

חבורות p ומשפטי קושי

הגדרה - חבורות p

חבורת p היא חבורה שסדרה חזקה של ראשוני p (שאינה $1 = p^0$)

משפט 1

לחבורת G יש מרכז לא טריוויאלי (ז"א $|Z(G)| > 1$)

הוכחה

תהא G חבורה שסדרה p^n , ראשוני p , טבעי n . לפי משוואת המחלקות

$$|G| = |Z(G)| + \sum_{i=1}^l |\text{conj}(x_i)|$$

כאשר x_1, \dots, x_l נציגי מחלקות צמידות מסדר גדול מ-1

$$|Z(G)| = |G| - \sum_{i=1}^l |\text{conj}(x_i)|$$

$|G| = p^n$, לפי ההנחה n טבעי.

מאידך, לפי משפט משיעור קודם $|G| = p^n$, $\forall 1 \leq i \leq l$ $|\text{conj}(x_i)| = p^k$ כאשר $0 < k \leq n$ כך שלכל $1 \leq i \leq l$, $1 < |\text{conj}(x_i)| < p^n$ אבל הראינו $p \mid |\text{conj}(x_i)|$ לכל $1 \leq i \leq l$ לכן $p \mid \sum_{i=1}^l |\text{conj}(x_i)|$ אבל הראינו $p \nmid |G|$ לכן $1 \leq |Z(G)| < p^n$ תמיד $e \in Z(G)$ לכן $1 \leq |Z(G)| < p^n$ יהי $p \leq |Z(G)| < p^n$.

תזכורת

חבורה מסדר p היא ציקלית.

משפט 2

חבורה מסדר p^2 היא אבלית.

הערה

יש חבורות מסדר p^2 שאינן ציקליות. לדוגמא מרחב וקטורי ממימד 2 מעל \mathbb{F}_p חיבור וכפל מודולו p של $\{0, 1, 2, \dots, p-1\}$ שדה \mathbb{F}_p .

הוכחת משפט 2

יהא p ראשוני כנ"ל תהא G חבורה מסדר p^2 . לפי משפט 1, $|Z(G)|$ שווה ל p או ל p^2 . אם $|Z(G)| = p^2$ אז $G = Z(G)$ ולכן G אבלית. נניח בדרך השלילה $|Z(G)| = p$. תמיד $Z(G) \trianglelefteq G$. נתבונן ב $G/Z(G)$:

$$|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$$

ולכן $G/Z(G)$ ציקלית.

יהא x יוצר של $G/Z(G)$. ז"א $(*) \{x^k : 0 \leq k < p\}$.
 $x \in G/Z(G)$, לכן קיים $g \in G$ כך ש $x = gZ(G)$

$$(*) = \{(g \cdot Z(G))^k : 0 < k < p\} = \{g^k Z(G) : 0 < k < p\}$$

$$G = \prod_{k=0}^{p-1} g^k Z(G) \quad \text{מסקנה}$$

לכן כל איבר נמצא בדיוק באחת המחלקות $g^k Z(G)$ לאיזשהו $0 \leq k < p$, כלומר $a \in g^k Z(G) \iff a = g^k z$ כך ש $z \in Z(G)$. קיים $a_1, a_2 \in G$ קיימים $0 \leq k_1 < p, 0 \leq k_2 < p, z_1 \in Z(G)$ כך ש $a_1 = g^{k_1} z_1$ ו $a_2 = g^{k_2} z_2$ ואז

$$\begin{aligned} a_1 a_2 &= g^{k_1} z_1 g^{k_2} z_2 = g^{k_1} g^{k_2} z_1 z_2 = g^{k_1+k_2} z_1 z_2 \\ &= g^{k_2+k_1} z_2 z_1 = g^{k_2} g^{k_1} z_2 z_1 = g^{k_2} z_2 g^{k_1} z_1 = a_2 a_1 \end{aligned}$$

הוכחנו משפט 2

אם סדר G שווה ל p^2 אז G אבלית. מההוכחה דלעיל אפשר להסיק:

תרגיל

תהא G חבורה. לא ייתכן $|G/Z(G)| = p$, עבור איזהו ראשוני p מוטיבציה דוגמה: תהא G חבורה מסדר 15.

שאלה

האם אכן קיימות ת"ח מסדרים 1, 3, 5, 15:

תשובה

תמיד קיימות ת"ח טריויאלית $\{e\}$ ו G עצמה ולכן 1, 15

משפט קושי

תהא G חבורה סופית. p ראשוני. אם $p \mid |G|$ אזי קיים איבר מסדר p .

מסקנה

אם G חבורה סופית, וסדרה מתחלק ע"י ראשוניים, אזי קיימת ת"ח מסדרם. (הוכחה - תרגיל).

מסקנה ממשפט קושי

G חבורת p אמ"ם סדרי איבריה הם חזקות של p (הערה: מותר גם p^0)

הוכחה

נניח G חבורת p . על פי משפט לגרנז' לכל $g \in G$ כאשר G סופית $|G| \mid o(G)$ ולכן במקרה שלנו $|G| = p^n$ $\forall g \in G o(g) \mid |G|$ כאשר p ראשוני. \Leftarrow סדרי כל האיברים הם חזקות של p .

סדרי כל איברי G חזקות של p . נוכיח על דרך השלילה. \Leftarrow אם G לא חבורת p , אזי קיים q ראשוני שאינו p כך ש $q \mid |G|$ ואז לפי משפט קושי, קיים ב G איבר מסדר 1, בסתירה להנחה.

למה

תהא G חבורת p . נניח G פועלת על קבוצה X . כלומר קיים הומו' $\varphi : G \rightarrow S(X)$. תהא X_0 קבוצת נק' השבת ביחס לפעולה זו. כלומר

$$X_0 := \{x \in X : \forall g \in G \varphi(g)(x) = x\}$$

$$(x \in X_0 \Leftrightarrow \text{St}_x = G, \text{ במילים אחרות, } \\ X_0 \equiv |X| \pmod{p} \text{ אזי מתקיים})$$

דוגמה

G חבורת p . פעולת על $X = G$ ע"י הצמדה.

$$X_0 = \{x \in G : \forall g \in G \varphi(g)(x) = x\} = \{x \in G : \forall g \in G gxg^{-1} = x\} = \{x \in G : \forall g \in G gx = xg\} = Z(G)$$

קיבלנו מהלמה $|Z(G)| - |G| \pmod{p} = 0$ כלומר משפט 1, מקרה פרטי של הלמה.

הוכחת הלמה

הראינו בשיעור שעבר, אם G פועלת על X , אז X איחוד זר של כל המסלולים. נחלק את המסלולים לשני סוגים: מסלולים מסדר 1 ומסדר גדול מ-1.

יהיו x_1, \dots, x_k נציגי כל המסלולים מסדר 1, x_{k+1}, \dots, x_l נציגי כל המסלולים מסדר

$$1 < \sigma(x_i) \text{ וקיבלנו } X = \prod_{i=1}^l \sigma(x_i) \Leftarrow |X| = \sum_{i=1}^k |\sigma(x_i)| + \sum_{i=1}^l |\sigma(x_i)|. \text{ נשים לב } |\sigma(x_i)| = 1 \\ \text{אמ"ם } \forall g \in G \sigma(x_i) = \{x_i\}$$

$$\text{מסקנה: } |X| = |X_0| + \sum_{i=k+1}^l |\sigma(x_i)| \text{ ולכן } \sum_{i=1}^k |\sigma(x_i)| = |X_0|$$

אבל לכל $k < i \leq l$ הנחנו. כמו כן, לפי משפט $|G|$ $|\sigma(x_i)|$. חבורת p , ולכן לכל i $|\sigma(x_i)| = p^k$ לאיזשהו k שלם אי שלילי, ואם $1 < |\sigma(x_i)|$ אז $p \mid |\sigma(x_i)|$ ולכן

$$|X| = |X_0| \pmod p \Leftarrow p \mid \sum_{i=k+1}^l |\sigma(x_i)|$$

משפט קושי

תהא G חבורה סופית, p ראשוני, $|G| \not\equiv p \pmod p$ יש ב- G איבר מסדר p .

הוכחה

נתבונן בקבוצה $X = \{(g_1, g_2, \dots, g_p) : \forall_i g_i \in G, g_1 \cdots g_p = e\}$

טענת עזר: נשים לב, אם $g_1 g_2 \cdots g_p = e$ אז $g_2 g_3 \cdots g_p g_1 = e$

הוכחת טענת עזר: $g_2 \cdots g_p g_1 = g_1^{-1} (g_1 \cdots g_p) g_1 = g_1^{-1} e g_1 = g_1^{-1} g = e$

מכאן נובע ע"י הפעלה חוזרת של טענת העזר שלכל $1 \leq r < p$, $g_{r+1} g_{r+2} \cdots g_p g_1 g_2 \cdots g_r = e$

$$(g_{r+1}, g_{r+2}, \dots, g_p, g_1, \dots, g_r) \in X$$

נגדיר פעולה של \mathbb{Z}_p על X ע"י $\forall r \in \mathbb{Z}_p \varphi(r)(x_1, \dots, x_p) = (x_{r+1}, \dots, x_p, x_1, \dots, x_r)$ לפי הלמה $|X_0| = |X| \pmod p$ אבל $|X| = \{(g_1, \dots, g_p) : \forall_i g_i \in G, g_1 \cdots g_p = e\}$ לכל בחירה חופשית של g_1, \dots, g_{p-1} חייבים לבחור $g_p = (g_1 \cdots g_{p-1})^{-1}$ כדי לקבל סדרה ב- X

$$(1) \quad \text{ולכן } |X| = |G|^{p-1} \text{ הנחת המשפט } p \mid |G|$$

$$(2) \quad \text{ולכן } p \mid |X|$$

$$(1)+(2) \quad p \mid |X_0| \Leftrightarrow |X_0| = 0 \pmod p$$

אבל $(e, e, \dots, e) \in X_0$ ולכן $p \leq |X_0|$ כלומר יש איבר ב- X_0 שאינו (e, e, \dots, e) . איבר כזה מקיים לכל $1 \leq r < p$, $\forall_r x_{r+1} = x_1$ ולכן האיבר מהצורה (x, x, \dots, x) וכמו כן $x^p = e$ כי $(x, x, \dots, x) \in X \Leftarrow$ יש איבר $x \in G$ כך $x^p = e$ (הוא איבר מסדר p).