תורת החבורות 88-218-01 תשפ"א
הערות הרצאה 11

0.1 שימושים למשפטי סילו: חבורות פשוטות

תזכורת 0.1 (משפטי סילו)**.** תהי G חבורה מסדר $n = p^t m$ כאשר m זר לראשוני p.

1. יש ל-G תת־חבורת p-סילו. כל תת־חבורה $H \leq G$ שהיא חבורת-p מוכלת בתת־חבורת p-סילו.
2. כל שתי תת־חבורות p-סילו $P_1, P_2 \in \mathrm{Syl}_p(G)$ הן צמודות. כלומר קיים $g \in G$ כך ש-$P_1 = gP_2g^{-1}$.
3. נסמן $n_p := \left|\mathrm{Syl}_p(G)\right|$. אז $n_p \equiv 1 \pmod p$ וגם $n_p | m$.

הערה 0.2. הניסוח של המשפטים לא נפל לסילו מהשמיים.
חבורה G פועלת על עצמה על ידי כפל משמאל.
חבורה G פועלת על עצמה על ידי הצמדה.
אפשר להכליל: חבורה G פועלת על G/H על ידי כפל משמאל.
חבורה G פועלת על אוסף תת־החבורות שלה על ידי הצמדה.
אפשר לצמצם: תת־חבורה K פועלת על G/H על ידי כפל משמאל.
תת־חבורה $P \in \mathrm{Syl}_p(G)$ פועלת על $\mathrm{Syl}_p(G)$ על ידי הצמדה.
אפשר להוכיח יותר: פרובניוס הראה שאם $p^i \big| |G|$, אז מספר תת־החבורות מסדר p^i שקול ל-1 מודולו p.

טענה 0.3 (קשה). תהי G חבורה סופית, ותהי $N \lhd G$ תת־חבורה נורמלית שלה. אז $n_p(N) | n_p(G)$ וגם $n_p(G/N) | n_p(G)$.

הגדרה 0.4. חבורה G נקראת פשוטה אם לא קיימות לה תת־חבורות נורמליות לא טריוויאליות. כלומר כל תת־החבורות הנורמליות של חבורה פשוטה הן G ו-$\{e\}$.

טענה 0.5. תהי G חבורה אבלית. אז G פשוטה אם ורק אם G מסדר ראשוני.

הוכחה. אם G מסדר ראשוני, אז $G \cong \mathbb{Z}_p$ עבור p ראשוני כלשהו, ואין לה בכלל תת־חבורות לא טריוויאליות. אז היא בוודאי פשוטה.
בכיוון ההפוך, נניח כי G פשוטה.

אם G אינסופית, אז קיים $e \neq g \in G$. אם g מסדר סופי, אז $\langle g \rangle$ היא נורמלית לא טריוויאלית, כי G אבלית. אם g מסדר אינסופי, אז $\langle g^2 \rangle$ היא תת־חבורה נורמלית לא טריוויאלית, שהרי $g \notin \langle g^2 \rangle$. לכן לא קיימות חבורות פשוטות אבליות אינסופיות.

נניח כי G סופית. יהי p ראשוני המחלק את $|G|$. לפי משפט קושי, קיים איבר $g \in G$ מסדר p. אז $\langle g \rangle$ היא נורמלית, ובהכרח $G = \langle g \rangle$. אילו $\langle g \rangle$ לא הייתה טריוויאלית, אז G לא הייתה פשוטה. $\square$

כדי להבין קצת יותר חבורות סופיות, נכתוב רשימה של החבורות עד סדר 15:

1. החבורה הטריוויאלית.
2. $\mathbb{Z}_2$
3. $\mathbb{Z}_3$
4. $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$
5. $\mathbb{Z}_5$
6. $\mathbb{Z}_6$, $S_3 \cong D_3$
7. $\mathbb{Z}_7$
8. $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$,$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, D_4, Q_8
9. $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$
10. $\mathbb{Z}_{10}$, D_5
11. $\mathbb{Z}_{11}$
12. $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, D_6, A_4, Dic_3 (לפעמים מסמנים Dic_{12})
13. $\mathbb{Z}_{13}$
14. $\mathbb{Z}_{14}$, D_7
15. $\mathbb{Z}_{15}$

הערה 0.6. כמעט תמיד המיונים מהסגנון הזה משתמשים במשפטי סילו (לפעמים כמה וכמה פעמים). כדאי גם לבדוק את האתר.

נסמן ב-$\mathfrak{S}(n)$ את מספר החבורות מסדר n עד כדי איזומורפיזם. זו סדרה מספיק חשובה שהיא הראשונה באנציקלופדיה לסדרות של מספרים שלמים. אז

2^i	1	2	4	8	16	32	64	128	256	512
$\mathfrak{S}(2^i)$	1	1	2	5	14	51	267	2328	56092	10494213

אם p ראשוני, אז $\mathfrak{S}(p)=1$, $\mathfrak{S}(p^2)=2$ וכולן אבליות, $\mathfrak{S}(p^3)=5$ ו-$\mathfrak{S}(p^4)=15$ חוץ מהמקרה $\mathfrak{S}(2^4)=14$. מסדר $2^{10}=1024$ כבר יש $49{,}487{,}365{,}422$ חבורות עד כדי איזומורפיזם. עד סדר 2047 (כולל) יש $49{,}910{,}536{,}613$ חבורות עד כדי איזומורפיזם. כלומר יותר מ-99.15% מהחבורות עד סדר 2047 הן חבורות מסדר 1024. ידוע לפי היגמן וסימס:

$$\mathfrak{S}(p^k)\approx p^{2k^3/27+O(k^{8/3})}$$

ולפי נוימן ומק־איוור אם $n=p_1^{e_1}\dots p_r^{e_r}$, אז

$$\mathfrak{S}(n)\le n^{\mu^2+\mu+2}$$

כאשר $\mu=\max_i\{e_i\}$.

דוגמה 0.7. אם יש זמן, נדבר על Dic_n.

טענה 0.8. יהיו $p<q$ ראשוניים שונים, ותהי G חבורה מסדר $n=pq^k$ עבור $k\in\mathbb{N}$. אז G לא פשוטה.

דוגמה 0.9. אין חבורות פשוטות מסדר $14=2\cdot 7$ או מסדר $375=3\cdot 5^3$.

הוכחה. נעזר במשפטי סילו. לפי משפט סילו 3 ידוע כי

$$n_q\equiv 1 \pmod q$$

וגם $n_q|p$. כלומר $n_q\in\{1,p\}$. אבל $p<q$, ולכן $p\not\equiv 1 \pmod q$. אז $n_q=1$. אז כמסקנה ממשפט סילו 2 נסיק שיש ל-G תת־חבורת q-סילו יחידה שהיא נורמלית. היא לא טריוויאלית כי מסדר $1<q^k<pq^k$. לכן G לא פשוטה. $\square$

תרגיל 0.10 (לבית)**.** תהי G מסדר 12. הוכיחו כי $n_2=1$ או $n_3=1$, ובפרט G לא פשוטה. רמז: זה טיפה שונה מהטענה הקודמת, וכדאי לספור איברים לפי הסדר.

תזכורת 0.11. תהי G חבורה, ותהי $N\lhd G$ תת־חבורה נורמלית. אם $K\lhd N$, אז האם $K\lhd G$? לא בהכרח. למשל

$$\langle(12)(34)\rangle\lhd V\lhd A_4$$

טענה 0.12. תהי G חבורה סופית, ותהי $N\lhd G$ תת־חבורה נורמלית שלה. אם $P\lhd N$ היא תת־חבורת p-סילו של N, אז $P\lhd G$.

הוכחה. נוכיח כי P סגורה להצמדה מ-G. יהי $g\in G$. אז מפני ש-$P\subseteq N\lhd G$, אז $gPg^{-1}\subseteq N$. בנוסף gPg^{-1} היא תת־חבורת p-סילו של N, ולכן ממשפט סילו 2 היא צמודה ל-P. אבל $P\lhd N$, ולכן $gPg^{-1}=P$ לכל $g\in G$. כלומר $P\lhd G$. $\square$

טענה 0.13. תהי G חבורה מסדר 30. אז ל-G יש תת־חבורה נורמלית מסדר 5.

הוכחה. נשתמש בשיטה של ספירת איברים לפי סדר.

נשים לב כי $30 = 2 \cdot 3 \cdot 5$. כל תת־חבורת 5-סילו של G היא מסדר 5. לפי משפט סילו 3 נקבל $n_5|6$ וגם $n_5 \equiv 1 \pmod 5$. אז $n_5 \in \{1, 2, 3, 6\}$. נניח כי $n_5 \neq 1$, כי אחרת ניצחנו.

אז כרגע $n_5 = 6$. כלומר $|\mathrm{Syl}_5(G)| = 6$. בכל אחת מהן יש את איבר היחידה ועוד ארבעה איברים מסדר 5. בתרגיל בית ישן (4 בטוח) הראתם שחיתוך תת־חבורות שונות מסדר ראשוני הוא טריוויאלי (אם הסדר לא ראשוני, אז לא בהכרח). לכן יש בדיוק $4 \cdot 6 = 24$ איברים מסדר 5 ב-G.

עכשיו נבחן כמה תת־חבורות 3-סילו יש ל-G. עם חישוב דומה $n_3|10$ וגם $n_3 \equiv 1 \pmod 3$. אם $n_3 = 10$, נקבל שיש לפחות $1 + 24 + 20 > 30$ איברים ב-G (כי יש $10 \cdot 2 = 20$ איברים מסדר 3), וזו סתירה.

לכן $n_3 = 1$. כלומר יש תת־חבורת 3-סילו נורמלית ב-G, נניח $P_3 \lhd G$.

תהי $P_5 \in \mathrm{Syl}_5(G)$. ברור כי $P_3P_5 \leq G$ כי $P_3 \lhd G$. לפי משפט האיזומורפיזמים השני

$$P_3P_5/P_3 \cong P_5/(P_3 \cap P_5) \cong P_5$$

אבל $P_3 \cap P_5 = \{e\}$ כי הן מסדרים זרים. לכן הסדר של P_3P_5 הוא

$$|P_3P_5/P_3| = |P_5| = 5$$

ולכן $|P_3P_5| = 3 \cdot 5 = 15$. נסמן $H = P_3P_5$, ואז

$$[G : H] = \frac{30}{15} = 2$$

כלומר $G \lhd H$. בפרט H סגורה להצמדה, וגם $P_5 \leq H$. לכן $gP_5g^{-1} \leq H$ לכל $g \in G$. כלומר כל האיברים מסדר 5 של G מוכלים ב-H. זו סתירה כי יש 24 איברים כאלו בתת־חבורה מסדר 15.

לכן $n_5 = 1$, וסיימנו בעזרת משפטי סילו. □

טענה 0.14 (משפט וילסון). יהי $n > 1$ טבעי. אז n ראשוני אם ורק אם

$$(n-1)! \equiv -1 \pmod n$$

הוכחה. אם $n \leq 4$, תבדקו לבד. מעכשיו נניח $n > 4$.

נניח כי n פריק. אם $n = ab$ כאשר $1 < a < b < n-1$, אז המכפלה $(n-1)! = \prod_{i=1}^{n-1} i$ כוללת את a ואת b כגורמים, ולכן $(n-1)! \equiv 0 \pmod n$. אם אין ל-n פירוק כזה, אז $n = a^2$ עבור $1 < a < n-1$. אז המכפלה $(n-1)! = \prod_{i=1}^{n-1} i$ כוללת את a ואת $2a$ כמספרים שונים, והרי $1 < a < 2a < n-1$ עבור $n > 4$. אז $(n-1)! \equiv 0 \pmod n$.

כעת נניח כי $n = p$ ראשוני. בחבורה S_p האיברים היחידים מסדר p הם מחזורים מאורך p. יש $(p-1)!$ מחזורים מאורך p ב-S_p. תת־חבורת p-סילו של S_p היא מסדר

p, ולכן יש $(p-2)!$ תת־חבורות p-סילו, שהרי בכל אחת מהן יש $p-1$ איברים מסדר p ועוד את איבר היחידה (אותו טריק עם חיתוך תת־חבורות מסדר p).

$$\frac{(p-1)!}{p-1} = (p-2)!$$

לפי משפט סילו 3 אנחנו יודעים כי $n_p = (p-2)! \equiv 1 \pmod p$. נכפול ב-$(p-1)$ ונקבל

$$(p-1)! \equiv -1 \pmod p$$

כמו שרצינו. $\square$

טענה 0.15. תהי G חבורה מסדר 60. אם אין לה תת־חבורת 5-סילו נורמלית, אז G פשוטה.

הוכחה. תמיד טוב לדעת כי $60 = 2^2 \cdot 3 \cdot 5$. לפי משפט סילו 3 מתקיים $n_5 \equiv 1 \pmod 5$ וגם $n_5 | 12$. אז $n_5 \in \{1, 2, 3, 4, 6, 12\}$, ולפי הנתון $n_5 \neq 1$. כלומר $n_5 = 6$.

נניח בשלילה שקיימת ל-G תת־חבורה נורמלית $N \lhd G$ שאינה טריוויאלית.

אם 5 מחלק את $|N|$, אז יש ל-N תת־חבורת 5-סילו מסדר 5. נניח $P \in \mathrm{Syl}_5(N)$. אז $P \in \mathrm{Syl}_5(G)$, כי תת־חבורות 5-סילו של G גם הן מסדר 5. לפי משפט סילו 2 תת־חבורות 5-סילו הן צמודות, ולכן $gPg^{-1} \subseteq N$ לכל $g \in G$ כי N נורמלית. כלומר N מכילה את כל תת־חבורות 5-סילו של G.

החיתוך של שתי תת־חבורות 5-סילו שונות של G הוא טריוויאלי (כי הן מסדר ראשוני). באופן דומה לחישוב בתרגיל קודם, יש 24 איברים מסדר 5 ב-G (יש 6 תת־חבורות מסדר 5, בכל אחת יש את איבר היחידה ועוד 4 איברים מסדר 5). לכן יש גם 24 איברים מסדר 5 ב-N. לכן $|N| = 30$ כי הסדר של N מחלק את $|G| = 60$ ואינו 60. לפי טענה מלפני ההפסקה, לכל חבורה מסדר 30, כמו N, יש תת־חבורת 5-סילו יחידה ולא 6 כמו שקיבלנו. סתירה.

אחרת, אם 5 לא מחלק את $|N|$. הוא קצת יותר ארוך. בהכרח $|N|$ מחלק את 12. נפצל למקרים:

- המקרה $|N| = 1$ פוסלים כי N לא טריוויאלית.
- אם $|N| = 2$, אז חבורת המנה G/N מסדר 30, ולכן לפי התרגיל מכילה תת־חבורת 5-סילו נורמלית.
- אם $|N| = 3$, אז חבורת המנה G/N מסדר 20. נסמן ב-n_5' את מספר תת־חבורות 5-סילו של G/N. אז לפי משפט סילו 3 ידוע כי $n_5' | 4$ וגם $n_5' \equiv 1 \pmod 5$. אז בהכרח $n_5' = 1$, ולכן מכילה תת־חבורת 5-סילו נורמלית.
- אם $|N| = 4$, אז חבורת המנה G/N מסדר 15, גם כאן מראים מכילה תת־חבורת 5-סילו נורמלית.
- אם $|N| = 6$, אז חבורת המנה G/N מסדר 10, גם כאן מראים מכילה תת־חבורת 5-סילו נורמלית.

- אם $|N| = 12$, אז יש ל-N תת־חבורת 2-סילו או תת־חבורת 3-סילו נורמלית לפי התרגיל לבית, נניח $P \lhd N$. לכן לפי טענה קודמת $P \lhd G$, והיא מסדר 4 או 3, ואנחנו באחד מן המקרים הקודמים כי 5 לא מחלק את $|P|$.

בכל מקרה שבו יש לחבורת המנה G/N תת־חבורה נורמלית מסדר 5, אז לפי משפט ההתאמה ל-G יש תת־חבורה נורמלית $H \lhd G$ (המכילה את N) וגם 5 מחלק את הסדר של H. אז הגענו למקרה הראשון שבו יש תת־חבורה מסדר המתחלק ב-5, וסיימנו. □

מסקנה 0.16. החבורה A_5 היא פשוטה.

הוכחה. קל לחשב כי $|A_5| = \frac{5!}{2} = 60$. אפשר למצוא במפורש 6 תת־חבורות 5-סילו ב-A_5. אנחנו נסתפק בלמצוא לפחות שתי תת־חבורות כאלו. למשל אחת מהן היא

$$P = \langle (12345) \rangle = \{\mathrm{id}, (12345), (13524), (14253), (15432)\}$$

והיא אכן מסדר 5. בנוסף

$$(345)(12345)(345)^{-1} = (12453) \notin P$$

ולכן P לא נורמלית ב-A_5. כלומר יש עוד תת־חבורות 5-סילו. □

עובדה 0.17. לכל $n \geq 5$ החבורה A_n פשוטה.

הוכחה. החלטנו לוותר על ההוכחה של העובדה הזו.
יש הוכחות באינדוקציה על n.
יש הוכחות שמוכיחות בבת־אחת לכל n (לפעמים נעזרים בזה ש-A_5 פשוטה).
יש הוכחות שבודקות קבוצות יוצרים ב-A_n (היא נוצרת על ידי מחזורים מאורך 3, שהרי

$$(13)(24) = (123)(124)$$

אז מראים שכל תת־חבורה נורמלית לא טריוויאלית של A_n מכילה מחזור מאורך 3) □

טענה 0.18. יהי $n \geq 5$. אז תת־החבורות הנורמליות היחידות של S_n הן $S_n, A_n, \{\mathrm{id}\}$.

הוכחה. תת־החבורות ברשימה הן נורמליות, כמו שראינו פעם.
תהי $N \lhd S_n$ שאינה S_n. אז $N \cap A_n \lhd A_n$. מפני ש-A_n פשוטה לפי העובדה (שלא הוכחנו!), אז יש רק שתי אפשרויות:
אם $N \cap A_n = A_n$, אז $A_n \subseteq N$. לכן $2 \leq [S_n : N]$, ומפני ש-$N \neq S_n$, אז $[S_n : N] = 2$. אז משיקולי סדר $N = A_n$.
אחרת, בהכרח $N \cap A_n = \{\mathrm{id}\}$. אז נקבל

$$N \cong N/(N \cap A_n) \cong (NA_n)/A_n \leq S_n/A_n \cong \mathbb{Z}_2$$

כאשר האיזומורפיזם השני הוא לפי משפט האיזומורפיזמים השני. כלומר N איזומורפית לתת־חבורה של $\mathbb{Z}_2$. אם $N \cong \{\mathrm{id}\}$, סיימנו. אחרת, הסדר של N הוא 2. כלומר $N = \{\mathrm{id}, \sigma\}$ כאשר $\sigma \neq \mathrm{id}$ איבר מסדר 2 (לכן הוא מכפלה של חילופים זרים). מפני ש-N נשמרת תחת הצמדה מ-S_n, אז היא צריכה להכיל את מחלקת הצמידות $\mathrm{conj}(\sigma)$. אבל כל מחלקת צמידות ב-S_n שאינה של איבר היחידה כוללת יותר מאיבר אחד. זו סתירה לכך ש-$|N| = 2$. □

0.2 עוד חבורות לינאריות

דוגמה 0.19. הנה עוד דוגמאות לחבורות לינאריות ולמשפט האיזומורפיזמים הראשון:

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & \mu_n(F)\cdot I_n \arrow[r, hook] \arrow[d, hook] & \{c\cdot I_n\}\cong F^* \arrow[r, two heads, "\det\cong\cdot^n"] \arrow[d, hook] & (F^*)^n \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & \mathrm{SL}_n(F) \arrow[r, hook] \arrow[d, two heads] & \mathrm{GL}_n(F) \arrow[r, two heads, "\det"] \arrow[d, two heads] & F^* \arrow[r] \arrow[d, two heads] & 1 \\
1 \arrow[r] & \mathrm{PSL}_n(F) \arrow[r, hook] \arrow[d] & \mathrm{PGL}_n(F) \arrow[r, two heads, "\det"] \arrow[d] & F^*/(F^*)^n \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

כל שורה וכל עמודה בתרשים הזה הן סדרה מדויקת קצרה מן הצורה

$$1\to N\hookrightarrow G\twoheadrightarrow G/N\to 1$$

באופן כללי סדרה של חבורות עם הומומורפיזמים בינהן כמו

$$\dots\xrightarrow{f_{i-1}}G_i\xrightarrow{f_i}G_{i+1}\xrightarrow{f_{i+1}}G_{i+2}\xrightarrow{f_{i+2}}G_3\xrightarrow{f_{i+3}}\dots$$

תקרא מדויקת ב-G_i אם $\ker f_i=\operatorname{im} f_{i-1}$. הסדרה מדויקת אם היא מדויקת בכל גורם. אפשר לוודא שהסדרה $1\to G\xrightarrow{f}H$ היא מדויקת אם ורק אם f הוא מונומורפיזם. בנוסף הסדרה $G\xrightarrow{f}H\to 1$ היא מדויקת אם ורק אם f אפימורפיזם. בשילוב שתי התכונות האלו הסדרה $1\to G\xrightarrow{f}H\to 1$ היא מדויקת אם ורק אם f איזומורפיזם.

הערה 0.20. החבורות לעיל מעניינות להרבה תחומים. ספציפית לגבי מיון של חבורות פשוטות סופיות:

- המיון קשה ממה שאפשר לצפות.
- גלואה הוכיח כי A_n פשוטה לכל $n\geq 5$ וגם $PSL_2(\mathbb{F}_p)$ עבור $p\geq 5$.
- המיון כולל את החבורות מסדר ראשוני, את A_n עבור $n\geq 5$, משפחה של חבורות מטריצות כמו $PSL_n(\mathbb{F}_q)$ וחברים שלהן ועוד רשימה של 26 חבורות ספורדיות.
- מסקנה ממשפט פייט-תומפסון היא שחבורות פשוטות מסדר אי זוגי הן ציקליות.
- יש חבורה פשוטה יחידה מסדר 60, והיא A_5.

- יש חבורה פשוטה יחידה מסדר $168 = 2^3 \cdot 3 \cdot 7$, והיא $PSL_3(\mathbb{F}_2)$.
- עד סדר 720 יש חבורה פשוטה רק מהסדרים $60, 168, 360, 504, 660$. מסדר 504 יש את $PSL_2(\mathbb{F}_8)$, ומסדר 1092 יש את $PSL_2(\mathbb{F}_{13})$ ואלו כל החבורות הפשוטות עד סדר 2000.
- לכל n טבעי יש לכל היותר שתי חבורות פשוטות מסדר n.
- יש שתי חבורות פשוטות לא איזומורפיות מסדר 20160, וזהו הסדר הקטן ביותר שבו יש שתי חבורות פשוטות לא איזומורפיות. אחת היא $PSL_3(\mathbb{F}_4)$ והשניה היא $A_8 \cong PSL_4(\mathbb{F}_2)$.
- יש מעט איזומורפיזמים חריגים:

$A_4 \cong PSL_2(\mathbb{F}_3)$	12
$A_5 \cong PSL_2(\mathbb{F}_4) \cong PSL_2(\mathbb{F}_5)$	60
$GL_3(\mathbb{F}_2) \cong PSL_2(\mathbb{F}_7) \cong PSL_3(\mathbb{F}_2)$	168
$A_6 \cong PSL_2(\mathbb{F}_9)$	360
$A_8 \cong PSL_4(\mathbb{F}_2) \cong GL_4(\mathbb{F}_2)$	20160