משפט קיילי:

הערה: אם חבורה G פועלת על קבוצה X, אז יש הומו' טבעי $\varphi: G \to \underbrace{S_X}$
כל התמורות על איברי X

אם הפעולה נאמנה, אז φ הוא שיכון $G \hookrightarrow S_X$

כל חבורה G פועלת בצורה נאמנה על G. על ידי כפל משמאל

$g * x = gx$

לכן $G \to S_{|G|}$

דוגמא:

$G = D_3 \Rightarrow G = \{\underset{1}{id}, \underset{2}{\tau}, \underset{3}{\sigma}, \underset{4}{\tau\sigma}, \underset{5}{\sigma^2}, \underset{6}{\tau\sigma^2}\}$ לכן G משוכנת ב- S_6

נחשב את $\varphi(\tau)$

$\tau id = \tau$ $\quad 1 \to 2$

$\tau \cdot \tau = id$ $\quad 2 \to 1$

$3 \to 4 \quad 5 \to 6$

$4 \to 3 \quad 6 \to 5$

$\varphi(\tau) = (1\,2)(3\,4)(5\,6)$

$\sigma id = \sigma \quad 1 \to 3 \to 5 \quad , 2 \to 6 \to 4$

$\varphi(\sigma) = (1,3,5)(2,6,4)$

העידון של משפט קיילי:

אם ל- G יש תת חבורה מאינדקס n, אז G פועלת על הקוסטים

G/H לכן יש הומו' $\varphi_H: G \to S_n$. אם במקרה G פשוטה אז כל הומו'

לא טריוויאלי הוא שיכון

תרגיל:

יהי $n\geq 5$ ו- $H\leq A_n$. הוכיחו כי $n\leq[A_n:H]$

כתכון:

A_n פשוטה. נסמן $[A_n:H]=m$ $\Leftarrow$ $A_n\hookrightarrow S_m$ $\Leftarrow$ $\frac{n!}{2}\mid m!$

לא ייתכן ש $m<n$

דוגמא:

$|A_6|=360$. אין ל- A_6 תתי חבורות מגודל $72, 90, 120, 180$

תרגיל:

תהי G חבורה, ו- $H\leq G$ מאינדקס m. הוכיחו שיש ל- G תת חבורה נורמלית, N, כך ש: $N\leq H$, ו- $[G:N]\mid m!$

הוכחה:

מהעיקרון של משפט קיילי, קיים $\varphi_H: G\to S_m$

$N=\ker\varphi_H \trianglelefteq G$

$G/N\cong Im\,\varphi_H < S_m$

לכן $|G/N|\mid m!$

φ_H הגיע מהפעולה של G על המחלקות gH. איבר בגרעין הוא איבר שפועל טריוויאלית. כלומר $x\in\ker\varphi_H \Leftarrow xgH=gH \Leftarrow x\in H$

$\Downarrow$

$N=\ker\varphi_H\leq H$

מסקנה:

אם $|G|>m!$ ויש ל- G תת חבורה מאינדקס m. אז G לא חבורה פשוטה.

תרגיל:

נניח $|G|=2m$ (m - אי זוגי). הוכיחו שיש ל-G תת חבורה מאינדקס 2.

פתרון:

$G \hookrightarrow S_{2m}$. $G \cong$ תת חבורה של S_{2m}. נחליף את G בתמונה של G.

מעכשיו $G \le S_{2m}$. נגדיר כי $H = G \cap A_{2m}$. $H \le G$

$G \underset{\text{שיכון קיילי}}{\hookrightarrow} S_{2m} \hookrightarrow S_{2m}/A_{2m}$ הגרעין הוא $G \cap A_{2m}$ $G/H \hookrightarrow S_{2m}/A_{2m}$

לכן $[G:H]=1 \vee 2$. $[G:H]=1 \iff G=H$ כלומר $G = G \cap A_{2m}$

$$\Downarrow$$

$G \subseteq A_{2m}$

נותר להוכיח שיש ב G לפחות תמורה אחת אי זוגית.

נזכר כי G היא התמונה של חבורה מסדר $2m$ תחת שיכון קיילי.

קיים ב-G איבר מסדר 2. כלומר, מכפלה של חילופים זרים

תחת שיכון קיילי כל איבר הולך לתמורה שמציבה את כל המספרים. ולכן האיבר

מסדר 2 הוא מכפלה של m חילופים ומכיוון ש m אי זוגי, נקבל

תמורה אי זוגית.

משפטי סילו:

$G = p^n \cdot m$ כאשר m זר ל-p

$P \le G$ מגודל p^n נקראת p-סילו

דוגמאות:

1) $|S_3| = 2 \cdot 3$. חבורות 2-סילו: $<(1,3)>$, $<(1,2)>$, $<(2,3)>$

חבורות 3-סילו: A_3

משפטים:

1) כל תת חבורה מסדר p^k מוכלת בחבורת p-סילו

2) כל חבורות p-סילו צמודות

3) נסמן ב- r_p את מס' חבורות p-סילו $r_p = 1 \mod p$, $r_p \mid m$

מסקנה ממשפט 2:

חבורת p-סילו נורמלית $\Longleftrightarrow$ היא חבורת p-סילו היחידה

תרגיל:

הוכיחו כי כל חבורה מסדר 45 אינה פשוטה.

פתרון:

$45 = 5\cdot 9 = 5\cdot 3^2$. $\quad r_5 = 1 \mod 5 \quad r_5 \mid 9 \Rightarrow r_5 = 1$

חבורת 5-סילו היא תת חבורה נורמלית

תרגיל:

תהי $|G| = 21$ לא אבלית. כמה תתי חבורות סילו יש לה מכל סדר?

פתרון

$21 = 3\cdot 7$. $\quad r_7 = 1 \mod 7 \ , \ r_7 \mid 3 \Rightarrow r_7 = 1$

$r_3 = 1 \mod 3 \ , \ r_3 \mid 7 \Rightarrow r_3 = 7, 1$

נספור סדרים של איברים:

סדר	מס' איברים	
1	1	- איבר יחידה
3	14	
7	6	
21	0	כי אחרת ציקלית ולכן אבלית

יש 7 חבורות 3 סילו

הערה: נשים לב ש- G פועלת על אוסף תתי החבורות שלה ע"י הצמדה

$H \le G$ $\quad$ $g^{-1}Hg \le G$

המסלול של תת חבורה הוא כל תתי החבורות שצמודות אליה

כלומר לכל p, הגודל של המסלול של חבורת p-סילו הוא r_p. לפי משפט

מסלול מייצב:

$[G : \text{המייצב של תת חבורת p-סילו}] = |\text{מסלול של תת חבורות p-סילו}| = r_p$

לכן ב-G יש תת חבורה מאינדקס r_p

תרגיל:

הוכיח שכל חבורה מסדר 224 אינה פשוטה

פתרון:

$224 = 7\cdot 2^5$. נניח בשלילה ש-G פשוטה. לכן כל תתי חבורות p-סילו אינן יחידות.

$r_7 = 1 \bmod 7 \qquad r_7 | 32 \Leftarrow r_7 = 8$

$r_2 = 1 \bmod 2 \qquad r_2 | 7 \Leftarrow r_2 = 7$

לכן ל-G יש תת חבורות מאינדקס 8 ומאינדקס 7

G פשוטה ולכן $G \hookrightarrow S_8$, $G \hookrightarrow S_7$

$224 | 7!$

$\underset{2^4 \cdot m}{\overset{\|}{2\cdot3\cdot4\cdot5\cdot6\cdot7}} \quad \overset{\|}{7\cdot2^5}$ בסתירה

תרגיל:

תהי $|G| = p^2 q$. הוכיחו ש G אינה פשוטה

פתרון:

אם $q<p$, אז $r_p = 1 \bmod p \qquad r_p | q \Leftarrow r_p = 1$. G אינה פשוטה

נניח ש $1<p<q$. נניח בשלילה ש G פשוטה. $r_p = q$

$r_q | p^2 \Rightarrow r_q = p \vee p^2$

חבורות q-סילו הן חבורות מסדר q. לכן החיתוך של כל 2 טריוויאלי

כי אם $e \neq x \in Q_1 \cap Q_2$. אז x יוצר את Q_1 ואת Q_2 ואז $(Q_1 = Q_2$

מספר האיברים מסדר q הוא $r_q(q-1)$, $r_p = q$ ולכן $q = 1 \bmod p$

$\Downarrow$

$p < q \Rightarrow r_q \equiv 1 \bmod p \qquad r_q \neq p \Rightarrow r_q = p^2$

מספר האיברים מסדר q הוא:

$p^2(q-1) = p^2q - p^2$

כל האיברים בחבורות p-סילו אינם מסדר q. נשארו רק p^2 איברים

לא מסדר q. זה מספיק רק לחבורת p-סילו אחת בדיוק.

חבורות אוטומורפיזמים:

לכל חבורה G ניתן להגדיר $Aut(G) = \left\{ \substack{f: G \to G \\ \text{איזומורפיזם}} \right\}$

ביחד עם פעולת ההרכבה ונקבל חבורה.

דוגמאות:

1) $Aut(\mathbb{Z}_n) \cong U_n$ בשביל להגדיר איזו' מ-$\mathbb{Z}_k$, מספיק להגדיר לאן 1 הולך.

בשביל לקבל איזו', ולא סתם הומ' צריך לשלוח את 1 ליוצר

$Aut(\mathbb{Z}_n) \to U_n$

$f \to f(1)$

$f \circ g \to f \circ g(1)$

$\left(\begin{array}{l} f(1) = m_1 \\ g(1) = m_2 \end{array} \right.$

$f \circ g(1) = f(m_2) = f(1 + \ldots + 1) = f(1) + \ldots + f(1) = m_2 f(1) = m_2 m_1$

2) $G = \mathbb{F}^n \qquad Aut(\mathbb{F}^n) = GL_n(\mathbb{F})$

3) $G = \mathbb{Z}_2 \times \mathbb{Z}_2$

טענה: $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$

$(0,0) \to (0,0)$

$v_1(0,1)$

$v_2(1,0)$

$v_3(1,1)$

הסכום של כל 2 איברים שווה לאיבר השלישי. אז כל תמורה על 3 הוקטורים היא למעשה איזומורפיזם

הגדרה: $Inn(G)=\{\gamma_g \mid g\in G\} \le Aut(G)$ חבורת האוטו' הפנימיים

$\gamma_g(x)=g^{-1}xg$

$G \to Inn(G)$
$g \to \gamma_g$

$\ker = Z(G)$

$G/Z(G) \cong Inn(G)$

תזכורת:

אם $G/Z(G)$ ציקלית אז G אבלית

תרגיל:

חשבו את $|Inn(G)|$ $G=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \mid a,b,c\in \mathbb{Z}_3\right\}$

$Inn(G)\cong G/Z(G)$

$Z(G) = 1 \lor 3 \lor 9 \lor 27$

חבורת-p המרכז לא טריוויאלי

לא אבלית

אם $Z(G)=9$ אז $|G/Z(G)|=3$ ציקלית $\Leftarrow$ אבלית בסתירה

$\Leftarrow |Inn(G)|=9$

מיון חבורות אבליות סופיות:

משפט:

כל חבורה אבלית סופית מתפרקת למכפלה של חבורות מסדר חזקת p

חבורות אבליות מסדר p^n הם מהצורה $\mathbb{Z}_{p^{n_1}}\times\dots\times\mathbb{Z}_{p^{n_m}}$

$n_1+\dots+n_m=n$

דוגמא:

כמה חבורות אבליות יש מסדר 27?

$\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

$\mathbb{Z}_3 \times \mathbb{Z}_9$

$\mathbb{Z}_{27}$

כמה חבורות אבליות יש מסדר p^n?

$P(n) \quad n = \sum n_i$

$27 = 3^3$

$3 = 3$

$3 = 1 + 2$

$3 = 1+1+1$

תרגיל:

כמה חבורות אבליות יש מסדר 200?

פתרון:

$200 = 2^3 \cdot 5^2$

$P(3) \cdot P(2) = 6$

$2^4 \cdot 3^5 \Rightarrow 5 \cdot 7$

$$P(4) = \left.\begin{array}{l} 4 \\ 1+3 \\ 2+2 \\ 2+1+1 \\ 1+1+1+1 \end{array}\right\} 5$$

$$P(5) = \left.\begin{array}{l} 5 \\ 1+4 \\ 2+3 \\ 1+1+3 \\ 2+2+1 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{array}\right\} 7$$

תרגיל:

הוכיחו ש $\mathbb{Z}_{200}\times\mathbb{Z}_{20} = \mathbb{Z}_{100}\times\mathbb{Z}_{40}$

פתרון:

$$\mathbb{Z}_{200}\cong\underbrace{\mathbb{Z}_8\times\mathbb{Z}_{25}}$$

הפרק היחידה
לייצור חבורה ציקלית
מסדר 200

$\mathbb{Z}_2\times\mathbb{Z}_4\times\mathbb{Z}_{25}$ - כל איבר מתאפס בחזקת 4x25

$$\mathbb{Z}_{20}\cong\mathbb{Z}_4\times\mathbb{Z}_5$$

$$\mathbb{Z}_{100}\cong\mathbb{Z}_{25}\times\mathbb{Z}_4$$

$$\mathbb{Z}_4\cong\mathbb{Z}_8\times\mathbb{Z}_5$$