משפטי סילוא

משפט קושי

תהא G חבורה סופית, p ראשוני. אז אם $p||G|$ אזי קיים בה איבר מסדר p.

משפט סילוא I

תהא G חבורה סופית, p_0 ראשוני. אז לכל m טבעי אם $p^m||G|$ אז קיימת בG ת"ח מסדר p^m.

הוכחה

נקבע p ראשוני. נוכיח את המשפט באינדוקציה על סדר G. אם סדר G הוא p אז המשפט תקף כמובן(כי $G \leq G$ מסדר p). נוכיח שהמשפט תקף עבור כל חבורה מסדר n.

נניח $p^m|n$. תהא G חבורה מסדר n. צ"ל יש לה ת"ח מסדר p^m.

מקרה א

יש בG איבר $x \in G$ כך ש$x \notin Z(G)$ ו$p^m||Z_x|$. במקרה זה - מכיוון ש$x \notin Z(G) \Leftarrow$ $G \subsetneq Z_x$. לכן $|Z_x|$. לפי הנחת האינדוקציה מכיוון ש$n > |Z_x|$ וגם $p^m||Z_x|$, יש בZ_x ת"ח מסדר p^m וזו ת"ח של G מסדר p^m.

מקרה ב

לכל איבר $x \in G \backslash Z(G)$ מתקיים $p^m \nmid |Z_x|$.

נשתמש במשפט: לכל $g \in G$ (G סופית) $|G| = |\text{conj}(g)||Z_g|$. מסקנה - לכל איבר $x \in G \backslash Z(G)$ $|G| = |\text{conj}(x)||Z_x|$. הנחנו $p^m||G|$ וגם $p^m \nmid |Z_x|$ ולכן

$$\boxed{\forall_{x \in G \backslash Z(G)} p|\,|\text{conj}(x)|} \quad (*)$$

לפי משוואת המחלקות $|G| = |Z(G)| + \sum_{i=1}^{k} |\text{conj}(x_i)|$ כאשר $x_1, ...x_k$ נציגי מחלקות צמידות מסדר > 1, בפרט $x_1, ...x_k$ לא במרכז(להסביר למה...).

לפי $(*)$ $1 \leq i \leq k$, $p|\,|\text{conj}(x_i)|$ לכן $p|\sum_{i=1}^{k} |\text{conj}(x_i)|$. הנחנו ש$p^m||G|$ ולכן $p|\,|G|$

$\Leftarrow p|\,|G| - \sum_{i=1}^{k} |\text{conj}(X_i)| \Leftarrow p|\,|Z(G)|$.

לכן לפי משפט קושי יש במרכז איבר $x \in Z(G)$ מסדר p:

$$\exists_{x \in Z(G)} |\langle x \rangle| = p$$

לכל $g \in Z(G)$ $\langle g \rangle \trianglelefteq G$ ולכן מצאנו תח"נ של G $\langle x \rangle \trianglelefteq G$ מסדר p.

נתבונן ב$G/\langle x\rangle$, סידרה(לפי לגרנז')

$$|G/\langle x\rangle| = [G:\langle x\rangle]$$

$$|G/\langle x\rangle| = \frac{|G|}{|\langle x\rangle|} = \frac{|G|}{p} < |G| = n$$

כמו כן $p^{m} \mid |G| \Leftarrow p^{m-1} \mid |G/\langle x\rangle|$.
לפי הנחת האינדוקציה יש ב$G/\langle x\rangle$ ת"ח מסדר p^{m-1}. יהיו איבריה $g_1\langle x\rangle, g_2\langle x\rangle, ...g_{p^{m-1}}\langle x\rangle$.
מכיוון שזו ת"ח של $G/\langle x\rangle$ היא סגורה תחת כפל והופכי. ז"א:

1. לכל $1 \le i < j \le p^{m-1}$, $g_i\langle x\rangle g_j\langle x\rangle = g_k\langle x\rangle$ לאיזשהו $1 \le g_k \le p^{m-1}$.
2. וכן $(g_i\langle x\rangle)^{-1} = g_r\langle x\rangle$ עבור איזשהו $1 \le r \le p^{m-1}$

נתבונן ב$B := \coprod_{i=1}^{p^{m-1}} g_i\langle x\rangle$ איחוד זר של איברי המחלקות של $\langle x\rangle$ בG. מכיוון שהמל-חקות זרות ומכיוון ש$|\langle x\rangle| = p$. על כן $|B| = p\cdot p^{m-1} = p^m$. B לא ריקה כי $|B| > 0$.
נותר להראות B סגורה תחת כפל והופכי. נשים לב:

$$\langle x\rangle = \left\{x^i : 0 \le i < p\right\}$$

לכן כל שני איברים בB $g_ix^{d_1}, g_jx^{d_2}$ מתקיים

$$g_ix^{d_1}\cdot g_jx^{d_2} \in g_i\langle x\rangle g_j\langle x\rangle = g_k\langle x\rangle$$

לאיזשהו $p^{m-1} \le k \le 1$ לפי 1, וכן לכל איבר g_ix^d בB מתקיים $\left(g_1x^d\right)^{-1} \in$ $(g_i\langle x\rangle)^{-1} = g_r\langle x\rangle$ לאישזהו $1 \le r \le p^{m-1}$ לפי 2.