

**הגדרה.** תהי  $G$  חבורה סופית מסדר  $p^t m$  כאשר  $1 < p < m$  ראשוני. תהי  $P \leq G$ . אנחנו אומרים ש- $P$  היא תת חבורת  $p$ -סילו אם  $|P| = p^t$ .

**דוגמה.**  $G = S_3$ .  $|S_3| = 6 = 2 \cdot 3$ . נמצא תת חבורות 2 סילו ו-3 סילו. תת חבורת 2 סילו צריכה להיות בגודל 2 כי זאת החזקה הכי גדולה של 2 שמחלקת את 6. תת חבורה מגודל 2 זה פשוט מה שנוצר ע"י איבר מסדר 2. ולכן יש 3 חבורות 2 סילו:  $\langle(1, 2)\rangle$ ,  $\langle(1, 3)\rangle$ ,  $\langle(2, 3)\rangle$ . תת חבורת 3 סילו היא מסדר 3 ולכן נוצרת ע"י איבר מסדר 3. לכן יש תת חבורת 3 סילו אחת:  $\langle(1, 2, 3)\rangle$ .

**משפט.** משפטי סילו:

- תהי  $G$  חבורה סופית מסדר  $p^t m$  כאשר  $p$  ראשוני ו- $1 < p < m$ . אזי:
0. קיימת תת חבורת  $p$  סילו.
  1. כל תת חבורת  $p$  של  $G$  מוכלת באיזשהי תת חבורת  $p$  סילו.
  2. כל שתי תתי חבורות  $p$  סילו צמודות זו לזו. וכן, אם נצמיד תת חבורות  $p$  סילו נקבל תת חבורת  $p$  סילו.
  3. נסמן ב- $n_p$  את מספר תתי חבורות  $p$  סילו. מתקיים:

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

$$n_p \mid m$$

**מסקנה.** תת חבורת  $p$  סילו היא יחידה אמ"ם היא נורמלית.

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

1. כל תת חבורת  $p$  סילו של  $G$  מקיימת שהחיתוך שלה עם  $H$  הוא תת חבורת  $p$  סילו של  $H$ .
2. לכל תת חבורת  $p$  סילו של  $H$ , יש תת חבורת  $p$  סילו של  $G$ ,  $P'$ , שמקיימת:

$$P' \cap H = P$$

פתרון. 1. הפרכה:  $G = S_3$ .  $P = \langle(1, 3)\rangle$  זאת תת חבורת 2 סילו.  $H = \langle(1, 2)\rangle$ .  $P \cap H = \{e\}$  זאת לא תת חבורת 2 סילו של  $H$ , כי החזקה המקסימלית של 2 שמחלקת את הגודל של  $H$  היא  $2^1$ .

2. תהי  $P$  תת חבורת  $p$  סילו של  $H$ . בפרט, היא  $P$  היא תת חבורת  $p$  כי הגודל שלה הוא איזושהי חזקה של  $p$ . אז ממשפט סילו 1 (או ממסקנה שלו) היא מוכלת בתת חבורת  $p$  סילו של  $G$ ,  $P'$ . צריך להוכיח ש- $P' \cap H = P$ . ברור.  $P \subseteq P' \cap H$  כי התחלנו עם זה ש- $P$  היא תת חבורה של  $H$ , ולקחנו את  $P'$  להיות תת חבורה שמכילה את  $P$ .

נשים לה  $P' \cap H$  היא תת חבורה של  $P'$  ולכן היא תת חבורת  $p$ . היא מכילה את  $P$ , ולכן הסדר שלה גדול שווה. נניח ש- $|P| = p^i$ , אז  $|P' \cap H| = p^j$  כאשר  $i \leq j$ . נניח בשלילה ש- $i < j$ .  $P' \cap H$  היא תת חבורה של  $H$ . ולכן הגודל שלה מחלק את הגודל של  $H$ . קיבלנו חזקה יותר גדולה של  $p$  שמחלקת את הגודל של  $H$ , בסתירה לכך ש- $p$  היא תת חבורת  $p$  סילו של  $H$ . לכן  $i = j$ . וזה אומר ש- $P = P' \cap H$ .

**תרגיל.** יהי  $\varphi : G \rightarrow H$  אפימורפיזם. הוכיחו/ הפריכו:

1. אם  $P$  היא תת חבורת  $p$  סילו של  $G$  אז  $\varphi(P)$  היא תת חבורת  $p$  סילו של  $H$ .
2. אם  $P$  היא תת חבורת  $p$  סילו של  $H$  אז  $\varphi^{-1}(P)$  היא תת חבורת  $p$  סילו של  $G$ .

פתרון. 1. ראשית  $\varphi(P)$  היא תת חבורת  $p$  כי הסדר שלה מחלק את הסדר של  $P$ . השאלה האם היא מקסימלית. אם היא לא מקסימלית, אז יש חבורת  $P', p$  שמכילה ממש את  $\varphi(P)$ .  $P \subsetneq \varphi^{-1}(P')$ . אפימורפיזם. כי  $\varphi$  הוא השערה:

$$[H : \varphi(P)] \mid [G : P]$$

$$K = \ker \varphi$$

$$H \cong G/K$$

$$\varphi(P) = PK/K$$

נובעת מתרגיל ב"ב שאמר ש  $\varphi^{-1}(\varphi(P)) = P \ker \varphi$ . אז לשתי תתי החבורות האלו יש את אותה תמונה.  $P \ker \varphi$  היא תת חבורה שמכילה את הגרעין ואז אפשר להשתמש במשפט ההתאמה ואיזו 3.

$$[H : \varphi(P)] = [G/K : PK/K] = [G : PK] \mid [G : P]$$

ולכן נקבל ש  $[H : \varphi(P)]$  זר ל  $p$  ולכן  $\varphi(P)$  היא תת חבורת  $p$  סילו. 2. הפרכה:  $G = S_n$ .  $H = \Omega_2$  והעתקה הסימן. אז  $H$  היא תת חבורת 2 סילו של עצמה.  $\varphi^{-1}(H) = S_n$  שאינה תת חבורת 2 סילו.

**תרגיל.** הוכיחו שכל תת חבורה מסדר 45 אינה פשוטה.

$$45 = 3^2 \cdot 5$$

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

$$n_5 \mid 9$$

לכן  $n_5 = 1$ , כלומר תת חבורת 5 סילו היא יחידה ועל כן נורמלית.

**תרגיל.** תהי  $G$  חבורה לא אבלית מסדר 21. חשבו כמה תתי חבורות סילו יש לה מכל ראשוני שמחלק אותה.

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

$$n_7 \equiv 1 \pmod{7}$$

$$n_7 \mid 3$$

לכן  $n_7 = 1$ .

$$n_3 \equiv 1 \pmod{3}$$

$$n_3 \mid 7$$

$$n_3 = 1 \vee 7$$

נשתמש בספירת איברים:

הסדרים האפשריים של איברים הם:

1- יש רק אחד.

3 - נשארו 14 איברים.

7-6. הסבר: חבורת 7 סילו היא מסדר 7, ולכן כל איבר בה חוץ מהיחידה הוא מסדר 7, יש 6

כאלה. כמו כן, כל איבר מסדר 7 יוצר תת חבורה מסדר 7 ולכן חייב להיות מוכל בחבורת 7 סילו.

ויש רק אחת כזאת.

21-0. אחרת אם היה איבר מסדר 21 היא הייתה ציקלית ולכן אבליית.

לכן יש 7 חבורות 3 סילו. כי כל איבר מסדר 3 יוצר תת חבורה מסדר 3 ולכן מוכל בחבורת 3

סילו. הגודל של חבורת 3 סילו הוא 3 כי זאת החזקה הכי גדולה של 3 שמחלקת את 21. בחבורה

מגודל 3 יש 2 איברים מסדר 3. אז ברור שחבורת 3 סילו אחת לא יכולה להספיק.

למעשה, כל שתי תתי חבורות 3 סילו שונות החיתוך שלהן טריוויאל. כי אם  $P_1, P_2$  מגודל 3,

אז  $P_1 \cap P_2$  הוא תת חבורה של שתיהן מסדר שמחלק את הסדר של כל אחת מהן אז מחלק את 3. אז

החיתוך הוא או מגודל 1 או מגודל 3. אם הוא היה מגודל 3 אז היינו מקבלים  $P_1 = P_1 \cap P_2 = P_2$

בסתירה לכך שהן שונות.

טענה. בהוכחה של משפטי סילו השתמשנו בפעולת ההצמדה של  $G$  על תתי החבורת שלה. אז

בעצם  $n_p$  שווה לגודל של המסלול של תת חבורת  $p$  סילו, ממשפט מסלול מייצב נקבל שזה שווה

ל  $[G : \text{stab}(P)]$ . מה זה מייצב של תת חבורה ביחס לפעולת ההצמדה? זה כל האיברים  $x \in G$

כך ש  $xPx^{-1} \in P$ , זה מה שנקרא "המנרמל" של  $P$ , שמסומן  $N_G(P)$ .

כלומר,

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

**תרגיל.** הוכיחו שכל חבורה מסדר 224 אינה פשוטה.

$$224 = 2^5 \cdot 7. \text{ פתרון.}$$

$$n_2 \equiv 1 \pmod{2}$$

$$n_2 \mid 7$$

$$n_2 = 1 \vee 7$$

$$n_7 \equiv 1 \pmod{7}$$

$$n_7 \mid 32$$

$$n_7 = 1 \vee 8$$

נניח בשלילה שהחבורה פשוטה, אז  $n_2 = 7$  ו  $n_7 = 8$  (כי אם מישהו מהם שווה ל 1, את התת חבורת  $p$  סילו המתאימה היא נורמלית).  $[G : N_G(P_2)] = 7$  ו  $[G : N_G(P_7)] = 8$ . לפי משפט העידון של קיילי, אם יש תת חבורה מאינדקס  $k$ , אז יש הומומורפיזם  $G \rightarrow S_k$ . הנחנו ש  $G$  פשוטה ולכן כל הומומורפיזם יהיה שיכון.  $G \hookrightarrow S_7, S_8$ . אבל  $7! \nmid |G|$ . אז לא שיכון להיות שיכון של  $G$  בתוך  $S_7$ . סתירה.

**תרגיל.** תהי  $G$  חבורה מסדר  $p^2q$  כאשר  $p, q$  ראשוניים. הוכיחו ש  $G$  אינה פשוטה. פתרון. נניח בשלילה ש  $G$  פשוטה.

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

$$n_p \mid q$$

$$n_p = 1 \vee q$$

אבל  $G$  פשוטה אז  $n_p \neq 1$  ולכן  $n_p = q$ . בפרט מקבלים ש  $q \equiv 1 \pmod{p}$  ולכן  $q > p$ .

$$n_q \equiv 1 \pmod{q}$$

$$n_q \mid p^2$$

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

לא 1, כי  $G$  פשוטה. לא  $p$ , כי  $p$  לא שקול ל 1 מודולו  $q$ , כי  $q$  גדול מ  $p$ . לכן  $n_q = p^2$ . ספירת איברים: כמה איברים יש מסדר  $q$ ? יש  $p^2$  חבורות  $q$  סילו. כל חבורת  $q$  סילו היא מגודל  $q$ . חבורה מגודל ראשוני- כל האיברים בה, חוץ מאיבר היחידה, הם מהסדר של הראשוני הזה. אז בכל חבורה כזאת יש  $q - 1$  איברים מסדר  $q$ . כל שתי חבורות  $q$  סילו שונות הן זרות, (אותה הוכחה שעשינו עם החבורות 3 סילו), כי החיתוך שלהן מוכל בכל אחת מהן, והסדר שלו צריך לחלק את הסדר של כל אחת מהן שהוא  $q$ , לכן החיתוך הוא או מסדר  $q$  או מסדר 1. אם החיתוך יהיה מסדר  $q$  הוא יהיה שווה לכל אחת מהן ונקבל שהן שוות. סתירה. לכן החיתוך טריוויאלי. יש  $p^2$  חבורות  $q$  סילו, כל אחת מהן תורמת  $q - 1$  איברים שונים מסדר  $q$ , אז בסה"כ קיבלנו  $(q - 1)p^2$  איברים מסדר  $q$ . נשאר  $p^2$  איברים, זה מספיק רק לחבורת  $p$  סילו אחת (כי הגודל של חבורת  $p$  סילו הוא  $p^2$ ) בסתירה לכך שיש יותר מאחת ( $n_p \neq 1$ )