תזכורת

תהי G חבורה, $H \leq G$ תת חבורה.

לכל $g \in G$ יש $\gamma_g: G \to G$; $x \mapsto gxg^{-1}$.

$g \mapsto \gamma_g$ מגדירה $G \to \mathrm{Aut}(G)$.

זה משרה שיכון:

$$G/_{Z(G)} \hookrightarrow \mathrm{Aut}(G)$$

המנרמל של H ב $-$ G:

$$N_G(H) = \{g \in G | gHg^{-1} = H\}$$

זו תת החבורה המקסימלית של G ש $-$ H נורמלית בה.

אם $g \in N_G(H)$, $\gamma_G|_H \in \mathrm{Aut}(H)$.

המרכז של H ב $-$ G:

$$C_G(H) = \{g \in G | \forall x \in H: gx = xg\}$$

נובע משפט $N/_C$:

$$N_G(H)/_{C_G(H)} \hookrightarrow \mathrm{Aut}(H)$$

$$C_G(\langle h \rangle) = C_G(h)$$

חבורות p

שוויון המחלקות

$$|G| = |Z(G)| + \sum_{\substack{x \notin Z(G) \\ \text{אחד מכל} \\ \text{מחלקה}}} [G : C_G(x)]$$

$$(x \in Z(G) \Leftrightarrow [x]_{\substack{\text{מחלקת} \\ \text{צמידות}}} = \{x\})$$

דוגמא

שוויון המחלקות של S_3:

$$6 = 1 + (2_{(..)} + 3_{(...)})$$

שוויון המחלקות של D_4:

$$8 = 2 + (2 + 2 + 2)$$

משפט קושי

נניח שראשוני p מחלק את הסדר של G, אז קיים $x \in G$ מסדר p.

הוכחה ראשונה

$$p \mid |G| = n$$

<u>מקרה ראשון: $G = \langle x \rangle$ ציקלית.</u>

$$o\left(x^{\frac{n}{p}}\right) = p$$

<u>מקרה שני: G אבלית.</u>

נבחר $1 \neq y \in G$. אם $p \mid o(y)$, יש איבר מסדר p ב- $\langle y \rangle$.

אחרת, $p \mid \left|{}^{G}/_{\langle y \rangle}\right|$.

לפי הנחת האינדוקציה יש איבר $x\langle y \rangle$ מסדר p בחבורת המנה ${}^{G}/_{\langle y \rangle}$ ($x\langle y \rangle \in {}^{G}/_{\langle y \rangle}$ כאשר $\langle y \rangle$ קוסט),

כלומר $x^p \in \langle y \rangle$.

אבל $p = o(x\langle y \rangle) \mid o(x)$ ושוב סיימנו לפי המקרה הראשון.

<u>מקרה שלישי: G לא אבלית.</u>

אם $p \mid |Z(G)|$, סיימנו לפי המקרה השני.

אחרת בהכרח יש $x \notin Z(G)$ כך ש - $p \nmid [G: C_G(x)]$.

לכן $p \mid |C_G(x)|$.

לפי הנחת האינדוקציה, ב - $C_G(x)$ יש איבר מסדר p.

הוכחה שנייה

נתבונן במרחב:

$$\Omega \coloneqq \{(g_1, \cdots, g_p) \in G \times \cdots \times G \mid g_1 \cdots g_p = 1\}$$

החבורה $\mathbb{Z}_p = \langle \tau | \tau^p = 1 \rangle$ פועלת על Ω באופן הבא:

$$T(g_1, \cdots, g_p) = (g_2, \cdots, g_p, g_1)$$

נשים לב ש - $g_2 \cdots g_p g_1 = g_1^{-1}(g_1 \cdots g_p)g_1$ לכן המכפלה נשארת 1.

ברור ש – $\tau^p = 1$.

הגודל של מסלול = אינדקס המייצב ובפרט מחלק את סדר החבורה הפועלת.

נשים לב שבהכרח נקודת שבת של T היא בהכרח מהצורה $(g_1, \cdots, g_p) = (x, \cdots, x)$ כאשר מתקיים $x^p = 1$ (חייב להתקיים $g_1 = g_2$, $g_2 = g_3$, $\cdots$, $g_p = g_1$).

אבל,

$$|\Omega| = |G|^{p-1} \equiv 0 \ (mod\ p)$$

לכן מספר הפתרונות למשוואה $x^p = 1$ ב – G מתחלק ב – p.

לכן, מכיוון ש - $x = 1$ פתרון, כלומר חייבים להיות גם אחרים (אחרת זה לא יחלק את p).

הגדרה

חבורה G נקראת "**חבורת-p**" אם הסדר של כל איבר הוא חזקה של p.

טענה

תהי G חבורה סופית.

$$G \text{ חבורת } p - \iff |G| = p \text{ חזקת}$$

הוכחה

ברור: G חבורת $p-$ $\Rightarrow$ $|G|=$ חזקת p

משפט קושי: G חבורת $p-$ $\Leftarrow$ $|G|=$ חזקת p

משפט

תהי G חבורת $p-$ סופית, אזי $Z(G)\neq\{1\}$

הוכחה

$$|G|\overset{p^n}{\coloneqq}|Z(G)|+\sum_{\substack{x\notin Z(G)\\ \text{אחד מכל}\\ \text{מחלקה}}}[G:C_G(x)]$$

האינדקסים $[G:C_G(x)]$ מחלקים את p^n לכן שווים ל- p^i עבור $i>0$.

(מסתכלים $mod\ p$)

□

הערה

כל חבורה מסדר p – ציקלית.

תרגיל

אם ${}^{G}/_{Z(G)}$ ציקלית, אז G אבלית.

מסקנה

כל חבורה מסדר p^2 – אבלית (כי המרכז לא יכול להיות מסדר p אז החבורות הן $\mathbb{Z}_{p^2},\mathbb{Z}_p^2$.

טענה

בחבורת $p-$ G, לכל $H\lneqq G$:

$$H\lneqq N_G(H)\leq G$$

הוכחה

$$H \lneqq G$$

אם $Z(G) \nsubseteq H$, אז $H \subset H \cdot Z(G) \subseteq N_G(H)$.

אחרת, $Z = Z(G) \subseteq H$, אז $H/Z(G) \lneqq G/Z(G)$.

לפי הנחת האינדוקציה:

$$H/Z \lneqq N_{G/Z}(H/Z) \overset{*}{=} N_G(H)/Z$$

המעבר $*$:

יהי $g \in G$ איבר כך ש-:

$$\forall h \in H: ghg^{-1}Z = (gZ)(hZ)(gZ)^{-1} \in H/Z$$

(כי $gHg^{-1} \in H$ אז $g \in N_G(H)$)

□

דוגמא

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\}$$

"מטריצות יוניפוטונטיות" מעל $\mathbb{Z}_p$.

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$$

$|G| = p^3$ ולכן היא חבורת $p-$.

$$|Z(G)| = p$$

תרגיל

$$Z(G) = \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad G/Z(G) \leq \mathbb{Z}_p^2$$

הערה

לכל $p > 2$, יש בדיוק 5 חבורות מסדר p^3:

$\mathbb{Z}_{p^3}$,	$\mathbb{Z}_p \times \mathbb{Z}_p^2$,	$\mathbb{Z}_p^3$,	H_p,	חבורה לא אבלית נוספת

הגדרה

G חבורה כלשהי, $|G|$ | p ראשוני. נכתוב $|\boldsymbol{G}|$ || $\boldsymbol{p^t}$ כאשר $|G|$ | p^t, $|G|$ ł p^{t+1}.

תת חבורה מסדר p^t של G נקראת **תת חבורת $\boldsymbol{p}$ – סילו ($\boldsymbol{Sylow}$)**.