τη γραμμική ανεξαρτησία.

$$\begin{aligned}
 & k_1 x_1 + \dots + k_j (x_j + a x_i) + \dots + k_n x_n = 0 \Rightarrow \\
 & \Rightarrow k_1 x_1 + \dots + (k_i + k_j a) x_i + \dots + k_j x_j + \dots + k_n x_n = 0 \Rightarrow \\
 & \Rightarrow k_1 = \dots = k_n = 0 \text{ και } k_i + k_j a = 0, \text{ άρα } k_i = 0 \blacksquare
 \end{aligned}$$

Θεώρημα:

F ελεύθερη αβελιανή βαθμού n και $G < F$

Τότε υπάρχει βάση $\{x_1, \dots, x_n\}$ της F , r ($1 \leq r \leq n$) και θετικοί ακέραιοι $d_1 | d_2 | \dots | d_r$, ώστε η G είναι ελεύθερη αβελιανή ομάδα στο $\{d_1 x_1, \dots, d_r x_r\}$.

Απόδειξη Θεωρήματος:

Για $n=1$, εντάξει! Επαγωγικά, υποθέτουμε ότι ισχύει για όλες τις (ελεύθερες αβελιανές) ομάδες βαθμού $< n$. Έστω $S =$ το σύνολο όλων των s , ώστε $\exists$ βάση $\{y_1, \dots, y_n\}$ της F και ένα στοιχείο της G της μορφής $s y_1 + k_2 y_2 + \dots + k_n y_n$. Επειδή $k_2 y_2 + s y_1 + k_3 y_3 + \dots + k_n y_n \in G$, τότε $k_2 \in S$ και $k_j \in S$, $j=2, \dots, n$. Επειδή $G \neq 0$, $S \neq \emptyset$ και ο ελάχιστος θετικός ακέραιος στο S , είναι ο d_1 και για μία βάση $\{y_1, \dots, y_n\}$ της F , $v = d_1 y_1 + k_2 y_2 + \dots + k_n y_n \in G$. Γράφουμε $k_i = q_i d_1 + r_i$, $0 \leq r_i < d_1$.

$$v = d_1 (y_1 + q_2 y_2 + \dots + q_n y_n) + r_2 y_2 + \dots + r_n y_n$$

Όλα τα $r_2, \dots, r_n \in S$. Άρα, επειδή d_1 ελάχιστο, παίρνουμε $r_2 = \dots = r_n = 0$. Άρα $v = d_1 x_1 \in G$.

$W = \{x_1, y_2, \dots, y_n\}$ βάση της F

Τότε $H = \langle y_2, \dots, y_n \rangle$ ελεύθερη αβελιανή ομάδα με βαθμό $n-1$ και $F = \langle x_1 \rangle \oplus H$. Επίσης έχουμε ότι: $G = \langle v \rangle \oplus (G \cap H)$. Πράγματι, $\langle v \rangle \cap (G \cap H) = 0$, γιατί $\{x_1, y_2, \dots, y_n\}$ βάση της F . Τώρα, αν $u = t_1 x_1 + \dots + t_n x_n \in G$ και $t_1 = d_1 q_1 + r_1$, $0 \leq r_1 < d_1$, τότε η G περιέχει: $u - q_1 v = r_1 x_1 + \dots + t_n y_n$. Είναι δι' ελάχιστο $\Rightarrow r_1 = 0$ και $t_2 y_2 + \dots + t_n y_n \in H \cap G$, $u = q_1 v + (t_2 y_2 + \dots + t_n y_n)$. Άρα $G = \langle v \rangle + G \cap H$.

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{3^4} \oplus \mathbb{Z}_{5^3} \cong \mathbb{Z}_{40500}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{4 \cdot 8 \cdot 25} = \mathbb{Z}_5 \oplus \mathbb{Z}_{8100}$$

(καλύτερα σαν γραμμές)

$$2 \quad 1+1$$

$$3 \quad 2+1 \quad 1+1+1$$

$$4 \quad 3+1 \quad 2+2 \quad 2+1+1 \quad 1+1+1+1$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{1820}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{13500} = \mathbb{Z}_3 \oplus \mathbb{Z}_{4 \cdot 27 \cdot 125}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{2700}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{540}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{1500}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{45} \oplus \mathbb{Z}_{900}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{13500}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{900}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{180}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{30}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{900}$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{60}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{20250}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{40050}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{10} \oplus \mathbb{Z}_{810}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_{125} \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{6750}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30} \oplus \mathbb{Z}_{1350}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{270}$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{125} \cong \mathbb{Z}_{18} \oplus \mathbb{Z}_{2250}$$

Δευτέρα 13/10/2025

Διάλεξη 3

Θεώρημα:

Εστω G πεπερασμένη παραχόμενη αβελιανή ομάδα. Τότε η $G \cong$ με το πεπερασμένο ευθύ άθροισμα κυκλικών ομάδων όπου οι πεπερασμένες (αν υπάρχουν) έχουν τάξεις $m_1 \dots m_t$.
 $G \cong G_{m_1} \oplus \dots \oplus G_{m_t}$, $F \cong \mathbb{Z} \oplus \dots \oplus \mathbb{Z}$

$$G_t < G$$

$$G \cong G_t \oplus F$$

F ελεύθερη αβελιανή (ελεύθερας στρέψης)

$$G_t = \{g \in G \mid |g| < +\infty\} \text{ (ομάδα στρέψης)}$$

Σ αβελιανές ομάδες: $(ab)^m = a^m b^m$.

Παρατήρηση:

Αν $m = p_1^{n_1} \dots p_t^{n_t}$, τότε $\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{n_t}}$.

(Αρα $G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{n_t}} \oplus F$.)

Θεώρημα Lagrange:

Αν $H < G$, τότε $|G| = |H| \cdot |G:H|$. ($|H| \mid |G|$)

Πόρισμα:

Αν $|G| = n$, τότε η G έχει υποομάδα τάξης κάθε διαιρέτη του n (σε αβελιανές).

Λήμμα:

Ισχύει ότι $p^{r-1} \mathbb{Z}_{p^r} \cong \mathbb{Z}_{p^1}$.

Απόδειξη πορίσματος:

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \dots \oplus \mathbb{Z}_{p_t^{n_t}}$$

$$n = p_1^{n_1} \dots p_t^{n_t}$$

$$m \mid n \Rightarrow m = p_1^{m_1} \dots p_s^{m_s} = p_1^{m_1} \dots p_t^{m_t}, \quad m_i \leq n_i, \quad m_i \geq 0.$$

Λήμμα:

Έστω G αβελιανή, $m \in \mathbb{Z}$, $p \in \mathbb{P}$. Τότε οι επόμενες είναι υποομάδες της G .

(i) $mG = \{mg \mid g \in G\}$

(ii) $G[m] = \{g \in G \mid mg = 0\}$

(iii) $G(p) = \{g \in G \mid |g| = p^n \text{ για κάποιο } n\}$

(iv) $G_t = \{g \in G \mid |g| < +\infty\}$

Ειδικότερα, $\exists$ ισομορφισμοί:

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p$, $p^m \mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^{n-m}}$

(vi) $h: G \rightarrow \sum G_i$ ισομορφισμός

Τότε ο h περιορίζεται σε ισομορφισμό στο mG και στο $G[m]$ και $mG \cong \sum mG_i$ και $G[m] \cong \sum G_i[m]$.

(vii) $h: G \rightarrow H$ ισομορφισμός

Τότε $h: G_t \rightarrow H_t$ ισομορφισμός, $G(p) \xrightarrow{h} H(p)$

Απόδειξη:

(v) $\mathbb{Z}_{p^n}[p] \cong \mathbb{Z}_p = \langle p^{n-1} \rangle$

$$u \in \mathbb{Z}_{p^n}[p] \Rightarrow pu = 0 \Rightarrow pu \equiv 0 \pmod{p} \Rightarrow p^n | pu \Rightarrow \\ \Rightarrow p^{n-1} | u \Rightarrow u \in \langle p^{n-1} \rangle \quad (\Leftarrow)$$

Άρα $\mathbb{Z}_{p^n}[p] = \langle p^{n-1} \rangle$.

$p^m \in \mathbb{Z}_{p^n}$, τότε $p^{n-m} \Rightarrow p^m \mathbb{Z}_{p^n} \cong \langle p^m \rangle \cong \mathbb{Z}_{p^{n-m}}$.

Τα υπόλοιπα είναι (λίγο πολύ) άμεσα. ■

Θεώρημα:

Έστω G πεπερασμένη παραχόμενη αβελιανή ομάδα.

(i) Υπάρχει s , ώστε ο αριθμός των απείρων κυκλικών ομάδων σε κάθε διάσπαση της G να είναι s .

(ii) Είτε η G είναι ελεύθερη, ή υπάρχει μία λίστα (έχει α-παραίτητα διαφορετικών) ακεραίων $m_1 | \dots | m_t$; $G \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_t} \oplus F$ (F ελεύθερη αβελιανή).

(iii) Είτε η G είναι ελεύθερη, ή υπάρχει μία λίστα $p_1^{s_1}, \dots, p_k^{s_k}$ που είναι μοναδική (επτός της διάταξης), $p_1, \dots, p_k \in \mathbb{P}$, $s_1, \dots, s_k \in \mathbb{N}^*$, $G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus F$.

Απόδειξη:

(i) $G \cong H \oplus F$, $H =$ ευθύ άθροισμα πεπερασμένων κυκλικών, F ελεύθερη βαθμού s

$$i: H \rightarrow H \oplus F \quad i(H) = G_t \\ h \mapsto (h, 0)$$

$$G/G_t \cong F \oplus H/i(H) \cong F$$

Κάθε διάσπαση της G δίνει στην G/G_t τη δομή ελεύθερης αβελιανής βαθμού s , που δεν εξαρτάται απ' τη διάσπαση.

$$(iii) \quad G \cong \sum_{i=1}^s \mathbb{Z}_{n_i} \oplus F \cong \sum_{j=1}^t \mathbb{Z}_{k_j} \oplus F'$$

n_i, k_j δυνάμεις πρώτων

F, F' ελεύθερες αβελιανές

$$G_t = \sum_{i=1}^s \mathbb{Z}_{n_i} \cong \sum_{j=1}^t \mathbb{Z}_{k_j}$$

$$\left(\sum_{i=1}^s \mathbb{Z}_{n_i} \right) (p) \cong \left(\sum_{j=1}^t \mathbb{Z}_{k_j} \right) (p)$$

Άρα οι άρρι που έχουν την δύναμεις του p είναι ισόμορφοι.

$$\sum_{i=1}^s \mathbb{Z}_{p_i^{a_i}} \cong G \cong \sum_{j=1}^t \mathbb{Z}_{p_j^{b_j}}$$

$$\begin{array}{l} r \Leftarrow s \\ d \Leftarrow t \\ c_j \Leftarrow b_j \end{array} \quad G[p] \cong \sum_{i=1}^s \mathbb{Z}_{p_i^{a_i}}[p] \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{s \text{ άρρι}} \cong \underbrace{\sum_{j=1}^t \mathbb{Z}_{p_j^{b_j}}[p]}_{t \text{ άρρι}} \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{t \text{ άρρι}}$$

Έστω $0 \leq v \leq s$ ο πρώτος δείκτης με $a_i = b_i$, $i \leq v$ και $a_v \neq b_v$. Υποθέτουμε ότι $a_v < b_v$. Επειδή:

$$p^{a_v} \sum_{i=1}^v \mathbb{Z}_{p_i^{a_i}} \cong 0, \quad a_i \leq a_v, \quad p^{a_v} \sum_{i=1}^s \mathbb{Z}_{p_i^{a_i}} \cong \sum_{i=v+1}^s \mathbb{Z}_{p_i^{a_i} - a_v}$$

$$p^{a_v} \sum_{i=1}^t \mathbb{Z}_{p_i^{b_i}} \cong \sum_{i=v+1}^t \mathbb{Z}_{p_i^{b_i} - a_v} \quad (\text{η συνέχεια την Τετάρτη})$$

Δράσεις Ομάδων -

- Θεωρήματα Sylow

Δράσεις ομάδων:

Δράση της G στο σύνολο S , είναι μία απεικόνιση $G \times S \rightarrow S$, $(g, s) \mapsto gs$, ώστε να ισχύουν τα παρακάτω.

i. $e \cdot s = s$

ii. $g_1(g_2 s) = (g_1 g_2) s$

Παραδείγματα:

1. S_n δρα στο $I_n = \{1, \dots, n\}$

$$S_n \times I_n \rightarrow I_n \quad \text{π.χ. } S_3, I_3$$

$$(\sigma, a) \mapsto \sigma(a) \quad ((1, 2), (1)) \mapsto (2)$$

2. $H < G, \quad H \times G \rightarrow G$

$$(h, g) \mapsto hg$$

3. H δρα στην G με συζυγία :

$$H \times G \rightarrow G$$

$$(h, g) \mapsto hgh^{-1}$$

4. $S = \{K \mid K < G\}$

$$H \text{ δρα στο } S \text{ με συζυγία :}$$

$$H \times S \rightarrow S$$

$$(h, k) \mapsto hkh^{-1}$$

★ Έχουμε έναν ομομορφισμό :

$$\alpha : G \rightarrow \text{Aut}(S) = \{f : S \rightarrow S \mid f \text{ 1-1 και επί}\}$$

$$\alpha(g)(s) = gs \quad \text{αυτομορφισμοί στο } S$$

$$(\alpha(g))^{-1} = \alpha(g^{-1})$$

Θεώρημα :

Έστω ότι η G δρα στο S .

(i) $x \sim x' \iff \exists g \in G : gx = x'$ (όπου $x, x' \in S$)

$\sim$ σχέση ισοδυναμίας

(ii) $\forall x \in S, G_x = \{g \mid gx = x\} < G$ (ισοτροπική ομάδα ή σταθεροποιητής του x)

Οι κλάσεις ισοδυναμίας ονομάζονται «τροχιές».

$$[x] = \{y \in S \mid \exists g \in G, gx = y\}$$

$$\text{Σύνολο τροχιών : } S/G$$

★ $\mathbb{Z}$ δρα στο $\mathbb{R}, \quad \mathbb{Z} \times \mathbb{R} \rightarrow \mathbb{R}, \quad (n, r) \mapsto n+r$
 $\mathbb{R}/\mathbb{Z} \cong S^1$ (δυσκολό...)

Απόδειξη :

(i) • $x \sim x \quad (ex = x) \quad \text{[ανακλαστική]}$

• $x \sim y \Rightarrow gx = y \Rightarrow x = g^{-1}y \quad \text{[συμμετρική]}$

$$\bullet \begin{cases} x \sim y \\ y \sim z \end{cases} \Rightarrow \begin{cases} gx = y \\ hy = z \end{cases} \Rightarrow hgx = hy = z \text{ [μεταβατική]}$$

$$(ii) \quad g_1, g_2 \in G_x$$

$$g_1 g_2 x = g_1 x = x \Rightarrow g_1 g_2 \in G_x$$

$$gx = x \Rightarrow g^{-1}x = x \Rightarrow g^{-1} \in G_x \quad \blacksquare$$

Παράδειγμα :

$$G \times G \rightarrow G$$

$$(g, x) \mapsto gxg^{-1}$$

Τροχιά ονομάζεται «κλάση συζυγίας».

$$G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} =$$

$$= \text{«κέντροποίησης του } x \text{»}$$

$$Z(G) := \{g \in G \mid gx = xg, \forall x \in G\} =$$

$$= \text{«κέντρο της } G \text{»}$$

$$S = \{K \mid K < G\}$$

$$G \times S \rightarrow S$$

$$(g, K) \mapsto gKg^{-1}$$

$$G_H = \{g \in G \mid gHg^{-1} = H\} = N_G(H) =$$

$$= \text{«κανονικοποίησης της } G \text{ στην } H \text{»}$$

$$H \triangleleft G \Leftrightarrow N_G(H) = G$$

Θεώρημα :

$$G/G_x \cong [x]$$

Απόδειξη :

$$A : G/G_x \rightarrow [x], \quad gG_x \mapsto gx$$

$$\text{Αν } gG_x = g'G_x, \text{ τότε } g^{-1}g' \in G_x \Rightarrow g^{-1}g'x = x \Rightarrow g'x = gx$$

$$\Rightarrow A(gG_x) = A(g'G_x), \text{ άρα έχουμε καλό ορισμό.}$$

$$\text{Μάλιστα, η } A \text{ είναι αντιστρέψιμη.} \quad \blacksquare$$

Τετάρτη 15/10/2025

Διάλεξη 4

Θεώρημα:

- (i) Έστω G πεπερασμένα παραχόμενη αβελιανή ομάδα. Υπάρχει μοναδικός s , ώστε ο αριθμός των απείρων κυκλικών παρα-
χόντων σε κάθε διάσπαση της G να είναι s .
- (ii) Είτε G ελεύθερη αβελιανή ή υπάρχει μοναδική συλλογή
αναλλοίωτοι
παράγοντες
(όχι απαραίτητα διακριτών) θετικών ακεραίων $1 < m_1 | \dots | m_t$,
ώστε $G \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_t} \oplus F$.
- (iii) Είτε G ελεύθερη αβελιανή ή υπάρχει μοναδική συλλογή
στοιχειώδεις
διαίρετες
θετικών ακεραίων $p_1^{s_1}, \dots, p_k^{s_k}$, ώστε $p_1, \dots, p_k$ (όχι απαραίτητα διακριτοί) πρώτοι και $G \cong \mathbb{Z}_{p_1^{s_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{s_k}} \oplus F$.

Απόδειξη:

$$(iii) \quad G \cong \sum_{i=1}^r \mathbb{Z}_{n_i} \oplus F \cong \sum_{j=1}^d \mathbb{Z}_{k_j} \oplus F'$$

$$G(p) \cong \sum_{i=1}^r \mathbb{Z}_{n_i}(p) \cong \sum_{j=1}^d \mathbb{Z}_{k_j}(p)$$

Θέλουμε να δείξουμε ότι $r = d$ και $n_i = k_j$. Αρχικά να υποθέσουμε ότι $G = G_t$ και ναθε n_i, k_j είναι δύναμη του p . Άρα παίρνουμε τα ακόλουθα.

$$\sum_{i=1}^r \mathbb{Z}_{p^{a_i}} \cong G \cong \sum_{j=1}^d \mathbb{Z}_{p^{c_j}}$$

$$1 \leq a_1 \leq \dots \leq a_r \quad \text{και} \quad 1 \leq c_1 \leq \dots \leq c_d$$

$$G[p] \cong \sum_{i=1}^r \mathbb{Z}_{p^{a_i}}[p] \cong \sum_{j=1}^d \mathbb{Z}_{p^{c_j}}[p]$$

Όμως $\mathbb{Z}_{p^a}[p] \cong \mathbb{Z}_p$, γιατί: $x \in \mathbb{Z}_{p^a}[p]$ έχει τάξη p ,
αν $px \equiv 0 \pmod{p^a} \Rightarrow p^a | px \Rightarrow p^{a-1} | x \Rightarrow x \in \langle p^{a-1} \rangle \subset \mathbb{Z}_p$.
 $G[p] \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{r \text{ φορές}} \cong \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{d \text{ φορές}}$. Άρα $r = d$.

Έστω v ($1 \leq v \leq r$) ο πρώτος ακεραίος, ώστε $a_i = c_i$ για όλα τα $i < v$ και $a_v \neq c_v$. Τότε: $p^{a_v} \mathbb{Z}_{p^{a_i}} = 0$ για $a_i \leq a_v$
 $\Rightarrow p^{a_v} G \cong \sum_{i=v+1}^r \mathbb{Z}_{p^{a_i-a_v}}$ με $r - (v+1) + 1 = r - v$ όρους, με
το παλιό

$a_{v+1} - a_v \leq a_{v+2} - a_v \leq \dots \leq a_r - a_v$, Όμοια, παίρνουμε
 ότι $a_i = c_i$, $1 \leq i \leq v-1$ και $p^{a_v} G \cong \sum_{i=v}^r \mathbb{Z}_{p^{c_i - a_v}}$, $a_v \leq c_v$
 τουλάχιστον

που έχει $r - v + 1$ μη μηδενικούς όρους. Άρα $c_v - a_v = 0$,
 δηλαδή $c_v = a_v$.

(ii) $G \cong \mathbb{Z}_{m_1} \oplus \dots \oplus \mathbb{Z}_{m_t} \oplus F \cong \mathbb{Z}_{k_1} \oplus \dots \oplus \mathbb{Z}_{k_d} \oplus F'$, όπου
 $1 < m_1 | \dots | m_t$ και $1 < k_1 | \dots | k_d$. Μπορούμε να προσθέ-
 τουμε πρώτους σε μηδενική δύναμη, ώστε τα m_i και k_j να
 έχουν την ίδια διάσπαση σε πρώτους.

$$m_1 = p_1^{a_{11}} \dots p_r^{a_{1r}} \quad k_1 = p_1^{c_{11}} \dots p_r^{c_{1r}}$$

$\vdots$

$\vdots$

(p_i διακριτοί)

$$m_t = p_1^{a_{t1}} \dots p_r^{a_{tr}} \quad k_d = p_1^{c_{d1}} \dots p_r^{c_{dr}}$$

$$1 < m_1 | \dots | m_t \Rightarrow 0 \leq a_{ij} \leq \dots \leq a_{tj}$$

$$1 < k_1 | \dots | k_d \Rightarrow 0 \leq c_{ij} \leq \dots \leq c_{dj}$$

$$G_t \cong \sum_{i,j} \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^t \mathbb{Z}_{m_i} \cong \sum_{i=1}^d \mathbb{Z}_{k_i} \cong \sum_{i,j} \mathbb{Z}_{p_j^{c_{ij}}}$$

$$G(p_j) \cong \sum_{i=1}^t \mathbb{Z}_{p_j^{a_{ij}}} \cong \sum_{i=1}^d \mathbb{Z}_{p_j^{c_{ij}}}$$

$$m_1 > 1 \Rightarrow m_i > 1$$

Άρα $\exists p_j : 1 \leq a_{1j} \leq \dots \leq a_{tj}$.

Άρα $\sum_{i=1}^t \mathbb{Z}_{p_j^{a_{ij}}}$ θα έχει t μη μηδενικούς όρους.

Αν' το (iii), το $\sum_{i=1}^d \mathbb{Z}_{p_j^{c_{ij}}}$ θα έχει ακριβώς t μη

μηδενικούς όρους $\Rightarrow t \leq d$. Όμοια $d \leq t$. Άρα $t = d$.

Αν' το (iii), $a_{ij} = c_{ij}$, $\forall i, j \Rightarrow m_i = k_i$. ■

Παραδείγματα :

(i) Να υπολογίσετε την $U(13)$ (ομάδα μονάδων στην $\mathbb{Z}_{13}$).

$$U(\mathbb{Z}_n) = \{x \in \mathbb{Z}_n \mid \exists y : xy = 1\} = \{x \in \mathbb{Z}_n \mid (x, n) = 1\}$$

$$U(\mathbb{Z}_{13}) = \{x \in \mathbb{Z}_{13} \mid (x, 13) = 1\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$$

$$= \mathbb{Z}_{13} - \{0\}$$

Υπάρχουν 2 αβελιανές ομάδες τάξης 12.

$$\mathbb{Z}_{12} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_3 \quad (\text{τάξεις } 2, 3, 6)$$

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \mathbb{Z}_2 \oplus \mathbb{Z}_6 \quad |S| = 4$$

Τα στοιχεία της $\mathbb{Z}_{12}$ έχουν τάξη 2, 3, 4, 6, 12.

Άρα $V(13) = \mathbb{Z}_{12}$.

$$(ii) \quad G \cong \mathbb{Z}_8 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

Να βρεθούν οι αναλλοίωτοι παράγοντες.

$$(\mathbb{Z}_8 \oplus \mathbb{Z}_{27} \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_3) \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong \\ \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{1080}$$

$$(iii) \quad G \cong \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{81} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$$

Να βρεθούν οι αναλλοίωτοι παράγοντες.

$$\mathbb{Z}_3 \oplus \mathbb{Z}_{18} \oplus \mathbb{Z}_{90} \oplus \mathbb{Z}_{11340}$$

(iv) Να βρεθούν όλες οι ομάδες τάξης 200 με 4 στοιχεία τάξης 5 (αβελιανές).

$$200 = 2^3 \cdot 5^2$$

$$G \cong G(2) \oplus G(5)$$

Κάθε στοιχείο τάξης 5 ανήκει στην $G(5)$.

$$G(5) = \mathbb{Z}_{25} \text{ ή } \mathbb{Z}_5 \oplus \mathbb{Z}_5$$

Έχουμε ότι 3 ομάδες περιέχουν το $\mathbb{Z}_{25}$.

- $\mathbb{Z}_8 \oplus \mathbb{Z}_{25}$
 - $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$
 - $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{25}$
- } αυτές είναι!

Τα στοιχεία τάξης 5 στις παραπάνω ομάδες, είναι :

$$(0, 5), (0, 10), (0, 15), (0, 20).$$

Κάθε μία από αυτές έχουν 4 στοιχεία τάξης 5.

- $\mathbb{Z}_8 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Η $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ έχει 24 στοιχεία τάξης 5, (x, y) , $x, y \neq 0$.

Θεώρημα :

$$G / G_x \cong [x]$$

$$[G : G_x] = |[x]|$$

$$[G : G_x] \mid |G|$$

Η τροχιά του x έρχεται σε 1-1 και επί αντιστοιχία με τα συμπόδια της ισοτροπικής ομάδας στην G .

Πρόταση:

Έστω $g \in G$. Ορίζουμε $c_g: G \rightarrow G$, $x \mapsto gxg^{-1}$. Η c_g είναι αυτομορφισμός της G .

Απόδειξη:

$$c_g(x_1 x_2) = g x_1 x_2 g^{-1} = g x_1 g^{-1} g x_2 g^{-1} = c_g(x_1) c_g(x_2)$$
$$x \in \ker c_g \Rightarrow c_g(x) = e \Rightarrow g x g^{-1} = e \Rightarrow x = e \Rightarrow \ker c_g = \{e\} \Rightarrow$$

$\Rightarrow c_g$ μονομορφισμός

$$\forall x: c_g(g^{-1} x g) = g g^{-1} x g g^{-1} = x \Rightarrow c_g \text{ επιμορφισμός} \blacksquare$$

«Εσωτερικοί αυτομορφισμοί της G »:

$$\text{Inn}(G) = \{c_g \mid g \in G\} \text{ ομάδα}$$

$$c_{g_1} \circ c_{g_2} = c_{g_1 g_2}, \quad c_g^{-1} = c_{g^{-1}}$$

Υπάρχει $i: G \rightarrow \text{Inn}(G)$, $g \mapsto c_g$ ομομορφισμός ομάδας,
με $\ker i = C(G)$, $i(g)(x) = c_g(x) = gxg^{-1}$.

$$g \in \ker i \Rightarrow c_g = \text{id}_G \Rightarrow c_g(x) = x, \forall x \in G \Rightarrow$$

$$\Rightarrow gxg^{-1} = x \Rightarrow gx = xg \Rightarrow g \in C(G)$$

$$\text{Επίσης } \text{Inn}(G) \triangleleft \text{Aut}(G), \quad \text{Inn}(G) \cong C_G(G) = Z(G).$$

Πόρισμα:

Έστω ομάδα G , ώστε $|G| < \infty$ και $k < G$.

(i) Ο αριθμός των στοιχείων σε μια κλάση συζυγίας είναι $[G : C_G(x)]$ και διαιρεί το $|G|$.

(ii) Αν $\bar{x}_1, \dots, \bar{x}_n$ οι διακριτές κλάσεις συζυγίας της G , τότε $|G| = \sum_{i=1}^n [G : C_G(x_i)]$. («Εξίσωση τάξης»)

$$C_G(x) = \{g \in G \mid gx = xg\}$$

(iii) Ο αριθμός των υποομάδων της G συζυγείς με την k είναι $[G : N_G(k)]$ και διαιρεί το $|G|$.

Απόδειξη:

(i), (iii) Προφανή!

$$[x] = \{y \in G \mid x = gyg^{-1}\} \text{ και } G_x = C_G(x) \Rightarrow$$
$$\Rightarrow G/G_x = [x] \Rightarrow |[x]| = [G : G_x]$$

(ii) Επειδή η συζυγία είναι σχέση ισοδυναμίας, οι κλάσεις σχηματίζουν μία διαμέριση της G . Οι κλάσεις είναι $\bar{x}_1, \dots, \bar{x}_n$ και $|\bar{x}_i| = [G : C_G(x_i)]$.

$$G = \bigsqcup_{1 \leq i \leq n} [x_i] \Rightarrow |G| = \sum_{1 \leq i \leq n} [G : C_G(x_i)] \quad \blacksquare$$

$$|G| = |C(G)| + \sum_{i=1}^n [G:G_i(x_i)], [G:C_G(x_i)] > 1.$$

(A6)
(I)

Πρόβλημα: $|G| < \infty$, $H < G$ $[G:H] = p$ όπου $p = \text{πρώτος αριθμός πρίμος που διαιρείται}$
 στο $|G| \Rightarrow H \trianglelefteq G$.

Αν: $S = \text{αριθμός διαιρετών με } H \text{ στο } G, |S| = p$.
 και $A(S) \cong S_p$. Έχουμε $G \rightarrow A(S)$ με αμοιβαία αντιστοιχία $\varphi: G \rightarrow A(S)$

Τότε $K \trianglelefteq G$.
 Επιπλέον G/K ισόμορφο με H και ισχύει $|G/K| = |H| = 1$.

Άρα $[G:K] |p| = |S|$.

Αλλά κάθε διαιρετός του $|G/K|$ ορίζει να διαιρείται στο $|G|$.

$[G:K] \cdot |K| = |G|$

Επειδή κανένα από τα $|K|$ ή στο $|G/K|$ δεν είναι $|G/K| = p \cdot 1$.

Διαφορά των τριών $|K|$ ή στο $|G/K|$ $\Rightarrow x^{-1}gx = H$, $\forall x \in G \Rightarrow x^{-1}gx \in H$, $\forall x \in G \Rightarrow g \in H \Rightarrow$

$\Rightarrow K \trianglelefteq H$

$|G/K| = [G:H] \cdot [H:K] = p \cdot [H:K] \geq p \Rightarrow [H:K] = 1, H=K \Rightarrow H \trianglelefteq G$.

Πρόταση: Αν $G/K \cong \text{κυκλικός}$. $\Rightarrow G = \text{αβελιανός}$. ($G \cong Z(G)$).

Αν: $G/K \cong \langle gZ(G) \rangle$.

Για $x, y \in G \Rightarrow x = g^k a, y = g^l a$ όπου $k, l \in \mathbb{Z}$ και $a \in Z(G)$

$$xy = g^k a \cdot g^l a = g^k g^l a a = g^{k+l} a a = g^l g^k a a = g^l a g^k a = yx.$$

Λήμμα: Έστω

$$|H| = p^n$$

δρά στο " S " (γεν. σέλιδο) και $S_0 := \{x \in S \mid hx = x\}$ ^($Hx = H$)

$\forall h \in H$. Τότε $|S| \equiv |S_0| \pmod{p}$

(!) Ομομορφισμός $\alpha: G \rightarrow S$ τότε απεικονίζει h σε $\alpha(h) \in \text{Aut}(S)$. αν είναι διττός, άρα $\exists \ker \alpha$, και αν $\ker \alpha = \{1\} \Rightarrow$ έπεται = πεισμή. (faithful). και αν $\ker \alpha > \{1\} \Rightarrow G/\ker \alpha \rightarrow \text{Aut}(S)$ πεισμή.

Αν $G_S = \{1\} \Rightarrow$ έπεται άμεσα $gx = x \Leftrightarrow g = 1$.
 ^{καρπανάκι/ισοσταθμική δράση (stabilizer)}

Αν: Μια ποσότητα " x " έχει ακριβώς ένα στοιχείο αν $x \in S_0$. Τότε μπορούμε να γράψουμε το $S = S_0 \sqcup \overline{x_1} \sqcup \dots \sqcup \overline{x_n}$ με $|\overline{x_i}| > 1$ για $i=1, \dots, n$. και επομένως το $|S| = |S_0| + |\overline{x_1}| + \dots + |\overline{x_n}|$. Αλλά $|\overline{x_i}| = [H : H_{x_i}] > 1$ και διαιρεί το $|H| = p^n$. Άρα $|\overline{x_i}| \equiv 0 \pmod{p}$. Άρα $|S| \equiv |S_0| \pmod{p}$.

Προίγγελος D. Sylow

(!) Αυτό είναι το αντιστ. D. Lagrange για πρῶτο " p ".

Θεώρημα (Cauchy): $|G| < \infty$ και $p \mid |G| \Rightarrow$ η " G " περιέχει στοιχείο τάξεως " p ".

Απν: Έστω $S = \{ (a_1, \dots, a_p) : a_i \in G \text{ με } a_1 \dots a_p = 1 \}$. Κάθε στοιχείο της " S " καθορίζεται μοναδικά από " $p-1$ " στοιχεία. (γιατί $a_p = (a_1 \dots a_{p-1})^{-1}$).

Άρα, αν $|G| = n$, τότε $|S| = n^{p-1}$.

Επειδή $p \mid n \Rightarrow |S| \equiv 0 \pmod{p}$.

Η κυκλική ομάδα " $\mathbb{Z}_p$ " δρα με κυκλικές μεταθέσεις στο " S ": $k \cdot (a_1, \dots, a_p) =$

$$= (a_{k+1}, a_{k+2}, \dots, a_p, a_1, \dots, a_k)$$

Βασικά παρατηρούμε $k(a_1, \dots, a_p) \in S$ γιατί αν $ab=1 \Rightarrow ba=1$. ($ba = \sigma^{\pm 1}(ab)a = a^{\pm 1} \cdot 1 \cdot a = 1$).

Επίσης $0 \cdot x = x, \forall x \in S$.

Επίσης μπορούμε να δούμε ότι $(k+k') \cdot x = k(k'x)$ άρα " $\mathbb{Z}_p$ " δρα στο " S ".

Τότε $(a_1, \dots, a_p) \in S_0 \Leftrightarrow a_1 = \dots = a_p$ και $(1, 1, \dots, 1) \in S_0$.

Άρα, $S_0 \neq \emptyset \Rightarrow |S_0| > 0$

Άρα $0 \equiv |S| \equiv |S_0| \pmod{p} \Rightarrow 0 \equiv |S_0| \pmod{p}$ το " S_0 " περιέχει τουλάχιστον " p " στοιχεία δηλ.

$$\exists a \neq e: a^2 = 1.$$

Ορισμός: Μια ομάδα των κάθε στοιχείο της έχει τάξη δύναμη του p ονομάζεται p -ομάδα. Αν $H < G$ και $H = p$ -ομάδα $\Rightarrow$ " H " ονομάζεται p -υποομάδα της " G ".

Πρόταση: $G = \text{πεντερ. } p\text{-ομάδα} \iff |G| = p^n$.

Αν: Έστω $G = p$ -ομάδα ($\delta\lambda\omega\sigma\tau\epsilon\ \sigma(g) = p^k, \forall g \in G$) και θεωρούμε $g \in G$. $g \mid |G| \xrightarrow{\text{Θ. Cauchy}}$ Ισορριχτείται της " G " τάξης " g ". Αλλά κάθε στοιχείο της " G " έχει τάξη δύναμη του p άρα από Θ.Α. $g = p$. Άρα $|G| = \text{δύναμη του } p$. Το αντισφ. είναι προφανές.

Πρόταση: $Z(G)$ μιας πεντερ p -ομάδας περιέχει περισσότερα από 1 στοιχεία.

Αν: Το $|G| = |Z(G)| + \sum_{i=1}^k [G : C_G(x_i)]$ $\forall x_i \in [G : C_G(x_i)] > 1$ και η $G = p$ -ομάδα $\Rightarrow |G| = p^n$ και $[G : C_G(x_i)] \mid |G|, \forall i$. Άρα, και το $p \mid [G : C_G(x_i)] \Rightarrow |Z(G)| \equiv 0 \pmod{p}$. Αλλά $|Z(G)| \geq 1 \Rightarrow |Z(G)| > 1$.

Λήμμα: Έστω $H = p$ -υποο. της $G = \text{πεντερ}$. Τότε για $[N_G(H) : H] = [G : H] \pmod{p}$.

Απ: Το $S = \text{αριστερά } H\text{-οὐκλόουα της } "G"$ και $G \curvearrowright S$ με αριστερό πολλαπλασιασμό.

Το $|S| = [G : H]$

Το $xH \in S_0 \iff xHx^{-1} = xH, \forall h \in H. \iff x^{-1}hx \in H, \forall h \in H. \iff x^{-1}Hx = H \iff xHx^{-1} = H.$
 $\iff x \in N_G(H)$. Άρα το $|S_0| = [N_G(H) : H]$ και $|S| \equiv |S_0| \pmod{p} \Rightarrow [G : H] \equiv [N_G(H) : H] \pmod{p}$.

Πρόταση: Αν $\sim H = p$ -υποο. της " G ", $G = \text{πεντερ}$ τ.ο. $p \mid [G : H]$ τότε $N_G(H) \neq H$. (πάρνα $H < N_G(H)$).

Αν: Επειδή $p \mid [G : H] \Rightarrow 0 \equiv [G : H] \equiv [N_G(H) : H] \pmod{p}$. Επειδή $[N_G(H) : H] \geq 1 \Rightarrow [N_G(H) : H] > 1$.

Αν $H, K < G$ τότε $HK = \{hk : h \in H, k \in K\} \subset G$ (είναι " $\leq$ " όταν είτε H είτε K είναι $\leq$).

για $HK < G \iff HK = KH \iff (h_1 k_1)(h_2 k_2) = h_2 k_2 h_1 k_1 = h_2 h_1 k_2 k_1 = h_2 h_1 k_1 k_2 \in HK$ ικανοποιεί οποιοδήποτε $c \in (hk)^{-1} = k^{-1}h^{-1} \in KH = HK \Rightarrow (hk)^{-1} \in HK$ άρα " $\Rightarrow$ " άμεσα. Αν υπαρχε ανόμοιο $\exists h \in H, k \in K$ τότε

Δευτέρα 27/10/2025

Διάλεξη 7

$$I \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow I$$

(i) $\ker f = \{1\} \Rightarrow f$ 1-1

(ii) $\operatorname{Im} g = C \Rightarrow g$ επί

(iii) $\operatorname{Im} f = \ker g$



$g \circ f = \text{τετριμμένη} \Rightarrow$
(εύκολη)
 $\Rightarrow \operatorname{Im} f \subseteq \ker g$

(split short exact sequence)

$$I \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow I$$

$g \circ s = \operatorname{id}_C$

$$0 \rightarrow \mathbb{Z} \xrightarrow{i} \mathbb{Z} \xrightarrow{p} \mathbb{Z}_2 \rightarrow 0$$

Αν υπάρχει s , τότε η $\mathbb{Z}_2$ που είναι στρέψης θα απεικονιζόταν στη $\mathbb{Z}$ που είναι ελεύθερης στρέψης.
($p(1) \neq 0$, αλλά $0 = p(1 \cdot 1) + p(1) = 2p(1)$, δεν υπάρχει μη μηδενικός ακεραίος ώστε $2n=0$) Bockstein

Πρόταση:

Εστω G, H ομάδες, $f: G \rightarrow H$, $g: H \rightarrow G$, $f \circ g = \operatorname{id}_H$.
Τότε $G \cong \ker f \rtimes_{\varphi} H$, $\varphi: H \rightarrow \operatorname{Aut}(\ker f)$ για κάποιον ομομορφισμό φ .

Απόδειξη:

$f \circ g = \operatorname{id}_H \Rightarrow f$ επιμορφισμός, $K = \ker f$
Η ακολουθία $1 \rightarrow K \xrightarrow{i} G \xrightarrow{f} H \rightarrow 1$ είναι ακριβής (i εμφύτευση) και μάλιστα διασπώμενη, ($g: H \rightarrow G$)
Μάλιστα, $K \triangleleft G$. Έχουμε $\varphi(h): K \rightarrow K$, $\varphi(h)(k) = g(h)kg(h)^{-1}$
 $\Rightarrow \varphi(h)(k) \in K$. Ορίζουμε $\alpha: G \rightarrow K \rtimes_{\varphi} H$. Είναι:
 $f(xgf(x^{-1})) = f(x)fgf(x^{-1}) = f(x)f(x^{-1}) = 1 \Rightarrow xgf(x^{-1}) \in K$.
Ορίζουμε λοιπόν $\alpha(x) = (xgf(x^{-1}), f(x))$, $\forall x \in G$. Τότε α ομομορφισμός. Πράγματι, παίρνουμε τα παρακάτω.

$$a(xy) = (xyg(y^{-1}x^{-1}), \#(xy))$$

$$\begin{aligned} a(x)a(y) &= (xg\#(x^{-1}), \#(x))(yg\#(y^{-1}), \#(y)) = \\ &= (xg\#(x^{-1}), \varphi(\#(x))(yg\#(y^{-1})), \#(x)\#(y)) = \\ &= (xg\#(x^{-1}) \cdot \#(x)yg\#(y^{-1})\#(x^{-1}), \#(xy)) = \\ &= (xyg\#(y^{-1}x^{-1}), \#(xy)) \end{aligned}$$

$$K \times_{\varphi} H \xrightarrow{\beta} G$$

$$\beta(k, h) = k \cdot g(h)$$

$$\begin{aligned} a\beta(k, h) &= a(k \cdot g(h)) = \\ &= (kg(h) \cdot g\#(g(h)^{-1}k^{-1}), \#(kg(h))) = \\ &= (k \cdot g(h) \cdot g\#(g(h)^{-1}) \cdot g\#(k^{-1}), \#(k)\#(g(h))) = \\ &= (k \cdot g(h) \cdot g(h^{-1}) \cdot 1, h) = (k, h) \text{ κτλ} \blacksquare \end{aligned}$$

$$I \rightarrow K \xrightarrow{\beta} G \xrightarrow{\alpha} H \rightarrow I$$

$$\begin{array}{ccccccc} & & & \text{II} & & \text{II} & \\ & & & \text{III} & \xrightarrow{\quad} & \text{II} & \\ I & \rightarrow & K & \xrightarrow{\beta} & K \times_{\varphi} H & \xrightarrow{\beta} & H \rightarrow I \end{array}$$

Υπενθύμιση:

Εστω $H, K < G$. Τότε $HK < G \Leftrightarrow HK = KH$.

Παράδειγμα:

Θα βρούμε το $\mathbb{Z}_8 \rtimes \mathbb{Z}_2$.

Υπάρχουν 4 αυτομορφισμοί του $\mathbb{Z}_8$.

$$(x \mapsto x, x \mapsto 3x, x \mapsto 5x, x \mapsto 7x)$$

{1, 3, 5, 7 σχετίζονται
πρώτοι με το 8}

$$(0) \quad (a, b)(c, d) = (a+c, b+d)$$

$$(1) \quad (a, b)(c, d) = (a+3^b c, b+d)$$

$$(2) \quad (a, b)(c, d) = (a+5^b c, b+d)$$

$$(3) \quad (a, b)(c, d) = (a+7^b c, b+d)$$

} μη ισομορφικά!

$$\text{π.χ. } (a, b)(c, d) = (a + \varphi(b)(c), b+d)$$

$$(\varphi : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_8))$$

$$(\varphi(1) : \mathbb{Z}_8 \rightarrow \mathbb{Z}_8, x \mapsto 3x)$$

$$(1) \quad (a, b)^2 = (a, b)(a, b) = (a(1+3^b), 2b) = (a(1+3^b), 0) = (0, 0) \Rightarrow a(1+3^b) \equiv 0 \pmod{8}$$

1η περίπτωση: $b \equiv 0 \pmod{2}$

Τότε $(2a, 0) = (0, 0)$ αν $2a \equiv 0 \pmod{8} \Rightarrow a = 4$ ή 8 .

2η περίπτωση: $b \equiv 1 \pmod{2}$

Τότε $(4a, 0) = (0, 0) \Rightarrow a$ άρτιος. $(0, 2, 4, 6)$

Συνολικά $2+4=6$ στοιχεία με τετράγωνο $(0, 0)$.

$$(2) \quad (a, b)^2 = (a(1+5^b), 0) = (0, 0)$$

$$b \equiv 0 \pmod{2} \Rightarrow 2a \equiv 0 \pmod{8} \Rightarrow a \equiv 0, 4 \pmod{8} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \Rightarrow 4 \text{ στοιχεία}$$

$$b \equiv 1 \pmod{2} \Rightarrow 6a \equiv 0 \pmod{8} \Rightarrow a \equiv 0, 4 \pmod{8}$$

Άρα (1), (2) όχι ισομορφά!

$$(3) \quad (a, b)^2 = (a(1+7^b), 0) = (0, 0)$$

$$b \equiv 0 \pmod{2} \Rightarrow 2 \text{ στοιχεία} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \Rightarrow (1), (2), (3) \text{ όχι}$$

$$b \equiv 1 \pmod{2} \Rightarrow 8a \equiv 0 \pmod{8} \text{ (όλα)} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \text{ ισομορφά}$$

Πρόταση:

Έστω $p > q$ πρώτοι και $q \mid p-1$. Τότε, μετά από ισομορφισμό, υπάρχουν 2 ομάδες τάξης pq .

(i) Η αβελιανή $\mathbb{Z}_{pq}$

(ii) Η μη αβελιανή $\mathbb{Z}_p \rtimes_{\varphi} \mathbb{Z}_q$, όπου $\varphi: \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_p)$ οποιοςδήποτε μη τετριμμένος ομομορφισμός

[Έστω $\varphi: K \rightarrow \text{Aut}(H)$ και $\# \in \text{Aut}(K)$. Τότε :

$$H \rtimes_{\varphi} K \cong H \rtimes_{\varphi \circ \#} K.]$$

$$\alpha: H \rtimes_{\varphi} K \rightarrow H \rtimes_{\varphi \circ \#} K$$

$$(h, k) \mapsto (h, \#^{-1}(k))$$

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot \varphi(k_1)(h_2), k_1 k_2)$$

$$\alpha((h_1, k_1)(h_2, k_2)) = (h_1 \varphi(k_1)(h_2), \#^{-1}(k_1 k_2))$$

$$\alpha(h_1, k_1) \alpha(h_2, k_2) = (h_1, \#^{-1}(k_1)) (h_2, \#^{-1}(k_2)) = \\ = (h_1 \varphi(\#^{-1}(k_1))(h_2), \#^{-1}(k_1 k_2)) \text{ κτλ}$$

Απόδειξη πρότασης:

$S_p = 1 \Rightarrow$ Sylow p -υποομάδα της G είναι κανονική: $P \triangleleft G$

Έστω Q q -Sylow υποομάδα. Υπάρχει ομομορφισμός μη-δίκος $\# : G \rightarrow G/P$, $\ker(\#|_Q) = \ker \# \cap Q = P \cap Q = \{1\}$.

Άρα $\#|_Q$ 1-1. Επειδή $|Q| = q = |G/P|$, άρα $\#|_Q$ είναι

ισομορφισμός. Έχουμε ομομορφισμό $g: G/P \xrightarrow{(\#P)^{-1}} \mathbb{Q}_p^*$
 $\hookrightarrow G$. Τώρα, $f \circ g = f \circ i(\#P)^{-1} = 1_{G/P}$ (γιατί). Άρα
 $G \cong P \rtimes_{\varphi} G/P$. Επίσης $G/P \cong \mathbb{Z}_q$, $P \cong \mathbb{Z}_p$. Άρα
 $G \cong \mathbb{Z}_p \rtimes_{\varphi} \mathbb{Z}_q$, $\varphi: \mathbb{Z}_q \rightarrow \text{Aut}(\mathbb{Z}_p)$.

Αν φ τετριμμένη, τότε $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. Πρέπει να
 δείξουμε για δύο μη τετριμμένους ομομορφισμούς $\varphi, \psi: \mathbb{Z}_q \rightarrow$
 $\rightarrow \text{Aut}(\mathbb{Z}_p)$, ότι $\mathbb{Z}_p \rtimes_{\varphi} \mathbb{Z}_q = \mathbb{Z}_p \rtimes_{\psi} \mathbb{Z}_q$.

Είναι $\text{Aut}(\mathbb{Z}_p) \cong (\mathbb{Z}_p)^{\times} \cong \mathbb{Z}_{p-1}$ (γιατί) και $|\mathbb{Z}_{p-1}| = p-1$.
 Η εικόνα του 1 απεικονίζεται στο $z \in \mathbb{Z}_{p-1}$, με $z^q \equiv 1 \pmod{p}$
 (1 έχει τάξη q στο $\mathbb{Z}_q$). Αν $z=1$, τότε έχουμε τον τετριμ-
 μένο αυτομορφισμό (δεν μας ενδιαφέρει).

Αλλά $|\mathbb{Z}_{p-1}| = p-1$ και $q \mid p-1$, υπάρχουν στοιχεία τάξης
 q στο $\mathbb{Z}_{p-1}$ (Cauchy).

Για κάθε λύση της $z^q \equiv 1 \pmod{p}$ ($z \neq 1$), έχουμε ένα μη-
 ευθύ γινόμενο $\mathbb{Z}_p \rtimes_{\varphi} \mathbb{Z}_q$:

$$(a, b)(c, d) = (a + \varphi(b)(c), b + d).$$

Το σύνολο $\{z \in \mathbb{Z}_{p-1} \mid z^q \equiv 1 \pmod{p}\} \subsetneq \mathbb{Z}_{p-1}$ και δεν είναι
 τετριμμένο. Για κάθε $z \neq 1$, $\langle z \rangle < (\mathbb{Z}_p)^{\times} \cong \mathbb{Z}_{p-1}$ τάξης q,
 της οποίας όλα τα στοιχεία έχουν τάξη q. Άρα ο αριθμός
 των στοιχείων (μη τετριμμένων) τάξης q στο $(\mathbb{Z}_p)^{\times}$ είναι q-1.

★ στην
 $\langle z \rangle$

Εστω δύο στοιχεία z_1, z_2 τάξης q. Παράγουν την ίδια
 υποομάδα, αν $z_2 = z_1^r$, $(r, q) = 1$.

$$\varphi_1, \varphi_2: \mathbb{Z}_q \rightarrow (\mathbb{Z}_p)^{\times}$$

$$\varphi_1(b) = z_1^b, \quad \varphi_2(b) = z_2^b = z_1^{br}$$

$$(a, b)(c, d) = (a + z_1^b c, b + d)$$

$$(a, b)(c, d) = (a + z_1^{br} c, b + d)$$

$$\varphi_2 = \varphi_1 \circ f, \text{ όπου } f: \mathbb{Z}_q \rightarrow \mathbb{Z}_q, f(x) = rx$$

$$\mathbb{Z}_p \rtimes_{\varphi_1} \mathbb{Z}_q \cong \mathbb{Z}_p \rtimes_{\varphi_2} \mathbb{Z}_q \quad \blacksquare$$

Παράδειγμα:

$$q = 2, \quad p > 2 \Rightarrow p \equiv 1 \pmod{2}$$

$$\mathbb{Z}_p \rtimes_{\varphi} \mathbb{Z}_2, \quad \varphi: \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}_p) = (\mathbb{Z}_p)^{\times}, \quad \varphi(1) = -1$$

$$(a, b)(c, d) = (a + (-1)^b c, b + d)$$

$$\mathbb{Z}_2 \rtimes_{\varphi} \mathbb{Z}_2 \rightarrow D_{2p}$$

$$(a, b) \mapsto r^a s^b$$

$r =$ στροφή

$s =$ μία ανάκλαση που περιέχει μία κορυφή του πολυγώνου

Τετάρτη 29/10/2025

Διάλεξη 8

Παραδείγματα:

1. Όλες οι ομάδες τάξης $99 = 3^2 \cdot 11$
 $S_3 \equiv 1 \pmod{3} \quad \left. \begin{array}{l} S_3 \equiv 1 \pmod{3} \\ S_3 \mid 11 \Rightarrow S_3 = 1, 11 \end{array} \right\} \Rightarrow S_3 = 1 \Rightarrow P_3 \triangleleft G$
 $|P_3| = 9 = 3^2 \Rightarrow P_3$ αβελιανή $\Rightarrow P_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_3$ ή $\mathbb{Z}_9$
 $S_{11} \equiv 1 \pmod{11}$
 $S_{11} \mid 3^2 \Rightarrow S_{11} = 1, 3, 9$
Άρα $G \cong P_3 \times P_{11} \begin{cases} \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11} \\ \mathbb{Z}_9 \times \mathbb{Z}_{11} \end{cases}$

(Θεώρημα Burnside: Ομάδες τάξης $p^a q^b$ είναι επιλύσιμες (ωστόσο όχι απλές...))

μη κυκλική

2. Να βρεθεί ο αριθμός στοιχείων τάξης 3 σε μία ομάδα τάξης 57. ($57 = 3 \cdot 19$)

$$S_{19} \equiv 1 \pmod{19} \quad \left. \begin{array}{l} S_{19} \equiv 1 \pmod{19} \\ S_{19} \mid 3 \Rightarrow S_{19} = 1, 3 \end{array} \right\} \Rightarrow S_{19} = 1 \Rightarrow P_{19} \triangleleft G$$

Αν $g \in G$, τότε $|g| = 1, 3, 19, 57$. Όμως $|g| \neq 57$, γιατί G όχι κυκλική. Άρα $|g| = 1, 3, 19$. Κάθε στοιχείο της P_3 έχει τάξη 3. Έχουμε 18 στοιχεία τάξης 19 στην G , αλλά όλα τα υπόλοιπα εντός απ' το τετριμμένο έχουν τάξη 3. Άρα έχουμε $57 - 19 = 38$ στοιχεία τάξης 3.

(Κόλπο: Κατά την εφαρμογή των θεωρημάτων Sylow, ξεκινάμε απ' τον μεγαλύτερο πρωτό.)

3. Έστω ότι $|G| = 231 = 3 \cdot 7 \cdot 11$. Νόο $P_{11} < Z(G)$.
 $S_{11} \equiv 1 \pmod{11} \quad \left. \begin{array}{l} S_{11} \equiv 1 \pmod{11} \\ S_{11} \mid 21 \end{array} \right\} \Rightarrow S_{11} = 1 \Rightarrow P_{11} \triangleleft G$ (Aut(P_{11}) ή Aut(G/P_{11}) ή Sym(G/P_{11}))
 $P_{11} \cong \mathbb{Z}_{11}$

Άρα έχουμε δράση $\psi: G \rightarrow \text{Aut}(\mathbb{Z}_{11}) \cong \mathbb{Z}_{11}^* = \mathbb{Z}_{10}$
με ομομορφισμό.

$$\boxed{\text{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_{\varphi(n)}}$$

Είναι $G/\ker\psi \cong \text{Im}\psi < \mathbb{Z}_{10}$. Άρα $|\text{Im}\psi| = 1, 2, 5, 10$.
Άρα $|G/\ker\psi| = 1, 2, 5, 10$. Τότε $|G/\ker\psi| = 1$, άρα
 $G \cong \ker\psi$, $\forall g \in G$.

$$\psi(g): P_{11} \rightarrow P_{11}, \quad g x g^{-1} = x, \quad \forall x \in P_{11} \quad (\forall g \in G) \Rightarrow \\ \Rightarrow g x = x g, \quad \forall x \in P_{11} \Rightarrow x \in Z(G) \Rightarrow P_{11} < Z(G)$$

4. Έστω $A_4 \triangleleft S_4$ (εναλλάσσουσα υποομάδα).

$$\boxed{A_5 \text{ απλή}}$$

$$|A_4| = 12 = 2^2 \cdot 3$$

Sylow 2-υποομάδες με τάξη 4

$$\{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} = \\ = \langle (1\ 2)(3\ 4), (1\ 4)(2\ 3) \rangle$$

Υπάρχουν 4 Sylow 3-υποομάδες.

$$\langle (1\ 2\ 3) \rangle, \langle (1\ 2\ 4) \rangle, \langle (1\ 3\ 4) \rangle, \langle (2\ 3\ 4) \rangle$$

5. Μια ομάδα τάξης 24 περιέχει μία κανονική τάξης 4 ή 8.
 $|G| = 24 = 2^3 \cdot 3$

Έστω $P = \text{Sylow } 2\text{-υποομάδα της } G$.

$$|P| = 8, \text{ οπότε αν } S_2 = 1, \text{ τότε } P \triangleleft G$$

Γενικά έστω $\alpha: G \rightarrow \text{Sym}(G/P) \cong S_3$ (με αριστερό πολλαπλασιασμό). Έστω $K = \ker\alpha$. Άρα $\forall x \in G$ είναι:
 $k(xP) = xP \quad (k \in K) \Rightarrow x^{-1} k x \in P, \quad \forall x \in G \Rightarrow k \in P \quad (x \in P)$.

Άρα $K < P$. ($K \triangleleft G$) Άρα $|K| \mid 8 \Rightarrow |K| = 1, 2, 4, 8$
και $G/K \leq S_3 \Rightarrow |G/K| = 1, 2, 3, 6$. Άρα $24/|K| = 1, 2, 3, 6 \Rightarrow |K| = 24, 12, 8, 4$. Άρα $|K| = 4, 8$. ($K \triangleleft G$)

6. Να βρεθούν οι ομάδες τάξης $105 = 3 \cdot 5 \cdot 7$.
($|G| = 105$)

$$S_3 \equiv 1 \pmod{3} \quad \} \Rightarrow S_3 = 1, 7$$

$$S_3 \mid 35 \Rightarrow S_3 = 1, 5, 7, 35$$

$$S_5 \equiv 1 \pmod{5} \quad \} \Rightarrow S_5 = 1, 21$$

$$S_5 \mid 21 \Rightarrow S_5 = 1, 3, 7, 21$$

$$S_7 \equiv 1 \pmod{7} \quad \} \Rightarrow S_7 = 1, 15$$

$$S_7 \mid 15 \Rightarrow S_7 = 1, 3, 5, 15$$

Αν $S_5 > 1$ και $S_7 > 1$, τότε $S_5 = 21$ και $S_7 = 15$.

Αρα θα είχαμε $4 \cdot 21 = 84$ στοιχεία τάξης 5 και $6 \cdot 15 = 90$ στοιχεία τάξης 7, όμως $84 + 90 > 105$, άτοπο! Έστω $S_5 = 1 \Rightarrow P_5 \triangleleft G$, Έστω P_7 και $P_5 \cdot P_7 < G$, $(P_7 \cdot P_5 = P_5 \cdot P_7)$ και $|P_7 \cdot P_5| = 35$, αφού $(5, 7) = 1$.

$$\boxed{|K \cdot H| = \frac{|K| \cdot |H|}{|K \cap H|}}$$

Αν $S_7 = 1$, τότε $P_7 \triangleleft G$ και πάλι $|P_7 \cdot P_5| = 35$. Δηλαδή σε κάθε περίπτωση η G έχει μία υποομάδα H με $|H| = 35$, $|G/H| = 3$. Θέω $H \triangleleft G$.

$\alpha: G \rightarrow \text{Sym}(G/H) \cong S_3$ με αριστερό πολλαπλασιασμό $K = \ker \alpha$ και $G/K \cong \alpha(G) \Rightarrow |G/K| \mid 6 \Rightarrow |G/K| = 1, 2, 3, 6$ και $|G/K| \mid |G|$ (Θεώρημα Lagrange), άρα $|G/K| \mid 105$. Άρα $|G/K| \mid (6, 105) = 3 \Rightarrow |G/K| = 1, 3$.

$k \in K: k \cdot g \cdot H = gH \Rightarrow g^{-1}kgH = H, \forall g \in G \Rightarrow k \in H \Rightarrow K \leq H$

Άρα $|G/K|$ διαιρείται διά του $|G/H| = 3$ (Θεώρημα Lagrange). Άρα $|G/K| = 3$.

$$3 = [G:K] = [G:H][H:K] = 3[H:K] \Rightarrow [H:K] = 1 \Rightarrow H = K$$

Άρα $H \triangleleft G$. Επίσης $|H| = 5 \cdot 7$ και $5 \nmid 7-1$. Άρα θα πάρουμε ότι $H \cong \mathbb{Z}_{35}$, στην H

Οι 5 και οι 7 Sylow υποομάδες της H είναι κανονικές. Τότε είναι κανονικές στην G .

Γενικά: Έστω Sylow p -υποομάδα της N , $P \triangleleft N \triangleleft G$. Τότε παίρνουμε ότι $P \triangleleft G$.

$$D_8 = \langle r, s : r^4 = s^2 = 1, rsr^{-1} = s^{-1} \rangle$$

$$\langle r^2 \rangle \triangleleft \langle r \rangle \triangleleft D_8$$

P είναι η μόνη Sylow p -υποομάδα της $N \Rightarrow$

$$\Rightarrow \forall g \in G : gPg^{-1} \leq gNg^{-1} = N \text{ και } |gPg^{-1}| = P \Rightarrow$$

$\Rightarrow gPg^{-1}$ Sylow p -υποομάδα της $N \Rightarrow$

$$\Rightarrow gPg^{-1} = P \text{ (από μοναδικότητα)}$$

Άρα $P_5 \triangleleft G$ και $P_7 \triangleleft G$. Έστω P Sylow 3-υποομάδα της G , $|P|=3$. Τότε για $K = P_7 \cdot P \leq G$ (αφού P_7 είναι κανονική) και $|K|=21$ και $|P_5 \cdot K|=105 \Rightarrow P_5 \cdot K = G$.

Θαό $G \cong P_5 \times K$, δηλαδή τα στοιχεία της P_5 μετατίθενται με τα στοιχεία της K .

Η K δρα στο P_5 με συζυγία.

$$\iota: K \rightarrow \text{Aut}(P_5) \cong \text{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_4$$

$$|K|=21, |\text{Im} \iota| \mid 4 \Rightarrow |\text{Im} \iota| = 1, 2, 4$$

Άρα $|\text{Im} \iota| = 1 \Rightarrow$ τετριμμένη δράση!

$$\text{Άρα } knk^{-1} = n, \forall k \in K, \forall n \in P_5 \Rightarrow kn = nk.$$

$$\text{Άρα } K \cdot P_5 \cong K \times P_5 \text{ (γιατί)}. (K \cap P_5 = \{1\})$$

Άρα έχουμε 2 ομάδες τάξης 105, γιατί έχουμε 2 ομάδες τάξης $21 = 3 \cdot 7$: $\mathbb{Z}_{21}, \mathbb{Z}_7 \times \mathbb{Z}_3$.

Άρα οι ομάδες τάξης 105 είναι: $\mathbb{Z}_5 \times \mathbb{Z}_{21} \cong \mathbb{Z}_{105}$ και $\mathbb{Z}_5 \times (\mathbb{Z}_7 \times \mathbb{Z}_3)$.

7. Έστω $|G| = 72 = 2^3 \cdot 3^2$. Η G δεν είναι απλή.

$$S_3 \cong 1 \pmod{3} \quad \left. \begin{array}{l} \\ \\ \end{array} \right\} \Rightarrow S_3 = 1, 4$$

$$S_3 \mid 8 \Rightarrow S_3 = 1, 2, 4, 8$$

Αν $S_3 = 1$, τότε $P_3 \triangleleft G$, G δεν είναι απλή!

Αν $S_3 = 4$, τότε $S_3 = [G, N_G(P_3)]$. Άρα παίρνουμε ότι $4 = [G : N_G(P_3)]$. Αλλά $N_G(N_G(P_3)) = N_G(P_3)$.

$\iota: G \rightarrow \text{Sym}(G/N_G(P_3)) \cong S_4$, $|S_4| = 24$ με άριστο πολλαπλασιασμό, $|G| = 72 \Rightarrow \ker \iota \neq \{1\} \Rightarrow \ker \iota \triangleleft G$

8. Έστω $|G| = 300 = 2^2 \cdot 3 \cdot 5^2$ (όχι απλή).

$$S_5 \equiv 1 \pmod{5}$$

$$\} \Rightarrow S_5 = 1, 6$$

$$S_5 \mid 12 \Rightarrow S_5 = 1, 2, 3, 4, 6, 12$$

Αν $S_5 = 1$, τότε $P_5 \triangleleft G$ (G όχι απλή).

Αν $S_5 = 6$, τότε $d: G \rightarrow \text{Sym}(G/N_G(P_5)) \cong S_6$.

Είναι $300 \nmid 720$, άρα $\ker d \neq \{1\} \Rightarrow \ker d \triangleleft G$.

9. Έστω $|G| = pqr$. Τότε G όχι απλή.

Αν $p=q=r$, τότε G p -ομάδα, $Z(G) \neq \{1\}$, $Z(G) \triangleleft G$.

Αν $|G| = p^2q$, $p < q$, τότε έχουμε Q Sylow q -υποομάδα.

Αν $Q \triangleleft G$, τότε τελειώσαμε! Κάθε Sylow q -υποομάδα περιέχει $q-1$ στοιχεία τάξης q και είναι διαφορετικά.

$$S_q \equiv 1 \pmod{q}$$

$$S_q \mid p^2 \Rightarrow S_q = 1, p, p^2$$

Αν $S_q = p^2$, τότε θα είχαμε $p^2(q-1) = p^2q - p^2$ στοιχεία τάξης q . Αλλά τα υπόλοιπα p^2 στοιχεία θα ήταν τάξης p και $S_p = 1$. Άρα $\exists$ υποομάδα τάξης p^2 .

Αν $S_q = p$, τότε $p \equiv 1 \pmod{q}$, άτοπο, γιατί $p < q$.

Αν $p < q < r$, τότε παίρνουμε τα παραπάνω.

$$S_r \equiv 1 \pmod{r}$$

$$S_r \mid pq \Rightarrow S_r = 1, p, q, pq$$

Αν $S_r = 1$, τότε τελειώσαμε!

Επίσης $S_r \neq p, q$, γιατί $r > q > p$.

Άρα $S_r = pq$. Άρα έχουμε $pq(r-1)$ στοιχεία τάξης r .

Αν $S_q > 1$, τότε $S_q > p$, άρα έχουμε περισσότερα από $p(q-1) = pq - p$ στοιχεία τάξης q .

$$pq(r-1) + pq - q = pqr - p + p - q = pqr - q$$

Δευτέρα 03/11/2025

Διάλεξη 9

$|G| = r p q \Rightarrow$ δεν είναι απλός!

Αν $n_r = p q$, τότε έχουμε $p q (r-1)$ στοιχεία τάξης r .

Αν $n_q = 1$, τότε εντάξει! Αν $n_q > 1$, τότε $n_q > p$, οπότε έχουμε περισσότερα από $p(q-1)$ στοιχεία τάξης q .

$x_n = \#$ στοιχείων τάξης n στην G

Τότε $xr + xq' > prq - pr + pq - p = prq - p$. Τα στοιχεία τάξης p είναι $|G| - xr - xq < prq - prq + p < p$, άτοπο.
 Άρα $nq = 1 \Rightarrow p_q \triangleleft G$.

Έστω G ομάδα. Ο μεταθετής δύο στοιχείων της G ορίζεται ως: $[x, y] = xyx^{-1}y^{-1}$.

G αβελιανή $\Leftrightarrow [x, y] = 1, \forall x, y \in G$

Η ομάδα μεταθετών $[G, G]$ είναι η υποομάδα της G που παράγεται από τους μεταθετές.

$$[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$$

Άρα κάθε στοιχείο της G είναι γινόμενο μεταθετών.

Επίσης $[G, G] \triangleleft G$.

Έστω $c, d \in [G, G]$ ώστε $c = x_1 \dots x_n, d = y_1 \dots y_n$, όπου x_i, y_i μεταθετές.

$$g c g^{-1} = (g x_1 g^{-1}) (g x_2 g^{-1}) \dots (g x_n g^{-1}), g \in G \Rightarrow$$

$\Rightarrow$ Άρα θα πρέπει $g x_i g^{-1} \in [G, G], \forall i$.

$$\begin{aligned} g x_i g^{-1} &= g a_i b_i a_i^{-1} b_i^{-1} g^{-1} = \\ &= (g a_i g^{-1}) (g b_i g^{-1}) (g a_i^{-1} g^{-1}) (g b_i^{-1} g^{-1}) = \\ &= [g a_i g^{-1}, g b_i g^{-1}] \in [G, G] \end{aligned}$$

Θεώρημα:

Έστω $N \triangleleft G$. Τότε G/N αβελιανή $\Leftrightarrow [G, G] \leq N$.

Ειδικότερα $G/[G, G]$ αβελιανή.

Απόδειξη:

" $\Rightarrow$ " Έστω G/N αβελιανή. Τότε $(aN)(bN) = (bN)(aN), \forall a, b \in G$.
 Άρα $(ab)N = (ba)N \Rightarrow a^{-1}b^{-1}ab \in N \Rightarrow [a^{-1}, b^{-1}] \in N$, άρα η N περιέχει όλους τους μεταθετές $\Rightarrow [G, G] \leq N$.

" $\Leftarrow$ " Ασκηση ...

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & A \text{ αβελιανή} \\ \downarrow \leftarrow p & & \uparrow \\ \text{προβολή } G/[G, G] & \xrightarrow{\exists! \varphi} & \end{array}$$
 ομομορφισμός
 ώστε $\varphi p = \varphi$ (γιατί;)

Έστω G ομάδα, $C(G) \triangleleft G$ το κέντρο της G .

$G \xrightarrow{p_1} G/[G, G]$ p_1 επιμορφισμός

$$C_1(G) = C(G)$$

$$C_2(G) = p_1^{-1}(C(G/[G, G])) \triangleleft G$$

"Ascending Central Series"

(«Αύζουσα Κεντρική Σειρά»)

$$C_3(G) = p_2^{-1}(C(G/C_2(G)))$$

$$p_2: G \rightarrow G/C_2(G)$$

$$\langle 1 \rangle \subset C_1(G) \subset C_2(G) \subset \dots$$

Ορισμός:

G «μηδενοδύναμη», αν $\exists n: C_n(G) = G$

Ισχύει:

Οι αβελιανές ομάδες είναι μηδενοδύναμες.

Θεώρημα:

Κάθε πεπερασμένη p -ομάδα είναι μηδενοδύναμη.

Απόδειξη:

Αν G p -ομάδα, τότε $C_1(G) \neq 1$. Επίσης όλες οι ομάδες $G/C_i(G)$ είναι p -ομάδες, άρα $C(G/C_i(G)) \neq C_i(G)$. Στην αύζουσα κεντρική σειρά έχουμε αυστηρή ανισότητα. Αρα G πεπερασμένη, κάποια στιγμή η σειρά θα τερματίσει. ■

Ορισμός:

G έχει κεντρική σειρά πεπερασμένου μήκους:

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft G_3 \triangleleft \dots \triangleleft G_n = G$$

$$\text{αν } G_{i+1}/G_i \leq C(G/G_i) \triangleleft [G, G_{i+1}] \leq G_i$$

($[H, K]$ η υποομάδα της G που παράγεται απ' τα $[h, k]$, όπου $h \in H, k \in K$).

Αν έχει τέτοια σειρά, τότε είναι μηδενοδύναμη.

$$C_i(G) \neq G, \quad C_i(G) = C_{i+1}(G)$$

$$p_i: G \rightarrow G/C_i(G)$$

$$C_{i+1}(G) = p_i^{-1}(C(G/C_i(G)))$$

«Φθίνουσα Κεντρική Σειρά»

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{1\}$$

Τότε G μηδενοδύναμη.

$$G_{i+1} = [G, G_i]$$

Θεώρημα:

Πεπερασμένο ευθύ γινόμενο μηδενοδύναμων ομάδων είναι μηδενοδύναμη ομάδα.

Απόδειξη:

Έστω $G = H \times K$, Θ δὲ επαγωγικά: $C_i(G) = C_i(H) \times C_i(K)$, Για $i=1$ ισχύει!

$$\begin{array}{ccc} G = H \times K & \xrightarrow{\pi = (\pi_H, \pi_K)} & H/C_i(H) \times K/C_i(K) \\ \varphi \swarrow & & \downarrow \psi \\ \pi_H: H & \rightarrow & H/C_i(H) \\ \pi_K: K & \rightarrow & K/C_i(K) \\ \downarrow & & \downarrow \psi \\ G/C_i(G) = H \times K / C_i(H \times K) & \xleftarrow[\text{επαγωγική υπόθεση}]{} & H \times K / C_i(H) \times C_i(K) \end{array}$$

$$\begin{aligned} C_{i+1}(G) &= \varphi^{-1}(C(G/C_i(G))) = \pi^{-1}\psi^{-1}(C(H/C_i(H) \times K/C_i(K))) = \\ &= \pi^{-1}(C(H/C_i(H) \times K/C_i(K))) = \\ &= \pi^{-1}(C(H/C_i(H)) \times C(K/C_i(K))) = \\ &= \pi_H^{-1}(C(H/C_i(H))) \times \pi_K^{-1}(C(K/C_i(K))) = \\ &= C_{i+1}(H) \times C_{i+1}(K) \end{aligned}$$

Επειδή H, K μηδενοδύναμες, $C_n(H) = H, C_n(K) = K$, άρα $C_n(G) = H \times K = G$. ■

Λήμμα:

G μηδενοδύναμη, $H < G$ μη τετριμμένη
Τότε H μη τετριμμένη υποομάδα του $N_G(H)$.

Απόδειξη :

Ισχύει πάντα ότι $H < N_G(H)$, οπότε αρκεί να δείξουμε ότι $H \leq N_G(H)$.
Αρκεί να βρούμε στοιχείο της $N_G(H)$ που δεν ανήκει στην H . Έχουμε τη φθίνουσα κεντρική σειρά :

$$G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\},$$

Άρα, επειδή $H \neq \{e\}$, $\exists k$ ώστε $G_{k+1} \subseteq H$ και $G_k \not\subseteq H$.

Είναι $G_i = [G_{i-1}, G]$. Έστω $x \in G_k \setminus H$. Τότε $x \in N_G(H)$.

$(G_{k+1} = [G_k, G] < H \Rightarrow \forall y \in H : xyx^{-1}y^{-1} \in H \Rightarrow xyx^{-1} \in H \Rightarrow x \in N_G(H))$. Άρα $H \leq N_G(H)$. ■

Πρόταση :

Μία πεπερασμένη ομάδα είναι μηδενοδύναμη $\Leftrightarrow$ είναι το ευθύ γινόμενο των Sylow υποομάδων της.

Πόρισμα :

G πεπερασμένη μηδενοδύναμη και $m \mid |G| \Rightarrow$
 $\Rightarrow H \leq G$ περιέχει μία υποομάδα τάξης m .

Απόδειξη :

Αν $|G| = p^k$, $(p, n) = 1$ και $1 \leq i \leq k$, τότε η G περιέχει υποομάδα τάξης p^i , $1 \leq i \leq k$ η οποία θα περιέχεται στην p -Sylow υποομάδα. Έστω $p_1^{n_1} p_2^{n_2} \mid |G|$. Τότε $|H_1| = p_1^{n_1}$, $|H_2| = p_2^{n_2}$, τότε $H_1 \cap H_2 = \{e\}$ και $H_1 H_2 = H_2 H_1$. Άρα $H_1 H_2 < G$, $|H_1 H_2| = p_1^{n_1} p_2^{n_2}$. ■

Απόδειξη πρότασης :

" $\Leftarrow$ "

Κάθε πεπερασμένη p -ομάδα είναι μηδενοδύναμη. Άρα αν $G =$ γινόμενο Sylow υποομάδων τότε G μηδενοδύναμη.

" $\Rightarrow$ "

Έστω $P < G$ Sylow p -υποομάδα. Αν $P = G$, τότε τελειώσαμε! Αν $P \neq G$, δηλαδή $P \leq G$, τότε $P \leq N_G(P)$ και φέρουμε ότι $N_G(N_G(P)) = N_G(P)$. Άρα $N_G(P) = G$. Άρα $P < G$. Αν $|G| = p_1^{n_1} \dots p_k^{n_k}$ και $P_1, \dots, P_k$ οι αντίστοιχες Sylow υποομάδες, τότε $|P_i| = p_i^{n_i}$, άρα $P_i \cap P_j = \{e\}$ και $xy = yx$ για

$x \in P_i, y \in P_j$, Άρα $\forall i: P_1 \cdots P_{i-1} P_{i+1} \cdots P_k < G$ και
 κάθε στοιχείο θα έχει τάξη $p_1^{m_1} \cdots p_{i-1}^{m_{i-1}} p_{i+1}^{m_{i+1}} \cdots p_k^{m_k}$
 $(m_i < n_i)$. Άρα $P_i \cap (P_1 \cdots P_{i-1} P_{i+1} \cdots P_k) = \{1\} \Rightarrow$
 $\Rightarrow P_1 \cdots P_k \cong P_1 \times \cdots \times P_k$. Άρα $|P_1 \times \cdots \times P_k| = G \Rightarrow$
 $\Rightarrow G \cong P_1 \times \cdots \times P_k$. ■

Τετάρτη 05/11/2025

Διάλεξη 10

Θεώρημα:

G μη τετριμμένη και μηδενοδύναμη ($G \neq 1$)

$1 \neq N \triangleleft G \Rightarrow N \cap C(G) \neq 1$ και $[G, N] \neq N$

Ειδικά μία μηδενοδύναμη ομάδα έχει μη τετριμμένο κέντρο και η ομάδα μεταθετών είναι μη τετριμμένη υποομάδα.

Απόδειξη:

Έστω $C_i = G$ για κάποιο i . Έστω ότι το i είναι το ελάχιστο έτσι, ώστε $N \cap C_i \neq \{1\}$. Επειδή $[G, C_i] \subseteq C_i$, $[G, N \cap C_i] \subseteq N \cap C_{i-1}$ (άσκηση). Επειδή i ελάχιστο, παίρνουμε: $N \cap C_{i-1} = \{1\} \Rightarrow [G, N \cap C_i] = \{1\} \Rightarrow N \cap C_i \subseteq C(G) = C_1$. Άρα $N \cap C_i \subseteq N \cap C(G)$ και $N \cap C(G) \subseteq N \cap C_i$. Άρα $N \cap C(G) = N \cap C_i \neq 1$. Όσον αφορά το δεύτερο ζητούμενο, αν $[G, N] = N$, τότε $N \leq [G, G] \subseteq C_1$. Επίσης: $N = [G, N] \subseteq [G, C_1] \subseteq C_2$. (Υπενθύμιση: $G^i = [G, G^{i-1}]$). Επαγωγικά, $N \subseteq G^i, \forall i$. Άρα $N = \{1\}$, άτοπο! ■

Θεώρημα:

G μηδενοδύναμη

- (1) Κάθε ελάχιστη κανονική υποομάδα έχει τάξη πρώτο και περιέχεται στο κέντρο,
- (2) Κάθε μέγιστη υποομάδα M είναι κανονική με δείκτη πρώτο και περιέχει την $[G, G]$.

- (3) Αν G πεπερασμένη, $p \mid |G|$, p πρώτος, τότε $\exists$ ελάχιστη κανονική υποομάδα τάξης p και περιέχει μέγιστη υποομάδα με δείκτη p .

Απόδειξη:

- (1) Έστω $N \triangleleft G$ ελάχιστη. Τότε $N \cap C(G) \neq 1$ και $N \cap C(G) \triangleleft G$. Είναι N ελάχιστη, $N = N \cap C(G) \Rightarrow N \subseteq C(G)$. Επειδή $N \subseteq C(G)$, κάθε υποομάδα της N είναι κανονική στην G . Η N είναι ελάχιστη, που σημαίνει $|N| = p$ (N δεν έχει μη τετριμμένη υποομάδα).
- (2) Είναι M μέγιστη, $M \neq N_G(M) \Rightarrow N_G(M) = G \Rightarrow M \triangleleft G$. Το πηλίκο G/M δεν περιέχει μη τετριμμένη υποομάδα ($p: G \rightarrow G/M$ και $H/M < G/M$, τότε $p^{-1}(H/M) \triangleleft G$ και $M \triangleleft M$), $H = M$. Αν G/M έχει τάξη p , τότε G/M αβελιανή $\Rightarrow [G, G] \leq M$.
- (3) Έστω $|G| = p^k m$, $(p, m) = 1$. Γράφουμε $G = P \rtimes H$, P Sylow p -υποομάδα και το H το γινόμενο όλων των άλλων υποομάδων και $C(P) \neq 1$. Μία υποομάδα τάξης p στο $C(P)$ είναι κανονική υποομάδα της G και θα είναι αναγκαστικά ελάχιστη. Η P περιέχει μία υποομάδα K με δείκτη p . Η ομάδα $K \rtimes H$ έχει δείκτη p στην G , άρα είναι μέγιστη. ■

Πόρισμα:

Μη τετριμμένη πεπερασμένη ομάδα G είναι μηδενοδύναμη $\Leftrightarrow$ κάθε μέγιστη υποομάδα είναι κανονική.

Απόδειξη:

" $\Rightarrow$ " Το αποδείξαμε.

" $\Leftarrow$ " Υποθέτουμε ότι κάθε μέγιστη υποομάδα είναι κανονική. Έστω P Sylow με $P \leq N_G(P) < G$. Αν $N_G(P) \neq G$, τότε $\exists M$ μέγιστη: $N_G(P) < M \leq G$. Τότε $M \triangleleft G$ και $P \leq M \leq G$. Η P είναι Sylow υποομάδα της M . (Αν πάρουμε $c_g: G \rightarrow G$ με $c_g(x) = gxg^{-1}$ (εσωτερικός αυτομορφισμός), τότε $c_g|_M: M \rightarrow M$, $\forall g \in G$, P Sylow υποομάδα της M , άρα gPg^{-1} θα είναι και αυτή

Sylow ($|gPg^{-1}| = |P|$) υποομάδα της M . Άρα $gPg^{-1} = hPh^{-1}$, $h \in M \Rightarrow g^{-1}h = x \in N_G(P) \Rightarrow g = hx^{-1}$, $h \in M$, $x^{-1} \in N_G(P)$, άρα $G = M \cdot N_G(P)$. Επειδή M μέγιστη, $M \cdot N_G(P) = M$, αφού $N_G(P) \subseteq M$. Άρα $M = G$. Αφού M μέγιστη, είναι $N_G(P) = G$, οπότε $P \triangleleft G$. Άρα G μηδενοδύναμη. ■

Derived (παράγωγη) σειρά

$$G^{(1)} = G' = [G, G]$$

$$G^{(i)} = (G^{(i-1)})' = [G^{(i-1)}, G^{(i-1)}]$$

$$G > G^{(1)} > G^{(2)} > \dots$$

Η $[G, G]$ είναι πλήρως αναλλοίωτη υποομάδα της G .

Η «πλήρως αναλλοίωτη» $< G \Leftrightarrow \forall$ επιμορφισμό $\varphi: G \rightarrow G; \varphi(H) \subseteq H$

Η $[G, G]$ είναι χινομένο αντιμεταθετών.

$$\varphi([x, y]) = [\varphi(x), \varphi(y)]$$

$$\varphi([G, G]) \subseteq [G, G]$$

Πλήρως αναλλοίωτη υποομάδα είναι κανονική και οι συζυγίες είναι επιμορφισμοί και επομένως $G^{(1)} \triangleleft G$.

Επιλύσιμες Ομάδες

Η G είναι «επιλύσιμη», αν $G^{(n)} = 1$ για κάποιο n .

Η $G^{(i)}$ είναι πλήρως αναλλοίωτη.

Η $G^{(i)} / G^{(i+1)}$ είναι αβελιανή.

Οι αβελιανές ομάδες είναι επιλύσιμες.

Πρόταση:

«Μηδενοδύναμη» $\Rightarrow$ «Επιλύσιμη»

Απόδειξη:

$$1 = C_0(G) \subseteq C_1(G) \subseteq \dots \subseteq C_n(G) = G$$

$$C_i(G) / C_{i-1}(G) = C(G / C_{i-1}(G)) \text{ αβελιανή}$$

$$C_i(G)' < C_{i-1}(G), \quad \forall i > 1$$

αβελιανή

$$\text{Άρα } C(G/C_{n-1}(G)) = C_n(G)/C_{n-1}(G) = G/C_{n-1}(G).$$

Επίσης $G^{(1)} = G' < C_{n-1}(G)$

$$G^{(2)} = (G^{(1)})' < (C_{n-1}(G))' < C_{n-2}(G)$$

$$G^{(3)} < (C_{n-2}(G))' < C_{n-3}(G)$$

$$\vdots$$

$$G^{(n-1)} < (C_2(G))' < C_1(G)$$

$$G^{(n)} < (C_1(G))' = \{e\}.$$

Άρα G επιλύσιμη. ■

Θεώρημα:

- (1) Κάθε υποομάδα και κάθε ηγλίο (ομομορφική εικόνα) μιας επιλύσιμης είναι επιλύσιμη.
- (2) Έστω $N \triangleleft G$ ώστε $N, G/N$ επιλύσιμες. Τότε G επιλύσιμη.

Απόδειξη:

- (1) Έστω $H < G \Rightarrow H^{(i)} < G^{(i)}$. Άρα αν $G^{(n)} = 1$, τότε $H^{(n)} = 1$, άρα H επιλύσιμη.
Έστω $f: G \rightarrow G/H$ επιμορφισμός. Τότε $f(G^{(i)}) = (G/H)^{(i)}$.
Αν $G^{(n)} = 1$, τότε $(G/H)^{(n)} = 1$, άρα G/H επιλύσιμη.
- (2) Έστω $N \triangleleft G$, $N^{(m)} = 1$, $(G/N)^{(n)} = 1$. Τότε $f: G \rightarrow G/N$, $f(G^{(n)}) = f(G/N)^{(n)} = 1$. Άρα $G^{(n)} < \text{Ker } f = N$. Τότε:
 $G^{(n+m)} = (G^{(n)})^{(m)} \leq N^{(m)} = 1$. ■

Θεώρημα Feit-Thompson: (σπουδαίο)

Κάθε ομάδα περττής τάξης είναι επιλύσιμη.

Απόδειξη:

255 σελίδες ... ■

Το αντίστροφο δεν ισχύει, αφού η S_4 είναι επιλύσιμη και $|S_4| = 24$ άρτιος.

Παρατήρηση:

Υπάρχουν επιλύσιμες ομάδες που δεν είναι μηδενοδύναμες.

$$S_3 = G_T = D_6$$

$$C(G_T) = I \Rightarrow C_i(G_T) = I, \forall i$$

Άρα δεν είναι μηδενοδύναμη. Όμως είναι επιλύσιμη!

$\{I\} \subseteq \{I, R_1, R_2\} \subseteq G_T$ derived series (άσκηση:

παρατηρούμε ότι $[G_T, G_T] = \{I, R_1, R_2\}$)

Θεώρημα:

- (1) Κάθε υποομάδα μηδενοδύναμης ομάδας είναι μηδενοδύναμη.
- (2) Κάθε πηλίκο μηδενοδύναμης είναι μηδενοδύναμο.
(Δεν ισχύει το αντίστροφο.)

Απόδειξη:

$$C_0 = G, C_{i+1} = [G, C_i], C_n = I$$

Αν $H \leq G$, τότε $H_i \leq G_i, \forall i$ (επαγωγικά). Για $i=0$ ισχύει. Έστω ότι $C_i(H) \leq C_i(G)$.

$$\{[x, y] \mid x \in H_i, y \in H\} \leq \{[x, y] \mid x \in G_i, y \in G\} \Rightarrow H_{i+1} \leq G_{i+1}$$

Αν $C_n(G) = I$, τότε $C_n(H) = I \Rightarrow H$ μηδενοδύναμη.

Έστω $\varphi: G \rightarrow K$ επιμορφισμός. Έστω $\varphi(C_i(G)) \supseteq \varphi(C_i(K))$.
 $\{[x, y] \mid x \in C_i(K), y \in K\} \subseteq \{[x, y] \mid x \in \varphi(C_i(G)), y \in \varphi(G)\} =$
 $= \{\varphi([x, y]) \mid x \in C_i(G), y \in G\} = \varphi(C_{i+1}(G))$

Αν $C_n(G) = I$, τότε $C_n(K) = I \Rightarrow K$ μηδενοδύναμη. ■

Προσοχή!

$H, G/H$ μηδενοδύναμες $\nRightarrow G$ μηδενοδύναμη

π.χ. $G = S_3, H = \langle (1\ 2\ 3) \rangle = \{I, (1\ 2\ 3), (1\ 3\ 2)\} \cong \mathbb{Z}_3$

$$H \triangleleft G \quad ([G: H] = 2)$$

$$G/H \cong \mathbb{Z}_2$$

$H, G/H$ αβελιανές $\Rightarrow$ μηδενοδύναμες

$C(G) = I \Rightarrow C_n(G) = I, \forall n \Rightarrow G$ όχι μηδενοδύναμη!

Δευτέρα 10/11/2025

Διάλεξη 11

Παραδείγματα:

1. $U = \text{Heis}(\mathbb{R})$ ("Heisenberg") =

$$= \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{R} \right\} \text{ πολύ ενδιαφέροντα!}$$

$$g = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

$$[g, h] = ghg^{-1}h^{-1} = \begin{pmatrix} 1 & 0 & za - xc \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$g \in C(U) \Leftrightarrow \forall x, z: za - xc = 0 \Rightarrow a = c = 0$$

$$B = C(U) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\} \cong \mathbb{R}$$

ως προσθετική ομάδα

$[U, U] = B$, γιατί κάθε στοιχείο του B είναι μεταθέτης και το B είναι ήδη ομάδα

$$U_1 = [U, U] = C_1(U) = C(U)$$

$$C_1(U) = [U, U]$$

$$U/C_1(U) \text{ αβελιανή}, \quad C_2(U)/C_1(U) = C(U/C_1(U)) = U/C_1(U)$$

$$U_2 = [U, U_1] = [U, C(U)] = 1 \Rightarrow C_2(U) = U$$

$$C_0(U) = 1, \quad C_1(U) = B, \quad C_2(U) = U, \dots$$

Έστω F διανυσματικός χώρος.

$$\text{Heis}_n(F) = (n+2) \times (n+2) \text{ πίνακες:}$$

$$\begin{pmatrix} 1 & x_1 & \dots & x_n & z \\ 0 & 1 & \dots & 0 & y_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & y_n \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & * & z \\ 0 & I_n & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & *' & z' \\ 0 & I_n & y' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & *+*' & z+z'+* \cdot y' \\ 0 & I_n & y+y' \\ 0 & 0 & 1 \end{pmatrix}$$

$$(\mathbb{X}, \mathbb{Y}, z) \cdot (\mathbb{X}', \mathbb{Y}', z') = (\mathbb{X} + \mathbb{X}', \mathbb{Y} + \mathbb{Y}', z + z' + \mathbb{X} \cdot \mathbb{Y}')$$

$$(\mathbb{X}, \mathbb{Y}, z)^{-1} = (-\mathbb{X}, -\mathbb{Y}, -z + \mathbb{X} \cdot \mathbb{Y})$$

2. $G = D_{2n}$, $G_1 = [G, G] = \langle r^2 \rangle$ Για D_2, D_4 , εύκολο!

$$G = \langle r, s \mid r^n = s^2 = 1, srs = r^{-1} \rangle =$$

$$= \langle x, y \mid x^2 = y^2 = (xy)^n = 1 \rangle$$

Αν n περιττός, τότε $\langle r^2 \rangle = \langle r \rangle$, $[D_{2n}, \langle r \rangle] = \langle r^2 \rangle = \langle r \rangle$,
άρα $G_i = \langle r \rangle$ για $i \geq 1$.

Αν n άρτιος, τότε $n = 2^k m$, $G_i = \langle r^{2^i} \rangle$, $1 \leq i \leq k$, G_1 σταματάει στο $i = k$, γιατί το r^{2^k} έχει περιττή τάξη, $G_i = \langle r^{2^k} \rangle$, $i \geq 1$.

3. $G = S_n$, $n \geq 3$, $S_n' = A_n = [S_n, S_n]$

Γράφουμε $(abc) = (ab)(bc) \in A_n$, $a \neq b \neq c \neq a$.

$$[(ab), (abc)] = (abc)$$

Άρα $[S_n, A_n] = A_n = G_2$. Τότε $G_i = G_1$, $i \geq k$.

4. $G = A_n \Rightarrow A_n' = A_n$, $n \geq 5 \Rightarrow G_i = G$, $\forall i \geq 0$

Για $n = 4$: $V = \{(1), (12)(34), (13)(24), (14)(23)\} \triangleleft A_4$.

$A_4' = V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, είναι άβα τάξης 2

Για $n = 3$: $G_1 = A_3' = \{1\}$.

5. D_{2n} , $C(D_{2n}) = 1$, n περιττός

$$D_{2n} = \langle x, y \mid x^n = y^2 = e, yxy^{-1} = x^{-1} \rangle$$

1^η περίπτωση: $n = 2m$, $m \geq 3$ περιττός

$$C_1 = \langle r^m \rangle$$

$D_{2n}/C_1 = \langle \bar{r}, \bar{s} \rangle$, $\bar{r}$ έχει τάξη $n/2$ και η ομάδα έχει παράσταση με γεννήτορες και σχέσεις της διεφινής (τάξη 2).

$$D_n/C_1 \cong D_n = D_{2n}, C(D_{2m}) = 1$$

$$C_2 = C_1 \Rightarrow C_1 = C_i, \forall i \geq 1$$

2^η περίπτωση: $n = 2^k m$, m περιττός

$$C_1 = \langle r^{n/2} \rangle, D_{2n}/C_1 = \langle \bar{r}, \bar{s} \rangle = D_{n/2} \cdot 2$$

$$C(D_{2n}/C_1) = \langle \bar{r}^{n/4} \rangle \text{ και } D_2/C_2 \text{ έχει τάξη } n/4$$

$$D_n/C_2 \cong D_{n/4}$$

επαγωγικά

Για $i \leq k$: $C_i \cong \langle r^{\frac{n}{2^i}} \rangle$, $D_n / C_i \cong D_2 \cdot n/2^i$.

$D_n / C_k \cong D_m$ έχει τετριμμένο κέντρο

$C_{k+1} = C_k \Rightarrow C_i = C_k, i \geq k$

3η περίπτωση: $n = 2^k$

(D_2, D_4 αβελιανές)

$C_i = \langle r^{n/2^i} \rangle = \langle r^{2^{k-i}} \rangle$

$D_n / C_i = D_2 \cdot n/2^i \cong D_2 \cdot 2^{k-i}, 0 \leq i \leq k-1$

$D_n / C_{k-1} = \langle \bar{r}, \bar{s} \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2 = D_2$ αβελιανή

$C_k = D_{2n}$

$G_0 = \{1\} \subseteq \langle r^{n/2} \rangle \subseteq \langle r^{n/4} \rangle \subseteq \langle r^{n/8} \rangle \subseteq \dots \subseteq \langle r^{n/2^{k-1}} \rangle = G.$

Ορισμός:

Μία υποκανονική σειρά της G είναι μία σειρά: $G_0 = G > G_1 > \dots > G_n$, όπου $G_{i+1} \triangleleft G_i, i = 0, 1, \dots, n$ και G_i / G_{i+1} το πηλίκο της σειράς. Το μήκος είναι το πλήθος των αυστηρών εμφυτεύσεων ή το πλήθος των μη τετριμμένων παραχόντων. Μία υποκανονική σειρά λέγεται κανονική, αν $G_i \triangleleft G$.

Παράδειγμα:

$S_4 \triangleright A_4 \triangleright V \triangleright 1$ κανονική

Έστω $K = \{1, (1\ 2)(3\ 4)\} \cong \mathbb{Z}_2$.

$K \triangleleft V$, τότε: $S_4 \triangleright A_4 \triangleright V \triangleright K \triangleright 1$ είναι υποκανονική, αλλά όχι κανονική, γιατί $K \ntriangleleft S_4$.

Ορισμός:

$G = G_0 > G_1 > \dots > G_n$

Ένα βήμα εκτένυνσης (refinement) είναι μία σειρά της μορφής $G = G_0 > \dots > G_i > N > G_{i+1} > \dots > G_n$. Μία εκτένυνση είναι μία πεπερασμένη ακολουθία βημάτων εκτένυνσης. Μία εκτένυνση ονομάζεται κατάλληλη, αν το μήκος της είναι αυστηρά μεγαλύτερο της αρχικής. Μία υποκανονική σειρά $G = G_0 > \dots > G_n = \{e\}$ είναι σειρά σύνθεσης, αν κάθε πηλίκο είναι απλή και επιλύσιμη αν κάθε πηλίκο

είναι αβελιανή. Αν $N \triangleleft G$, τότε κανονική υποομάδα της G/N έχει τη μορφή H/N , όπου $N \triangleleft H$. Άρα G/N είναι απλή, αν N μέγιστη στο σύνολο των κανονικών υποομάδων της G , $\neq G$, N μέγιστη κανονική υποομάδα.

Θεώρημα:

- (i) Κάθε πεπερασμένη ομάδα G έχει σειρά σύνθεσης.
- (ii) Κάθε εκτένυνση μιας επιλύσιμης σειράς είναι επιλύσιμη.
- (iii) Μια υποκανονική σειρά είναι σειρά σύνθεσης $\Leftrightarrow$ δεν έχει κατ'άλληλη εκτένυνση.

Απόδειξη:

- (i) $G_1 =$ μέγιστη κανονική υποομάδα της $G \Rightarrow G/G_1$ απλή
 $G_2 =$ μέγιστη κανονική υποομάδα της $G_1 \Rightarrow G_2/G_1$ απλή
 Αυτή η διαδικασία είναι πεπερασμένη, γιατί G πεπερασμένη, και τερματίζει στο 1.
- (ii) G_i/G_{i+1} είναι αβελιανή και $G_{i+1} \triangleleft H \triangleleft G_i$
 Τότε $H/G_{i+1} < G_i/G_{i+1}$ αβελιανή.
 $G_i/H \cong (G_i/G_{i+1}) / (H/G_{i+1})$ (3^ο Θεώρημα ισομορφισμών)
 Άρα G_i/H αβελιανή.
- (iii) Αν $G_{i+1} \not\trianglelefteq H \not\trianglelefteq G_i$, τότε $H/G_{i+1} \not\trianglelefteq G_i/G_{i+1}$ και καθε κανονική υποομάδα της G_i/G_{i+1} έχει αυτή τη μορφή. Άρα αν G_i/G_{i+1} απλή, τότε δεν έχουμε κατ'άλληλη εκτένυνση. Και το αντίστροφο ισχύει! ■

Θεώρημα:

G επιλύσιμη $\Leftrightarrow$ έχει επιλύσιμη σειρά

Απόδειξη:

- " $\Rightarrow$ " $G > G^{(1)} > \dots > G^{(n)} = \{e\}$ επιλύσιμη ($G^{(i+1)} = [G^{(i)}, G^{(i)}]$)
- " $\Leftarrow$ " Αν $G = G_0 > \dots > G_n = \{1\}$ επιλύσιμη σειρά της G , τότε:
 G/G_1 αβελιανή $\Rightarrow G_1 > G^{(1)}$, G_1/G_2 αβελιανή $\Rightarrow G_2 > G^{(2)}$, ..., $G_i > G^{(i)}$ και $\langle e \rangle = G_n > G^{(n)} \Rightarrow G$ επιλύσιμη. ■

Πρόταση :

Έστω G πεπερασμένη. Τότε G επιλύσιμη $\Leftrightarrow G$ έχει σειρά σύνθεσης, όπου τα ητλήματα είναι κυκλικές πρώτης τάξης.

Απόδειξη :

" $\Leftarrow$ " Μία σειρά σύνθεσης με ητλήματα κυκλικές πρώτης τάξης έχει ητλήματα αβελιανές, άρα είναι επιλύσιμη σειρά, άρα G επιλύσιμη.

" $\Rightarrow$ " Έστω $G = G_0 > \dots > G_n = \{e\}$ επιλύσιμη σειρά. Αν $G \neq G_1$ και H_1 μέγιστη κανονική υποομάδα που περιέχει την G_1 , τότε: αν $H_1 \not\leq G_1$, τότε H_2 μέγιστη κανονική υποομάδα της H_1 , $G > H_1 > H_2 > \dots > H_k > G_1$ και κάθε υποομάδα είναι μέγιστη κανονική της προηγούμενης. Τότε H_i/H_{i+1} απλές αβελιανές, άρα κυκλικές πρώτης τάξης. ■

Ορισμός :

Δύο υποκανονικές σειρές S, T είναι ισοδύναμες, αν $\exists$ μία $1-1$ αντιστοίχια των μη τετριμμένων ητλήματων, έτσι ώστε τα ητλήματα να είναι ισομορφα.

Λήμμα :

Αν S σειρά σύνθεσης, τότε κάθε εκλήπτυνση της S είναι ισοδύναμη με την S .

Λήμμα : (Zassenhaus)

$A, A^*, B, B^* < G$, όπου $A^* \triangleleft A, B^* \triangleleft B$

(i) $A^*(A \cap B^*) \triangleleft A^*(A \cap B)$

(ii) $B^*(A^* \cap B) \triangleleft B^*(A \cap B)$

(iii) $A^*(A \cap B) / A^*(A \cap B^*) \cong B^*(A \cap B) / B^*(A^* \cap B)$

Απόδειξη :

$$B^* \triangleleft B \Rightarrow A \cap B^* \triangleleft (A \cap B) \cap B^* \triangleleft A \cap B$$

$$A^* \triangleleft A \triangleleft A \cap B$$

$$D = (A \cap B^*) / (A^* \cap B) \triangleleft A \cap B$$

$$A^*(A \cap B) \triangleleft A \text{ και } B^*(A \cap B) \triangleleft B$$

$$\mathbb{F}: A^*(A \cap B) \rightarrow A \cap B / D, \ker \mathbb{F} = A^*(A \cap B^*)$$

$$\text{Τότε } A^*(A \cap B^*) \triangleleft A^*(A \cap B),$$

$$A^*(A \cap B) / A^*(A \cap B^*) \cong A \cap B / D \cong B^*(A \cap B) / B^*(A^* \cap B)$$

$$a \in A^*, c \in A \cap B, \mathbb{F}(ac) := Dc \quad \blacksquare$$

$$F_n = \pi_1 \left(\text{flower with } n \text{ petals} \right) \rightarrow \text{algebraic topology}$$

Λήμμα: (Zassenhaus)

$A, A^*, B, B^* < G$, όπου $A^* \triangleleft A, B^* \triangleleft B$

$$(i) \quad A^*(A \cap B^*) \triangleleft A^*(A \cap B)$$

$$(ii) \quad B^*(A^* \cap B) \triangleleft B^*(A \cap B)$$

$$(iii) \quad A^*(A \cap B) / A^*(A \cap B^*) \cong B^*(A \cap B) / B^*(A^* \cap B)$$

Απόδειξη:

$A^* \cap B \triangleleft A \cap B$ όπου

$$B^* \triangleleft B \Rightarrow A \cap B^* = (A \cap B) \cap B^* \triangleleft A \cap B$$

$$A^* \triangleleft A \triangleleft A \cap B$$

$$D = (A \cap B^*) / (A^* \cap B) \triangleleft A \cap B$$

$$A^*(A \cap B) \triangleleft A \text{ και } B^*(A \cap B) \triangleleft B$$

$$\neq: A^*(A \cap B) \rightarrow A \cap B / D, \ker \neq = A^*(A \cap B^*)$$

Τότε $A^*(A \cap B^*) \triangleleft A^*(A \cap B)$, $\neq$ επιμορφισμός

$$A^*(A \cap B) / A^*(A \cap B^*) \cong A \cap B / D \cong B^*(A \cap B) / B^*(A^* \cap B)$$

$$a \in A^*, c \in A \cap B, \neq(ac) := cD \quad \blacksquare \text{ όμοια}$$

$$F_n = \pi_1 \left(\text{η πέταλα} \right) \rightarrow \text{αλγεβρική τοπολογία}$$

Τετάρτη 12/11/2025

Διάλεξη 12

$\neq$ καθώς ορισμένη:

$$a_1 c_1 = ac \Rightarrow a_1^{-1} a = c c_1^{-1} \in (A \cap B) \cap A^* = A^* \cap B \triangleleft D \Rightarrow \\ \Rightarrow cD = c_1 D \text{ και } \neq(ac) = \neq(a_1 c_1)$$

$\neq$ επί: προφανές!

$\neq$ ομομορφισμός:

$$\neq(a_1 c_1 | a_2 c_2) = \neq(a_1 a_3 c_1 c_2) = \star$$

$$A^* \triangleleft A \Rightarrow c_1 a_2 \in c_1 A^* = A^* c_1 \Rightarrow c_1 a_2 = a_3 c_1$$

$$\star = c_1 c_2 D = (c_1 D) (c_2 D) = \neq(a_1 c_1) \neq(a_2 c_2)$$

Πυρήνας της $\neq$:

$$ac \in \ker \neq \Leftrightarrow c \in D \Leftrightarrow c = a_1 c_1, \text{ όπου } a_1 \in A^* \cap B, c_1 \in A \cap B^* \\ \Leftrightarrow ac = (a a_1) c_1 \in A^*(A \cap B^*) \rightsquigarrow \ker \neq = A^*(A \cap B^*) \quad \blacksquare$$

Θεώρημα: (Schröder)

Δύο Κάθε υποκανονική (ή κανονική) σειρά μιας ομάδας έχει υπο-κανονικές (ή κανονικές) εκθετίκοντες που είναι ισοδύναμες.

Θεώρημα: (Jordan-Hölder)

Κάθε δύο σειρές σύνθεσης της G είναι ισοδύναμες. Άρα κάθε ομάδα έχει μία σειρά σύνθεσης που ορίζει μία μοναδική σύνθεση απλών ομάδων.

(i) Κάθε ομάδα έχει μία κανονική σειρά. ($1 \triangleleft G$)

(ii) $1 \triangleleft (2) \triangleleft \mathbb{Z}_6$ } Αμφότερες είναι σειρές σύνθεσης,

$$1 \triangleleft (3) \triangleleft \mathbb{Z}_6 \quad (2)/(1) \cong \mathbb{Z}_3 \text{ και } \mathbb{Z}_6/(2) \cong \mathbb{Z}_2 \quad (1 \cong)$$

$$(3)/(1) \cong \mathbb{Z}_2 \text{ και } \mathbb{Z}_6/(3) \cong \mathbb{Z}_3 \quad (2\eta)$$

$$(iii) \quad 1 \triangleleft \langle r^2 \rangle \triangleleft D_8$$

$$D_8 = \langle r, s \mid r^4 = s^2 = 1, srs = r^{-1} \rangle$$

$$1 \triangleleft \langle r^2 \rangle \triangleleft \langle r \rangle \triangleleft D_8$$

$$\langle r^2 \rangle / (1) \cong \mathbb{Z}_2$$

$$\langle r \rangle / \langle r^2 \rangle \cong \mathbb{Z}_2$$

$$D_8 / \langle r \rangle \cong \mathbb{Z}_2$$

$$D_8 / \langle r^2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$1 \triangleleft \langle s \rangle \triangleleft \langle r^2, s \rangle \triangleleft D_8$$

$$(iv) \quad 1 \triangleleft A_4 \triangleleft S_4$$

$$V := \{(1), (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

(Κάθε στοιχείο της V έχει τάξη 2.)

$$U := \{(1), (1\ 2)(3\ 4)\} \cong \mathbb{Z}_2$$

$$1 \triangleleft U \triangleleft V \triangleleft A_4 \triangleleft S_4, \text{ αλλά } U \not\triangleleft A_4$$

$$(v) \quad \text{Ομάδα } D_{2p}: \quad (p \text{ πρώτος})$$

$$1 \triangleleft \langle r \rangle \triangleleft D_{2p} \quad \left. \vphantom{1 \triangleleft \langle r \rangle \triangleleft D_{2p}} \right\} \text{ ισοδύναμες}$$

$$1 \triangleleft \langle z \rangle \triangleleft \mathbb{Z}_{2p}$$

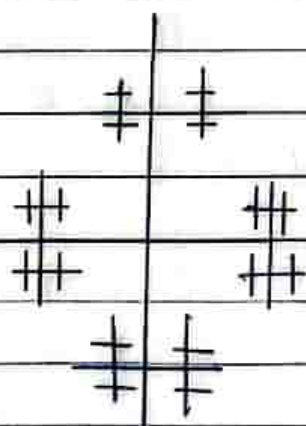
ΕΛΕΥΘΕΡΕΣ ΟΜΑΔΕΣ

Παράδειγμα:

$$F_2 = \langle a, b \rangle = \{1, a, b, a^{-1}, b^{-1}, ab, ba, ab^{-1}, b^{-1}a, a^{-1}b, ba^{-1}, aba, \dots\}$$

Πολλαπλασιασμός είναι (juxtaposition) επικόλληση.

$$X = \begin{array}{c} \circ \\ \diagup \quad \diagdown \\ \text{loop} \end{array} \quad n \text{ φύλλα} \quad \pi(X, x_0) \cong F_n$$

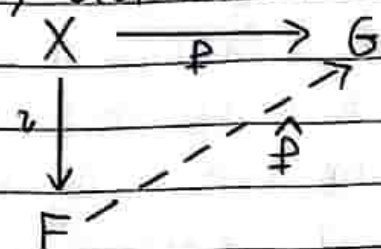


4-κανονικό δέντρο
(νιφάδα)

$$T_4 / F_2 = 8$$

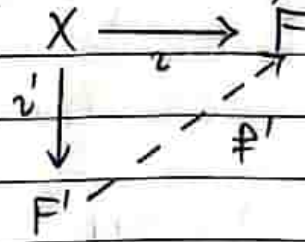
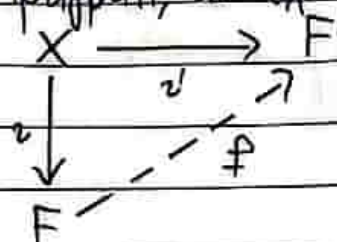
Ορισμός:

Η F είναι «ελεύθερη στο σύνολο X », αν $\exists$ μία εμφύτευση $\iota: X \rightarrow F$, έτσι ώστε:

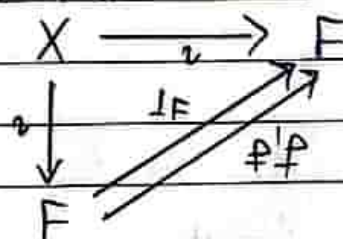


για κάθε ομάδα G και
συνάρτηση $f, \exists! \hat{f}$ ώστε:
 $\hat{f} \circ \iota = f$. $\hookrightarrow$ ομομορφισμός

Αν η F υπάρχει, τότε είναι μοναδική (μετά από ισομορφισμό). Πράγματι, αν έχουμε $F', \iota': X \rightarrow F'$, τότε:



$$f \circ \iota' = \iota \text{ και } f' \circ \iota = \iota$$



$$f' \circ \iota = \iota = f \circ \iota'$$

Από μοναδικότητα:

$f' \circ f = \text{id}_F$ (όμοια $f \circ f' = \text{id}_{F'}$),
άρα f, f' ισομορφισμοί.

Υπαρξη:

$$X \cup X^{-1}$$

X^{-1} ξένο προς το X σύνολο με μία 1-1 επί συνάρτηση στο X , $X \rightarrow X^{-1}, x \mapsto x^{-1}$

Έστω $X' = \text{μονοσύνολο}$, ξένο προς το $X \cup X^{-1}$ που συμβολίζεται με 1 .

Γράφουμε $x^1 = x$ και $x^0 = 1$.

Ορισμός:

Μία λέξη στο X είναι μία ακολουθία $w = (a_1, a_2, \dots)$, όπου $a_i \in X \cup X^{-1} \cup \{1\}$, ώστε $\exists n \in \mathbb{N} : a_i = 1, \forall i \geq n$. Η σταθερή ακολουθία $(1, 1, \dots)$ ονομάζεται «κενή λέξη». Γράφουμε: $w = x_1^{e_1} \dots x_n^{e_n}$, $x_i \in X$, $e_i = \pm 1, 0$ (και $x_i^{-1} \in X^{-1}$). Η ορθογραφία των λέξεων είναι μοναδική $(a_i) = (b_i) \Leftrightarrow a_i = b_i$. Το μήκος της κενής λέξης είναι 0 και το μήκος της λέξης

$\omega = x_1^{e_1} \dots x_n^{e_n}$ είναι η, ορίζουμε $\omega^{-1} := x_n^{-e_n} \dots x_1^{-e_1}$ («αντίστροφη λέξη»). Μια λέξη ονομάζεται «ευτελισμένη» (reduced), αν η ω είναι κενή ή x και x^{-1} δεν είναι γειτονικά. Η αντίστροφη μιας ευτελισμένης λέξης είναι ευτελισμένη. Η v ονομάζεται «υπολέξη» της ω , αν $\omega = \omega' v \omega''$. Μια μη κενή λέξη είναι ευτελισμένη αν δεν περιέχει υπολέξεις της μορφής $x^e x^{-e}$, x^0 . Αν $\omega = x_1^{e_1} \dots x_n^{e_n}$ και $u = y_1^{\delta_1} \dots y_m^{\delta_m}$, τότε $\omega u := x_1^{e_1} \dots x_n^{e_n} y_1^{\delta_1} \dots y_m^{\delta_m}$ και η ωu δεν είναι απαραίτητα ευτελισμένη, εστω και αν οι ω, u είναι. Αν $\omega = \omega' v$ και $u = v^{-1} u'$, τότε $\omega u := \omega' u'$ juxtaposition (αντιπαράθεση).

Θεώρημα:

Για ένα σύνολο X υπάρχει μία ελεύθερη ομάδα με βάση X .

Απόδειξη:

- F = ευτελισμένες λέξεις στο X
- πράξη = η αντιπαράθεση
- μοναδιαίο στοιχείο = η κενή λέξη
- έχουμε αντίστροφο
- Προσεταιριστικότητα: Έχει δαλεια (περιπτώσεις).

Για $x \in X$ ορίζουμε συναρτήσεις $|x|: F \rightarrow F$, $|x^{-1}|: F \rightarrow F$.

$$|x^e| (x_1^{e_1} \dots x_n^{e_n}) = \begin{cases} x^e x_1^{e_1} \dots x_n^{e_n}, & x^e \neq x_1^{-e_1} \\ x_2^{e_2} \dots x_n^{e_n}, & x^e = x_1^{-e_1} \end{cases}$$

Παρατηρούμε ότι $|x^e| \circ |x^{-e}| = |x^{-e}| \circ |x^e| = 1_F$. Άρα η $|x^e|$ είναι μετάθεση της F με αντίστροφο $|x^{-e}|$. Έστω $S_F :=$ συμμετρική ομάδα στην F και $\mathcal{F} := \langle |x| \mid x \in X \rangle \leq S_F$. Τότε η $\mathcal{F}$ είναι ελεύθερη ομάδα με βάση το $[X]$.

Υπάρχει 1-1 και επί $[X] \rightarrow X$, $|x| \mapsto x$.

Ενα $g \in \mathcal{F} - \{1\}$, $g = |x_1^{e_1}| \dots |x_n^{e_n}|$, $e_i = \pm 1$, $|x^e|$ και $|x^{-e}|$ δεν είναι ποτέ γειτονικά. Μια τέτοια παραγοντοποίηση του g είναι μοναδική, γιατί η αλφαριθμητική των λέξεων είναι μοναδική.

$\mathcal{F}$ ελεύθερη :

Έστω $\mathcal{F} : [X] \rightarrow G$, G ομάδα, $\mathcal{F}$ συνάρτηση. Επειδή η παραχρηματοποίηση στην $\mathcal{F}$ είναι μοναδική, ρίχνουμε $\varphi : \mathcal{F} \rightarrow G$ με $\varphi(|x_1^{e_1}| \dots |x_n^{e_n}|) = \mathcal{F}(|x_1^{e_1}|) \dots \mathcal{F}(|x_n^{e_n}|)$. Η φ είναι καλά ορισμένη και επεκτείνει την $\mathcal{F}$. Επειδή το $[X]$ παράγει την $\mathcal{F}$, αρκεί νός η φ είναι ομομορφισμός. Είναι προφανές ότι : $\varphi(\omega \circ \nu) = \varphi(\omega)\varphi(\nu)$, αν ω, ν ετελειωμένα. Αν $\omega = \omega' \nu$, $\nu = u^{-1} \nu'$, τότε $\varphi(\omega) = \varphi(\omega')\varphi(u)$, $\varphi(\nu) = \varphi(u^{-1})\varphi(\nu') = \varphi(u)^{-1}\varphi(\nu')$ αλλά $\varphi(\omega' \nu') = \varphi(\omega')\varphi(\nu') = \varphi(\omega \nu)$. Άρα δείξαμε ότι $\mathcal{F}$ ελεύθερη στο σύνολο X .

$$\tilde{\mathcal{F}} : \mathcal{F} \rightarrow F \quad 1-1 \text{ και επί}$$

$$|x_1^{e_1}| \dots |x_n^{e_n}| \mapsto x_1^{e_1} \dots x_n^{e_n}$$

$$\tilde{\mathcal{F}}([X]) = \mathcal{F}(X) = X \quad (\mathcal{F} : X \rightarrow F)$$

Μπορούμε να θεωρήσουμε ότι η F είναι ισομορφή της $\mathcal{F}$ και είναι ελεύθερη ομάδα με βάση το X . ■

Πόρισμα :

Κάθε ομάδα είναι πηλίκο ελεύθερης ομάδας.

Απόδειξη :

$X = \{x_g : g \in G\}$, $\mathcal{F}$ ελεύθερη ομάδα στο X

$$X \xrightarrow{\mathcal{F}} G$$

$$\begin{array}{ccc} & & (x_g \rightarrow g) \\ \downarrow & \nearrow \varphi & \\ F & & \end{array}$$

Είναι επί, γιατί $\varphi(x_g) = g$, $\forall g \in G$.
Άρα $G \cong F / \ker \varphi$.

Έστω $\Delta =$ συλλογή λέξεων στο X .

$G \cong F/R$, όπου $\mathcal{F}$ ελεύθερη σε κάποιο X και $R =$ κανονική υποομάδα της F που παράγεται απ' το Δ

$(X | \Delta) = \langle X, \Delta \rangle$ παράσταση της G

Για κάθε $v \in \Delta$ γράφουμε $v = 1$ στην G και $\omega \nu \omega^{-1} = 1 \in G$.

Τετάρτη 19/11/2025:

Διάλεξη 13

- (1) Μία ομάδα είναι ελεύθερη αν δρα ελεύθερα σε δέντρο (= γράφημα που δεν έχει loops, δηλαδή κλειστά μονοπάτια), χωρίς αναστροφή.
- (2) Κάθε καλύπτων χώρος (covering space) ενός δέντρου είναι δέντρο.
- (3) Κάθε υποομάδα μίας δεμελιώδους ομάδας είναι δεμελιώδους ομάδα καλύπτοντος χώρου.
- (4) Τελειώσαμε!
(Κάθε υποομάδα ελεύθερης ομάδας είναι ελεύθερη.)

Πόρισμα:

Κάθε ομάδα είναι ηθλίκο ελεύθερης ομάδας.

Απόδειξη:

$$X = \{x_g : g \in G\}$$

$$\begin{array}{ccc} X & \xrightarrow{\iota} & G \\ \downarrow & \nearrow & \\ F(X) & \xrightarrow{\neq} & \end{array} \quad \begin{array}{l} \iota(x_g) = g \\ \neq \text{ επιμορφισμός} \end{array}$$

Ορισμός:

Έστω X σύνολο και Δ οικογένεια λέξεων στο X . Μία ομάδα G έχει γεννήτορες X και σχέσεις Δ , αν $G \cong F/R$, όπου F η ελεύθερη ομάδα στο X και R η κανονική υποομάδα που παράγεται απ' το Δ . Το διατεταγμένο ζεύγος $\langle X | \Delta \rangle$ ή $(X | \Delta)$ ονομάζεται «παράσταση της G ». Τη σχέση: $v \in \Delta$ την γράφουμε $v=1$ στην G . Αν $v=1$ στην G , τότε $wv^{-1}=1$ στην G , $\forall w \in F$.

Η παράσταση ομάδας δεν είναι μοναδική!

Παραδείγματα:

$$(1) \quad \mathbb{Z}_6 = \langle x \mid x^6 = 1 \rangle \quad \langle x, y \mid x^2 = y^3 = 1 \rangle = \mathbb{Z}_2 * \mathbb{Z}_3$$

ελεύθερο γινόμενο

$$F = \langle x \rangle \text{ και } \mathbb{Z}_6 \cong \langle x \rangle / \langle x^6 \rangle$$
$$\mathbb{Z}_6 = \langle x, y \mid \underbrace{x^2 = y^3 = 1}_{\mathbb{Z}_2 \times \mathbb{Z}_3}, \underbrace{xyx^{-1}y^{-1} = 1}_{\text{η ομάδα είναι αντιμεταθετική}} \rangle$$

$$(2) \quad D_{2n} = \langle x, y \mid x^n = y^2 = 1, yxy = x^{-1} \rangle$$

$G = F/R$, $F = \langle x, y \rangle$, $R =$ κανονική υποομάδα που παράγεται απ' το $\langle x^n, y^2, xyxy \rangle$

$$\varphi: F \rightarrow D_{2n}$$

$$\varphi(x) = s \text{ (στροφή)}$$

$$\varphi(y) = \tau \text{ (αντανάκλαση)}$$

Γνωρίζουμε ότι $R \leq \ker \varphi$.

Άρα $F/R \rightarrow F/\ker \varphi$ και έχουμε επιμορφισμό:

$$G = F/R \rightarrow D_{2n} \Rightarrow |G| \geq 2n$$

Κάθε στοιχείο της G έχει τη μορφή $x^i y^j R$ ($0 \leq i < n$, $0 \leq j < 2$).

Άρα $|G| = 2n$ και $G \cong D_{2n}$.

$$(3) \quad \text{«Τετρακτόνια» (quaternions)}$$

$$\left(\begin{array}{ll} n=1 : \mathbb{R} & \Rightarrow S^0 = \{\pm 1\} \\ n=2 : \mathbb{C} & \Rightarrow S^1 \\ n=4 : \mathbb{H} & \Rightarrow S^3 \cong SU(2) = \{A \mid A^{-1} = A^*, \det A = 1\} \\ n=8 : \mathbb{K} & \Rightarrow S^7 \end{array} \right)$$

χάνουμε προσεταιριστικότητα του πολλαπλασιασμού
χάνουμε αντιμεταθετικότητα του πολλαπλασιασμού

αζήν 8

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}$$

$$ij = k, jk = i, ki = j, \quad (3 \text{ complex structures})$$

$$ij = -ji, jk = -kj, ki = -ik, i^2 = j^2 = k^2 = -1$$

$$Q_8 = \langle x, y \mid xyx = y, x^2 = y^2 \rangle$$

$$(4) P(d, m, n) = \langle s, t \mid s^d = t^m = (st)^n = 1 \rangle_K$$

$$P(n, 2, 2) = D_{2n}$$

πολυεδρικές

$$P(2, 3, 3) = A_4$$

ομάδες

$$P(2, 3, 4) = S_4$$

$$P(2, 3, 5) = A_5$$

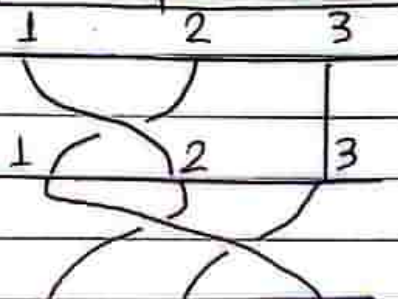
Όλες οι άλλες ομάδες είναι άπειρες.

$$A_4 = ((123), (124)) \quad [(123)(124) = (13)(24)]$$

$$S_4 = ((123), (1324)) \quad [(123)(1324) = (14)]$$

$$A_5 = ((12)(34), (135))$$

(5) «Braid groups» (ομάδες κοτσιδιών):



"συνδέω τα σημεία στον $\mathbb{R}^3$ "

Πώς πολλαπλασιάζω αυτές τις δυο;

$$B_n = \langle c_1, \dots, c_n \mid [c_i, c_j] = 1 \text{ για } j \neq i \pm 1 \text{ και } :$$

$$(*) \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \rangle$$

braid relations

(Αν είναι μακριά, μετατίθενται. Αν όχι, τότε ισχύει η (*).)

Υπάρχει μια προφανής $B_n \rightarrow S_n$ (π.χ. η πρώτη πάνω είναι η (12)). Έχει πυρήνα το P_n ("pure braid groups").

(6) Ελεύθερη αβελιανή ομάδα:

$$G = \langle X \mid xyx^{-1}y^{-1} = 1, \forall x, y \in X \rangle$$

↳ μόνη σχέση: να είναι αβελιανή

Λήμμα:

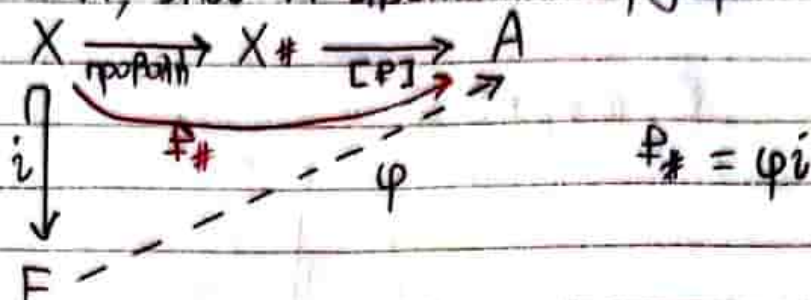
Αν F ελεύθερη ομάδα, τότε F/F^1 ελεύθερη ομάδα, όπου $F^1 = [F, F]$ ομάδα μεταθέσεων.

αβελιανή

Απόδειξη:

Έστω F ελεύθερη ομάδα στο X . Θέω F/F^1 ελεύθερη αβελιανή ομάδα στο $\{xF^1 : x \in X\} = X^\#$.

Έστω $\varphi: X^\# \rightarrow A$, όπου A αβελιανή. Ορίζουμε:



Αν A αβελιανή, $F^1 \leq \ker \varphi$ (επεκτείνει την φ). Άρα, $\tilde{\varphi}: F/F^1 \rightarrow A$, $\omega F^1 \mapsto \varphi(\omega)$. Πρέπει νδὲ $\tilde{\varphi}$ μοναδική. Έστω ὅτι $\theta: F/F^1 \rightarrow A$ επίσης επεκτείνει την φ . Τότε: $\theta(xF^1) = \varphi(xF^1)$, $\forall x \in X$. Παίρνουμε $F \xrightarrow{\pi} F/F^1 \xrightarrow{\theta} A$ ισομορφισμός με $\theta\pi(x) = \theta(xF^1) = \varphi(x)$, $\forall x \in X$ και ξέρουμε ὅτι X βάση F . Άρα $\theta\pi \stackrel{\text{από πριν}}{=} \varphi = \tilde{\varphi}\pi$ και π επί, άρα $\theta = \tilde{\varphi}$. ■

Θεώρημα:

Έστω F, G ελεύθερες με βάσεις X, Y . Τότε $F \cong G \Leftrightarrow |X| = |Y|$.

Απόδειξη:

" $\Rightarrow$ " Έστω $\varphi: F \rightarrow G$ ισομορφισμός. Τότε $F/F^1 \cong G/G^1$ (αβελιανή νοημοποίηση) με βάσεις $X^\# = \{xF^1 | x \in X\}$, $Y^\# = \{yG^1 | y \in Y\}$ (λήμμα). Άρα $|X^\#| = |Y^\#|$ (απ' το αντιστοίχο αποτέλεσμα για αβελιανές, βαθμός $F/F^1, G/G^1$), άρα $|X| = |Y|$.

" $\Leftarrow$ " Αν $|X| = |Y|$, τότε $F \cong G$ (παρόμοια). ■

Ορισμός:

Το $|X|$ ονομάζεται «βαθμός της F ».

Πόρισμα:

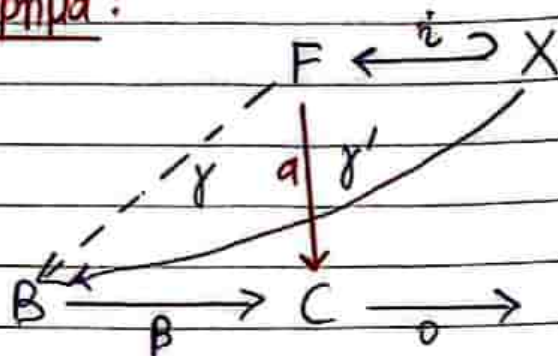
Αν $F = F(X)$ (F ελεύθερη πάνω απ' το X), τότε X παράγει την F .

Απόδειξη:

Έστω Y σύνολο με $|Y| = |X|$ και $\varphi: Y \rightarrow X$ 1-1, επί. Η ελεύ-

Θερή ομάδα G που κατασκευάστηκε χρησιμοποιώντας λέξεις απ' το Y , παράχεται απ' το X . Έστω f ισομορφισμός. Τότε F παράχεται απ' το X . ■

Θεώρημα:



Αν β επιμορφισμός, F ελεύθερη στο X , τότε υπάρχει γ , ώστε: $\beta\gamma = \alpha$.

Απόδειξη:

$$\forall x \in X \exists b_x : \beta(b_x) = \alpha(x)$$

Ορίζουμε $\gamma'(x) = b_x$ (στο X) και επεκτείνουμε σε ομομορφισμό $\gamma: F \rightarrow B$. Τότε $\beta\gamma(x) = \beta\gamma'(x) = \beta(b_x) = \alpha(x)$, άρα αφού συμφωνούν στους γεννήτορες ($x \in X$): $\beta\gamma = \alpha$. ■

Παραδείγματα:

(1) $H = \langle x, y \mid x^n = 1 = y^m, yx = xy^t \rangle$

Τότε $H = \{x^i y^j \mid 0 \leq i < n, 0 \leq j < m\}$. Άρα $|H| = nm$.

Επαγωγικά: $y^k x^j = x^j y^{kt}$ για $0 \leq k \leq m, 0 \leq j < n$.

Για $j=1$ ισχύει και $y^{k+1}x = y(y^k x) = yx y^{kt} = xy^{t(k+1)} = x y^{t(k+1)}$. Είναι $x^k y^j = x^j y^{kt}$ (επαγωγή στο k).

Έστω $G = \{x^i y^j \mid 0 \leq i < n, 0 \leq j < m\}$. Ορίζοντας πολλαπλασιασμό $(x^i y^k)(x^j y^l) = x^{i+j} y^{kt+ld}$, η G γίνεται ομάδα (επαλήθευση $\Rightarrow$ πράξεις). Είναι $|G| = mn = |H|$.

(2) Τετρακτόνια:

$$R = \{i^4 = 1, i^2 = j^2, ji = i^3 j\} \text{ (σχέσεις)}$$

$$G = \langle X \mid R \rangle = \langle x, y \mid x^4 = 1, x^2 = y^2, yx = x^3 y \rangle$$

$$G = \{x^s y^t \mid 0 \leq s, t < 3\} = \{x^s y^t \mid 0 \leq s < 3, 0 \leq t < 2\}$$

$$\bullet \quad x^s y^2 = \begin{cases} y^2 = x^2, s=0 \\ xy^2 = x^3, s=1 \\ x^2 y^2 = x^4 = 1, s=2 \end{cases} \quad x^3 y^2 = x(x^2 y^2) = x, s=3$$

$$\bullet \quad x^s y^3 = \begin{cases} y^3 = yx^2 = yxx = x^3 yx = x^3 x^3 y = x^2 y, s=0 \\ \vdots \end{cases}$$

$$GL_2(\mathbb{C}), I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ ΣΧΕΣΕΙΣ: } A^2 = B^2 = C^2 = ABC = I$$

$$Q = \{\pm I, \pm A, \pm B, \pm C\}$$

(Αναπαράσταση Q με 2x2 πίνακες ...)

(3) $F = F(X)$ δεν είναι αβελιανή αν $|X| \geq 2$.

$$\begin{array}{ccc} X & \xrightarrow{\neq} & G \\ \downarrow & \searrow \varphi & \\ F & & \end{array}$$

Αν F αβελιανή, $\varphi(F)$ αβελιανή. Αν $\exists x, y \in G: xy \neq yx$, τότε για $X = \{x_i: i \in I\}$ και $\neq$ με $\neq(x_1) = x, \neq(x_2) = y$, τότε η φ δεν μπορεί να υπάρχει, γιατί μετατίθεται στην X , όχι στην G (χρησιμοποιήσαμε ότι $|X| \geq 2$ παίρνοντας $x_1, x_2 \in X$).

(4) $F = F(X)$ ελεύθερος στρέψης

(Γενικό: Αν $\neq: G \rightarrow H$ ομομορφισμός, $g^n = 1$, τότε $|\neq(g)| \leq n$.)

Αν η F έχει 1 στοιχείο πεπερασμένης τάξης, παίρνουμε:

$$\begin{array}{ccc} X & \xrightarrow{\neq} & \mathbb{Z} \\ \downarrow i & \searrow \varphi & \\ F & & \end{array}$$

Αν το $i(x)$ έχει τάξη n και $\neq(x) = 1$, τότε $\varphi i(x) = 1$, άτοπο!

(Αν $g \in F$, $g = x_1^{e_1} \dots x_n^{e_n}$ και επιλέξουμε $\neq(x_1) = \dots = \neq(x_n) = 1$, τότε $|\varphi(g)| < \infty$, άτοπο.)

Δευτέρα 24/11/2025

Διάλεξη 14

$$\text{Hom}(F(X), G) = \text{Set}(X, G)$$

$$R[G] = \left\{ \sum_{g \in G} r_g g \mid r_g \in R, g \in G \right\}$$

↗ εδω "γέφυρα" ότι G ομάδα
↘ δακτύλιος

$$R[\mathbb{Z}] = R[t, t^{-1}] = \left\{ \sum_{i=-n}^m r_i t^i \mid r_i \in R \right\}$$

↘ δακτύλιος Laurent

$$R[\mathbb{Z}^n] = R[t_1^{\pm 1}, t_2^{\pm 1}, \dots, t_n^{\pm 1}], \quad t_i t_j = t_j t_i$$

$$R[F(x, y)] = R[t^{\pm 1}, s^{\pm 1}], \quad ts \neq st$$

Παράδειγμα:

(1) $F = F(x, y)$

$$H = \langle x^n y^n \mid n \in \mathbb{N} \rangle \text{ ελεύθερη}$$

$$F(x, y) < F(x, y, z)$$

Άρα η F περιέχει ελεύθερες ομάδες βαθμού $0 \leq r \leq \aleph_0$.

(2) $\langle y^n x y^{-n} \mid n \in \mathbb{N} \rangle < F_2$

↗ ελεύθερη

(3) $\mathbb{Z} = \langle x \rangle$ ελεύθερη και μάλιστα η μόνη αβελιανή ελεύθερη ομάδα

(4) $SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}$

$$GL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = \pm 1 \right\}$$

$$1 \rightarrow SL_2(\mathbb{Z}) \rightarrow GL_2(\mathbb{Z}) \xrightarrow{\det} \{\pm 1\} \rightarrow 0$$

$$\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

$$a, \beta: \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}} \quad (2 \text{ Möbius μετασχηματισμοί})$$

$$a(z) = z + 2 \quad \left(\frac{1}{0} = \infty, \frac{a\infty + b}{c\infty + d} = \frac{a}{c} \right)$$

$$\beta(z) = \frac{z}{2z + 1}$$

$$\alpha = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Θα δώσουμε $\langle \alpha, \beta \rangle$ παράγει ελεύθερη υποομάδα της $SL_2(\mathbb{Z})$
και είναι $\ker(SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}_2))$

ενί $\forall n \Rightarrow$ όχι τετριμμένο

$$\alpha^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, \quad \beta^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}$$

$$\alpha^n \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x+2ny}{y}, \quad \beta^n \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x}{2nx+y}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

$$A = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid |x| > |y| \right\} \subseteq \mathbb{R}^2$$

$$B = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \mid |x| < |y| \right\} \subseteq \mathbb{R}^2$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \in A, \quad \beta^n \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x}{2nx+y}$$

$$|x| > |y| \Rightarrow -|y| > -x$$

$$|2nx+y| \geq 2n|x| - |y| \geq 2n|x| - |x| = (2n-1)|x| > |x| \Rightarrow$$

$$\Rightarrow \frac{x}{2nx+y} \in B$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \in B \Rightarrow |x| < |y|, \quad \alpha^n \begin{pmatrix} x \\ y \end{pmatrix} = \frac{x+2ny}{y}$$

$$|x+2ny| \geq 2n|y| - |x| \geq 2n|y| - |y| = (2n-1)|y| \geq |y| \Rightarrow$$

$$\Rightarrow \frac{x+2ny}{y} \in A$$

$$\alpha^n B \subseteq A, \quad \forall n \in \mathbb{Z} \text{ (αν } n < 0, \text{ τότε βάζω } |n|)$$

Άρα $\langle \alpha, \beta \rangle$ είναι ελεύθερη. Γιατί;

Πινγκ - πονγκ λήμμα:

Αν $A \cap B \neq \emptyset$ και $\alpha^n B \subseteq A, \beta^n A \subseteq B$ τότε παίρνουμε
ότι $\langle \alpha, \beta \rangle \cong F_2$ (δηλαδή είναι ελεύθερη).

(χρησιμ: $A \not\subseteq B$)

Απόδειξη:

Έστω w μη κενή λέξη στα a, b . Τότε $w \neq 1$. Έστω προς άτοπον ότι $w = 1$.

(i) $w = a^{n_0} b^{m_1} \dots b^{m_r} a^{n_s} = 1$

(Η w ξεκινά με δύναμη του a και τελειώνει πάλι με δύναμη του a)

$$B = 1 B = w B = a^{n_0} b^{m_1} \dots b^{m_r} a^{n_s} (B) \leq \\ \leq a^{n_0} b^{m_1} \dots b^{m_r} (A) \leq a^{n_0} b^{m_1} \dots a^{n_{s-1}} (B) \leq \dots \\ \dots \leq a^{n_0} (B) \leq A, \text{ άτοπο!}$$

(ii) $w = b^{m_0} a^{n_1} \dots a^{n_s} b^{m_r}$

Τότε $a w a^{-1}$ στην $1^{\text{η}}$ περίπτωση. Άρα $a w a^{-1} = 1 \Rightarrow w = 1$.

(iii) $w = a^{n_0} b^{m_1} \dots a^{n_s} b^{m_r}$

$$a^r a^{n_0} b^{m_1} \dots a^{n_s} b^{m_r} a^{-r} = a^r w a^{-r} \Rightarrow w = 1$$

(iv) Παρόμοια. Αφήνεται ως άσκηση. ■

Θεώρημα Nielsen - Schreier:

Αν F ελεύθερη και $H < F$, τότε H ελεύθερη.

Απόδειξη:

Ορίζουμε μια διάταξη στην $F = F(X)$. Πρώτα ορίζουμε μια διάταξη $\prec$ στο $X^{\pm 1}$. Ορίζουμε μια διάταξη στην F με: αν $a = a_1 \dots a_n$, $b = b_1 \dots b_m$ λέξεις στην F , τότε αν $n < m$, τότε $a < b$, ενώ αν $n = m$, τότε $a < b$, αν $a_i < b_i$ στο πρώτο i για το οποίο $a_i \neq b_i$ (λέξιμογραφική διάταξη).

Λήμμα 1:

Έστω $x_1, \dots, x_n \in F$, $x_i \in X^{\pm 1}$, $n > 1$. Για $v \in F$, αν $v < x_1 \dots x_{n-1}$, τότε $v x_n < x$.

Απόδειξη Λήμματος 1:

Αν $|v| < n-1$, τότε $|v| < n \Rightarrow |v x_n| < n \Rightarrow v x_n < x$.

Αν $|v| = n-1$, τότε επειδή $v < x_1 \dots x_{n-1}$, $\exists 1 \leq r \leq n-1$, ώστε το v να διαφέρει απ' το x στο r γράμμα, δηλαδή

$y = x_1 \dots x_{r-1} y_r \dots y_{n-1} < x_1 \dots x_{n-1}$ ($y_r < x_r$). Πολλά-
πλάσιόφοντας με το x_n και τις δύο πλευρές, $yx_n < x$, γιατί οι
δύο πλευρές της ανισότητας δεν αλλάζουν. ■

Ορισμός:

- (1) Έστω $H < F$. Το δεξί εγκάρσιο (right transversal) της H στην F είναι ένα σύνολο U που περιέχει ακριβώς ένα στοιχείο από κάθε δεξί συμπόκο.
- (2) Ένα $S \subseteq F$ έχει την ιδιότητα Schreier, αν $w = x_1 \dots x_n \in S$ και όλες οι $x_1 \dots x_{n-1}$ (υπολέξεις) ανήκουν στο S (άρα και η κενή). Αν είναι και εγκάρσιο, τότε ονομάζεται «Schreier εγκάρσιο».

Λήμμα 2:

Κάθε $H < F$ έχει ένα Schreier εγκάρσιο που αποτελείται επιλέγοντας το ελάχιστο στοιχείο στο συμπόκο με τη διατάξη.

Απόδειξη:

$U =$ εγκάρσιο που σχηματίζεται επιλέγοντας το ελάχιστο στοιχείο σε κάθε δεξί συμπόκο

Θεώ: $x_1 \dots x_{n-1} \notin U \Rightarrow w = x_1 \dots x_{n-1} x_n \notin U$. Πράγματι, έστω $x_1 \dots x_{n-1} \notin U$. Τότε $\exists v \in Hx_1 \dots x_{n-1} : v < g, \forall g \in Hx_1 \dots x_{n-1} \Rightarrow Hv = Hx_1 \dots x_{n-1} \Rightarrow Hv x_n = Hx_1 \dots x_n = Hw$, άρα βρήκαμε στοιχείο μικρότερο του w στο συμπόκο ($v x_n < w$), άρα παίρνουμε ότι $w \notin U$. ■

Ορισμός:

Έστω $w \in F$. Τότε $\exists! u \in U$ και στο Hw . Θέτουμε $\bar{w} =$ το μοναδικό στοιχείο στο $Hw \cap U$.

Λήμμα 3:

- (1) $\bar{\bar{w}} = \bar{w}$
- (2) $\bar{w} = w \Leftrightarrow w \in U$
- (3) $\overline{ux} \cdot x^{-1} = u, \forall x \in X, \forall u \in U$

Απόδειξη:

$$(1) \quad Hw = H\bar{w} \Rightarrow \bar{w} \in U$$

$$\bar{\bar{w}} = H\bar{w} \cap U = \bar{w}$$

$$(2) \quad \bar{w} = Hw \cap U$$

Αν $w \in U$, τότε $\bar{w} = w$. Αν $\bar{w} = w$, τότε $w \in U$.

$$(3) \quad u \in U \Rightarrow Hu x = H\bar{u}x \Rightarrow Hu = H\bar{u}x x^{-1} \Rightarrow \bar{u}x x^{-1} = u \quad \blacksquare$$

Λήμμα 4:

$A = \{ux \bar{u}x^{-1} \mid u \in U, x \in X\}$ παράγει την H

Απόδειξη:

Πρώτα θδδ $A \subseteq H$. Το $\bar{u}x$ είναι μέρος δεξιού H -συμπόκου $\Rightarrow \exists h \in H: \bar{u}x = uxh$ ($uxH = \bar{u}xH$). Άρα: $h = ux \bar{u}x^{-1} \Rightarrow A \subseteq H$.

Έστω $h = x_1 \cdots x_n$, $x_i \in X^{\pm 1}$. Επαγωγικά ορίζουμε:

$$u_1 = 1 \quad (H = H \cdot 1)$$

$$u_{i+1} = \bar{u}_i x_i, \quad 1 \leq i \leq n$$

$$\text{Θέτουμε } a_i := u_i x_i u_{i+1}^{-1} = u_i x_i \bar{u}_i x_i^{-1} \in A.$$

$$\text{Είναι } a_1 \cdots a_n = u_1 x_1 u_2^{-1} u_2 x_2 u_3^{-1} \cdots u_n x_n u_{n+1}^{-1} = u_1 x_1 \cdots x_n u_{n+1}^{-1} \\ = 1 \cdot h \cdot u_{n+1}^{-1} \in H u_{n+1}^{-1}, \text{ Άρα } u_{n+1} \in U \text{ και επειδή είναι } H \cap U = \{1\}, \text{ παίρνουμε } u_{n+1} = 1. \text{ Άρα } h \in \langle A \rangle. \quad \blacksquare$$

Λήμμα 5:

Ορίζουμε $B := \{ux \bar{u}x^{-1} \mid u \in U, x \in X, ux \notin U\}$ και

$$B^{-1} = \{ux \bar{u}x^{-1} \mid u \in U, x^{-1} \in X, ux \notin U\}, \quad B^{-1} = \{b^{-1} \mid b \in B\}.$$

Τότε $B = B^{-1}$ και $B \cup B^{-1} = A - \{1\}$.

Απόδειξη:

Έστω ότι $x \in X^{\pm 1}$, $u \in U$ απ' το (3) του λήμματος 3:

$$(ux \bar{u}x^{-1})^{-1} = (\bar{u}x x^{-1})u^{-1} = (\bar{u}x x^{-1})(\bar{u}x x^{-1})^{-1}. \text{ Είναι } ux \notin U \\ \Rightarrow \bar{u}x \neq ux \Rightarrow u \neq \bar{u}x x^{-1} \Rightarrow \bar{u}x x^{-1} \neq \bar{u}x x^{-1} \Rightarrow \bar{u}x x^{-1} \notin U.$$

Έστω $b^{-1} \in B^{-1}$. Τότε $b^{-1} = (ux \bar{u}x^{-1})^{-1}$ (και $ux \notin U$ από ορισμό).

$$\text{Άρα } b^{-1} = \bar{u}x x^{-1} (\bar{u}x x^{-1})^{-1} \in B \Rightarrow B^{-1} \subseteq B.$$

Έστω $x^{-1} \in X^{-1}$, $\bar{u}x \in U$, $\bar{u}x x^{-1} \notin U$. Τότε παίρνουμε ότι $\bar{u}x x^{-1} (\bar{u}x x^{-1})^{-1} \in \hat{B}$. Αν $x \in X^{-1} \Rightarrow ux \bar{u}x^{-1} \in \hat{B}$, $ux \notin U$ και $(ux \bar{u}x^{-1})^{-1} = \bar{u}x x^{-1} (\bar{u}x x^{-1})^{-1}$.
Τότε $x^{-1} \in X$, $u' = \bar{u}x$, $\bar{u}x x^{-1} \in U \Rightarrow \hat{B} \subseteq B^{-1}$. ■

Απόδειξη θεωρήματος:

B βάση της H

Απ' τα λήμματα 4, 5 : $\langle B \rangle = H$. Κάθε μη-τετριμμένο γινόμενο της B δεν είναι 1, $w = b_1 \dots b_n = u_1 x_1 \bar{u}_1 x_1^{-1}$. Ο μέσος όρος είναι γινόμενο στην F , $\neq 1$. ■

Τετάρτη 26/11/2025

Διάλεξη 15

$$1) \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle \cong F_2 < SL_2(\mathbb{Z})$$

$$\text{Ισχύει ότι } \forall z \in \mathbb{C}, |z| \geq 2: \left\langle \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix} \right\rangle \cong F_2.$$

Ερώτηση: Υπάρχει $a \in \mathbb{Q}$ $0 < |a| < 2$ ώστε να ισχύει
ότι $\left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \right\rangle \cong F_2$;

2) p περιττός πρώτος, $G_p < S(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{R} \mid f \perp 1, \text{ επι} \}$ που
παράγεται από $x \mapsto x+1, x \mapsto x^p$
Η G_p είναι ελεύθερη βαθμού 2.

$$3) \left\langle y = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, x = \begin{pmatrix} 1 & e \\ 1 & 1 \end{pmatrix} \right\rangle \cong F_2$$

$x^{a_1} y^{b_1} \dots x^{a_r} y^{b_r}$ έχει $(1,1)$ συντεταγμένη
 $e^{\sum_{i=1}^r a_i b_i + p(e)} (2,2)$ συντεταγμένη $q(e)$
 $1 \leq i \leq r$

p, q πολυώνυμα

$$x^2 = \begin{pmatrix} 1+e & 2e \\ 2 & e+1 \end{pmatrix}, y^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, y^n = \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}$$

Αρκεί να κάθε λέξη στα x, y δεν είναι 1.

Αν αρχίζει από y :

Αν $y^{b_0} x^{a_1} \dots y^{b_r} = I$ ($r > 0$), τότε $x^{a_1} \dots y^{b_r} = y^{-b_0}$
(στην $(1,1)$ -θέση διαφέρουν).

Επίσης $x^a y^b = \begin{pmatrix} 1+abe & ae \\ b & 1 \end{pmatrix}$.

$n > 1$: $x^{a_1} y^{b_1} \dots x^{a_n} y^{b_n}$ $(1,1)$ θέση $e^n \prod a_i b_i + p(e)$
 $(2,1)$ θέση $q(e)$ $1 \leq i \leq n$

$n+1 \Rightarrow$ με επαγωγή!

(4) $F_2' = [F_2, F_2]$ είναι άπειρα παραγόμενη

Θέτουμε $H = \bigoplus_{n \in \mathbb{Z}} \mathbb{Z}_2$, $C = \langle t \rangle \cong \mathbb{Z}$.

Το C δρα στο H : $\varphi: C \rightarrow \text{Aut}(H)$ ώστε $t \mapsto$
 $\mapsto$ δεξιά μετατόπιση ενός βήματος.

$(\dots, 0, \underset{\substack{\uparrow \\ n \text{ θέση}}}{1}, 0, \dots) \xrightarrow{\varphi} (\dots, 0, \underset{\substack{\uparrow \\ n+1 \text{ θέση}}}{1}, 0, \dots)$

Ορίζουμε $G := H \rtimes_{\varphi} C$. Τι είναι το $G' = [G, G]$;
 $A \rtimes_{\varphi} B$

$(a_1, b_1)(a_2, b_2) = (a_1 \cdot \varphi(b_1)(a_2), b_1 b_2)$

$(a_1, b_1)(x, y) = (1, 1)$ Ποιος είναι ο αντίστροφος;

$(a_1 \cdot \varphi(b_1)(x), b_1 y) = (1, 1) \Rightarrow$

$\Rightarrow a_1 \cdot \varphi(b_1)(x) = 1, b_1 y = 1 \Rightarrow$

$\Rightarrow \varphi(b_1)(x) = a_1^{-1}, y = b_1^{-1}$

$(a_1, b_1)^{-1} = (\varphi(b_1)^{-1}(a_1^{-1}), b_1^{-1})$

$((x_n), t^k) \in G$

$x_n = 0$ εντός από πεπερασμένους όρους

$((x_n), t^k)^{-1} = (\varphi(t^k)^{-1}(x_n)^{-1}, t^{-k}) = (\varphi(t^{-k})(x_n)^{-1}, t^{-k})$

$[(x_n, t^k), (y_m, t^d)] = (x_n, t^k)(y_m, t^d)(x_n, t^k)^{-1}(y_m, t^d)^{-1} =$

$= ((x_n)\varphi^k(y_m), t^{k+d}) (\varphi^{-k}((x_n)^{-1}), t^{-k}) (\varphi^{-d}((y_m)^{-1}), t^{-d}) =$

$= ((x_n)\varphi^k(y_m)\varphi^d((x_n)^{-1}), t^d) (\varphi^{-d}((y_m)^{-1}), t^{-d}) =$

$= ((x_n)\varphi^k((y_m)\varphi^d((x_n)^{-1} \cdot (y_m))), 1)$

αθροισμα συντεταγμένων = 0

Είναι $G' < H$ στοιχείων που οι συγγεταγμένες αφορίζουν στο 0. Άρα έχουμε άρτιο αριθμό μη μηδενικών συγγεταγμένων.
 $\langle (1, 0, \dots, 1, 0, \dots, 0), 1 \rangle, \langle (0, 1, \dots, 1, 0, \dots, 0), 1 \rangle = G$

Άρα $\exists \phi: F_2 \rightarrow G$ επιμορφισμός, και $\phi(F') = G'$. Αν F' ήταν πεπερασμένα παραγόμενη, τότε θα ήταν και η G' . Όμως η G' περιέχει $(0, \dots, \frac{1}{2}, \frac{1}{2}, 0, \dots), (0, \dots, 0, \frac{1}{2}, \frac{1}{2}, 0, \dots), \dots$
 Άτοπο! (G' άπειρα παραγ.) ο $\frac{1}{2}$

Πόρισμα:

Αν F ελεύθερη βαθμού n και $H < F$ με $[F, H] = m$, τότε H ελεύθερη βαθμού $m(n-1) + 1$. (από Nielsen-Schreier)

Ελεύθερα Γινόμενα Ομάδων

Έστω $\{G_i : i \in I\}$ οικογένεια ομάδων που οι ομάδες είναι ξένες μεταξύ τους σαν σύνολα. Έστω $X = \bigcup_{i \in I} G_i$ και ένα στοιχείο $1 \in X$. Μία λέξη στο X είναι μία ακολουθία $(a_1, a_2, \dots)$, $a_i \in X \cup \{1\}$, $n \in \mathbb{Z}^+$, $a_n = 1 \Rightarrow a_i = 1, \forall i \geq n$. Μία λέξη είναι εκφυλισμένη (reduced), αν:

- (1) $a_i \neq e_i, \forall i$
- (2) $i \in \mathbb{Z}^+, a_i, a_{i+1} \notin G_i$
- (3) $a_k = 1 \Rightarrow a_i = 1, \forall i \geq k$.

Κάθε εκφυλισμένη λέξη γράφεται $a = (a_1, \dots, a_n), a_i \in X$.

Το σύνολο των εκφυλισμένων λέξεων $\ast_{i \in I} G_i$ με πράξη την απηπαράθεση και κατάλληλες διαγραφές και συμπληρώσεις αποτελεί ομάδα («ελεύθερο γινόμενο»). Υπάρχουν μονομορφισμοί $\forall k \in I, \nu_k: G_k \rightarrow G, e_k \mapsto 1, a \mapsto (1, 1, \dots, a, \dots, 1)$.

$$X, \mathbb{Z}_i \cong \mathbb{Z}, \forall i \in X$$

$$\ast_{i \in I} \mathbb{Z}_i \cong F(X), \quad \mathbb{Z} \ast \mathbb{Z} \cong F(\mathbb{Z})$$

Θεώρημα:

Αν $\{\psi_i : G_i \rightarrow H \mid i \in I\}$ οικογένεια ομομορφισμών, τότε
 $\exists!$ ομομορφισμός $\psi : G \rightarrow H$, όπου $G = \ast_{i \in I} G_i$, ώστε:
 $\psi \circ \iota_i = \psi_i$ και η ιδιότητα αυτή χαρακτηρίζει την G ,
 $\ast$ = coproduct in the category of groups

Παρατήρηση:

(1) Αν $G_i = \langle X_i \mid \Delta_i \rangle$, τότε $G = \langle \sqcup X_i \mid \sqcup \Delta_i \rangle$.
Εστω $\psi_i : G_i \rightarrow H$, $\forall i \in I$. Ορίζουμε $\psi : \langle \sqcup X_i \mid \sqcup \Delta_i \rangle \rightarrow H$ με $\psi(x) = \psi_i(x)$, αν $x \in X_i$. Αν $r \in \Delta_i$, τότε r λέγεται στο $X_i \cup X_i^{-1}$ και $\psi(r) = \psi_i(r) = 1$ (γιατί $r=1$ στην G_i).
Άρα ψ καλά ορισμένη. Επίσης $\psi \circ \iota_i = \psi_i$. $\square$

(2) «Κανονική μορφή»: Κάθε μη τετριμμένο στοιχείο της $\ast_{i \in I} G_i$ μπορεί να γραφεί ως $v_1 \dots v_n$, $v_i \neq 1$ στην G_{a_i} και γειτονικά στοιχεία ανήκουν σε διαφορετικές ομάδες.

van der Waerden Εστω $S =$ σύνολο των λέξεων $v_1, \dots, v_n$ και της κενής λέξης. Η G_i δρα στο S .

$$(v_1 \dots v_n)w = \begin{cases} v_1 \dots v_{n-1} v_n', & v_n' = v_n w, \text{ αν } v_n \in G_i \\ v_1 \dots v_n w, & \text{ διαφορετικά} \end{cases}$$

Έχουμε $\#_i : G_i \rightarrow \text{Perm}(S)$, $\forall i$ και παίρνουμε $\psi : \ast_{i \in I} G_i \rightarrow \text{Perm}(S)$, 1-1 και επί (από την καθολική ιδιότητα του ελεύθερου γινόμενου) και ουσιαστικά $\psi^{-1}(v_1 \dots v_n) = v_1 \dots v_n$. $\square$

Παραδείγματα:

(1) $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$

$$\varphi : \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}), \quad \varphi(t)(n) = -n$$

$$D_\infty \cong \mathbb{Z}_2 \ast \mathbb{Z}_2' = \langle x, y \mid x^2 = y^2 = 1 \rangle$$

Κανονική μορφή:

(i) $(xy)^n = xyxy \dots xy$

(ii) $(yx)^m = yxyx \dots yx = (xy)^{-m}$

(iii) $x(xy)^m = yxyx \dots yxy$

(iv) $x(yx)^n = xyxyx \dots yx$

$x^{-1} = x, y^{-1} = y$ γιατί έχουν τάξη 2

$$D_\infty = \langle s, t \mid s^2 = 1 = (st)^2 \rangle$$

$$\psi: \mathbb{Z}_2 * \mathbb{Z}_2 \rightarrow D_\infty, \psi(x) = ts, \psi(y) = s$$

Λήμμα: $\rightarrow$ θα το αποδείξουμε

$$SL_2(\mathbb{Z}) = \langle A, B \rangle, A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, B^2 = -I, B^4 = I$$

Απόδειξη:

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$A^n T = \begin{pmatrix} a+cn & b+dn \\ c & d \end{pmatrix}, BT = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

$\Rightarrow$ Αν $c=0$, τότε $a=d=\pm 1$.

$$A^n T = \begin{pmatrix} 1 & b+dn \\ 0 & 1 \end{pmatrix} = A^{b+dn} \text{ για } d=1=a$$

$$BT = \begin{pmatrix} 0 & 1 \\ -1 & b \end{pmatrix} \text{ για } a=d=-1$$

$$-A^n T = B^2 A^n T = \begin{pmatrix} 1 & -b+dn \\ 0 & 1 \end{pmatrix} = A^{-b+dn}$$

Άρα για $c=0$: $T \in \langle A, B \rangle$.

$\Rightarrow$ Αν $c \neq 0$, τότε για $|a| < |c|$, παίρνουμε $T' = BT = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$.

Για $|a| \geq |c|$, γράφουμε $a = cq + r$, $0 \leq r < |c|$. Τότε:

$$A^{-q} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}, A^{-q} T = \begin{pmatrix} a-qc & b-qd \\ c & d \end{pmatrix} = T^{(1)}$$

και $a-qc = r < |c|$. Σε κάποια στιγμή: $a-qc=0$.

$$\text{Τότε } B \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & -d \\ 0 & b \end{pmatrix} \in \langle A, B \rangle$$

Άρα $T \in \langle A, B \rangle$. Οπότε $SL_2(\mathbb{Z}) = \langle A, B \rangle$.

Παραδείγματα :

(2) $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \{\pm I\} \cong \mathbb{Z}_2 * \mathbb{Z}_3$

Οι εικόνες $\tilde{A}, \tilde{B}$ παράχουν το $PSL_2(\mathbb{Z})$.

$$\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z})$ δρα με Möbius μετασχηματισμούς

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d} \quad \left(\frac{1}{0} = \infty, \frac{\infty}{\infty} = \frac{a}{c} \right)$$

$$C = AB = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$$

$SL_2(\mathbb{Z})$ παράχεται απ' τα $\langle B, C \rangle$

$A = CB^{-1} \in \langle B, C \rangle$, $\tilde{C}, \tilde{B}$ παράχουν το $PSL_2(\mathbb{Z})$

Προσέχως :

Έστω $P = \{\text{θετικοί άρρητοι}\}$, $N = \{\text{αρνητικοί άρρητοι}\}$.

Είναι $P, N \subseteq \mathbb{R} \subseteq \hat{\mathbb{C}}$. Το $\tilde{C}$ έχει τάξη 3 και το $\tilde{B}$ τάξη 2. Είναι $\tilde{B}^n(P) \subseteq N$ και $\tilde{C}^m(N) \subseteq P$.

$$\tilde{B}(z) = -\frac{1}{z}, \quad \tilde{C}(z) = \frac{z-1}{z} \text{ πινγκ-πονγκ}, \quad \tilde{C}^{-1}(z) = \frac{1}{1-z}$$

Άρα $PSL_2(\mathbb{Z}) \cong \langle \tilde{B} \rangle * \langle \tilde{C} \rangle \cong \mathbb{Z}_2 * \mathbb{Z}_3$.

Δευτέρα 01/12/2025

Διάλεξη 16

$$SL_2(\mathbb{Z}) = \left\langle A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$$

$$PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}) / \{\pm I\} = \mathbb{Z}_2 * \mathbb{Z}_3 = \langle \tilde{B} \rangle * \langle \tilde{C} \rangle$$

projective special linear group

$$SL_2(\mathbb{Z}) := \{A \in GL_2(\mathbb{Z}) \mid \det A = 1\}$$

Θεώρημα: (μέσω Chinese Remainder Theorem)

$$SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}_N) \text{ επιμορφισμός}$$

$$SL_2(\mathbb{Z}) \xrightarrow{p} SL_2(\mathbb{Z}_2) \text{ επι}$$

$$\Gamma_2 = \ker p = \left\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\rangle \cong F_2$$

$$SL_2(\mathbb{Z}) \rightarrow PSL_2(\mathbb{Z})$$

$$B \mapsto \tilde{B}$$

$$C \mapsto \tilde{C}$$

$$C = AB = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \tilde{C}^3 = I \in \text{PSL}_2(\mathbb{Z})$$

Πινγκ - Πονγκ Λήμμα :

Έστω ότι η G δρα στο σύνολο X και $H_1, H_2 < G$ ώστε :
 $|H_1| \geq 3$, $\forall \exists X_1, X_2 \subseteq X$ ($X_1, X_2 \neq \emptyset$) ώστε $X_2 \not\subseteq X_1$,
 $h(X_2) \subseteq X_1, \forall h \in H_1 - \{1\}$ και $h(X_1) \subseteq X_2, \forall h \in H_2 - \{1\}$, τότε
 $\langle H_1, H_2 \rangle = H_1 * H_2$.

Πόρισμα :

Έστω ότι η G δρα στο σύνολο X και $g_1, g_2 \in G$ ώστε : $|g_i| \geq 3$,
 $\forall \exists X_1, X_2 \subseteq X$ ($X_1, X_2 \neq \emptyset$) ώστε $X_2 \not\subseteq X_1$ και $\forall h \geq 0$:
 $g_1^h(X_2) \subseteq X_1, g_2^h(X_1) \subseteq X_2$, τότε $\langle g_1, g_2 \rangle = g_1 * g_2$.

Παράδειγμα :

$$D_\infty = \mathbb{Z}_2 * \mathbb{Z}_2 = \langle s, t \mid s^2 = t^2 = 1 \rangle$$

$$D_\infty = \{1, s, t, st, ts, sts, tst, stst, tsts, \dots\} \quad -1: \mathbb{Z} \rightarrow \mathbb{Z}$$

$$D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2, \text{ όπου } \mathbb{Z}_2 \rightarrow \text{Aut}(\mathbb{Z}) \text{ με } t \mapsto (-1)$$

Kurosh Theorem :

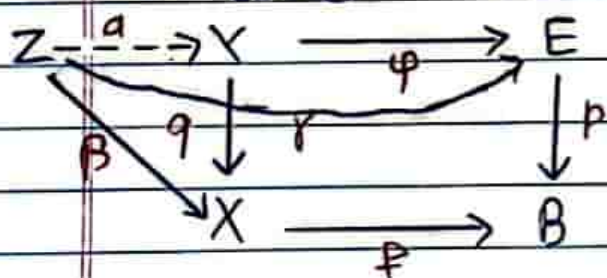
Έστω $G = A * B$ και $H \leq G$. Τότε $\exists A_i \leq A, i \in I$ και $B_j \leq B$,
 $j \in J, g_i \in G, f_j \in G, X \subseteq G$, ώστε να ισχύει το ακόλουθο.

$$H \cong F(X) * \left(\bigast_{i \in I} g_i A_i g_i^{-1} \right) * \left(\bigast_{j \in J} f_j B_j f_j^{-1} \right)$$

$$\left(F(X) \cong \bigast_{x \in X} \mathbb{Z}_x, \text{ όπου } \mathbb{Z}_x \cong \mathbb{Z} \right) \quad F_2 \cong \mathbb{Z} * \mathbb{Z}$$

$$F_3 \cong \mathbb{Z} * \mathbb{Z} * \mathbb{Z} \text{ κτλ}$$

Push-Back

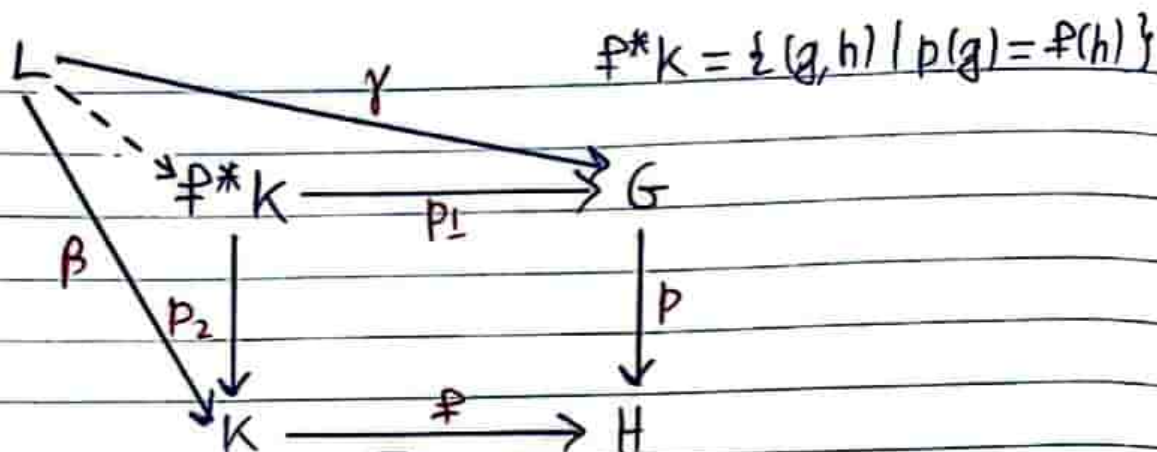


$$pqa = pq a,$$

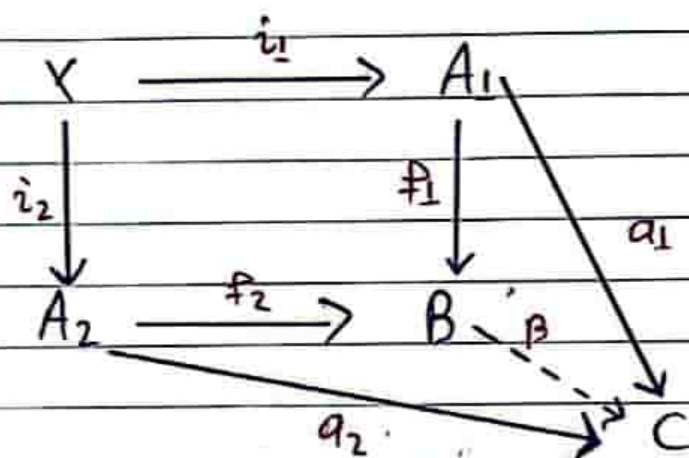
$$qa = \gamma$$

$$qa = \beta$$

(commutative diagram)



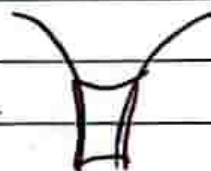
Push-Out δυνάμει του pull-back



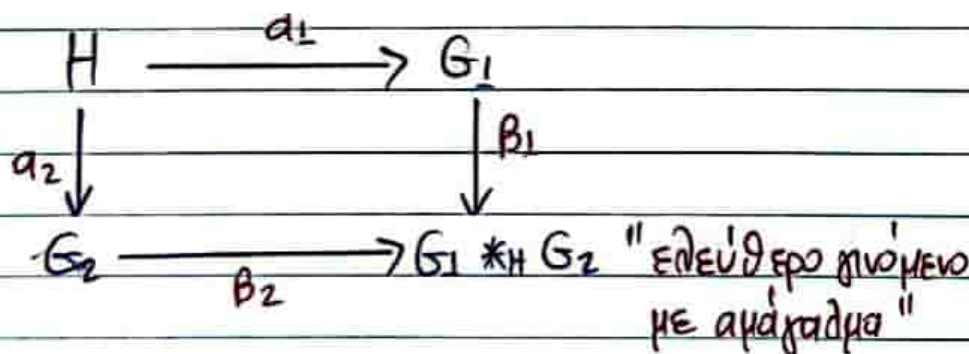
"τα κολλάμε"

Στην κατηγορία των τοπολογικών χώρων:

$$B = A_1 \cup_X A_2 = A_1 \amalg A_2 / y \sim y, y \in X$$



Στις ομάδες παίρνουμε τα παραπάνω.



Θεώρημα:

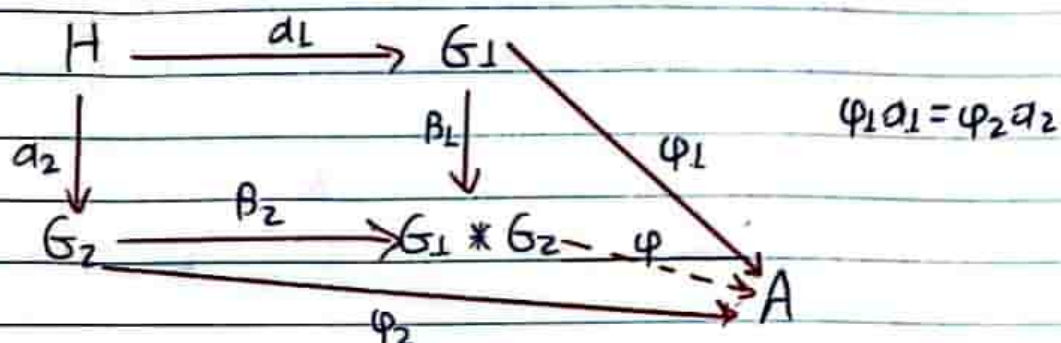
$G_1 *_H G_2$ υπάρχει και είναι μοναδικό!

Απόδειξη:

Μοναδικότητα: Αν υπάρχει, τότε η μοναδικότητα είναι προφανής.

Υπαρξη: Έστω $G = \langle \{x_g \mid g \in G_1\} \amalg \{x_g \mid g \in G_2\} \mid R_{G_1} \cup R_{G_2} \cup$

$\cup \{x_{a_1}(h) x_{a_2}(h)^{-1} \mid h \in H\} > .$ Έχουμε $\beta_j : G_j \rightarrow G, g \mapsto x_g$.
 $R_{G_j} = \{x_g x_h x_k^{-1} \mid g, h, k \in G_j, gh = k \in G_j\}$
 Επειδή $x_{a_1}(h) x_{a_2}(h)^{-1} = 1$ (στην G), παίρνουμε ότι $\beta_1 a_1 = \beta_2 a_2$



Η $\varphi(x_g) = \begin{cases} \varphi_1(g), & g \in G_1 \\ \varphi_2(g), & g \in G_2 \end{cases}$ είναι καλά ορισμένη :

Είναι φ_j ομομορφισμός, άρα αν $x_g x_h x_k^{-1} \in R_j$, τότε παίρνουμε ότι $\varphi(x_g x_h x_k^{-1}) = \varphi_j(ghk^{-1}) = 1$. Αν' την άλλη, παίρνουμε ότι $\varphi(x_{a_1}(h) x_{a_2}(h)^{-1}) = \varphi_1 a_1(h) \circ \varphi_2 a_2(h)^{-1} = 1$.

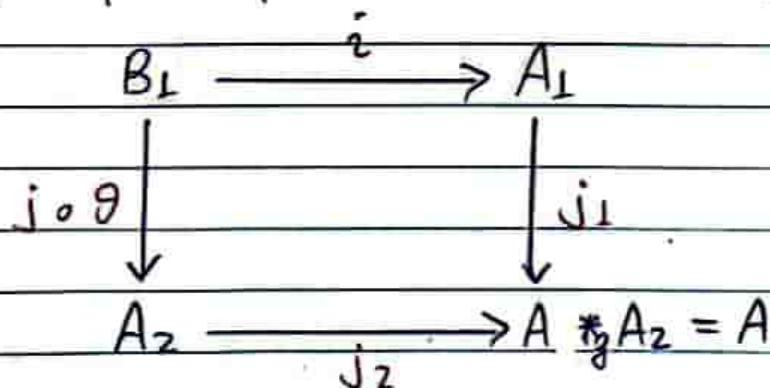
Άρα φ καλά ορισμένος ομομορφισμός. Επίσης $\varphi \beta_1 = \varphi \beta_2 \Rightarrow \Rightarrow \varphi$ μοναδικός. ■

Κανονική μορφή :

$g \in G * H$

$g = g_1^{e_1} h_1^{e'_1} g_2^{e_2} h_2^{e'_2} g_3^{e_3} h_3^{e'_3} \dots$, όπου $g_i \in G, h_i \in H, e_i \in \mathbb{N}$

Θεωρούμε τώρα 2 ομάδες A_1, A_2 και $B_i \leq A_i, B_1 \cong B_2$.



$A = A_1 \times A_2 / N$

$N = \langle b \theta(b)^{-1} \mid b \in B_1 \rangle$ κανονική υποομάδα του $A_1 * A_2$

(Magnus - Karrass - Solitar, Lyndon - Schupp)

$j : B_2 \rightarrow A_2$ η εμφύτευση

Ορίζουμε $\forall a \in A_i : d(a) := 0$ ανιπρόσωπος στο $a \in B_i$, δηλαδή $a = d(a) \cdot b, b \in B_i$.

Η « κανονική μορφή » στο $A_1 *_{\theta} A_2$ είναι $d(a_1) \cdots d(a_n) b$, $b \in B_1$, $n \geq 0$, $d(a_j)$ τα επιλεγμένα εγγράφοι στο B_{i_j} , $a_j \in B_{i_j}$ και γιγονιμά $d(a_i)$ ανήκουν σε διακεκριμένα A_i , B_1 ή στο B_2 .

Θεώρημα Κανονικής Μορφής :

Εστω $w \in A_1 *_{\theta} A_2$, Θα είναι $F(w)$ έτσι ώστε $wN = F(w)N$.

Απόδειξη :

Κάθε στοιχείο στο $A_1 *_{\theta} A_2$: $w = x_1 y_1 \cdots x_n y_n$ (θα έχει αυτή τη μορφή) στο ελεύθερο γινόμενο $A_1 * A_2$, όπου $x_i \in A_1$, $y_i \in A_2$, και μόνο το x_1 και το y_n επιτρέπεται να είναι 1. Αν $w = x_1 y_1$, τότε αν $y_1 = 1$, τότε $x_1 = d(x_1)b$, όπου $b \in B_1$ και $d(x_1) = F(w)$ ($wN = d(x_1)N$). Αν $x_1 = 1$, τότε : $w = y_1 = d(y_1)b$, $b \in B_2$. Άρα $F(w) = d(y_1)\theta^{-1}(b)$. Κατόπιν επαναλαμβάνουμε τη διαδικασία αυτή. ■

Θεώρημα στρέψης :

Το $g \in A_1 *_{\theta} A_2$ έχει πεπερασμένη $\Leftrightarrow$ το g είναι συζυγές με στοιχείο πεπερασμένης τάξης στο A_1 ή A_2 .

$$SL_2(\mathbb{Z}) = \left\langle \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{=S}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = I, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$$

$$SL_2(\mathbb{Z}) = \left\langle \underbrace{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}_{=S}, \underbrace{\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}}_{=R} \right\rangle$$

$$S^4 = I, \quad R^6 = I = S^3$$

$$S^2 = R^3$$

$$N = \langle S^2 \rangle < Z(SL_2(\mathbb{Z})), \quad N \triangleleft SL_2(\mathbb{Z})$$

$$G/N = SL_2(\mathbb{Z})/\pm I = PSL_2(\mathbb{Z})$$

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : \text{αντίστροφή } (z \mapsto -\frac{1}{z})$$

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = R^{-1} : \text{μεταφορά } (z \mapsto z+1)$$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ σαν γινόμενο } S \text{ και } T$$

$$A = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} \in SL_2(\mathbb{Z})$$

$$17 = 2 \cdot 7 + 3 \text{ (διαίρεση του } a \text{ με το } c)$$

$$T^{-2}A = \begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix} \quad (|a| < |c|)$$

$$ST^{-2}A = \begin{pmatrix} -7 & -12 \\ 3 & 5 \end{pmatrix} \quad (|a| > |c|)$$

$$-7 = -3 \cdot 3 + 2$$

$$T^3(ST^{-2}A) = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \quad (|a| < |c|)$$

$$ST^3ST^{-2}A = \begin{pmatrix} -3 & -5 \\ 2 & 3 \end{pmatrix} \quad (|a| > |c|)$$

$$-3 = -2 \cdot 2 + 1$$

$$T^2ST^3ST^{-2}A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \quad (|a| < |c|)$$

$$ST^2ST^3ST^{-2}A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} = -R = -T^{-1}$$

$$A = (ST^2ST^3ST^{-2})^{-1} \cdot (-T^{-1}) = -(TST^2ST^3ST^{-2})^{-1}$$

$$SL_2(\mathbb{Z}) = \mathbb{Z}_4 *_{\mathbb{Z}_2} \mathbb{Z}_6$$

Κάθε στοιχείο στρέψης στο $SL_2(\mathbb{Z})$ έχει τάξη 1, 2, 3, 4, 6.

$$\chi : SL_2(\mathbb{Z}) \rightarrow \mathbb{C}^\times \text{ ομομορφισμός}$$

Τα στοιχεία στρέψης απεικονίζονται στις δεδομένες ρίζες του 1.

$$\chi(S) = -i, \quad \chi(T) = e^{2\pi i/12} = -i \left(\frac{-1 + i\sqrt{3}}{2} \right)$$

$$\chi \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = e^{\frac{2\pi i}{12} ((1-c^2)(bd+3(c-d)d+c+3)+c(ad-3))}$$

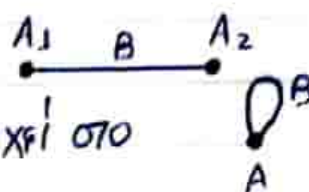
(χαρακτήρες της $SL_2(\mathbb{Z})$)

η-συναρτήσεις

HNN - EXTENSIONS

$\Rightarrow$ Γραφήματα Ομάδων

$A_1 *_B A_2$ αντιστοιχεί στο



HNN-extension $A *_B \langle t \rangle$ αντιστοιχεί στο

Προσέχως ...

ΜΕΤΑΠΤΥΧΙΑΚΗ ΑΛΓΕΒΡΑ Ι

Τετάρτη 03/12/2025

Διάλεξη 17

HNN - ΕΠΕΚΤΑΣΕΙΣ

HNN- επέκταση της G σε σχέση με τις υποομάδες A, B της G και τον ομομορφισμό ρ

$$G^* = \langle G, t \mid t^{-1}at = \rho(a), a \in A \rangle$$

t = σταθερό γράμμα (stable letter), $t \in G$

$$\rho: A \xrightarrow{\cong} B$$

Το γράφουμε ως $G *_\rho$ ή $G *_\rho \langle t \rangle$.

Κανονική μορφή: $g_0 t^{\epsilon_1} g_1 \dots t^{\epsilon_n} g_n$, όπου $g_i \in G$, $\epsilon_i \in \{\pm 1\}$, έτσι ώστε T_A, T_B σύνολα αντιπροσώπων λέξεων συμπλοκών των $G/A, G/B, 1 \in T_A, 1 \in T_B$ και:

(i) Αν $\epsilon_i = -1$, τότε $g_i \in T_A$.

(ii) Αν $\epsilon_i = 1$, τότε $g_i \in T_B$.

(iii) Δεν υπάρχει ακολουθία $t^{\epsilon_1} t^{\epsilon_2} \dots t^{\epsilon_n}$.

Η σχέση $t^{-1}at = \rho(a) \Leftrightarrow at = t\rho(a)$ αποκαλείται "quasi-commuting relation". Μας επιτρέπει να μετακινήσουμε $a \in A$ στα αριστερά του t^{-1} με το να μετατρέψουμε σε $\rho(a)$ και ένα b στα αριστερά του t με το να το μετατρέψουμε σε $\rho^{-1}(b)$.

Παράδειγμα:

$$F = \langle c, d \rangle$$

$$F^* = \langle c, d, t \mid t^{-1}ct = d^2 \rangle$$

$$\rho: \langle c \rangle \xrightarrow{\cong} \langle d^2 \rangle$$

$T_{\langle c \rangle}^A$ έχει ως αντιπροσώπους λέξεις που δεν ξεκινούν με το c και $T_{\langle d^2 \rangle}^B$ λέξεις που δεν ξεκινούν με το c ή με δύναμη του d , εκτός αν' το d^1

$$w = cd t^{-1} c^3 t d^5 c d t^{-1} c^3 d^3$$

Αντιπροσώπος της $A c^3 d^3$ είναι το d^3 και $t^{-1} c^3 = d^6$.

$$w = cd t^{-1} c^3 t d^5 c d^7 t^{-1} d^3$$

Αντιπροσώπος της $B d^5 c d^7$ είναι το $d c d^7$ και $t d^4 = c^2 t$.

$$w = cd t^{-1} c^3 c^2 t d c d^7 t^{-1} d^3, \text{ όμως } t^{-1} c^5 t = d^{10}$$

Συγκεκριμένα $w = \underbrace{cd^{12}cd^7t^{-1}d^3}$.

Britton's lemma:

$w = g_0 t_1^{e_1} \dots g_{n-1} t_n^{e_n} g_n$

- Α) $w \neq 1 \in G^*$
- (1) Είτε $w = 1 \in G^*$, δίνει $n=0$ και $g_i = 1$.
- (2) Είτε (i) $e_i = 1$ και $e_{i+1} = -1$, $g_i \in A$
 (ii) $e_i = -1$, $e_{i+1} = 1$, $g_i \in B$.

Αν w είναι τέτοιο, τότε:

- Β) $w \neq 1 \in G^*$
- (1) Είτε $n=0$, $g_0 \neq 1 \in G$
- (2) Είτε $\exists$ υπολέξη της μορφής $t a t^{-1}$, $a \in A$ ή $t^{-1} b t$, $b \in B$,
 τότε $w \neq 1 \in G^*$.

Ισχύει:

- (1) Κάθε στοιχείο πεπερασμένης τάξης στην G^* είναι συζυγές με ένα στοιχείο πεπερασμένης τάξης στην G .
- (2) $G^* = G *_{\varphi}$, $\varphi: G \xrightarrow{\cong} G$
 $G *_{\varphi} \xrightarrow{\cong} G \rtimes \mathbb{Z}$, $gt \rightarrow (g, t)$
 $\mathbb{Z} \rightarrow \text{Aut}(G)$, $t \mapsto \varphi$

Θεώρημα 1:

Κάθε αριθμητική ομάδα C εμπεριέχεται σε μία ομάδα G που παράγεται από 2 στοιχεία άπειρης τάξης. Η G έχει στοιχεία πεπερασμένης τάξης, αν η C έχει. Η G είναι πεπερασμένα παρισπώμενη, αν η C είναι.

(Αν F ελεύθερη και $|F| \leq \aleph_0$, τότε $F \hookrightarrow F(a, b)$. Αυτό είναι ειδική περίπτωση του θεωρήματος 1 - το είδαμε.)

Απόδειξη:

Έστω $C = \langle c_1, c_2, \dots, c_n, \dots \mid s_1, s_2, \dots \rangle$ και παράγεται από αριθμητικό σύνολο γεννητόρων. Έστω $F = C * \langle a, b \rangle$. Το σύνολο $\{a, b^{-1}ab, b^{-2}ab, \dots, b^{-n}ab, \dots\}$ παράγει ελεύθερη υποομάδα της $\langle a, b \rangle$, ενώ το $\{b, c_1 a^{-1} b a, \dots, c_n a^{-n} b a^n\}$ παράγει ελεύθερη υποομάδα της F . ($\pi: F \rightarrow \langle a, b \rangle$, $a \mapsto a$, $b \mapsto b$, $c_i \mapsto 1$)

Έστω $G = \langle F, t \mid t^{-1}at = b, t^{-1}b^{-1}ab^{-1}t = c, a^{-1}ba, i \geq 1 \rangle$.
 Άρα η C εμφυτεύεται στην G . $G = \langle a, t \rangle = \langle b, t \rangle$ ■

Θεώρημα 2: (Neumann)

Υπάρχουν υπεραριθμήσιμες μη ισομορφες ομάδες 2 γεννητόρων

Απόδειξη:

S = κάποιο σύνολο πρώτων αριθμών

$T_S = \sum_{p \in S} C_p$, C_p = κυκλική ομάδα τάξης p

Εμφυτεύουμε κάθε T_S σε μία ομάδα 2 γεννητόρων G_S .
 Τώρα η T_S και άρα η G_S έχει ένα στοιχείο τάξης p αν $p \in S$. Υπάρχουν μη αριθμήσιμα S (έχουμε άπειρους πρώτους).
 Άρα έχουμε μη αριθμήσιμα μη ισομορφα G_S . ■

Θεώρημα 3:

Κάθε αριθμήσιμη ομάδα C εμφυτεύεται σε μία αριθμήσιμη G , στην οποία όλα τα στοιχεία ίδιας τάξης είναι συζυγή.

Απόδειξη:

Έχουμε $C \rightarrow C^*$ (HNN-επέκταση), όπου κάθε 2 στοιχεία ίδιας τάξης στην C είναι συζυγή. Θεωρούμε σύνολο $\{(a_i, b_i) : i \in \mathbb{N}\}$ διατεταγμένων ζευγών ίδιας τάξης στην C .
 $C^* = \langle C, t_i \mid t_i a_i t_i^{-1} = b_i, i \in \mathbb{N} \rangle$ έχει αυτή την ιδιότητα (repeated HNN-extension). Θέτουμε $G_0 = C$, G_{i+1} ορίζεται έτσι, ώστε $G_i \hookrightarrow G_{i+1}$ και κάθε 2 στοιχεία ίδιας τάξης στην G_i να είναι συζυγή στην G_{i+1} . Άρα θέτουμε $G = \bigcup_{i=1}^{\infty} G_i$.
 (Αν $G_1, G_2 \leq G$, τότε $G_1 \cup G_2 \leq G \Leftrightarrow G_1 \leq G_2$ ή $G_2 \leq G_1$).
 (G "διαίρεσιμη" $\Leftrightarrow \forall g \in G, \forall n \in \mathbb{N}$ η εξίσωση $g = y^n$ έχει λύση στην G , δηλαδή η G έχει n -οστές ρίζες) ■

Θεώρημα:

Κάθε αριθμήσιμη ομάδα μπορεί να εμφυτευτεί σε μία αριθμή-

σημη, αληή, διαιρέσιμη ομάδα.

Απόδειξη:

Πρώτα εμφυτεύουμε την C σε μία αριθμητική ομάδα K που έχει ένα στοιχείο τουλάχιστον κάθε τάξης.

$$π.χ. C * \mathbb{Z} * \left(*_{n \in \mathbb{N}} \mathbb{Z}_n \right)$$

Εμφυτεύουμε τώρα $K * \langle x \rangle \hookrightarrow U$, όπου του U έχει 2 γεννιότερες άπειρης τάξης. Εμφυτεύουμε επίσης το U σε ομάδα, όπου όλα τα στοιχεία ίδιας τάξης είναι συζυγή.

$$C \hookrightarrow K \hookrightarrow K * \langle x \rangle \hookrightarrow U \hookrightarrow G, \quad x \notin K$$

Τότε G αληή και διαιρέσιμη (divisible). Έστω $1 \neq N \trianglelefteq G$. Επειδή η K περιέχει στοιχεία κάθε τάξης και όλα τα στοιχεία ίδιας τάξης είναι συζυγή στην G , η N περιέχει $1 \neq z \in K$. Άρα $x^{-1}zx \in N$, άρα $x^{-1}z^{-1}xz$ άπειρης τάξης. Η N περιέχει τους γεννιότερους της U (άπειρης τάξης). Άρα $K \subseteq U \subseteq N$. Αλλά K περιέχει στοιχεία κάθε τάξης και τα στοιχεία ίδιας τάξης είναι συζυγή στην G . Άρα $N = G$. Έστω τώρα $g \in G$, $n \in \mathbb{N}$ και g τάξης m ($m=1, 2, \dots, \infty$). Επειδή η G περιέχει στοιχεία κάθε τάξης, περιέχει $z \in G$ τάξης mn και z^n έχει τάξη m . Άρα $\exists v \in G$, $v^{-1}z^n v = g \Rightarrow g = (v^{-1}zv)^n$. ■

Παρατήρηση:

Έχουμε υπεραριθμησιμες μη ισόμορφες αληές ομάδες. (Κάθε αριθμητική ομάδα έχει το πολύ αριθμησιμες 2 γεννιότερων υποομάδες.)

Haill:

Κάθε αριθμητική ομάδα εμφυτεύεται σε πεπερασμένα παραγόμενη αληή ομάδα. (με 6 γεννιότερες)