משפטי סילוב

שאלה: נניח G מסדר p^n. בנ"ל לכל $0 \le k \le n$ יש ת"ח $H \lhd G$ מסדר p^k.

פתרון: באינדוקציה על n. עבור $n=0,1$ הטענה ברורה.

נניח כי הטענה מתקיימת עבור $1-n$. תהי $|G| = p^n$. עבור $k=0$ - ברור ($H = \{e\}$). יהי $n \ge k > 0$. נניח כי $Z(G) \ne \{e\}$ (כלומר הטענה שקה תמיד משתמשים במרכז כאלה"). לכן יש $x \ne e$. נגדיר $L = \langle x \rangle \lhd G$. נבחר את x כך שיתקיים $p = |L|$ (זה אפשרי, לפי משפט קש' שאופיע על $Z(G)$). לכן $p^{n-1} = |G/L|$. מהנחת האינדוקציה על G/L, יש $H/L \lhd G/L$ מסדר $p^{k-1} = \frac{|H|}{|L|} = \frac{|H|}{p}$. ממשפט האיזומורפיזם הפש'י $G \rhd H$, וכן $|H| = p^{k-1}|L| = p^k$. □

שאלה: (הארגומנט של Frattini)

נניח כי G חבורה סופית, ו- P תת חבורת סילוב-p שלה, $G \rhd K$ כך ש- $K \ge P$.

אזי $G = K \cdot N(P)$.

הוכחה: יהי $g \in G$, אזי $gPg^{-1} \le gKg^{-1} = K$. כאשר $gKg^{-1} = K$. אזי P, gPg^{-1} הן תת-חבורות סילוב-p ב- K. לכן יש $k \in K$ כך ש: $P = kgPg^{-1}k^{-1}$.

לכן $g \in N(P)k^{-1} \Rightarrow g \in kN(P) \subseteq KN(P)$. □

שאלה: נניח $G \le T \le N(P)$. P סילוב-p ב-G. בנ"ל $T = N(T)$.

הוכחה: נפעיל את הארגומנט על הפרטיני $T = N(T)$, $G = N(T)$ ($N(T) \rhd T$), ונקבל:

$N(T) = T \cdot N_{N(T)}(P)$. אבל $N(T) \supseteq T = N(P) \cap T$

$\Leftarrow N(T) = T$.

מסקנה: $N(N(P)) = N(P)$ ל- P סילוב-p. (ניקח $T = N(P)$)

שאלה: יהי $n \ne m$, הוכח כי $\mathbb{Z}^m \not\cong \mathbb{Z}^n$.

הוכחה: שלב ראשון - נתאר ש- $\mathbb{Z}^n$ נוצרת ע"י n איברים, ולא ע"י $n-1$ איברים.

ברור ש: $\mathbb{Z}^n = \langle e_1, \dots, e_n \rangle$ (כאשר $e_i = (0, \dots, \underset{\text{מקום } i}{1}, \dots, 0)$). נניח כי $\mathbb{Z}^n = \langle b_1, \dots, b_\ell \rangle$.

לכן בהכרח: $\mathbb{Q}^\ell = \{b_1, \dots, b_\ell\}_{\mathbb{Q}} \supseteq \{b_1, \dots, b_\ell\}_{\mathbb{Z}} \supseteq \{e_1, \dots, e_n\}_{\mathbb{Z}}$

$\mathbb{Q}^\ell$ כ"מ מעל $\mathbb{Q}$. קבוצת יוצרים בת m איברים, $n > m$. ניקח X קבוצת יוצרים בת m איברים

$\varphi : \mathbb{Z}^n \to \mathbb{Z}^m$, כאשר $n > m$.

$\varphi(\mathbb{Z}^n) = \varphi(\langle x \rangle) = \langle \varphi(X) \rangle$

טענה ב': נניח $\mathbb{Z}^n \xrightarrow{\varphi} \mathbb{Z}^m$ הומומורפיזם. אזי $\varphi(\mathbb{Z}^n) = \mathbb{Z}^m$

□

שאלה: תהי G חבורה מסדר pq כך ש- $p<q$ ראשוניים. אזי $q \nmid p-1$ אם ורק אם G ציקלית, ואם $q \mid p-1$ אז G נוצרת ע"י a,b המקיימים $a^q = 1$, $b^p = 1$, $a^{-1}ba = b^r$, $r \not\equiv 1 \pmod p$, $r^q \equiv 1 \pmod p$.

הוכחה: מהשיעור נותר להוכיח במקרה $q \mid p-1$. נניח G לא ציקלית. מהשיעור, אזי p חבורת סילוב-p, Q חבורת סילוב-q, $Q \trianglelefteq G$ (הראנו בשיעור), $P = \langle b \rangle$, $Q = \langle a \rangle$.

$$|PQ| = pq = |G|$$

↑ משפט קודם

לכן $G = \langle a,b \rangle$.

כמו כן $a^q = 1$, $b^p = 1$.

$a^{-1}ba = b^r$ לאיזשהו $0 \le r < p$, שכן נורמלי P.

אם $r \equiv 1 \pmod p$, אזי $ba = ab \Leftarrow a^{-1}ba = b$ ומשפט קודם, חסדר של ab הוא מכפלת חסדרים (כי a,b מתחלפים ומסדרים זרים), כלומר pq, ולכן $G = \langle ab \rangle$ ציקלית.

סתירה כי G לא ציקלית ולכן $G \neq \langle ab \rangle$.

$$a^{-2}ba^2 = a^{-1}(a^{-1}ba)a = a^{-1}b^r a = (a^{-1}ba)^r = (b^r)^r = b^{r^2}$$

באופן דומה:

$$a^{-q}ba^q = b^{r^q}$$

אבל: $a^q = 1$, ולכן: (ע"י תלקה כ-q)

$$b^{r^q - 1} = 1$$

לכן $p \mid r^q - 1$ ומכאן $r^q \equiv 1 \pmod p$