תורת החבורות 88-218-01 תשפ"ב
הערות תרגול 12

שלום!

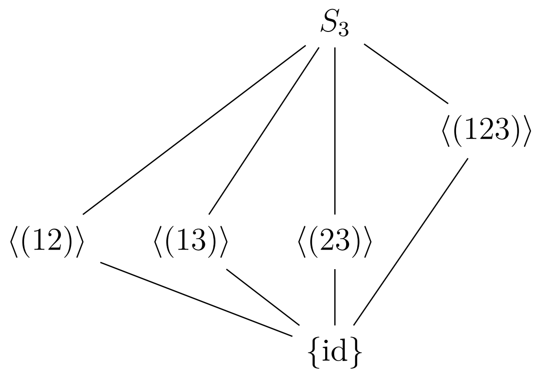
1 משפטי סילו

תזכורת 1.1. תהי G חבורה סופית, ויהי p ראשוני המחלק את הסדר של G. לפי משפט קושי, קיים ב-G איבר מסדר p.

אם p^k מחלק את הסדר של G, אז לא בהכרח קיים איבר מהסדר הזה ב-G.

הגדרה 1.2. תהי G חבורה סופית. נרשום את הסדר של G לפי $|G| = p^t m$ כאשר $p \nmid m$. כלומר p^t היא החזקה הגבוהה ביותר של p המחלקת את $|G|$. לתת־חבורה $H \leq G$ מסדר p^t קוראים תת־חבורה p-סילו של G. נסמן את אוסף תת־חבורות p-סילו של G ב-$\mathrm{Syl}_p(G)$.

דוגמה 1.3. נמצא את תת־חבורות סילו של S_3. נזכר $|S_3| = 2^1 \cdot 3^1$. נתבונן בסריג תת־החבורות של S_3:



וממנו נסיק כי $\mathrm{Syl}_3(S_3) = \{A_3\}$ ו-$\mathrm{Syl}_2(S_3) = \{\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle\}$.

משפט 1.4 (משפט סילו I)**.** לחבורה סופית G קיימת תת־חבורה p-סילו לכל p ראשוני. למעשה מתקיים יותר, אם p^i מחלק את $|G|$, אז קיימת ל-G תת־חבורה מסדר p^i.

משפט 1.5 (משפט סילו II)**.** תהי G חבורה סופית. אז

1. כל תת־חבורות p-סילו של G צמודות זו לזו. בפרט כל תת־חבורה הצמודה לתת־חבורה p-סילו, גם היא תת־חבורה p-סילו.

2. כל תת־חבורת-p של G מוכלת בתת־חבורה p-סילו כלשהי.

מסקנה 1.6. תהי H תת־חבורה p-סילו של G. אז $H \lhd G$ אם ורק אם היא יחידה מהסדר שלה.

משפט 1.7 (משפט סילו III)**.** נסמן $n_p := \left|\mathrm{Syl}_p(G)\right|$ את מספר תת־חבורות p-סילו של G. אז

1. מתקיים $n_p \mid |G|$.

2. מתקיים $n_p \equiv 1 \pmod{p}$.

כמסקנה, אז $n_p|m$ כאשר $|G| = p^t m$ כמו מקודם.

תרגיל 1.8. הוכיחו כי כל חבורה מסדר 45 אינה פשוטה (כלומר יש לה תת־חבורה נורמלית נאותה שאינה טריוויאלית).

פתרון. נחשב $45 = 3^2 \cdot 5$. לפי משפט סילו III נקבל כי $n_3|5$ וגם $n_3 \equiv 1 \pmod{3}$. כלומר $n_3 \in \{1, 5\}$ ולכן בהכרח $n_3 = 1$ כי $5 \equiv 2 \pmod{3}$.
כלומר יש תת־חבורה 3-סילו יחידה, והיא נורמלית. היא נאותה ולא טריוויאלית כי היא מסדר 9, ולכן G לא פשוטה.

תרגיל 1.9 (לבית)**.** תהי G חבורה מסדר אי זוגי. הוכיחו שאם $|G| < 21$, אז G אבלית. יותר קשה: מצאו חבורה לא אבלית מסדר 21.

תרגיל 1.10. תהי G חבורה לא אבלית מסדר 21. מצאו כמה תת־חבורות סילו יש לה מכל סדר.

פתרון. נחשב $21 = 3^1 \cdot 7^1$. אם $p \neq 3, 7$, זה לא מעניין.
לפי משפט סילו III מתקיים $n_7|3$ וגם $n_7 \equiv 1 \pmod{7}$. לכן $n_7 = 1$. בפרט יש ל-G תת־חבורה 7-סילו נורמלית.
עבור 3 מתקיים $n_3|7$ וגם $n_3 \equiv 1 \pmod{3}$. כעת $n_3 \in \{1, 7\}$. נספור כמה איברים יש מכל סדר אפשרי:

- מסדר 1 יש בדיוק 1.
- מסדר 3 יש N איברים.
- מסדר 7 יש בדיוק $7 - 1 = 6$, כי יש תת־חבורה 7-סילו יחידה, והיא ציקלית כי היא מסדר 7.

- מסדר 21 יש בדיוק 0 איברים, כי אחרת החבורה הייתה ציקלית, ולכן אבלית.

לכן $N = 21 - 1 - 6 = 14$. אילו הייתה רק תת־חבורה 3-סילו אחת, אז היו רק 2 איברים מסדר 3, וזה לא ייתכן. לכן בהכרח $n_3 = 7$. לא הראינו זאת, אבל אכן קיימת חבורה לא אבלית מסדר 21.

תזכורת 1.11. המנרמל $N(H) = N_G(H)$ של תת־חבורה $H \leq G$ הוא תת־החבורה הגדולה ביותר של G שבה H נורמלית. האינדקס של המנרמל $[G : N_G(H)]$ שווה למספר תת־החבורות (השונות) שצמודות ל-H. אפשר לראות זאת לפי משפט מסלול־מייצב לפעולה של G על קבוצת תת־החבורות שלה לפי הצמדה.

לכן אם $P \leq G$ היא תת־חבורת p-סילו של G, אז $n_p = [G : N(P)]$.

תרגיל 1.12. הוכיחו שכל חבורה מסדר 224 אינה פשוטה.

פתרון. נניח בשלילה כי G פשוטה מסדר $224 = 2^5 \cdot 7$. לפי משפט סילו III נקבל $n_2 \in \{1, 7\}$. אבל לפי ההנחה, בהכרח $n_2 \neq 1$ כי G פשוטה ולא נרצה שתהיה תת־חבורה 2-סילו נורמלית. כלומר $n_2 = 7$.

תהי P תת־חבורה 2-סילו כלשהי של G. אז $[G : N(P)] = 7$. לכן לפי העידון של משפט קיילי קיים הומומורפיזם לא טריוויאלי $f : G \to S_7$. אבל G פשוטה, ולכן $\ker f$ חייב להיות טריוויאלי (כי כל גרעין הוא תת־חבורה נורמלית). כלומר f שיכון, ולכן $224 | 7!$. זו סתירה כי $224 \nmid 7!$, ולכן G לא פשוטה.

$$7! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$$

טענה 1.13. תהיינה H_1, H_2 תת־חבורות מסדר p ראשוני כלשהו. אז או $H_1 = H_2$, או $H_1 \cap H_2 = \{e\}$.

תרגיל 1.14. תהי G חבורה מסדר $p^2 q$ כאשר $p \neq q$ ראשוניים. הוכיחו כי G לא פשוטה.

פתרון. נניח בשלילה כי G פשוטה. לפי משפט סילו III בהכרח

$$\begin{aligned} n_p &\equiv 1 \pmod p & \qquad n_p &| q \\ n_q &\equiv 1 \pmod q & \qquad n_q &| p^2 \end{aligned}$$

ולכן $n_p = q$ כי אחרת יש תת־חבורה נורמלית מסדר p^2. בנוסף $n_q \in \{p, p^2\}$ אבל לא $n_q = 1$ מסיבה דומה. מפני ש-$n_p = q \equiv 1 \pmod p$, אז $p < q$. לכן לא ייתכן כי $n_q = p$, שכן $p \not\equiv 1 \pmod q$. אז $n_q = p^2$.

תהי Q תת־חבורה q-סילו כלשהי של G. נשים לב שהיא מסדר q, ויש בה $q - 1$ איברים מסדר q (כולם חוץ מאיבר היחידה שהוא מסדר 1). אבל יש p^2 תת־חבורות q-סילו שונות, ולפי הטענה הקודמת נסיק שיש $p^2(q-1)$ איברים מסדר q. כלומר ב-G נשארו p^2 איברים שצריכים להספיק ל-q תת־חבורות p-סילו שונות מסדר p^2, וזה מספיק רק לתת־חבורה אחת כזו. סתירה! לכן G לא פשוטה.

דוגמה 1.15. כל חבורה מסדר $99 = 3^2 \cdot 11$ היא לא פשוטה.

2 מיון חבורות אבליות נוצרות סופית

בגדול, כל חבורה אבלית נוצרת סופית (ובפרט סופית) היא מכפלה ישרה של חבורות ציקליות.

משפט 2.1 (מיון חבורות אבליות נוצרות סופית). תהי G חבורה אבלית נוצרת סופית. אז יש לה צורה קנונית

$$G \cong \mathbb{Z}^r \times \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}$$

כאשר $d_i | d_{i+1}$ לכל i. למספר $r \geq 0$ קוראים הדרגה של G, ולמספרים $d_1, \ldots, d_s$ קוראים המחלקים האלמנטריים של G.

$$\mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_3 \cong \mathbb{Z}_3 \times \mathbb{Z}_{21}$$

הערה 2.2. לרוב מוצאים את הצורה הקנונית על ידי שימוש חוזר בטענה ש-$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ אם ורק אם $(n, m) = 1$. בנוסף ברור כי $H \times K \cong K \times H$. בנוסף $r = 0$ אם ורק אם החבורה האבלית סופית.

תרגיל 2.3. הוכיחו כי $\mathbb{Z}_{100} \times \mathbb{Z}_{40} \cong \mathbb{Z}_{200} \times \mathbb{Z}_{20}$.

פתרון. נמצא את הצורה הקנונית של שתי החבורות, ונראה שהצורות האלו שוות. לכן החבורות תהיינה איזומורפיות. באגף שמאל, הצורה הקנונית היא בוודאי $\mathbb{Z}_{20} \times \mathbb{Z}_{200}$ כי $20 | 200$. עבור החבורה באגף ימין נחשב

$$\begin{aligned} \mathbb{Z}_{100} \times \mathbb{Z}_{40} &\cong \mathbb{Z}_{25} \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \\ &\cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_{25} \cong \mathbb{Z}_{20} \times \mathbb{Z}_{200} \end{aligned}$$

כאשר ניסינו לפרק קודם למכפלה של חבורות ציקליות שהסדרים שלהן הם חזקות של ראשוניים.

טענה 2.4. יהי p ראשוני. תהי G חבורה מסדר p^n. אז בצורה הקנונית שלה מופיעות רק חבורות מסדר p^i עבור i כלשהו. כלומר קיימים מספרים טבעיים $m_1, \ldots, m_k$ כך ש-$n = m_1 + \cdots + m_k$ וגם

$$G \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \cdots \times \mathbb{Z}_{p^{m_k}}$$

ואפשר להניח כי $m_1 \geq m_2 \geq \cdots \geq m_k$ ונקבל שמדובר בחלוקה של המספר n.

בפרט, לכל n טבעי, אם נסמן ב-$\rho(n)$ את מספר החלוקות שלו, אזי יש בדיוק $\rho(n)$ חבורות אבליות מסדר p^n עד כדי איזומורפיזם.

דוגמה 2.5. נמצא את כל החבורות האבליות מסדר $27 = 3^3$. אז יש $\rho(3) = 3$ חלוקות והן

$$3 = 2 + 1 = 1 + 1 + 1$$

ולכן כל החבורות האבליות מסדר 27, איזומורפיות בדיוק לאחת מן החבורות הבאות:

$$\mathbb{Z}_{27}, \mathbb{Z}_9 \times \mathbb{Z}_3, \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

טענה 2.6. כל חבורה אבלית מסדר $p_1^{k_1}p_2^{k_2}\dots p_n^{k_n}$ כאשר p_i הם ראשוניים שונים איזומורפית למכפלה ישרה של חבורות אבליות $H_1\times\dots\times H_n$ כאשר H_i היא חבורה מסדר $p_i^{k_i}$. הצגה כזו של G נקראת פירוק פרימרי.

אם מסדרים את החזקות של הראשוניים לפי סדר, אז הפירוק הזה הוא יחיד.

דוגמה 2.7. מסדר $45=3^2\cdot 5^1$ כל חבורה איזומורפית לאחת משתי החבורות הבאות:

$$\mathbb{Z}_9\times\mathbb{Z}_5, \mathbb{Z}_3\times\mathbb{Z}_3\times\mathbb{Z}_5$$

מסקנה 2.8. מספר החבורות האבליות, עד כדי איזומורפיזם, מסדר $p_1^{k_1}\dots p_n^{k_n}$ הוא $\rho(k_1)\dots\rho(k_n)$.

דוגמה 2.9. נמצא את כל החבורות האבליות מסדר 200, גם לפי פירוק פרימרי שלהן וגם את הצורה הקנונית. נחשב $200=2^3\cdot 5^2$. לכן יש $\rho(3)\rho(2)=6$ חבורות אבליות מסדר 200, והן

$$\begin{gathered}
\mathbb{Z}_8\times\mathbb{Z}_{25}\cong\mathbb{Z}_{200}\\
\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_{25}\cong\mathbb{Z}_2\times\mathbb{Z}_{100}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{25}\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_{50}\\
\mathbb{Z}_8\times\mathbb{Z}_5\times\mathbb{Z}_5\cong\mathbb{Z}_5\times\mathbb{Z}_{40}\\
\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_5\times\mathbb{Z}_5\cong\mathbb{Z}_{10}\times\mathbb{Z}_{20}\\
\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_5\times\mathbb{Z}_5\cong\mathbb{Z}_2\times\mathbb{Z}_{10}\times\mathbb{Z}_{10}
\end{gathered}$$

כאשר באגף שמאל יש פירוק פרימרי, ובאגף ימין צורה קנונית.

$$\begin{aligned}
\mathbb{Z}_4\times\mathbb{Z}_{10}\cong\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_5&\to S_{11}\\
(i,j,k)&\mapsto\sigma^i\tau^j\mu^k
\end{aligned}$$