ולכן $|\mathcal{O}(x)| = \frac{|G|}{|G_x|} = \frac{5}{5!} = 3$.

וכמו כן $\exists g \in G$ כך ש $x = g \cdot x$ (כי $x \in \mathcal{O}(x)$)

שלב 1: נניח G פועל על X כך ש $|\mathcal{O}(x)| = 5$ לכל $\{\mathcal{O}_1(x), \ldots, \mathcal{O}_k(x)\} = X/G$

אזי $k = 1$ ו"נ

$$4 \mid 4k$$

כי $k \neq 0$

$$4 \mid 4k + 4$$

כאשר $k \geq 0$ מתקיים

מנוסחת המחלקות $|X| = 5k + 1$

נמנה את # המקיימים x באופן הבא

שלב 2: יהי מספר, שלא מתחלק ב- 5 נמנה את # המקיימים x כאלה ξ

וכיוון שמסלול כלשהו הוגדר G ו"נ, מתקיים $|\mathcal{O}(x)| = 1$ או 5 (הוא מתחלק אחד ו)

$\xi_{11} = |\mathcal{O}(x)|$. כזה ξ_{11} כאלה $\xi_{11} = |G/G_x| = 5$

שלב א: נראה $|\mathcal{O}(x)| = 1$;

אזי $\xi_{11} = |\mathcal{O}(x)|$ וכן $x \neq e$ כיוון $\xi_{11} = 5$

כי, יש $g \in G$ x ו $|G| > |\mathcal{O}(x)|$ ו $|G| \mid |\mathcal{O}(x)|$

תזכורת: נניח כי קיים G בעל ו"נ כיוון $G \neq Z(G)$. מהקשר, נסמן

ξ_{11}

אזי: ידוע G מספר של כיוון G ו"נ.

$$\frac{|x_G|}{|G|} = \text{כיוון מסלול}$$

$|Z(G)| = \#$ איברים שנמקים בהכרח כיוון 1

כאשר $g \in \exists x_1, \ldots, x_k$ כך שלפחות אחד מהמקיים כיוון > 1

$$|G| = |Z(G)| + \sum \frac{|x_G|}{|G|}$$

נוסחת המחלקות G-ב סופית.

לכן $Z(G) \subseteq$ מכילה את x.

השאלה $Z(G)$ נקראים מרכזיות בחוגים. ואיברים x_G משוואת

ידוע, G חבורה. G פועלת עם פעולה g_1 הבאה $(g \cdot x = g x g^{-1})$

הוכחה:

$\exists$! $\sigma \in S_n$

$\sigma = \tau_{i_1} \cdot \tau_{i_2} \cdots \tau_{i_k}$ (*) הוכחה מקורי

$\alpha_i = (a_{i1}, \cdots, a_{in_i})$ $\quad$ $(n_i = \ell(\alpha_i))$ $\quad$ נניח $\quad$ $((a_{11}) \cdots (a_{1n_1})) \cdots ((a_{i1}) \cdots (a_{in_i}))$ סוגר

$(\tau_{i_1}(a_{11}) \cdots)(\tau_{i_2}(a_{21}) \cdots) \cdots (\tau_{i_k}(a_{k1}) \cdots) = \sigma(a_{11}) \cdots$

משפט: $\{\tau \mid \tau \text{ מחזור} \ ; \ \sigma \in \tau\} = \Theta(\sigma)$ עם σ מקבלת הצמידות

$(1,1,1)$

$\xi \in (\xi)(\tau)(1)$

כיסוי עם σ $\quad$ $(1,\tau,\xi)$

$\sigma_1 \in (\xi)(\eta\tau)(\xi\tau 1) = \sigma$

כיסוי עם σ $\quad$ (τ,τ)

$\sigma_2 \in (\eta\xi)(\tau 1) = \sigma$

דוגמא:

$\sigma = ((\tau\rho)\sigma, \cdots, (\tau\rho)\sigma, (\rho)\sigma)$:הצגה עם σ של כיסוי

σ- σ_1 עם τ סוגר

$(\tau\rho)\sigma \leq \cdots \leq (\tau\rho)\sigma \leq (\rho)\sigma$ נניח (מתוארס) מיקום $\quad$ כפי שהוגדר לעיל

תזכורת: $\sigma \in \sigma_n$ נתון $\quad \tau_\rho \cdots \tau_1 = \sigma$ מכפלת

הוכחה: מציאו את כל המחלקות הצמידות של S_n.

תזכורת

($H_i \vee H_j = H_i$ אזי $\{e\}$ כי שלפי הנחות מספר 3) כמסקנה

סה"כ $\quad$ $\sum_{i=1}^{t} (|H_i| - 1) = \text{כל האיברים מסדר 3}$

מתקיים $\quad$ $|H_i| \geq 1$ $\quad$ $\forall i$ $\quad$ $|G| = n$ $\quad$ יהי

(חיפוש מספיק, ת.ב) נקבע $\quad$ $x \in \Theta(x)$

סה"כ, אם $\quad$ $|\Theta(x)| = 5$ $\quad$ אז $\quad$ $|\Theta(x)| = 3$ $\quad$ ומכאן

$H \lneq G$: מקרה

G פועלת על $X = \{G/H\}$ הקוסטים השמאליים $\{G > x_1 H\}$ כאשר $x_1 = e$

$$g \cdot aH = gaH$$

הגדרה: יהי $H \leq G$ תת־חבורה פרטית

$$\text{Core}_G(H) = \bigcap_{g \in G} gHg^{-1} \neq G$$

אבחנה: תהי G חבורה, $H \lneq G$

(א)

(ב)

(ג)

(ד)

הוכחה: $\varphi: G \to (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/2\mathbb{Z})^2$

φ הומומורפיזם לא טריוויאלי.

$\ker \varphi$ תת־חבורה נורמלית לא טריוויאלית של S_4.

$\ker \varphi$ חייבת להכיל את החבורה הנורמלית הלא טריוויאלית של S_4.

תזכורת:

$$\tau = \sigma\rho\sigma^{-1} \quad (*) \quad \text{נ}$$

ρ : $\rho(a_{ij}) = a_{ij}$ $\quad i \geq j$ $\quad i > j \geq 1$.

σ : $\sigma(i) = (i_1, \ldots, i_n)$ כך ש־$\sigma \in S_n$

τ : $\tau(i) = (i_{\sigma(1)}, \ldots, i_{\sigma(n)})$

τ מאותו סוג כמו ρ (τ, ρ מאותו סוג כמו σ).

הוכחה: נניח $\tau = \sigma_1 \cdots \sigma_k$.

יהי ρ סוג $\rho = \sigma\tau\sigma^{-1}$.

ρ : $\rho(a_{ij}) = a_{ij}$ $\quad i \geq j$ $\quad i > j \geq 1$.

σ : $\sigma(i) = (i_1, \ldots, i_n)$ כך ש־$\sigma \in S_n$

τ : $\tau(i) = (i_{\sigma(1)}, \ldots, i_{\sigma(n)})$

τ מאותו סוג כמו ρ (τ, ρ מאותו סוג כמו σ).

הוכחה: נניח $\tau = \sigma_1 \cdots \sigma_k$.

יהי ρ סוג $\rho = \sigma\tau\sigma^{-1}$.

$$\rho = \sigma\tau\sigma^{-1} \quad (*) \quad \text{נ}$$

ρ : $\rho(a_{ij}) = a_{ij}$ $\quad i \geq j$ $\quad i > j \geq 1$.

σ : $\sigma(i) = (i_1, \ldots, i_n)$ כך ש־$\sigma \in S_n$

τ : $\tau(i) = (i_{\sigma(1)}, \ldots, i_{\sigma(n)})$

τ מאותו סוג כמו ρ (τ, ρ מאותו סוג כמו σ).

הוכחה: נניח $\tau = \sigma_1 \cdots \sigma_k$.

יהי ρ סוג $\rho = \sigma\tau\sigma^{-1}$.

(מעבר הבאשה ←) $\frac{(H\oplus T)/\varphi}{(H\oplus T)/\varphi} = \frac{(H\oplus T)/\varphi}{H\oplus T}$

שאלה: לכאורה $\varphi \xrightarrow{\sim} H\oplus T/H\oplus T \not\Rightarrow H\oplus T/H\oplus T \xrightarrow{\sim} T$

שאלה: הוכח/הפרך: $H\oplus K \cong H\oplus T \Rightarrow K \cong T$.

$\ker f_i = G_1\times\cdots\times\hat{G}_i\times\cdots\times G_n$

הוכחה: נגדיר $f_i: G_i \to G_1\times\cdots\times G_n$ ע"י $f_i(g) = (e,\ldots,e,g,e,\ldots,e)$ - g במקום ה-i. f_i הומומורפיזם חח"ע (מונומורפיזם). $\ker f_i$ שווה לקבוצה $\{(e,\ldots,e,g,e,\ldots,e) : g\in G_i\}$ - כלומר $G_1\times\cdots\times\{e\}\times\cdots\times G_n$.

שאלה: נניח $G_1,\ldots,G_n$ חבורות. ראינו $\prod_{i=1}^n G_i \supseteq \prod_{i=1}^n N_i$. האם כל תת-חבורה N של $\prod G_i$ היא מהצורה $\prod N_i$ עבור $N_i \trianglelefteq G_i$?

תשובה: לא. למשל $n=2$, $G_1=G_2=\mathbb{Z}$. $N = \{(a,b) : a\equiv b \pmod 2\}$ תת-חבורה של $\mathbb{Z}\times\mathbb{Z}$ שאינה מהצורה $N_1\times N_2$. הוכחה: $N_1 = \{a : \exists b\in\mathbb{Z}, (a,b)\in N\}$, $N_2 = \{b : \exists a\in\mathbb{Z}, (a,b)\in N\}$. אז $N_1 = N_2 = \mathbb{Z}$ (למשל $(0,0),(1,1)\in N$). אבל $N \subsetneq \mathbb{Z}\times\mathbb{Z}$ (למשל $(1,0)\notin N$).

מכפלות ישרות

יהי $\{G_i\}_{i\in I}$ אוסף חבורות. הגדרנו: $\prod_{i\in I} G_i = \{(g_i)_{i\in I} : g_i\in G_i\}$. לדוגמה: $G_1\times G_2 = \{(g_1,g_2) : g_1\in G_1, g_2\in G_2\}$.

שאלה: נניח $G = H_1\times H_2$, $H_1\cap H_2 = \{e\}$, $H_1 H_2 = G$. אז $H_1\trianglelefteq G$ וכן $H_2\trianglelefteq G$. כמו כן $G/H_1 \cong H_2$ ו-$G/H_2\cong H_1$.

הוכחה: G פשוט $\Rightarrow G\triangleright H$ אז $H=\{e\}$ או $H=G$.

הגדרה: G פשוט $\Leftarrow G\triangleright H$ אז $H=\{e\}$ או $H=G$.

הגדרה: יהי G חבורה. G נקראת *חבורה פשוטה* אם $\{e\}$ ו-G הן התת-חבורות הנורמליות היחידות של G. כלומר, $\forall H\trianglelefteq G$ מתקיים $H=\{e\}$ או $H=G$.

שאלה: יהי G פשוט. $\varphi: G\to H$ הומומורפיזם. מה $\ker\varphi$? $\varphi(G)$?

תשובה: $\ker\varphi = \{e\}$ או $\ker\varphi = G$. $\varphi(G) = \{e\}$ או $\varphi(G)\cong G$.

דוגמא נוספת - $L=\{f:\mathbb{N}\to\mathbb{Z}\}$, $(g+f)(n)=g(n)+f(n)$. נראה:

$L\cong\mathbb{Z}\oplus L$ ואז ברור ש- $\mathbb{Z}\cong\{0\}\Leftarrow\{0\}\oplus L\cong\mathbb{Z}\oplus L$ בסתירה.

ל- $l\in\mathbb{Z}$, $f\in L$ נגדיר: $f'\in L$ ע"י $f'(1)=l$, $f'(n)=f(n-1)$.

אזי f' הוא איזומורפיזם (תבדקו)

תמורות

טענה- $(a_1,\dots,a_k)^{-1}=(a_k,\dots,a_1)$.

הוכחה- נסמן $\sigma=(a_1,\dots,a_k)$, $\gamma=(a_k,\dots,a_1)$ ואזי

$$\sigma\circ\gamma(x)=\begin{cases}\sigma(x)=x & x\neq a_i \quad \forall i\\ \sigma(a_{i-1})=a_i & a_i=x \quad i>1 \longleftarrow (a_{i-1}\neq a_k)\\ \sigma(a_k)=a_1 & x=a_1\end{cases}.$$

דוגמא- $((1,2)(3,4,1))^{-1}=(1,4,3)(2,1)$.

סימן של תמורה

$\varepsilon:S_n\to\{\pm1\}$ $(=sgn)$ סימן של תמורה.

דוגמא- $\varepsilon((1,2,3)(1,2))=\varepsilon(1,2)\varepsilon(1,2,3)=(-1)^{3-1}(-1)^{2-1}=-1$

$o((a_1,\dots,a_k))=k$

שאלה- האם $C_8\cong C_2\times\overset{\text{קליין}}{\overset{\downarrow}{V_4}}$?

תשובה- לא. נראה שמס' האיברים מסדר 2 שונה. באגף ימין כל איבר שונה מ-e הוא מסדר 2 כי $(x,y)^2=(x^2,y^2)=(e,e)$ ($x\in C_2$, $y\in V_4$). לעומת זאת, באגף שמאל יש איבר מסדר 8.

הגדרה - יהי G חבורה (כפלית) ו־$A,B\subseteq G$ תת־קבוצות. נסמן $[A,B]=\langle\{aba^{-1}b^{-1}: a\in A, b\in B\}\rangle$.

דוגמאות - חבורה קבילית מסוג ראשון היא פשוטה וקומוטיבית.

- החבורה הסימטרית S_3 אינה קבילית.

דוגמאות - $S_3 \trianglerighteq A_3 \trianglerighteq \{e\}$ היא הסדרה: $C_3 \cong A_3/S_3$, $C_2 = S_3/A_3$.

משפט - תהי G חבורה סופית. אז G פתירה. (סדרה: קומוטנטים נגזרים). ותהי G חבורה סופית. אז יש לה סדרה הרכב (סדרה: קומוטנטים נגזרים). החבורות המנה G_{i+1}/G_i נקראות **מנות הסדרה**. אלו הן חבורות פשוטות אבליות.

הגדרה - סדרה $G=G_m \trianglerighteq \dots \trianglerighteq G_0 \trianglerighteq G_{-1}=\{e\}$ נקראת **סדרה נורמלית** אם $G_{i-1}\trianglelefteq G_i$ לכל i.

הערה - מספיק לדרוש כי $G_{i-1}\trianglelefteq G_i$ לכל i ומזה נובע כי $G_i \trianglelefteq G$ לכל i.

$G=G_n \trianglerighteq [G,G]=G_{n-1} \trianglerighteq [G_{n-1},G]=G_{n-2} \trianglerighteq \dots$ כמו כן

2. יהי $H\leq G$ תת־חבורה. נסמן $[H,G]=\langle\{hgh^{-1}g^{-1}: h\in H, g\in G\}\rangle$. אזי $[H,G]\trianglelefteq H$ (ולכן $[H,G]\trianglelefteq G$ אם $H\trianglelefteq G$).

$H\trianglelefteq G \Leftrightarrow [H,G]\leq H \Leftrightarrow H=HH \overset{\text{אבליות}}{=} H\cdot H \overset{H\trianglelefteq G}{=} HxHx^{-1}H \overset{\text{אבליות}}{=} Hx^{-1}Hx = Hx^{-1}x = H$.

3. יהי G חבורה. נסמן $G^{(0)}=G$, $G^{(1)}=[G,G]$, $G^{(2)}=[G^{(1)},G^{(1)}]$, $\dots$, $G^{(n)}=[G^{(n-1)},G^{(n-1)}]$. נקרא לסדרה $G\trianglerighteq G^{(1)}\trianglerighteq G^{(2)}\trianglerighteq\dots$ **סדרת הקומוטנטים הנגזרים**.

4. תהי G חבורה. נסמן $G^{(0)}=G$, $G^{(1)}=[G,G]$, $G^{(2)}=[G^{(1)},G^{(1)}]$, $\dots$, $G^{(n)}=[G^{(n-1)},G^{(n-1)}]$. נקרא לסדרה $G\trianglerighteq G^{(1)}\trianglerighteq G^{(2)}\trianglerighteq\dots$ **סדרת הקומוטנטים הנגזרים**.

דוגמאות - $S_3 \trianglerighteq A_3 \trianglerighteq \{e\}$ היא סדרת הרכב.

משפט - תהי G חבורה סופית. אז G פתירה. (סדרה: קומוטנטים נגזרים). ותהי G חבורה סופית. אז יש לה סדרה הרכב (סדרה: קומוטנטים נגזרים). החבורות המנה G_{i+1}/G_i נקראות **מנות הסדרה**. אלו הן חבורות פשוטות אבליות.

סדרת הרכב וחבורה פתירה

$SL_n(F) \supset SL_n(F') \supset \dots$

דוגמה $G = GL_n(F)$ ($n \geq 2$, F שדה) נקראת פתירה כי $G' = SL_n(F)$, אך מסיבה שונה מהדוגמה שנתנו בהגדרה.

הגדרה – תת־חבורה H של חבורה פתירה G נקראת אופיינית.

תהי G חבורה פתירה. נסמן $G^{(i)} = (G^{(i-1)})'$ ו־$G^{(0)} = G$. אז $G^{(i)} \trianglelefteq G$ אופיינית.

הוכחה: יהי $\varphi \in Aut(G)$. נראה $\varphi(G^{(i)}) = G^{(i)}$ באינדוקציה על i. עבור $i=0$ זה ברור. נניח שהטענה נכונה עבור i, ונוכיח עבור $i+1$. מתכונות הקומוטטור נובע $\varphi([x,y]) = [\varphi(x), \varphi(y)]$ לכל $x, y \in G$. לכן $\varphi(G^{(i+1)}) = \varphi([G^{(i)}, G^{(i)}]) = [\varphi(G^{(i)}), \varphi(G^{(i)})] = [G^{(i)}, G^{(i)}] = G^{(i+1)}$ (השוויון האחרון מהנחת האינדוקציה). ■

הגדרה – תהי G חבורה פתירה. נסמן $e_G = G_0 \supset G_1 \supset \dots \supset G_m = \{e_G\}$ כאשר $G_{i+1} \trianglelefteq G_i$ ו־G_i/G_{i+1} אבלית לכל $0 \leq i < m$. נאמר שסדרה זו היא סדרה נורמלית של G (או סדרה נורמלית קצרה). הגורמים G_i/G_{i+1} נקראים הגורמים של הסדרה. אורך הסדרה הוא m.

דוגמה $G_i = G^{(i)}$ הנגזרות הן סדרה נורמלית של G כי $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_i, G_i] = G_{i+1}$ (הכלה מהנחת האינדוקציה). כמו כן G_i/G_{i+1} אבלית.

הערה אם G פתירה אז יש לה סדרה נורמלית שכל גורמיה ציקליים מסדר ראשוני. הוכחה: תהי $G = H_0 \supset H_1 \supset \dots \supset H_k = \{e\}$ סדרה נורמלית שכל גורמיה אבליים. נבנה סדרה עדינה יותר. H_i/H_{i+1} אבלית סופית, לכן $H_i/H_{i+1} \cong \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_s}$. נוסיף תת־חבורות $\tilde{H}_1, \dots, \tilde{H}_{s-1}$ כך ש־$H_i/\tilde{H}_1$ ו־$\tilde{H}_1/\tilde{H}_2$ וכו' הם מסדר $p_1, p_2, \dots$ בהתאמה. הסדרה $G = H_0 \supset \tilde{H}_1 \supset \dots \supset \tilde{H}_{s-1} \supset H_1 \supset \dots$ היא סדרה נורמלית עדינה יותר. המשך באינדוקציה.

משפט G חבורה סופית. G פתירה $\iff$ קיימת סדרה נורמלית $G = G_0 \supset G_1 \supset \dots \supset G_m = \{e\}$ כך שכל גורמיה G_i/G_{i+1} הם מסדר ראשוני.

הוכחה: $\Leftarrow$: נראה $G^{(i)} \subseteq G_i$ באינדוקציה. $G^{(0)} = G = G_0$. אם $G^{(i)} \subseteq G_i$ אז $G^{(i+1)} = [G^{(i)}, G^{(i)}] \leq [G_i, G_i] \subseteq G_{i+1}$ (האחרון מכך ש־G_i/G_{i+1} אבלית). לכן $G^{(m)} = \{e\}$.

$\Rightarrow$: נראה $G_i \trianglelefteq G$ ו־G_i/G_{i+1} אבלית. G_i נורמלי באופן אינדוקטיבי. $G_{i+1} \trianglelefteq G_i$ כי G_i/G_{i+1} אבלית. יהי $g \in G$. נגדיר $\varphi_g : G_i \to G_i$ ע"י $\varphi_g(x) = gxg^{-1}$. φ_g אוטומורפיזם. $\varphi_g(G_{i+1}) \subseteq G_{i+1}$ כי G_i/G_{i+1} אבלית. לכן φ_g משרה $\bar{\varphi}_g : G_i/G_{i+1} \to G_i/G_{i+1}$. ההעתקה $g \mapsto \bar{\varphi}_g$ היא הומומורפיזם $G \to Aut(G_i/G_{i+1})$. הגרעין N הוא נורמלי ב־G. אם $g \in N$ אז $\bar{\varphi}_g = id$, כלומר $gxg^{-1}x^{-1} \in G_{i+1}$ לכל $x \in G_i$. אבל $gxg^{-1}x^{-1} \in G_i$ כי $G_i \trianglelefteq G$. לכן $N \subseteq G_{i+1}$. מצד שני $G_{i+1} \subseteq N$ כי G_i/G_{i+1} אבלית. ■

משפט סילו

יהי G חבורה סופית מסדר $|G| = p^k \cdot m$ כאשר p ראשוני ו- $p \nmid m$.

א. קיימת $H < G$ מסדר p^k. H נקראת חבורת סילו-p.

ב. אם $H < G$ מסדר p^i כאשר $i < k$ ו- p ראשוני, אז H מוכלת בחבורת סילו-p של G.

ג. מספר חבורות סילו-p שונות ב- G מקיים $n_p \equiv 1 \pmod{p}$ ו- $n_p = (G : N(P))$ כאשר P חבורת סילו-p כלשהי. בפרט $n_p \mid (G:P)$.

ד. מספר חבורות סילו-p שונות ב- G שווה 1 אם"ם יש חבורת סילו-p נורמלית ב- G.

דוגמה: G חבורה מסדר 132 אינה פשוטה.

הוכחה: $132 = 2^2 \cdot 3 \cdot 11$. נניח בשלילה ש- G פשוטה. בפרט $n_{11} \neq 1$.

מצד שני $n_{11} \mid 12$ ו- $n_{11} \equiv 1 \pmod{11}$, לכן $n_{11} = 12$.

מאידך, $12 \cdot 10 = 120$ איברים מסדר 11.

$n_3 \neq 1$, $n_3 \equiv 1 \pmod{3}$, $44 \mid n_3$

לכן $n_3 = 4, 22$ אלמנטים $n_3 = 1, 4, 7, 10, 13, 16, 19, 22, 25, 28$

נניח $n_3 = 4$, ונראה שבכך נגיע לסתירה:

דרך I: $(G : N_G(P)) = 4$. כאשר P חבורת סילו-3.

יש הומומורפיזם $\varphi : G \to S_4$ עם $\ker\varphi < N(P) < G$ כך ש-

$|\varphi(G)| = 132$ | $|S_4| = 4! = 24$ משפט קיי.

זה סתירה לכך ש- G פשוטה.

דרך II: נניח בשלילה ש- $n_3 = 4$, כך ש- $8 = 2 \cdot 4$ איברים מסדר 3.

סה"כ $128 = \underbrace{8}_{\text{מסדר 3}} + \underbrace{120}_{\text{מסדר 11}}$. אם $n_2 \neq 1$ אז יש N איברים מסדר שאינו 2.

יש 2^2.

נסיק שיש N 132 איברים. לפי $n_3 = 22$ נקבל שאין

יש $2 \cdot 22 + 120$. ■

$n_3 \neq 22$, $n_3 \neq 4$ לפי הנחה 1 וסה"כ

שאלה: $|G|=pq$. $p>q>2$ אז חתוך סילו- p נורמלי ב-G.

הוכחה שקולה: $n_q=1$ או $n_p=1$

נניח בשלילה $n_p<q$, $n_q<p$ $(n_p \equiv 1 \pmod p)$

$$q \mid n_p \Rightarrow q \mid p-1 \quad \text{(*)}$$

אם $n_p=q$ נקבל $q \mid p-1$ בסתירה. ואם $n_p=1$ אז q מחלק את $p-1$ (ולכן q אי-זוגי מספר p).

כלומר $q \mid n_q$ בהכרח $(q<p)$ לכן מספרנו q אי-זוגי מספר p.

אם $n_q=1$ נקבל $q \mid p-1$ בסתירה. $(q>p)$.

אם $n_q \neq 1$ אזי $n_q \geq p$ לכן $q \mid n_q$ כלומר $n_q=kq$ $(k \pmod p)$ $n_q \equiv 1$

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

q איברים מסדר p | p איברים מסדר q | 1

$q<p$ מתקיים $q=z^{-1}$

שאלה ב: נניח שאין תת-חבורה מסדר p שהיא 1.

תהי R תת-חבורה סילו- p ב-G! $|R|=p$ תת-חבורה סילו-p.

מכאן ש- $R \trianglelefteq G$ אז לכן $G=QR$.

$p^2 = |QR|$ לכאן $|R|=p$, $|Q|=p$ $(\underbrace{z}_{\text{כיוון}}, z^{-1})$

מלמעלה, אם תת-חבורת סילו- p בתוך QR אחרת אז q:

$$q \mid (p^2-1)(p-1)$$

וכן $n_p(QR) \equiv 1 \pmod p$ ולכן $n_p(QR)=1$.

R תת-חבורה-סילו- p ב QR, לכן $QR \trianglelefteq R$.

p ו $(p^2-1)(p-1) > QR$.

~~[illegible]~~

$p \mid |N_G(R)| \mid n_r$ מתקיים p סילו ב-G.

$\Leftarrow$ אם $n_r = |N_G(R)|$.

אזי $n_r = |N_G(R)|$ מקיים $n_r \equiv 1 \pmod{p}$ ו- $n_r = \frac{|G|}{|N_G(R)|} = p$.

יהי $G = N_G(R)$ (סילוב $R \trianglelefteq G$).

שאלה: נניח כי $|G| = p^2 q$ ו- p, q ראשוניים. הוכיחו כי G אבלית.

מושג מתמטי

נניח בשלילה $n_p > 1$, $n_q > 1$; $n_p \mid q \equiv 1 \pmod{p}$ $\leftarrow$ $q = (G:P)$

לכן $q > p$ $\Leftarrow$ $p \mid q-1$ $\Leftarrow$ $q = pn$

~~מכיוון ש-q אבלי~~

$p^2 \mid n_q$ לכן $n_q = p^2 k$. אזי $n_q = p$ מכיוון ש- $n_q \equiv 1 \pmod{q}$ $\Leftarrow$ $q \mid p-1$ $\Leftarrow$ $q > p$ סתירה.

צמ $n_q = p^2$ אזי $N_G(Q)$ אבלי מסדר q.

$(q-1)p^2$ אברים מסדר q (מהו תנאי שפ אסג) (מס' סילוב q)

סילוב p אחת

כמה תבניות p^2 אברים מסדר $p, 1$ אזי $p^2 + (q-1)p^2 = q p^2$.