מופשטת 1,קיץ 2013
תרגול 12

משפט סילו 2
1. כל תתי חבורות p־סילו של חבורה סופית Gצמודות זו לזו.
2. כל תת חבורה־p של Gמוכלת בת"ח p־סילו כלשהי.

הסבר ל־1: $H, K \leq G$ הן ת"ח p־סילו אזי קיים $g \in G : gHg^{-1} = K$.
הערה:שימו לב:אם $H \leq G$ ת"ח p־סילו אזי גם gHg^{-1} p־סילו שכן $|H| = |gHg^{-1}|$.
מסקנה:ת"ח p־סילו היא יחידה אמ"מ היא נורמלית.
הוכחה:
$(\Leftarrow)$ יש ת"ח p־סילו Pוהיא יחידה. לכל $g \in G$: gPg^{-1} היא גם p־סילו ולכן $gPg^{-1} = P$. $P \triangleleft G \Leftarrow$.
$(\Rightarrow)G$ p־סילו נורמלית. נניח שהיא לא יחידה, כלומר קיים $K \leq G$ת"ח p־סילו אזי קיים $g \in G$: $gPg^{-1} = K$ אבל $gPg^{-1} = P$ולכן $P = K$. מ.ש.ל

משפט סילו 3
יהי n_p מס' תתי חבורות p־סילו של חבורה סופית G.
א. $n_p \mid |G|$
ב. $n_p = 1 (\mod p)$
הערה:נניח $|G| = p^k m$. $(m, p) = 1$ אזי $n_p \mid m$ (כי מתנאי ב' רואים ש־n_pזר ל־p ולכן לא מחלק את p^k).
מסקנה:תת חבורה p־סילו היא נורמלית $\Leftrightarrow n_p = 1$.
תרגיל:
הראו שחבורה מסדר 45 אינה פשוטה.
פתרון:
$|G| = 45 = 3^2 \cdot 5$. יש ל־G תת חבורה 5־סילו נסמנה P_5. כמו כן יש ל־G ת"ח 3־סילו נסמנה P_3. נבדוק אם אחת מהן נורמלית:
נתחיל עם n_3.
$n_3 \equiv 1 (\mod 3) \wedge n_3 \mid 5$
$n_3 \in \{1, 5\}$אבל נפסול את 5 כיוון ש$5 \not\equiv 1 (\mod 3)$. לכן $n_3 = 1 \Rightarrow P_3 \triangleleft G$ לכן G לא פשוטה.
הערה: אותו הליך היה עובד גם עם P_5:
n_5:
$9 \mid 9 \wedge n_5 \equiv 1 (\mod 5)$ ואזי $n_5 \in \{1, 3, 9\}$ נפסול שוב את 3,9 כיוון שהם לא שקולים ל$1 \mod 5$.
הערה: כל שתי ת"ח p־סילו שונות מסדר ראשוני p נחתכות טריוויאליות.
הסבר: אפשרויות לגודל החיתוך הן אך ורק אלו המחלקות את המס' (סדר החיתוך או כסדר החבורה [שלא מתקיים כיוון שהן שונות] או טריוויאלי). מצד שני אם הסדר לא ראשוני יתכן והחיתוך לא טריוויאלי (לדוג' אם הסדר של שתיהן היה 5 הסדר היה יכול להיות 1 או 5 אבל אם היה לדוגמה 5^2, סדרהחיתוך היה להיות גם 5)
תרגיל (ספירת איברים): נמצא את מס' ת"ח p־סילו של חבורה G לא אבלית מסדר 21.
פתרון:
$|G| = 21 = 3 \cdot 7$יש ל־G ת"ח 3־סילו P_3 ות"ח 7־סילו P_7. שואלים כמה ת"ח 3 סילו או 7 סילו יש?

$n_3 : n_3 \equiv 1(\mod 3) \wedge n_3 \mid 7 \Rightarrow n_3 \in \{1, 7\}$

ועבור n_7 באופן דומה:

$n_7 = 1(\mod 7) \wedge n_7 \mid 3 \Rightarrow n_7 \in \{1\}$ (3 נפסל) ולכן $n_7 = 1$. יש ת"ח 7-סילו יחידה.

ספירת איברים:

סדר של איבר	מס' איברים מסדר זה
1	1
3	$14(\star)$
7	6 (כי בP_7ישנם 7 איברים ו1 מהם הוא איבר היחידה ועוד 6 איברים מסדר 7)
21	0 (כי אחרת G הייתה ציקלית ואז אבלית)

$(\star)$: אם $n_3 = 1$ אזי היו לנו 2 איברים מסדר 3 ואז בספירת האיברים לא היינו מגיעים ל-21.

לכן $n_3 = 7$ ואז יש $2 \cdot 7 = 14$ איברים מסדר 3. מ.ש.ל

תזכורת/הבהרה: כל איבר מסדר p "יושב" בתוך ת"ח p-סילו כלשהיא.

הערות:

א. באותו אופן ניתן להראות כי לכל חבורה $|G| = pq$ עבור $p > q$ ראשוניים אם $p \not\equiv 1(\mod q)$ אזי G ציקלית.

ב. אם $p = 1(\mod q)$ אזי G אינה בהכרח ציקלית.

למשל: $|S_3| = 2 \cdot 3$ ואז $3 \equiv 1(\mod 2)$ ו S_3 איננה ציקלית.

הערה:

אם $H \leq G$ ת"ח p-סילו, $K \leq G$ת"ח q-סילו (p,q ראשונים שונים) אזי $H \cap K = \{e\}$.

תרגיל: הוכיחו כי לכל חבורה מסדר pq עבור $p > q$ ראשוניים, אם $p \not\equiv 1(\mod q)$ אזי G ציקלית.

פתרון:

עבור n_p:

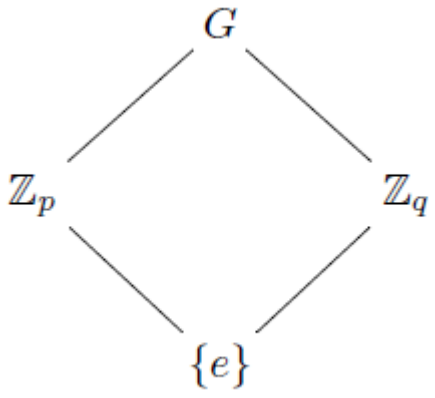
$n_p \mid q \wedge n_p \equiv 1(\mod p)$ כלומר לכאורה $n_p \in \{1, q\}$ אבל $q \not\equiv 1(\mod p)$ כי $p > q \Leftarrow n_p = 1 \Leftarrow P \triangleright G$ ת"ח p-סילו $P \cong \mathbb{Z}$.

ננקוט באופן דומה עבור n_q p:

$n_q \mid p \wedge n_q \equiv 1(\mod q)$ ושוב לכאורה $n_q \in \{1, p\}$ אבל $p \not\equiv 1(\mod q)$ לפני הנתון $\Leftarrow n_q = 1$.

$G \triangleleft Q$ת"ח p-סילו ומתקיים $Q \cong \mathbb{Z}_q$.

היינו רוצים:



וכן $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.
נראה שG היא מכפלה ישרה פנימית של ת"ח שלה P, Q. לשם כך יש להראות כי :
1. $P \cap Q = \{e\}$
2. $P, Q \triangleleft G$ - הוכחנו.
3. $P \cdot Q = G$ - נוכיח זאת כעת.
אזי לפי משפט מההרצאה נקבל ש- $G \cong P \times Q$ וזו התוצאה הדרושה.
$H = PQ \leq G \Leftarrow P, Q \triangleleft G$ (סימון: H) לפי ההגדרה היא מכפלה ישרה פנימית של Pו-Q.
לכן: $H \cong P \times Q$ולפי מכפלה של קבוצות:
$|H| = |P| \times |Q| = pq$.
$H \leq G$ וגם $|H| = pq \Leftarrow H = G \Leftarrow PQ = G$.
נסכם: $G = PQ$ ולכן $G \cong P \times Q$ אבל $P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q \Leftarrow \mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong G$
כאשר המעבר האחרון נובע מכך ש$(p, q) = 1$. על כן G ציקלית. מ.ש.ל.
<u>הערה:</u> דרכים נוספות להוכיח את הטענה:
1. ספירת איברים כמו שעשינו עם $|G| = 21$.
2.(דרך אלגנטית) להראות ישירות שיש איבר מסדר pq. {שני איברים מתחלפים ולכן הם זרים
וסדר המכפלה הוא מכפלת הסדרים. מופיע בשיעורי הבית.}.
<u>תרגיל:</u>
הראו שלא קיימת חבורה פשוטה מסדר 132.
<u>פתרון:</u>
$|G| = 132 = 2^2 \cdot 3 \cdot 11$
n_{11}
$n_{11} \mid 12 \wedge n_{11} \equiv 1 (\mod 11)$ ונוכל לפסול 2,3,4,6 להסיק $n_{11} \in \{1, 12\}$.
n_3
$n_3 \mid 44 \wedge n_3 \equiv 1 (\mod 3)$
$n_3 \in \{1, 4, 22\}$
n_2
$n_2 \mid 33 \wedge n_2 \equiv 1 (\mod 2)$ ושום אופציה לא נפסלת $n_2 \in \{1, 3, 11, 33\}$.
אם $n_{11} = 1$או $n_2 = 1$ או $n_3 = 1$ סיימנו ולכן נניח שהם לא 1. ההנחה באופן מפורש היא:

$n_{11} = 12$
$n_3 \in \{4, 22\}$
$n_2 \in \{3, 11, 33\}$

- $n_{11} = 12$ (כל חבורה 11 סילו היא מסדר 11 ויש בה 11 איברים 10 מסדר 11 ואיבר היחידה) לכן יש 120 איברים מסדר 11.
- האם יתכן ש$n_3 = 22$? לא. כי אז יש $2 \cdot 22 = 44$ איברים מסדר 3 ואז אנחנו חורגים מהסדר של החבורה. לכן: $n_3 = 4$ ולכן יש 8 איברים מסדר 3.

<u>סיכומון:</u>

איבר 1 מסדר 1, 120 איברים מסדר 11, 8 איברים מסדר 3. לכן ספרנו עד עכשיו 129 איברים.
נותר מקום ל-3 איברים מסדר 2. אבל חבורת 2- סילו היא מסדר 4 ולכן יש בה 3 איברים מסדר 2. כלומר יש ת"ח 2- סילו יחידה! ולכן היא נורמלית והחבורה G איננה פשוטה.
מ.ש.ל

תרגיל:תהא G חבורה מסדר p^2q עבור p,q ראשוניים שונים. הוכיחו ש־G אינה פשוטה.
פתרון:
$n_p : n_p \equiv 1(\mod p) \wedge n_p \mid q \Rightarrow n_p \in \{1,q\}$. אם $n_p = 1$ סיימנו ולכן נניח $n_p = q$.
$n_q = 1(\mod q) \wedge n_q \mid p^2, n_q \in \{1,p,p^2\}$.
אם $n_q = 1$ סיימנו.

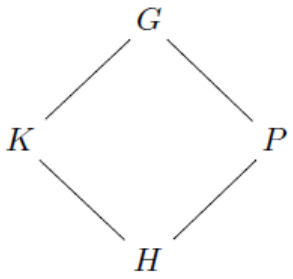
- אם $n_q = p^2$:

כמה איברים מסדרq יש ? $p^2(q-1) = p^2q - p^2$ איברים מסדר q. אבל אז יש מקום רק לחבורת $p-$סילו אחת שכן חבורת $p-$סילו היא מסדר p^2 וסיימנו$n_p = 1 \Leftarrow$.

- אם $n_q = p$ אזי $p \equiv 1(\mod q)$. אבל שימו לב שאנו תחת ההנחה ש־ $n_p = q$ כלומר $q \equiv 1(\mod p)$ כלומר יש שני תנאים:

$p \equiv 1(\mod q)$ וגם $q = 1(\mod p)$ אבל

שימו לב שמכיוון ש$p \neq q$ מתקיים ב.ה.כ ש$p > q$ ואזי $q \not\equiv 1(\mod p)$. סתירה.
מ.ש.ל
דוגמה:
$99 = 3^2 \cdot 11$ לא פשוטה.
תרגיל:
תהא G חבורה סופית ותהא $K \leq G$ ת"ח. תהא $H \leq K$ ת"ח $p-$סילו של K.
הוכיחו שקיימת ת"ח $P \leq G$ $p-$סילו של Gכ ש$H = P \cap K$.
שרטוט מסייע:

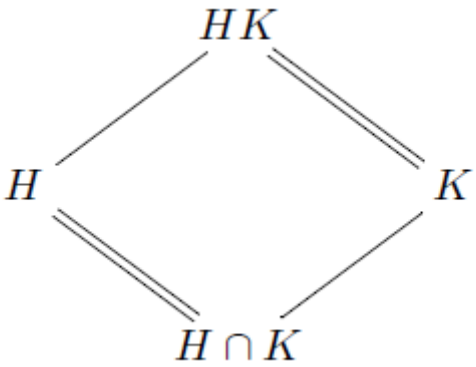


פתרון:
. H ת"ח של K ולכן הסדר שלה הוא חזקת p. לכן Hת"ח p של G.
לכן היא מוכלת בת"ח $p-$סילו של G שנסמנה P. כלומר $H \leq P \Leftarrow H \leq P \cap K$.
נוכיח ש־ $|H| = |P \cap K|$
וכך נקבל את הדרוש.
$P \cap K \leq K$ היא ת"ח p של K.לכן $P \cap K$ מוכלת באחד מהצמודים של H (מוכלת באחד מהסילואים שכולם צמודים לH). כלומר קיים g:
$|H| = |gHg^{-1}| \leq |P \cap K| \Rightarrow P \cap K \leq gHg^{-1}$ וקיבלנו הדרוש. (שכן כבר ראינו ש$|H| \leq |P \cap K|$
ולכן בסה"כ נקבל $|H| = |P \cap K|$. מ.ש.ל.
תזכורת: ראינו שלכל $H \leq G$ מתקיים $H \lhd N(H)$ כאשר $N(H) = \{g \in G : gHg^{-1} = H\}$
תרגיל:
תהא H־ ת"ח $p-$סילו של G. הוכיחו ש־Hהיא ת"ח p־סילו יחידה של $N(H)$.
פתרון:
למעשה מספיק להוכיח שהיא ת"ח $p-$סילו של $N(H)$ שכן כיוון ש$H \lhd N(H)$נקבל שהיא יחידה.
נניח $|G| = p^k m$ אזי $|H| = p^k$ מתקיים $H \leq N(H) \leq G$ ולכן קיים $t \mid m$: $|N(H)| = p^k t$ ולכן H ת"ח $p-$סילו של $N(H)$. מ.ש.ל.

תרגיל משמעותי בתרגול:
טענה: אם כל ת"ח הסילו של G הן נורמליות, אזי G היא מכפלה ישרה פנימית שלהן.
שימוש: בהנתן חבורה Gבעלת סדר $|G| = 1235 = 5 * 13 * 19$. מתקיים $n_5 = n_{13} = n_{19} = 1$. כל תת"ח שלה נורמליות ולכן $G \cong \mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19} \cong \mathbb{Z}_{1235}$.
המסקנה הנובעת היא שכל חבורה מסדר 1235 היא ציקלית
הוכחה:
שימו לב שהגדרנו מכפלה ישרה פנימית ל־2 ת"ח . ההגדרה למס' ת"ח היא:
G מכפלה פנימית של $A_1...A_n \leq G$ אם:
1. $\forall 1 \leq i \leq n : A_i \triangleleft G$
2. $\{e] = A_j \cap (\prod_{i \neq j} A_i)$
3. $\prod_{i=1}^{n} A_i = G$.

למה:
אם $A_1, ..., A_n \triangleleft G$ מסדרים זרים בזוגות אזי: $|A_1 \cdot A_2 ... \cdot A_n| = |A| \cdot |A_2| ... \cdot |A_n|$.
הוכחה:

באינדוקציה על n:
אם $n = 1$ הטענה ברורה.
עבור $n = 2$לפי איזו' II:



$|A_1 A_2| = \frac{|A_1| \cdot |A_2|}{|A_1 \cap A_2|}$. אצלנו $|A_1 \cap A_2| = 1$ ונקבל הדרוש.
נניח נכונות ל־n ונוכיח ל$n + 1$:
לפי המקרה של $n = 2$ וכיוון ש $|A_1 \cdot ... \cdot A_n| = |A_1|...|A_n|$
$|A_1....A_n \cdot A_{n+1}| = |A_1 \cdot ...A_n| \cdot |A_{n+1}| = |A_1| \cdot |A_2|...|A_n| \cdot |A_{n+1}|$.
מ.ש.ל ללמה.
בחזרה לטענה שלנו:
נניח $|G| = p_1^{k_1}...p_t^{k_t}$ ונסמן את ת"ח $p-$סילו ב$P_1...P_t$ הן נורמליות (לפי הנתון) והסדרים שלהם זרים בזוגות. לכן: יהי i כלשהו. מתקיים:
$1 = (|P_i|, |\prod_{j \neq i} P_j|)$ ולכן $\{e\} = P_i \cap (\prod_{j \neq i} P_j)$.
כמו כן:
$|G| = \prod_{i=1}^{t} |P_i| = |\prod_{i=1}^{t} P_i|$ ולכן $\prod_{i=1}^{t} P_i = G$. מ.ש.ל