חבורות סילוא

הגדרה

G חבורה סופית, p ראשוני, אזי קיים ויחיד m כך ש$p^m||G|$ וגם $p^{m+1}\nmid|G|$. תת חבורה של G מסדר p^m נקראת תת חבורה p-סילוא

מסקנה\משפט סילוא 1

אם G חבורה סופית, אזי לכל p ראשוני המחלק את $|G|$ קיימת תת חבורה p-סילוא.

הגדרה

נאמר ששתי תת קבוצות $S,T\subseteq G$ (יכולות להיות גם תת חבורות) הן צמודות אם קיים $g\in G$ כך ש $gSg^{-1}=T$.

תרגיל

הראו שאם $K,H\le G$ הן צמודות ושונות אזי הן לא נורמליות.

הוכחה

נניח בשלילה כי H נורמלית. כעת, K צמודה לH ולכן קיים $g\in G$ כך ש$gHg^{-1}=K$. אולם H נורמלית, ולכן $gHg^{-1}=H$, משמע $K=H$, סתירה.

משפט (סילוא 2)

כל תתי החבורות הp-סילוא הן צמודות.

תרגיל

אם H ת"ח p-סילוא של G, אז גם gHg^{-1} תת חבורה p-סילוא של G.

תרגיל

ישנה רק תת חבורה p-סילוא אחת

$\Updownarrow$

תת החבורה הp-סילוא היא נורמלית.

פתרון

הראנו כבר כי אם יש יותר מאחת אז היא לא נורמלית, שזה הכיוון $(\Uparrow)$

$(\Downarrow)$ ישנה רק תת חבורה p-סילוא אחת H. יהי $g \in G$, אזי gHg^{-1} היא גם כן תת-חבורה p-סילוא. אבל ישנה רק אחת כזאת, ולכן $H = gHg^{-1} \Leftarrow H \lhd G$

משפט(סילוא 3)

נסמן בr_p את מספר תת החבורות הp-סילוא בG. אזי:

א. $r_p \mid |G|$

ב. $r_p \equiv 1 \pmod{p}$

הערות

1. $\gcd(r_p, p) = 1$
2. אם תת חבורה p-סילוא היא נורמלית אזי $r_p = 1$

הגדרה

חבורת p היא חבורה מסדר p^k לאיזשהו k.

תרגיל

אם G אינה חבורת p, וגם $p \mid |G|$ וגם $r_p = 1$, אזי G לא פשוטה.

תזכורת חבורה פשוטה היא חבורה ללא תת חבורות נורמליות לא טריוויאליות.

הוכחה

$r_p = 1$ ולכן קיימת רק תת חבורה p-סילוא אחת H, ולכן H נורמלית.

- $H \neq \{e\}$ משום ש$p \mid |G|$ ולכן $p \mid |H|$, אז הm המקסימלי שעבורו $p^m \mid |G|$ הוא גדול או שווה ל1, בפרט $|H| = p^m$.
- $H \neq G$ משום שאם נניח בשלילה כי $H = G$ נקבל שG היא חבורת p.

תרגיל\משפט

r_p מחלק את $\frac{|G|}{p^m}$ כאשר m הוא המקסימלי כך ש$p^m \mid |G|$

הוכחה

נביט בתת חבורה p-סילוא H

$$\frac{|G|}{|H|}=[G:H]$$

$$|G|=|H|\,[G:H]$$

$$\left[K=\frac{|G|}{p^m}\right]$$

כעת, $r_p|\,|G|$ לכן $r_p|p^m\cdot k$ אבל $1=\gcd\left(r_p,p^m\right)$ ולכן $r_p|k$

[תזכורת: אם $x|a\cdot b$ וגם $1=\gcd\left(x,a\right)$ אזי $x|b$]

תרגיל

הראו שחבורה G מסדר 40 אינה פשוטה

תשובה

$40=2^3\cdot5^1 \Leftarrow$ ישנה תת חבורה 2-סילוא מסדר 8, וישנה תת חבורה 5-סילוא מסדר 5.

נראה כי $r_5=1$:

$r_5\in\{1,2,4,5,8,10,20,40\}$, ובנוסף צריך להתקיים $r_5\equiv1\left(\mathrm{mod}\ 5\right)$. 1 הוא המספר היחיד בקבוצה שמקיים את התנאי $\Leftarrow$ $r_5=1$ $\Leftarrow$ ישנה תת חבורה נורמלית מסדר 5 $\Leftarrow$ החבורה G לא פשוטה.

תרגיל

האם קיימת חבורה פשוטה מסדר 10?

תשובה

$10=2\cdot5$. G. אזי קיימת תת חבורה 5-סילוא H. $|H|=5\Leftarrow 2=\frac{|G|}{|H|}=[G:H]\Leftarrow$

$H\lhd G\Leftarrow G$ לא פשוטה.

תרגיל

p,q ראשוניים. אם $|G|=pq$ כך ש$q\neq p$ וגם $q\not\equiv1\left(\mathrm{mod}\ p\right)$ אז יש לG תת חבורה p-סילוא נורמלית.

פתרון

רוצים להראות ש$r_p=1$.

$$r_p|\,|G|\Rightarrow r_p|p\cdot q\Rightarrow r_p\in\{1,p,q,pq\}$$

אבל, $q\not\equiv1\left(\mathrm{mod}\ p\right)$, $p,pq\equiv\left(\mathrm{mod}\ p\right)$ $\Leftarrow$ $r_p=1$

משפט

יהיו p,q ראשוניים, $p<q$ ו$q\not\equiv 1\,(\mathrm{mod}\ p)$, אזי כל חבורה מסדר $p\cdot q$ היא ציקלית.

תרגיל

הוכח כי חבורה מסדר 84 אינה פשוטה

הוכחה

$84=7\cdot 12$. הראינו כבר כי $r_7|\frac{84}{7} \Leftarrow r_7|12 \Leftarrow r_7\in\{1,2,3,6,12\}$
$r_7\equiv 1\,(\mathrm{mod}\ 2) \Leftarrow r_7=1$.

תרגיל עזר

אם p ראשוני וG חבורה, אם H,K שתי תתי חבורות שונות מסדר p אזי $H\cap K=\{e\}$

פתרון

$$H\cap K\le K,H$$

$$\Downarrow$$

$$|H\cap K|\,|\,|K|=p$$

$$\Downarrow$$

$$|H\cap K|\in\{1,p\}$$

אם $|H\cap K|=p$ אזי $H\cap K=K \Leftarrow H=K$.

מסקנה

מספר האיברים מסדר p ראשוני בחבורה G מתחלק ב$p-1$

"הוכחה"

את האיברים מסדר p אפשר לסדר בתתי חבורות ציקליות שונות $H_1,...H_k$ שכוללות את כל האיברים מסדר p וגם את e. כעת, החיתוך של כל $H_i\cap H=\{e\} \Leftarrow$

$$|H_1\cup...\cup H_k\backslash\{e\}|=(p-1)\cdot k$$

תרגיל

אם $|G| = p^2 \cdot q$, p, q ראשוניים, אזי יש לG תת חבורה p-סילוא נורמלית או שיש לG תת חבורה q-סילוא נורמלית.

הוכחה

לG יש תת חבורה p-סילוא מסדר p^2 וq-סילוא מסדר q. נניח בשלילה כי $1 < r_p, r_q$.
לפי משפטי סילוא

$$r_p, r_q | \, |G| \Rightarrow r_p, r_q \in \left\{p, q, p^2, p^2 q, pq\right\}$$

$$r_p \equiv 1 \, (\mathrm{mod} \ p) \Rightarrow r_p = q \Rightarrow q > p$$

$$r_q \equiv 1 \, (\mathrm{mod} \ q) \Rightarrow r_q \in \left\{p, p^2\right\}$$

כל איבר מסדר q יוצר תת חבורה q-סילוא.
כל שתי תת חבורות q-סילוא שונות נחתכות ב$\{e\}$, ולכן $r_q \left(q-1\right)$ זה מספר האי-ברים מסדר q בG.
נזכור כי $r_q \in \left\{p, p^2\right\}$. אם:

- $r_q = p^2$ אזי מספר האיברים שאינם מסדר q בG הוא

$$|G| - p^2 \left(q-1\right) = p^2 q - p^2 \left(q-1\right) = p^2$$

אבל אם מסמנים בH את חבורת הp-סילוא של G, אזי $|H| = p^2$, וברור כי H לא מכילה איבר מסדר q. זה אומר שכל האיברים שאינם מסדר q בG נמצאים בH, ולכן ישנה רק חבורת p-סילוא אחת $\Leftarrow$ $r_p = 1$ בסתירה.
[אם היינו מניחים כי יש עוד ת"ח p-סילוא K, אז גם היא הייתה שווה לקבוצת האיברים בG מסדר לא q]

- $r_q = p$. $q > p$
$r_q \equiv 1 \, (\mathrm{mod} \ q) \Leftarrow p \equiv 1 \, (\mathrm{mod} \ q) \Leftarrow p = 1 \Leftarrow$סתירה.