

## תרגול 11: משפטי סילוא (Sylow)

**משפט קושי:** תהי  $G$  חבורה סופית, כך שמתקיים  $p \mid |G|$  עבור  $p$  ראשוני. אזי קיים איבר מסדר  $p$  ב  $G$ .

**תרגיל:** הראו שקיימת חבורה שלא לכל מספר  $m \mid |G|$  קיים איבר מסדר  $m$ .

**פתרון:** בחבורה  $S_4$  לא קיים איבר מסדר 12, למרות ש  $|S_4| = 24$ . זאת כיוון שכל איבר ב  $S_4$  הוא מאחד ממבני המחזוריים הבאים (שקובעים את סדר האיברים):

4 - סדר 4

3 - סדר 3

2 - סדר 2

2 - סדר 2

1 - סדר 1

**הערה:** כפי שראינו לעיל, לא ניתן להכליל את משפט קושי לכל מחלק  $m \mid |G|$ , אך משפטי סילוא נותנים לנו בכל זאת הכללה טובה.

**הגדרה:** תהי  $G$  חבורה סופית, כך שמתקיים  $p^m \mid |G|$ ,  $p^{m+1} \nmid |G|$ , עבור  $p$  ראשוני. תת חבורה מסדר  $p^m$  של  $G$  נקראת תת חבורה **פ-סילוא**.

**דוגמא:** נמצא חבורת 2-סילוא ב  $S_3$ : כיוון ש  $|S_3| = 6$  בהכרח חבורת 2-סילוא היא מסדר 2. יש 3 ת"ח כאלה:  $\langle (1,2) \rangle$ ,  $\langle (2,3) \rangle$ ,  $\langle (1,3) \rangle$ . נשים לב שהראינו כעת שתת-חבורת פ-סילוא לא בהכרח יחידה! בנוסף גם הראינו שתת-חבורת פ-סילוא לא בהכרח תת-חבורה נורמלית.

נמצא חבורת 3-סילוא ב  $S_3$ : כיוון ש  $|S_3| = 6$  בהכרח חבורת 2-סילוא היא מסדר 3. יש רק ת"ח אחת כזאת:  $\langle (1,2,3) \rangle$ , והיא נורמלית.

**משפט (הכללה של משפט קושי):** לכל  $G$  סופית,  $p$  ראשוני, אם  $p^m \mid |G|$  אז קיימת ת"ח של  $G$  מסדר  $p^m$ .

**מסקנה: משפט סילוא 1:** תהי  $G$  חבורה סופית. אז לכל ראשוני  $p$  המחלק את סדר  $G$ ,  $G$  מכילה תת חבורה  $p$  סילוא.

**הגדרה:** נאמר ששתי תת-קבוצות (בפרט ת"ח)  $S, T \subseteq G$  הן **צמודות** אם קיים  $g \in G$  כך ש  $gSg^{-1} = T$ . שימו לב שזאת פעולה של החבורה  $G$  על הקבוצה  $X$  של תת-הקבוצות של  $G$  (או פעולה של  $G$  על תת-החבורות של  $G$ ).

**תרגיל:** הראו שאם  $H, K \leq G$  ת"ח צמודות שונות של  $G$  אזי  $H, K$  אינן ת"ח של  $G$ .

**פתרון:** זאת כיוון שקיים  $g \in G$  כך ש  $gHg^{-1} = K \neq H$  ולכן  $H$  אינה אינוריאנטית להצמדה, ולכן אינה תח"נ (ואותו דבר עבור  $K$ ).

**משפט סילוא 2:** כל תתי חבורות  $p$ -סילוא של חבורה סופית  $G$  צמודות זו לזו.

**תרגיל:** אם  $H$  תח"פ-סילוא של  $G$ , אזי  $gHg^{-1}$  היא גם תח"פ-סילוא של  $G$ , לכל  $g \in G$ .

**פתרון:** זאת כיוון ש  $gHg^{-1} \cong H$ . נגדיר  $\varphi: H \rightarrow G$  המוגדרת ע"י  $\varphi(h) = ghg^{-1}$ . התמונה היא

$gHg^{-1}$ . לכן  $gHg^{-1}$  היא תח"פ, ו- $H$ ,  $gHg^{-1}$  הן מאותו סדר.

**תרגיל:** יש רק תח"פ-סילוא אחת אם ורק אם היא תח"נ.

**הוכחה:** אם קיימת תח"פ-סילוא אחת  $H$ , אזי לפי הנחה  $gHg^{-1} = H$  לכל  $g \in G$ , אחרת היו שתי תת-

חבורות  $p$ -סילוא לפי ההערה. לכן  $H$  תח"נ. אם  $H$  תח"פ-סילוא נורמלית, אזי  $gHg^{-1} = H$  לכל  $g \in G$ ,

ואם היתה תת-חבורת  $p$ -סילוא שניה  $K$  אזי הן היו צמודות לפי משפט סילוא 2, כלומר קיים  $g \in G$  כך ש

$gHg^{-1} = K \neq H$ , סתירה.

**משפט סילוא 3:** יהי  $r_p$  מספר תתי החבורות של  $p$ -סילוא של חבורה סופית  $G$  אז:

- $r_p \mid |G|$

- $r_p \equiv 1 \pmod{p}$

**מסקנה:**  $\gcd(r_p, p) = 1$ .

**מסקנה:** חבורת  $p$ -סילוא היא נורמלית אם ורק אם  $r_p = 1$  (נובע ישירות מהמסקנה ממשפט סילוא 2).

**תרגיל:** אם  $G$  אינה חבורת  $p$ , ומתקיים  $p \mid |G|$  וגם  $r_p = 1$  (כלומר יש תח"פ - סילוא יחידה) אז  $G$

אינה פשוטה. כלומר קיימת  $H < G$  כאשר  $H \neq G, \{e\}$ .

**פתרון:** תהי  $H$  תח"פ-סילוא, אזי בגלל ש  $r_p = 1$  מתקיים  $gHg^{-1} = H$  לכל  $g \in G$ , כיוון שגם  $gHg^{-1}$

היא חבורת  $p$ -סילוא (אבל יש רק אחת כזאת). לכן  $H$  תח"נ של  $G$ , והיא אינה תח"פ טריויאלית בגלל

ההנחות (מדוע?).

**משפטון:**  $r_p$  מחלק את  $\frac{|G|}{p^m}$ .

**הוכחה:**

$$H \leq G, |H| = p^m$$

$$|G| = |H| [G:H] = p^m * n, p \nmid n$$

$$r_p \parallel |G|, r_p \bmod p = 1 \Rightarrow \gcd(r_p, p^m) = 1 \Rightarrow r_p \mid n = \frac{|G|}{p^m}$$

**תרגיל:** הראו שחבורה מסדר 40 אינה פשוטה

**תשובה:**  $40 = 5 * 2^3$  לפי משפטי 40 סילוא יש תת חבורה 2 סילוא מסדר 8 ויש תת חבורה 5 סילוא

מסדר 5. ובאופן טריוואלי יש תת חבורה מסדר 1,40 שאלה האם חבורה מסדר 40 פשוטה? לפי

המשפט הקודם מספיק להוכיח  $r_5 = 1 \vee r_2 = 1$ .

לפי משפט סילוא 3 מתקיים  $r_5 \equiv 1 \pmod{5}, r_5 \mid 40$  לכן

$$r_5 \in A = \{1, 2, 4, 8, 5, 10, 20, 40\}$$

$$r_5 \in B = \{1, 6, 11, 16, 21, 26, 31, 36, 41, \dots\}$$

$$A \cap B = \{1\} \Rightarrow r_5 = 1$$

לכן חבורה מסדר 40 אינה פשוטה.

**תרגיל:** האם חבורה מסדר 10 פשוטה?

**תשובה:**  $10 = 5 * 2$  לפי משפט סילו קיימת תת חבורה 5 סילוא מסדר 5 נסמן אותה ב  $H \leq G, |G| = 10$

לפי לגראנז'  $|G| = |H| [G:H]$  במקרה שלנו  $[G:H] = 2 \Leftrightarrow [G:H] = 2$  וכבר הוכחנו כל תת

חבורה מאינדקס 2 נורמלית לכן חבורה מסדר 10 אינה פשוטה.

**מסקנה:** באופן כללי כל חבורה מסדר  $2p^m$  עבור  $p$  ראשוני אינה פשוטה (אותה הוכחה (בערך)).

**תרגיל:** אם  $|G| = pq$  כך ש  $p \neq q$  ראשוניים ו  $q \not\equiv 1 \pmod{p}$  אז יש ל  $G$  ת"ח  $p$  סילוא נורמלית:

**הוכחה:**

$$r_p \mid pq \in \{1, p, q, pq\},$$

$$r_p = 1 \pmod{p} \in \{1\}$$

$$\Rightarrow r_p = 1$$

ולכן לפי משפט  $G$  קיימת תת חבורה  $p$  סילוא שהיא נורמלית ולכן  $G$  אינה פשוטה.

**הערה:** אם מוסיפים את הדרישה  $p < q$  בתרגיל, נקבל שגם  $r_q = 1$ , זאת כיוון שאם  $p < q$  אזי

$$p \not\equiv 1 \pmod{q} \text{ ואז:}$$

$$r_q | pq \in \{1, p, q, pq\},$$

$$r_q = 1 \pmod q \in \{1\}$$

$$\Rightarrow r_q = 1$$

מכאן ניתן להסיק שהחבורה  $G$  היא ציקלית (נראה זאת בתרגול הבא), כלומר נקבל את המשפט:  
**משפט:** יהיו  $p, q$  ראשונים  $p < q$ ,  $q \not\equiv 1 \pmod p$ , כל חבורה מסדר  $pq$  היא ציקלית (כלומר איזומורפית ל  $Z_{pq}$ )

**תרגיל:** הוכח כי חבורה מסדר 84 אינה פשוטה.

**פתרון:** לפי המשפטון נקבל:

$$r_7 | \frac{84}{7} = 12 \Rightarrow r_7 \in \{1, 2, 3, 4, 6, 12\} \wedge$$

$$r_7 \pmod 7 = 1 \Rightarrow r_7 = 1$$

קיבלנו  $r_7 = 1$  ולכן לפי משפט החבורה  $G$  אינה פשוטה.

**תרגיל עזר:** יהי  $K$  ראשוני, תהי  $G$  חבורה, ויהיו  $H, K$  שתי תת-חבורות שונות מסדר  $p$ . אזי

$$H \cap K = \{e\}$$

**הוכחה:**  $H \cap K \leq G$  ולכן  $H \cap K \leq H$ , לכן לפי לגרנג' נקבל  $|H \cap K| = 1, p$  אבל אם  $|H \cap K| = p$

נקבל ש  $H=K$ , סתירה, לכן  $|H \cap K| = 1$ .

**מסקנה:** מספר האיברים מסדר  $p$  ראשוני בחבורה  $G$  מתחלק ב  $p-1$ .

**הוכחה:** כל איבר  $x$  מסדר  $p$  שייך לת"ח של  $G$  מסדר  $p$  (לדוגמא ל  $\langle x \rangle$ ), ובחבורה כזאת יש  $p-1$  איברים מסדר  $p$  (מדוע?). יהי  $k$  מספר הת"ח מסדר  $p$ . לפי תרגיל העזר נקבל שיש  $k(p-1)$  איברים מסדר  $p$ .

**תרגיל:** אם  $|G| = p^2q$ ,  $p, q$  ראשונים זרים. אז או שיש ל  $G$  תת חבורה נורמלית  $p$ -סילוא (מסדר ?)

או שיש ל- $G$  תת חבורה נורמלית  $q$ -סילוא (מסדר ?). בכל מקרה  $G$  אינה פשוטה!

**הוכחה:** יש ל  $G$  תתי חבורות  $p$ -סילוא מסדר  $p^2$  ו  $q$ -סילוא מסדר  $q$ . נניח בשלילה שאין ל  $G$  תח"נ

$$1 < r_p, r_q \parallel |G| = p^2q \Rightarrow r_p, r_q \in \{p, q, p^2, p^2q\}$$

$$r_p \pmod p = 1 \Rightarrow r_p = q \Rightarrow q > p \quad \text{לכן בהכרח } r_p, r_q > 1 \text{ לפי משפטי סילוא נקבל ש:}$$

$$r_q \pmod q = 1 \Rightarrow r_q \in \{p, p^2\}$$

עכשיו כל איבר מסדר  $q$  יוצר תת חבורה  $q$  סילוא בעלת  $q$  איברים מסדר  $q$ . כל 2 תתי חבורות שונות מסדר  $q$  נחתכות רק ב  $\{e\}$  ולכן ב  $G$  יש  $r_q(q-1)$  איברים מסדר  $q$ . אם:

- $r_q = p^2$ , אזי מספר האיברים שאינם מסדר  $q$  הם:

$$|G| - p^2(q-1) = p^2q - p^2q + p^2 = p^2$$

זו יש  $p^2$  שאינה מסדר  $q$  אבל יש בסך הכל  $p^2$  איברים שאינם מסדר  $q$  ולכן כולם  $P$

ואין עוד תת חבורה  $P$  סילוא אחרת (כי כל האברים נמצאים ב- $P$ ) לכן  $r_p = 1$ , סתירה.

- $r_q = p$  לכן  $p \equiv 1 \pmod{q} \wedge q > p \Rightarrow p = 1$  וקיבלנו סתירה.

לכן קיבלנו סתירה להנחה, ומכאן שבהכרח  $r_p = 1 \vee r_q = 1$ . בכל מקרה החבורה אינה פשוטה!

### תרגיל:

הוכיחו או הפריכו: אם  $H$  תת-חבורת- $q$  אבליית של  $G$  אזי  $H$  מוכלת בכל תת-חבורת- $p$ -סילוא של  $G$ .

### פתרון:

נפריך: ניקח  $G = S_3$ ,  $H = \langle (1,2) \rangle$ . בוודאי ש  $H$  אבליית, והיא חבורת-2, אבל היא אינה מוכלת בכל

תת-חבורת-2 סילוא של  $G$ , שהן כל החבורות מסדר 2.

### תרגיל:

תהי  $H$  תת-חבורת- $q$  המוכלת במרכז של  $G$  אזי  $H$  מוכלת בכל תת-חבורת- $p$ -סילוא של  $G$ .

### פתרון:

תהי  $K$  תת-חבורת- $p$ -סילוא כלשהי של  $G$  (קיימת כזאת לפי משפט סילוא 1). אזי  $K \triangleleft N(K)$  (זה נכון

לכל תת-חבורה, **הראו זאת**). כיוון ש  $H \leq Z(G)$ , גם  $H \leq N(K)$  (**הראו זאת**) ולכן  $HK \leq N(K)$ .

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

$$. H \leq K$$