משפט סילוא I

תהא G חבורה סופית. p ראשוני. אם $p^m | |G|$ אז יש בG ת"ח מסדר p^m

הגדרה

תהא G חבורה סופית, p ראשוני המחלק את סדר G. נניח $p^k | |G|$, $p^{k+1} \nmid |G|$
ת.ח מסדר נקראת ת.ת. סילוא.

מסקנה ממשפט 1

תהא G חבורה סופית, p ראשוני המחלק את סדר G אז יש בG ת"ח p-סילוא

ש1: האם ת"ח p-סילוא שונות איזומורפיות זו לזו?

ש2: כמה ת"ח p-סילוא יש?

משפט סילוא II

תהא G חבורה סופית, p ראשוני, $p| |G|$. כל ת"ח p-סילוא של G צמודות זו לזו
(ז.א אם H, K שתי ת"ח p-סילוא אז קיים $x \in G$ כך ש$xHx^{-1} = K$

משפט סילוא III

יהא r_p מס' ת"ח p-סילוא בG. אז:

(i) $r_p | |G|$

(ii) $r_p \equiv 1 \mod |G|$

הערה ביחס לת"ח צמודות

טענה: אם H, K שתי ת"ח צמודות בG אז $H \cong K$

הוכחה: H, K צמודות, ז"א קיים $x \in G$ כך ש$xHx^{-1} = K$. נגדיר העתקה $\varphi : H \to K$ ע"י $\varphi(h) := xhx^{-1}$. העתקה זו היא איז'(ז.א. חח"ע, על, הומ').
בדוק!

תרגיל

אם $H \le G$, $xHx^{-1} \le G$, ו $xHx^{-1} \cong H$

מסקנות מתרגיל

אם $H \le G$ ת"ח p-סילוא אז כל ת"ח הצמודות לH ג"כ ת"ח p-סילוא.

כדי להוכיח משפט סילוא II

צ,ל: אין ת"ח שאינן צמודות שהן p-סילוא.

טענה

משפט סילוא $II \Leftarrow$ סילוא $III\ (i)$

הוכחה

נוכיח טענה כללית יותר:

טענה כללית

תהא G חבורה סופית. $H \leq G$. מס' ת"ח הצמודות לH מחלק את סדר G.

הוכחת הטענה

נגדיר קבוצה $X(G)$ כל ת"ח של G. G פועלת על $X(G)$ ע"י הצמדה. $\varphi(x)(H) := xHx^{-1}$.

הגדרה המייצב של H תחת פעולת הצמדה נקרא <u>המנרמל</u> של H

$$N_G(H) := \left\{x \in G : xHx^{-1} = H\right\}$$

לפי משפט שלמדנו, $|G| = |N_G(H)|\,|O(H)| \Leftarrow |O(H)|$מחלק את סדר G. כלומר, מס' ת"ח הצמודות לH מחלק את סדר G. ■

הוכחת סילוא II וסילוא $III(ii)$

למה 1 תהא K חבורת p. אם K פועלת על X אז $|X| \equiv |X_0| \bmod p$ כאשר $X_0\left\{x \in X : \forall_{g\in K} p(g)(x) = x\right\}$

הוכחה הוכחנו בעבר

למה 2 תהא P ת"ח p-סילוא של G. $x \in G$ מסדר חזקת p, וכן $xPx^{-1} = P$. אזי $x \in P$.

הוכחה לפי תנאי המשפט $x \in N_G(P)$.

תרגיל לכל $H \leq G$, $N_G(H) \leq G$, ו$H \trianglelefteq N_G(H)$.

מסקנה $P \trianglelefteq N_G(P)$, ולכן $\overline{x} := xP \in {}^{\mathrm{N_G(P)}}/_{\mathrm{P}}$.

$o(x) = p^m$ לאיזשהו m. $(xP)^{o(x)} - x^{o(x)}P = P$.

עובדה אם $g^k = e$ אז $o(g)\,|k$.

לכן, $o(\overline{x})\,|o(x)$. מכאן, $o(\overline{x})$ חזקה של p.

- אם $o(\overline{x}) = 1$ אז $xP = P$ ולכן $x \in P$ וסיימנו.
- אם $o(\overline{x}) = p^d$, $1 \leq d$, אז $\overline{x}^0, \overline{x}^1, \overline{x}^2, ...\overline{x}^{p^d-1}$ איברים שונים ב${}^{\mathrm{N_G(P)}}/_{\mathrm{P}}$. איחוד אברי המחלקות האלה הוא ת"ק בG. $x^0P, xP, x^2P, ...x^{p^d}P$. $p^d\,|P|$ שהיא ת"ק(סגורה תחת כפל והופכי). בפרט ת"ח-p מסדר גדול מסדר P. בסתירה לכך שP p-סילוא. ■

ההוכחה

תהא P ת"ח p-סילוא של G. תהיינה $A = \{P=P_1, P_2, ...P_m\}$ קבוצת כל ת"ח הצמודות לP. לפי הערה מתחילת השיעור $1 \le i \le m$, P_i ת"ח p-סילוא. צ"ל: אין אחרות

ט.ע.1 $m \equiv 1 \bmod p$

הוכחה P פועלת על A ע"י הצמדה. לפי למה 1, $|A| \equiv |A_0| \bmod p$ (✡) כאשר A_0 נקודות שבת ביחס לפעולה זו. נניח P_i נקודת שבת. ז"א: לכל $x \in P$, $xP_ix^{-1} = P_i$. $x \in P$ לכן $o(x) \mid |P|$ ולכן סדר x חזקת p. כמו כן, P_i ת"ח p-סילוא(לפי $(*)$). לפי למה 2, $x \in P_i$. כלומר, לכל $x \in P$, $x \in P_i$ $\Leftarrow$ $P \subseteq P_i$, אבל $|P_i| = |P|$(כי הן צמודות). ולכן אם P_i נק. שבת אז $P_i = P$. ודאי P_i נק. שבת(מדוע?) לכן $|A_0| = 1$ (✡✡). (✡) + (✡✡)$\Leftarrow$ ט.ע 1. מש"ל ט.ע. 1

סיכום ביניים: סילדוא $(ii)III \Leftarrow II$. נותר להוכיח: סילוא II. נוכיח זאת ע"י השלילה:
תהא Q ת"ח p-סילוא שאינה צמודה לP. Q פועלת על A ע"י הצמדה.

ט.ע.2 אין נקודות שבת תחת פעולה זו.

הוכחה נניח P_i נקודת שבת. ז"א לכל $x \in Q$, $xP_ix^{-1} = P_i$. $x \in Q$ לכן $o(x) \mid |Q|$ ולכן סדר x חזקת p. כמור כן p_i ת"ח p-סילוא(לפי $(*)$). לפי למה 2, $x \in P_i$. כלומר, לכל $x \in P$, $x \in P_i$ $\Leftarrow$ $\backslash P \subseteq P_i$ אבל $|P_i| = |P|$(כי הן צמודות). ולכן אם P_i נק. שבת אז $P_i = Q$, כלומר Q צמודה לP בסתירה להנחה. לכן לפי למה 1, $|A| \equiv |A_0| \mod p$. אבל $|A_0| = 0$, מכאן $m = |A| \equiv 0 \bmod p$ בסתירה לט.ע.1. מכאן אין Q כזאת. ■

מסקנה

יהי $p < q$ ראשוניים. נניח $q \not\equiv 1 \bmod p$. אז כל חבורה מסדר pq ציקלית.

דוגמה

1. $p = 3$, $q = 5$. כל חבורה מסדר 15 ציקלית.
2. $p = 7$, $q = 101$. כל חבורה מסדר 707 ציקלית.

הוכחה

יהיו p, q כנ"ל, G חבורה מסדר pq. מ"ל: יש בG איבר מסדר pq. לפי משפט לגרנז' סדרים אפשריים לאיברים הם $1, p, q, pq$. לפי משפא קושי יש ת"ח מסדר q. זו ת"ח q-סילוא. לפי סילוא III מס' ת"ח מסדר q(שכולן q-סילוא) (יסומן r_q). מקיים $r_q|pq$ וגם $r_q \equiv 1 \bmod q$, לכן $r_q = 1$(מדוע?). נשים לב, כל האיברים שסדרם q יוצרים ת"ח מסדר q, ולכן נמצאים בת"ח מסדר q, ויש רק אחת כזו.

לכן, האיברים מסדר q הם בדיוק האיברים ב$H_q \backslash \{e\}$(H_q ת"ח q-סילוא יחידה). ולכן יש $q-1$ איברים מסדר q.

לפי משפט קושי יש ת"ח מסדר p. זו ת"ח p-סילוא(כי $|G| = pq$ $p^2 \nmid$. כמה ת"ח מסדר p יש?

כולן p-סילוא. לפי סילוא III מספרן r_p מקיים $r_p|pq$ $\Leftarrow$ $r_p \in \{1, p, q, pq\}$.

$r_p = 1 \bmod p \Leftarrow pq, r_p \neq p$ וכן $r_p \neq q$ לפי ההנחה $q \not\equiv 1 \bmod p$
$\Leftarrow r_p = 1$. כלומר יש ת"ח יחידה מסדר p, נסמנה H_p.
לכן יש $p-1$ איברים מסדר p(משיקולים כנ"ל). נסמן מס' האיברים מסדר pq בx.
כמובן מספר האיברים מסדר 1 שווה ל1.

- מספר האיברים מסדר 1 הוא 1
- מספר האיברים מסדר p הוא $p-1$
- מספר האיברים מסדר q הוא $q-1$
- מספר האיברים מסדר pq הוא x

מתקיים:

$$1 + (p-1) + (q-1) + x = pq$$

$$\Rightarrow x = pq - p - q + 1 = (p-1)(q-1) \geq 1$$

כי p, q ראשוניים.
קיבלנו: יש איבר מסדר pq ולכן G ציקלית.