פתרון תרגיל בית 10 במבוא לתורת החבורות
סמסטר א' תש"ף

שאלה 1. תהי G חבורת-p סופית שאינה מסדר p.

א. הוכיחו כי G אינה פשוטה.

ב. תהי $H \lhd G$ ת"ח נורמלית מסדר p. הוכיחו כי $H \subseteq Z(G)$ (מה שאומר כמובן ש-$H \lhd Z(G)$).

פתרון.

א. ניזכר שתמיד $Z(G) \lhd G$ ולכן אם $Z(G)$ אינה ת"ח טריוויאלית של G, סיימנו. כי לחבורת-p יש מרכז לא טריוויאלי, $Z(G) \neq \{e\}$, לכן אם $Z(G) \neq G$, סיימנו. אחרת, G אבלית ולכן כל ת"ח שלה נורמלית, אז מספיק למצוא ת"ח לא טריוויאלית כלשהי. משפט קושי יספק לנו כזו (גם ההכללה של משפט סילו הראשון).

ב. $H \lhd G$ ולכן סגורה להצמדה, כלומר: לכל $x \in H$, מתקיים: $\operatorname{conj}(x) \subseteq H$ ולכן $|\operatorname{conj}(x)| \leq p$. אך מכיוון שלכל $x \neq e$ מתקיים: $e \notin \operatorname{conj}(x)$, אז $|\operatorname{conj}(x)| \leq p-1$.
לפי טענה שראינו, סדר מחלקת צמידות מחלק את סדר החבורה שהוא p^n, ולכן $|\operatorname{conj}(x)| = 1$ לכל $x \in H$. מכאן ש- $x \in Z(G)$ לכל $x \in H$, כלומר: $H \subseteq Z(G)$.

שאלה 2. יהי p ראשוני.

א. הוכיחו כי כל חבורה מסדר p^2 היא אבלית.

ב. תהי $P \leq S_p$ תת־חבורת p-סילו. הוכיחו כי P אבלית.

ג. (רשות) תהי $P \leq S_{p^2}$ תת־חבורת p-סילו. הוכיחו שיש לה תת־חבורה אבלית $H \leq P$ שהיא מסדר p^p. רמז: מצאו תחילה $H \leq S_{p^2}$ כזו, ואחר כך טפלו בעניין P.

פתרון.

א. תהי G חבורה מסדר p^2. נניח בשלילה שהיא לא אבלית, כלומר: יש $g \in G \setminus Z(G)$. כיוון ש-G חבורת-p, המרכז שלה לא טריוויאלי. בסך הכל נובע ש- $|Z(G)| = p$. לכן $|C_G(g)| \geq p+1$ (כל איבר במרכָּז מתחלף עם g וכמובן גם הוא עצמו), מכאן ש-$|C_G(g)| = p^2$ לפי משפט לגרנז' (מְרַכֵּז הוא תמיד ת"ח), ולכן $C_G(g) = G$, כלומר $g \in Z(G)$, סתירה.

ב. החזקה הגבוהה ביותר של p שמחלקת את $|S_p| = p!$ היא כמובן p. לכן $|P| = p$, וכל חבורה מסדר ראשוני היא ציקלית, ולכן אבלית.

ג. כל תת־חבורות p-סילו הן צמודות, ולכן איזומורפיות. כלומר אם נמצא תת־חבורת p-סילו אחת P, סיימנו, כי נעביר את $H \leq P$ על ידי הצמדה לכל תת־חבורת p-סילו אחרת. בנוסף כל תת־חבורת-p של S_{p^2} מוכלת בתת־חבורת p-סילו, ולכן אם נמצא תת־חבורת-p של S_{p^2} שהיא אבלית מסדר p^p, סיימנו. נבחר את

$$\begin{aligned}K &= \langle\{(ip+1, ip+2, \ldots, ip+p) \mid 0 \leq i < p\}\rangle \\ &= \big\langle(1,2,\ldots,p),(p+1,p+2,\ldots,2p),\ldots,((p-1)p+1,(p-1)p+2,\ldots,p^2)\big\rangle\end{aligned}$$

וקל להוכיח $K \cong \mathbb{Z}_p^p$ כי כל המחזורים האלו מאורך p הם זרים. אגב, תת־החבורה P היא בהכרח מסדר p^{p+1} כי זו החזקה הגבוהה ביותר של p שמחלקת את $(p^2)!$, כי יש שם p כפולות של p ופעם אחת כפולה של p^2.

באופן כללי החבורה S_{p^2} פועלת על הקבוצה $A = \{1, \ldots, p^2\}$. נחלק את הקבוצה A ל-p גושים שכל אחד מהם כולל p איברים (ואיחוד הגושים הוא A) ונחשוב עליהם כמחזורים מאורך p. אז נבחר את H להיות תת־החבורה של כל התמורות ששומרות על החלוקה הזו לגושים, ושומרת את בתוך כל גוש על הסידור הציקלי של המחזור שהוא מייצג.

שאלה 3. תהי G חבורה סופית, ונניח כי מספר ראשוני p מחלק את $|G|$. הוכיחו שקיים $z \in G$ מסדר p כך ש-$C_G(z)$ מכיל תת־חבורת p-סילו של G. רמז: לתת־חבורת p-סילו יש מרכז לא טריוויאלי.

פתרון. תהי $P \leq G$ תת־חבורת p-סילו. אזי P היא חבורת-p לא טריוויאלית כי $p \mid |G|$. לכן יש לה מרכז לא טריוויאלי $Z(P)$. גם $Z(P)$ היא חבורת-p, ולפי משפט קושי קיים $z \in Z(P)$ מסדר p. לפי הגדרת המרכז, לכל $g \in P$ מתקיים כי $gz = zg$ ולכן

$$P \subseteq \{g \in G \mid gz = zg\} = C_G(z)$$

כלומר האיבר $z \in Z(P) \subseteq G$ הוא האיבר המבוקש.

שאלה 4. תהי G חבורה מסדר אי-זוגי. הוכיחו שאם $|G| < 21$ אז G אבלית. רשות: נסו למצוא חבורה לא אבלית מסדר 21.

פתרון. ראשית, נשים לב שאם הסדר של G הוא $1,3,5,7,11,13,17,19$, אז G ציקלית וסיימנו (ודאו שברור לכם למה).

נשאר לטפל במקרים שבהם הסדר הוא 9 או 15. אם $|G| = 9$, לפי שאלה 2, סעיף א', G אבלית.

אם $|G| = 15$, נובע ממשפטי סילו שיש ת"ח 3-סילו יחידה (מסדר 3), נקרא לה H, ות"ח 5-סילו יחידה (מסדר 5), נקרא לה K. מהיחידות נובע ש- $H, K \lhd G$.

כיוון ש-H, K מסדרים ראשוניים שונים, $H \cap K = \{e\}$, ולפי נוסחת המכפלה, $|HK| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{3 \cdot 5}{1} = 15 = |G|$. מאחר ש- $HK \subseteq G$, זה אומר ש- $HK = G$.

כל התנאים לכך ש-G היא מכפלה ישרה פנימית של H, K מתקיימים, ולכן לפי משפט, $G = HK \cong H \times K$, ומכאן ש-$G \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$ ולכן ציקלית ואבלית.

שאלה 5. יהיו $p \leq q$ ראשוניים (לאו דווקא שונים).

א. הוכיחו שכל חבורה מסדר pq^n עבור $n \in \mathbb{N}$ אינה פשוטה.

ב. הוכיחו שגם חבורות מסדר 56 או 63 אינן פשוטות (זה שונה מהסעיף הקודם).

ג. (רשות, קשה מאוד!) תהי חבורה G מסדר $p^a q^b$ עבור $a, b \in \mathbb{N}$. הוכיחו כי G אינה פשוטה לכמה שיותר זוגות אפשריים (a, b) שאתם מצליחים, שלא טיפלנו בהם עד כה בכיתה או בתרגיל.

רמז: התשובה היא לכל a, b. הוכחה לכך דורשת בדרך כלל כמה קורסים.

פתרון.

א. אם $p=q$, אז מדובר בחבורת-p מסדר p^2 לפחות. תהי G חבורה מסדר p^{n+1}. אם היא לא אבלית, אז נבחר $N=Z(G)$ שידוע לנו שהיא נורמלית. נשים לב כי $N\neq\{e\}$ לפי טענה מן ההרצאה, וגם $N\neq G$, כי G לא אבלית. אם G אבלית, אז נבחר איבר $g\in G$ מסדר p, שקיים לפי קושי. תת־החבורה $\langle g\rangle$ היא תת־חבורה נורמלית, כי G אבלית, והיא לא טריוויאלית כי היא מסדר $p<p^{n+1}$.
כעת נניח $p<q$. לפי משפט סילו III נקבל כי $n_q|p$ וגם $n_q\equiv 1\,(\mathrm{mod} q)$. מפני ש-$p<q$, אז $p\not\equiv 1\,(\mathrm{mod} q)$. לכן בהכרח $n_q=1$ ולפי המסקנה ממשפטי סילו, זה אומר שיש תת־חבורה q-סילו נורמלית, והיא אינה טריוויאלית.

ב. נחשב $63=3^2\cdot 7$ ו-$56=2^3\cdot 7$. שימו לב שבמונחי הסעיף הקודם $p>q$. לפי משפט סילו III עבור חבורה מסדר 63 נקבל $n_7|3^2$ ולכן $n_7\in\{1,3,9\}$. האפשרות היחידה שבה $n_7\equiv 1\,(\mathrm{mod} 7)$ היא $n_7=1$ ולכן ישנה תת־חבורה 7-סילו נורמלית.
באופן דומה בחבורה מסדר 56 נקבל $n_7|2^3$ ולכן $n_7\in\{1,2,4,8\}$. אם $n_7=1$, סיימנו כמו מקודם. אחרת, בהכרח $n_7=8$. נזכר שתת־חבורות שונות מסדר ראשוני נחתכות טריוויאלית. אצלנו תת־חבורות 7-סילו הן מסדר ראשוני ולכן יש בדיוק $(7-1)\cdot 8=48$ איברים מסדר 7. נשארנו עם $56-48=8$ שמונה איברים שיספיקו רק לתת־חבורת 2-סילו אחת, ולכן קיבלנו $n_2=1$. אגב, יש 12 חבורות מסדר 56 שבהן $n_7=1$ ורק אחת שבה $n_7\neq 1$.

ג. זו מסקנה מיידית של משפט ברנסייד.

שאלה 6. תהי חבורה G מסדר p^tm, כאשר p ראשוני, $m>1$ טבעי שזר ל-p ו-$t\in\mathbb{N}$.

א. נניח ש-$|G|$ לא מחלק את $m!$ (ניתן להסתפק בכך ש-$|G|$ לא מחלק את $n_p!$). הוכיחו כי G לא פשוטה. רמז: העידון של משפט קיילי.

ב. הוכיחו שחבורות מסדרים 36, 150 או 160 אינן פשוטות.

פתרון.

א. תהי P תת־חבורת p-סילו של G, ויהי $N_G(P)$ המנרמל שלה. ראינו בכיתה כי $n_p=[G:N_G(P)]$, שהוא גם מספר תת־החבורות הצמודות ל-P. אם G פשוטה, אז ההומומורפיזם

$$\varphi\colon G\to S_{n_p}$$

מהעידון של משפט קיילי הוא שיכון, כי φ אינו ההומומורפיזם הטריוויאלי והגרעין $\ker\varphi$ הוא תת־חבורה נורמלית של G. לכן $|\mathrm{im}\,\varphi|=|G|$ מחלק את $|S_{n_p}|=n_p!$.
אבל לפי משפט סילו III אנחנו יודעים כי $n_p|m$, ולכן $|G|$ מחלק גם את $m!$. זו סתירה לנתון, ולכן G אינה פשוטה.

ב. נחשב $36=2^2\cdot 3^2$. נפעיל את הסעיף הקודם עם $p=2$, ואכן $36\nmid 4!$. לכן אין חבורה פשוטה מסדר 36.
נחשב $150=2\cdot 3\cdot 5^2$. הפעם יש להפעיל את הסעיף הקודם עם $p=5$, ואכן $150\nmid 6!$.
לסיום, נחשב $160=2^5\cdot 5$. נפעיל את הסעיף הקודם עם $p=2$, ואכן $160\nmid 5!$.

שאלה 7. (רשות) תהי G חבורה מסדר n. הוכיחו כי השיכון $G\to S_n$ ממשפט קיילי אינו שיכון לתוך A_n אם ורק אם תת־חבורה 2-סילו של G היא ציקלית לא טריוויאלית. רמז: העזרו בשאלה מתרגיל בית קודם.

בהצלחה!