פתרון תרגיל בית 9 בתורת החבורות
88-218 סמסטר א' תשע"ט

שאלות חימום

שאלות החימום הן שאלות קלות יותר בדרך כלל, אבל כדאי מאוד לוודא שיודעים איך לפתור אותן, אפילו בעל פה.

שאלה 1.
תהי G חבורה סופית, ויהי $g \in G$ איבר מסדר k. הוכיחו שהשיכון ממשפט קיילי שולח את g למכפלת מחזורים זרים מאורך k.

פתרון. יהי $x \in G$. מה גודל הקבוצה $\{gx, g^2x, g^3x, \dots\}$? מתי $g^ix = g^jx$? כמו כן שימו לב שבשיכון ממשפט קיילי אם $g \neq e$, אז כל איבר $x \in G$ נשלח לאיבר אחר.

שאלה 2. מצאו בעזרת משפט קיילי שיכון $\varphi \colon U_8 \to S_4$ וכתבו אותו באופן מפורש.

פתרון. אנחנו יודעים כי $U_8 = \{1, 3, 5, 7\}$ לפי תרגיל בית 3. ניתן לכל איבר שם חדש

$$1 \mapsto 1, \qquad 3 \mapsto 2, \qquad 5 \mapsto 3, \qquad 7 \mapsto 4$$

ברור ש-1 נשלח ל-$\mathrm{id} \in S_4$. לשאר האיברים נעזר בטבלת הכפל שחישבנו בעבר, כדי לחשב לאן שאר האיברים נשלחים. למשל כפל משמאל ב-3 שולח את 1 ל-3 ולכן התמורה שאליה נשלח את 3 תעביר את 1 ל-2. חישוב סופי:

$$1 \mapsto \mathrm{id}, \qquad 3 \mapsto (12)(34), \qquad 5 \mapsto (13)(24), \qquad 7 \mapsto (14)(23)$$

שאלה 3. 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, 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.

שאלות רגילות

שאלה 4. יהיו $p \leq q$ ראשוניים (לאו דווקא שונים).

1. הוכיחו שכל חבורה מסדר pq^n עבור $n \in \mathbb{N}$ אינה פשוטה.
2. הוכיחו שגם חבורות מסדר 56 או 63 הן לא פשוטות. זה שונה מהסעיף הקודם.

פתרון.

1. 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.

2. נחשב $56=2^3\cdot 7$ ו-$63=3^2\cdot 7$. 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 $n_7\neq 1$.

שאלה 5. יהי p מספר ראשוני.

1. תהי G חבורה לא אבלית מסדר p^3. הוכיחו כי $Z(G)=G'$.

2. תהי G חבורה סופית, ונניח $p\,|\,|G|$. הוכיחו שקיים $z\in G$ מסדר p כך ש-$C_G(z)$ מכיל תת־חבורת p-סילו של G. רמז: בחרו איבר השייך למרכז של תת־חבורת p-סילו.

פתרון.

1. מפני ש-G מסדר p^3, אז $|Z(G)|$ מחלק את p^3. לא יתכן שהסדר הוא p^3 כי G לא אבלית, ולא יתכן שהוא 1 כי G היא חבורת-p סופית. אם $|Z(G)|=p^2$, אז מפני שהמרכז הוא נורמלי נקבל שחבורת המנה $G/Z(G)$ מוגדרת, והיא מסדר p. לכן היא ציקלית, ולפי תרגיל שעשינו בכיתה נקבל כי G אבלית, שזו סתירה. לכן $|Z(G)|=p$. חבורת המנה $G/Z(G)$ היא מסדר p^2, ולכן אבלית (שוב, לפי מה שראינו בהרצאה). לכן $G'\leq Z(G)$. אבל G לא אבלית, ולכן $G'\neq\{e\}$. כלומר $|G'|=p$, ומשיוויון מספר האיברים נקבל $Z(G)=G'$.

2. 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^tm, כאשר p ראשוני, $m>1$ טבעי שזר ל-p ו-$t\in\mathbb{N}$.

1. 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.

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

פתרון.

1. 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 $|\operatorname{im}\varphi| = |G|$ מחלק את $\left|S_{n_p}\right| = n_p!$. אבל לפי משפט סילו III אנחנו יודעים כי $n_p|m$, ולכן $|G|$ מחלק גם את $m!$. זו סתירה לנתון, ולכן G אינה פשוטה.

2. 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.

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

2. 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.

1. 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 7 בתרגיל בית 7.

2. אנחנו יודעים כי $Z(S_3) = \{\mathrm{id}\}$. לכן

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

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

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

אנחנו רוצים להראות כי $\varphi \in \operatorname{Aut}(G) \setminus \operatorname{Inn}(G)$ (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-

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

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

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

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

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

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

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

ששונה מ-$((13),(12))$, 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.

1. הוכיחו כי $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$. רמז: הראו כי $\varphi \circ \gamma_g \circ \varphi^{-1} = \gamma_{\varphi(g)}$ לאיברים מתאימים.
2. הוכיחו שאם $Z(G) = \{e\}$, אז $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = \{\mathrm{id}\}$ ובפרט מתקיים $Z(\mathrm{Aut}(G)) = \{\mathrm{id}\}$.

פתרון.

1. 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

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

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

2. 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

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

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

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

לכן $g^{-1}\varphi(g) \in Z(G)$, אך G חסרת מרכז לפי הנתון, ולכן $e = g^{-1}\varphi(g)$. 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 $Z(\mathrm{Aut}(G)) = \{\mathrm{id}\}$.

שאלה 9. תהי G חבורה, ותהי $H \lneq G$ תת־חבורה המוכלת ממש ב-G.

1. הוכיחו שאם G סופית, אז גם האיחוד $\bigcup_{g \in G} gHg^{-1}$ מוכל ממש ב-G. רמז: העזרו באינדקס של המנרמל.
2. כעת לא נניח ש-G סופית, אבל שהאינדקס $[G:H] < \infty$ עדין סופי. הוכיחו שהסעיף הקודם עדין נכון. רמז: H מכילה תת־חבורה נורמלית וקצת משפטי האיזומורפיזם.

פתרון.

1. מספר תת־החבורות הצמודות ל-H ב-G שווה לאינדקס של המנרמל $[G:N_G(H)]$. נסמן $|G| = n$ ו-$[G:H] = m$. מפני ש-$H \subseteq N_G(H)$, אז $[G:N_G(H)] \leq m$. בהרצאה ראינו כי $\left|gHg^{-1}\right| = |H|$ לכל $g \in G$. מפני שכל תת־חבורה הצמודה ל-H מכילה את איבר היחידה, אז נוכל לחסום את גודל האיחוד

$$\left|\bigcup_{g \in G} gHg^{-1}\right| \leq 1 + [G:N_G(H)]\left(|H|-1\right) \leq 1 + m\left(|H|-1\right)$$
$$= 1 + m\left(\frac{n}{m} - 1\right) = n - (m-1) < n = |G|$$

כשאי-השיוויון האחרון מסתמך על כך ש-H מוכלת ממש ב-G ולכן $m > 1$.

2. ראינו בכיתה שאם H מאינדקס סופי, אז קיימת $N \leq H$ תת־חבורה נורמלית של G שגם היא מאינדקס סופי. בפרט G/N חבורה סופית. תהי $\pi \colon G \to G/N$ ההטלה הטבעית, שהיא אפימורפיזם. לפי משפט האיזומורפיזם הרביעי, כל תת־החבורות של G/N הן מן הצורה K/N בהתאמה לתת־חבורות $K \leq G$ המכילות את N. לכן H/N תת־חבורה המוכלת ממש ב-G/N (כי H מוכלת ממש ב-G).
נוכל להפעיל את הסעיף הקודם על החבורה G/N לגבי תת־החבורה H/N ונקבל שאיחוד כל תת־החבורות הצמודות ל-H/N מוכל ממש ב-G/N. אבל כל תת־החבורות הצמודות ל-H ב-G הן תמונה הפוכה של π של תת־חבורות הצמודות ל-H/N ב-G/N. לכן האיחוד $\bigcup_{g \in G} gHg^{-1}$ הוא התמונה ההפוכה של תת־קבוצה המוכלת ממש ב-G/N ומכאן שהוא מוכל ממש ב-G (הרי $\pi(G) = G/N$).

שאלות אתגר

שאלה 10. 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 בשאלת חימום 1