

משפטי סילו

הגדרה. יהי p ראשוני ותהי G חבורה סופית מגודל $p^t m$ כאשר $(p, m) = 1$. תת חבורת p -סילו של G היא תת חבורה, נסמן ב- P מסדר p^t . כלומר, זאת תת חבורה שהסדר שלו הוא p בחזקת החזקה המקסימלית של p שמחלקת את הגודל של G .

דוגמה. נסתכל על $G = S_3$. $|G| = 6$. חבורת 2-סילו- החזקה הכי גדולה של 2 שמחלקת את 6 זה 2^1 . אז חבורת 2-סילו היא חבורה מגודל 2. כל התת חבורות מגודל 2 זה בעצם כל האיברים מסדר 2: $\langle (1, 2) \rangle, \langle (1, 3) \rangle, \langle (2, 3) \rangle$. תת חבורות 3-סילו- תת חבורה מגודל 3, זה נוצר ע"י איבר מסדר 3. $\langle (1, 2, 3) \rangle$.

משפט. משפטי סילו: תהי G חבורה סופית

0. לכל ראשוני p קיימת תת חבורת p -סילו של G .

1. כל תת חבורה- p (כלומר שהסדר שלה הוא חזקה של ראשוני p) מוכלת בתת חבורת p -סילו.
2. כל שתי תת חבורת p -סילו, עבור אותן צמודות זו לזו. כמו כן, אם מצמידים חבורת p -סילו, מקבלים חבורת p -סילו.
3. נסמן ב- n_p את מספר תתי חבורות p -סילו של G . מתקיים:

$$n_p \equiv 1 \pmod{p}$$

$$n_p \mid m$$

כאשר $(p, m) = 1$ ו- $|G| = p^t m$.

הסבר מקוצר: יש את פעולת ההצמדה של G על תתי חבורות. אז כל תתי חבורות p -סילו הן מסלול אחד. ולכן $n_p \mid |G|$.
אם אנחנו יודעים ש- $n_p \equiv 1 \pmod{p}$ אז $n_p \equiv 1 \pmod{p}$ ולכן $(n_p, p) = 1$ והוכחנו בתרגול הראשון שאם $n_p \mid p^t m$ אז $n_p \mid p^t$, אז n_p מחלק את m .

מסקנה. תת חבורת p -סילו היא יחידה (כלומר, שאין עוד תת חבורות p -סילו) אם היא נורמלית.

תרגיל. תהי G חבורה סופית ו- $H \leq G$. הוכיחו או הפריכו:

- א. אם P היא תת חבורת p -סילו של G אז $P \cap H$ היא תת חבורת p -סילו של H .
- ב. אם P היא תת חבורת p -סילו של H אז קיימת תת חבורת p -סילו של G , Q , כך ש- $Q \cap H = P$.

פתרון.

- ב. הוכחה: $|G| = p^t m$. אז $|P| = p^i$ כי P היא תת חבורת p -סילו של H . $|H| = p^i m'$. ממשפט סילו 1, קיימת תת חבורת p -סילו של Q של G שמכילה את P . צריך להראות ש- $Q \cap H = P$. נב"ש. אז $P < Q \cap H$. $Q \cap H$ הוא תת חבורה של Q ולכן הגודל שלו הוא חזקה של p , אבל הוא מכיל ממש את P , אז הגודל של $Q \cap H$ גדול שווה מ- p^{i+1} . אבל מצד שני, זה תת חבורה של H , ולכן צריך לחלק את הגודל של H , שזה $p^i m'$, $(p, m') = 1$. סתירה.
- א. הפרכה: נקח $H = \langle (1, 3) \rangle$, $P = \langle (1, 2) \rangle$. $P \cap H = \{e\}$. אבל $\{e\}$ היא לא תת חבורת 2-סילו של H . כי $|H| = 2$.

תרגיל. הוכיחו שכל תת חבורה מסדר 45 אינה פשוטה.

פתרון. לפי משפט 1 קיימת תת חבורת 5 סילו. כמה תתי חבורת 5 סילו יש?

$$n_5 \equiv 1 \pmod{5}$$

$$n_5 \mid 9$$

1 זה המספר היחיד שגם שקול ל-5 mod 1 וגם מחלק את 9. ולכן $n_5 = 1$. לכן תת חבורת 5 סילו היא נורמלית.

תרגיל. תהי G חבורה לא אבלית מסדר 21. כמה תתי חבורות p סילו יש לה מכל p רלוונטי?

פתרון. $21 = 3 \cdot 7$. יש תתי חבורות 3 סילו ו-7 סילו.

$$n_3 \equiv 1 \pmod{3}, n_3 \mid 7$$

$$n_3 = 1 \vee 7$$

$$n_7 \equiv 1 \pmod{7}, n_7 \mid 3$$

$$n_7 = 1$$

רמז: נספור כמה איברים יש מכל סדר.

סדרים אפשריים:

1- יש רק אחד.

3.14- כי זה מה שנשאר.

7- יש תת חבורת 7 סילו אחת. P_7 - מגודל 7. כל איבר ב- P_7 הסדר שלו מחלק את $|P_7| = 7$, ולכן זה 1 או 7. יש רק איבר אחד מסדר אחד. לכן כל השאר מסדר 7. יש שישה כאלה. ששת האיברים האלו הם היחידים מסדר 7 מ- G , כי אם יש עוד איבר מסדר 7, אז התת חבורה שהוא יוצר היא תת חבורה מסדר 7, לכן גם תת חבורת 7 סילו, שונה מ- P_7 כי האיבר הזה לא נמצא ב- P_7 , סתירה. כי אנחנו יודעים שיש תת חבורת 7 סילו אחת.

21- אם יש איבר מסדר 21, אז החבורה ציקלית, ולכן אבלית. סתירה.

יש 14 איברים מסדר 3.

הגודל של תת חבורת 3 סילו הוא 3. הסדרים של איברים בתת חבורת 3 סילו הם 1 ו-3. 1 זה רק

איבר היחידה, אז יש 2 איברים מסדר 3.

כל איבר מסדר 3 התת חבורה שהוא יוצר היא תת חבורת 3 סילו. ולכן אם יש רק אחת, אז יש

רק שני איברים מסדר 3.

מה שאומר שיש 7 תתי חבורות 3 סילו.

נראה שזה אכן מסתדר: בכל תת חבורת 3 סילו יש שני איברים מסדר 3. שתי תתי חבורות

שונות מגודל 3, H_1 ו- H_2 מקיימות שהחיתוך ביניהן טריוויאלי. כי $H_1 \cap H_2 \subseteq H_1, H_2$ אז הגודל

שלו מחלק את 3 אז זה 3 או 1. אם זה 3, אז $H_1 \cap H_2 = H_1, H_2$ ונקבל ש- $H_1 = H_2$, סתירה.

לכן כל תת חבורה תורמת 2 איברים שונים. וכך הגענו ל-14 איברים מסדר 3.

הגדרה 1. יהיו G, H שתי חבורות. $f : G \rightarrow \text{Aut}(H)$. $G \times H = G \times H$ כקבוצה זה האיברים. אבל הפעולה היא:

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, f(g_2)(h_1) h_2)$$

וזה אכן נותן פעולה של חבורה. וכך ניתן לייצר חבורה לא אבלית מסדר 21.

(ההגדרה היא העשרה. אלא אם כן בהרצאות שנשארו תעשו אותה) הערה. יש פעולה של G על תתי החבורות ע"י הצמדה. עבור חבורת p סילו המסלול שלה זה כל תתי חבורות p סילו. המייצב שלה זה $N_G(P)$ - המנרמל של P ב G . מפה אנחנו מסיקים ש

$$n_p = [G : N_G(P)]$$

תרגיל. הוכיחו שכל חבורה מסדר 224 אינה פשוטה. פתרון:

$$224 = 4 \cdot 56 = 2^5 \cdot 7$$

$$n_7 \equiv 1 \pmod{7}, n_7 \mid 2^5 = 32$$

$$n_7 = 1 \vee 8$$

$$n_2 \equiv 1 \pmod{2}, n_2 \mid 7$$

$$n_2 = 1 \vee 7$$

נניח בשלילה ש G פשוטה. זה אומר ש $n_7 = 8, n_2 = 7$ ולכן $[G : N(P_7)] = 8, [G : N(P_2)] = 7$

לפי העידון של משפט קיילי, $G \hookrightarrow S_7, S_8$. אבל $7! \nmid 224 = |G|$.

תרגיל. תהי $|G| = p^2 q$ כאשר p, q ראשוניים שונים. הוכיחו ש G אינה פשוטה.

פתרון. יש תתי חבורות q סילו ו p סילו. תתי חבורות q סילו הן מגודל q , ותתי חבורות p סילו הן מגודל p^2 .

$$n_p \equiv 1 \pmod{p}, n_p \mid q$$

$$n_p = 1 \vee q$$

כי q ראשוני.
נניח בשלילה ש G פשוטה. אז $n_p = q$.

$$n_q \equiv 1 \pmod{q}, n_q \mid p^2$$

$$n_q = 1 \vee p \vee p^2$$

הנחנו ש G פשוטה ולכן n_q לא יכול להיות 1.
מכיוון ש $n_p = q$ אז $n_p \equiv 1 \pmod{p}$. זה בפרט אומר ש $p < q$.
לכן לא ייתכן ש $n_q = p$, כי אז $n_q \equiv 1 \pmod{q}$, וזה יגיד ש $p > q$, סתירה.
אז

$$n_q = p^2$$

נספור סדרים של איברים.
הסדר יכול להיות $1, p, q, pq, p^2q, p^2$.
-1 איבר היחידה.
אין איבר מסדר p^2q כי אז החבורה הייתה ציקלית ולכן אבלית, ואז היא לא הייתה פשוטה.
כי כל תת חבורה הייתה נורמלית.
איברים מסדר q - כל איבר מסדר q יוצר תת חבורת q סילו. בכל תת חבורת q סילו יש $q - 1$ איברים מסדר q . והחיתוך של שתי תתי חבורות q סילו שונות הוא טריוויאלי, כי הגודל שלו מחלק את את בגודל של כל אחת מהן שזה q . אם זה יהיה q הן יהיו שוות. לכן זה יוצא 1.
לכן יש $p^2(q - 1)$ איברים מסדר q .
נותנו $1 - p^2$ איברים. נשארו מספיק איברים רק בשביל חבורה אחת מסדר p^2 . (וכמובן שחבורות p סילו וחבורות q סילו עבור $p \neq q$ הן זרות).
בסתירה להנחה שיש q חבורת p סילו.
ולכן החבורה אינה פשוטה.