פתרון תרגיל בית 11 בתורת החבורות
88-218 סמסטר א' תש"ף

שאלה 1 (חימום)**.** מצאו את הסדרים של כל תת־חבורות סילו של S_5. מי מהן אבליות?

פתרון. ידוע לנו כי $|S_5| = 5! = 2^3 \cdot 3 \cdot 5$. לכן (כל) תת־חבורת 2-סילו של S_5 היא מסדר 8, תת־חבורת 3-סילו היא מסדר 3, תת־חבורת 5-סילו היא מסדר 5 וכל השאר הן טריוויאליות. כל חבורה מסדר 3 או 5 היא ציקלית (כי היא מסדר ראשוני), ולכן אבלית. אנחנו יודעים שניתן לשכן את D_4 ב-S_4, ולכן גם ב-S_5. מפני ש-D_4 היא מסדר 8, אז כל תת־חבורת 2-סילו של S_5 איזומורפית ל-D_4, שאינה אבלית.

שאלה 2 (חזרה)**.** תהי $H \leq \mathbb{Q}$ תת־חבורה מאינדקס סופי. הוכיחו כי $H = \mathbb{Q}$.
הסיקו כי גם ל-$\mathbb{Q}/\mathbb{Z}$ אין תת־חבורות נאותות מאינדקס סופי.

פתרון. נניח $n = [\mathbb{Q} : H] \in \mathbb{N}$. מפני ש-$\mathbb{Q}$ אבלית, אז H תת־חבורה נורמלית. לפי תרגיל מהכיתה לכל איבר $a \in \mathbb{Q}$ יתקיים $n \cdot a \in H$. לכן $n\mathbb{Q} \subseteq H$. אבל לכל $a \in \mathbb{Q}$, מתקיים כי $a = n\frac{a}{n} \in n\mathbb{Q}$. כלומר $\mathbb{Q} \subseteq n\mathbb{Q} \subseteq H \subseteq \mathbb{Q}$. לכן $H = \mathbb{Q}$.
לחלק השני בשאלה, פשוט משתמשים במשפט ההתאמה. תת־החבורות מאינדקס סופי של $\mathbb{Q}/\mathbb{Z}$ הן מן הצורה $H/\mathbb{Z}$ כאשר H היא תת־חבורה מאינדקס סופי של $\mathbb{Q}$ שמכילה את $\mathbb{Z}$. אבל יש רק את $H = \mathbb{Q}$, ולכן תת־החבורה היחידה של $\mathbb{Q}/\mathbb{Z}$ מאינדקס סופי היא $\mathbb{Q}/\mathbb{Z}$.

שאלה 3. יהי p ראשוני.

א. (חימום) תהי $P \leq S_p$ תת־חבורת p-סילו. הוכיחו כי P אבלית.

ב. תהי $P \leq S_{p^2}$ תת־חבורת p-סילו. הוכיחו שיש לה תת־חבורה אבלית $H \leq P$ שהיא מסדר p^p.

ג. (קשה) עבור תת־החבורה H מהסעיף הקודם, הוכיחו שכל תמורה $\sigma \in S_{p^2}$ שאינה שייכת ל-H לא מתחלפת עם כל איברי H. בפרט, תת־החבורה $P \leq S_{p^2}$ לא אבלית.

פתרון.

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

ב. 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

$$\begin{aligned} H &= \langle \{(ip+1, ip+2, \ldots, ip+p) \,|\, 0 \leq i < p\} \rangle \\ &= \left\langle (1,2,\ldots,p), (p+1, p+2, \ldots, 2p), \ldots, ((p-1)p+1, (p-1)p+2, \ldots, p^2) \right\rangle \end{aligned}$$

קל להוכיח $H \cong \mathbb{Z}_p^p$ כי כל p המחזורים שיוצרים את K הם מאורך p וזרים בזוגות. החבורה $\mathbb{Z}_p^p$ היא אבלית.

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

ג. במילים אחרות מבקשים להוכיח כי $C_{S_{p^2}}(H) = H$.
אם $\sigma \in S_{p^2}$ מתחלף עם כל האיברים של H, נראה כי $\sigma \in H$. נניח שמדובר ב-H מהסעיף הקודם עם החלוקה לגושים. אם σ מעבירה איבר באחד מן הגושים לגוש אחר, אז σ לא תתחלף עם התמורות שמקבעות את האיברים של הגוש הראשון ומזיזות את האיברים של הגוש השני. לכן σ גם שומרת על החלוקה לגושים. אם σ לא שומרת על הסידור הציקלי בתור מחזור של גוש מסוים, אז היא לא תתחלף עם המחזור הזה, כי הוכחתם בעבר ששני מחזורים לא זרים מתחלפים אם ורק אם הם חזקה אחד של השני.
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. לכן יש איברים ב-P שאינם ב-H, ולכן הם לא מתחלפים עם איברי H. כלומר P לא אבלית.

שאלה 4. 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 הן לא פשוטות. זה שונה מהסעיף הקודם.

ג. (רשות מאוד קשה!) 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 $n_q \equiv 1 \pmod{q}$. מפני ש-$p < q$, אז $p \not\equiv 1 \pmod{q}$. 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 $n_7 \equiv 1 \pmod{7}$ 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 $48 = 8 \cdot (7 - 1)$ 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 5. 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.

פתרון. תהי $P \leq G$ תת־חבורת p-סילו. אזי P היא חבורת-p לא טריוויאלית כי $p||G|$. 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

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

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

שאלה 6. תהי חבורה G מסדר $p^t m$, 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 $|G| = |\operatorname{im}\varphi|$ 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. תהינה G, H חבורות.

א. הוכיחו כי $\operatorname{Inn}(G) \times \operatorname{Inn}(H) \cong \operatorname{Inn}(G \times H)$

ב. הוכיחו כי $\operatorname{Inn}(S_3) \cong S_3$ ומצאו אוטומורפיזם שאינו פנימי של החבורה $S_3 \times S_3$.
רמז: נוח לחשוב על $S_3 \times S_3$ כתת־חבורה של S_6 ושם לחפש אוטומורפיזם.

פתרון.

א. ראינו שלכל חבורה $G/Z(G) \cong \operatorname{Inn}(G)$. נעזר בכך ש-$Z(G \times H) = Z(G) \times Z(H)$ (ודאו שאתם יודעים להוכיח את זה!) ולכן

$$\begin{aligned}\operatorname{Inn}(G \times H) &\cong (G \times H)\,/Z(G \times H) = (G \times H)\,/\,(Z(G) \times Z(H)) \\ &\cong (G/Z(G)) \times (H/Z(H)) \cong \operatorname{Inn}(G) \times \operatorname{Inn}(H)\end{aligned}$$

כאשר האיזומורפיזם בין השורות הוא מקרה פרטי של שאלה מתרגיל בית 9.

ב. אנחנו יודעים כי $Z(S_3)=\{\mathrm{id}\}$ לפי תרגיל שראינו בכיתה. לכן

$$\mathrm{Inn}(S_3)\cong S_3/Z(S_3)=S_3/\{\mathrm{id}\}\cong S_3$$

נסמן $G=S_3\times S_3$ ונבחר $\varphi\colon G\to G$ להיות

$$\varphi(a,b)=(b,a)$$

אנחנו רוצים להראות כי $\varphi\in\mathrm{Aut}(G)\setminus\mathrm{Inn}(G)$ (אגב ל-G יש 36 אוטומורפיזמים לא פנימיים). קל לראות ש-φ על. לכן φ חח"ע, כי G סופית. זה אכן הומומורפיזם כי

$$\varphi(a_1,b_1)\varphi(a_2,b_2)=(b_1,a_1)(b_2,a_2)=(b_1b_2,a_1a_2)=\varphi(a_1a_2,b_1b_2)$$

למה הוא לא פנימי? אילו φ היה פנימי, אז היה איבר $(a,b)\in G$ כך ש-

$$\begin{aligned}\varphi\left((12),(12)\right)&=(a,b)\left((12),(12)\right)(a,b)^{-1}=\left(a\,(12)\,a^{-1},b\,(12)\,b^{-1}\right)\\&=\left((a(1),a(2)),(b(1),b(2))\right)=\left((12),(12)\right)\end{aligned}$$

לכן $a,b\in C_{S_3}((12))=\{\mathrm{id},(12)\}$. אם $a=b=\mathrm{id}$, אז $\varphi=\mathrm{id}_G$ ונקבל

$$\varphi((12),(13))=\left((a(1),a(2)),(b(1),b(3))\right)=\left((12),(13)\right)$$

ששונה מ-$((13),(12))$, כדרוש מהגדרת φ. אם $b=(12)$ ו-$a\in\{\mathrm{id},(12)\}$, אז

$$\varphi((12),(13))=\left((a(1),a(2)),(b(1),b(3))\right)=\left((12),(23)\right)$$

ששונה מ-$((13),(12))$, כדרוש מהגדרת φ. אם $a=(12)$ ו-$b\in\{\mathrm{id},(12)\}$, אז

$$\varphi((13),(12))=\left((a(1),a(3)),(b(1),b(2))\right)=\left((23),(12)\right)$$

ששונה מ-$((12),(13))$, כדרוש מהגדרת φ. לכן φ אינו אוטומורפיזם פנימי.
אם חושבים על שיכון $S_3\times S_3\to S_6$ שבו הרכיב הראשון הוא של תמורות המקבעות את $\{4,5,6\}$ וברכיב השני תמורות המקבעות את $\{1,2,3\}$, אז φ שבחרנו הוא הצמדה בתמורה $(14)(25)(36)$, ששייכת למנרמל של G ב-S_6, אבל לא ל-G.

שאלה 8. תהי G חבורה.

א. הוכיחו כי $\mathrm{Inn}\,(G)\lhd\mathrm{Aut}(G)$. רמז: בדקו מי הוא $\varphi\circ\gamma_g\circ\varphi^{-1}$ בכל בחירה.

ב. הוכיחו שאם $Z(G)=\{e\}$, אז $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))=\{\mathrm{id}\}$ ובפרט מתקיים $Z(\mathrm{Aut}(G))=\{\mathrm{id}\}$.

פתרון.

א. נעזר ברמז כדי להראות ש-$\mathrm{Inn}(G)$ סגורה להצמדה. יהי $\varphi\in\mathrm{Aut}(G)$ ויהי $\gamma_g\in\mathrm{Inn}(G)$. אז לכל $x\in G$ מתקיים

$$\begin{aligned}\varphi\circ\gamma_g\circ\varphi^{-1}(x)&=\varphi(\gamma_g(\varphi^{-1}(x)))=\varphi(g\cdot\varphi^{-1}(x)\cdot g^{-1})\\&=\varphi(g)\cdot\varphi(\varphi^{-1}(x))\cdot\varphi(g^{-1})=\varphi(g)\cdot x\cdot\varphi(g)^{-1}=\gamma_{\varphi(g)}(x)\end{aligned}$$

ולכן $\varphi\circ\gamma_g\circ\varphi^{-1}=\gamma_{\varphi(g)}\in\mathrm{Inn}(G)$.

ב. יהי $\varphi \in C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G))$, ונרצה להראות כי $\varphi = \mathrm{id}$. לפי הגדרה φ מתחלף עם כל אוטומורפיזם פנימי. כלומר $\varphi \circ \gamma_g = \gamma_g \circ \varphi$ לכל $g \in G$. נכפיל ב-φ^{-1} מימין ובעזרת הרמז מהסעיף הקודם נקבל

$$\gamma_{\varphi(g)} = \varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_g$$
$$\gamma_g^{-1}\gamma_{\varphi(g)} = \mathrm{id}$$

ראינו בכיתה כי $\gamma_g^{-1} = \gamma_{g^{-1}}$ ולכן $\gamma_g^{-1}\gamma_{\varphi(g)} = \gamma_{g^{-1}\varphi(g)}$. כלומר לכל $x \in G$ מתקיים

$$\gamma_{g^{-1}\varphi(g)}(x) = \mathrm{id}(x)$$
$$g^{-1}\varphi(g)x\left(g^{-1}\varphi(g)\right)^{-1} = x$$
$$g^{-1}\varphi(g)x = xg^{-1}\varphi(g)$$

לכן $g^{-1}\varphi(g) \in Z(G)$, אך G חסרת מרכז לפי הנתון, ולכן $g^{-1}\varphi(g) = e$. כלומר $\varphi(g) = g$ לכל $g \in G$, או במילים אחרות $\varphi = \mathrm{id}$, כדרוש.
לסיום, המֶרְכָּז של חבורה הוא חיתוך כל המְרַכְּזִים, ולכן מוכל בכל אחד מהם. כלומר $Z(\mathrm{Aut}(G)) \subseteq C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = \{\mathrm{id}\}$ ולכן גם $Z(\mathrm{Aut}(G)) = \{\mathrm{id}\}$.

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה שלחו לנו את הפתרון שלהן.

שאלה 9. 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!