פתרון תרגיל בית 6 בקורס 89-214 סמסטר א' תשע"ד

נהלים: בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך ההגשה הוא בשבוע המתחיל ב-19.12.2013 לידי המתרגל.

שאלה 1. תהי G חבורה ותהי $H \leq G$ תת־חבורה.

1. הוכיחו כי לכל $g \in G$ מתקיים כי gHg^{-1} היא תת־חבורה של G האיזומורפית ל-H.
2. הסיקו מן הסעיף הקודם כי אם H היא תת־החבורה היחידה מסדר n של G, אז $H \lhd G$.

פתרון.

1. יהא $g \in G$. נגדיר את ההעתקה $\varphi : H \to gHg^{-1}$ (באופן טבעי) לפי $\varphi(h) = ghg^{-1}$. נראה כי φ היא הומומורפיזם: לכל $h_1, h_2 \in H$ מתקיים
$$\varphi(h_1h_2) = gh_1h_2g^{-1} = gh_1g^{-1}gh_2g^{-1} = \varphi(h_1)\varphi(h_2)$$
כדרוש. נראה כי φ היא חח"ע: אם $\varphi(h_1) = \varphi(h_2)$, אז $gh_1g^{-1} = gh_2g^{-1}$. בחבורה ניתן לצמצם משמאל ומימין ונקבל $h_1 = h_2$ כדרוש. נראה כי φ היא על: יהי $y \in gHg^{-1}$, כלומר יש $h \in H$ כך שמתקיים $y = ghg^{-1}$. מתקיים כי $\varphi(h) = ghg^{-1} = y$, ולכן φ על כדרוש.
2. תהא $H \leq G$ תת־חבורה יחידה מסדר n. לכל $g \in G$ מתקיים כי gHg^{-1} איזומורפית לתת־החבורה H לפי הסעיף הקודם. בפרט, יש ל-gHg^{-1} את אותו מספר איברים כמו ל-H. כלומר תת־החבורה gHg^{-1} היא מסדר n, ולכן gHg^{-1} היא H בעצמה. לכן לכל $g \in G$ מתקיים $gHg^{-1} = H$, ומכאן H תת־חבורה נורמלית של G.

שאלה 2. תהי G חבורה. אם קיימת $\varnothing \neq S \subseteq G$ תת־קבוצה סופית כך שמתקיים $G = \langle S \rangle$, נאמר כי G חבורה נוצרת סופית.

הוכיחו כי החבורה $(\mathbb{Q}^*, \cdot)$ אינה נוצרת סופית. הדרכה: מצאו איבר (מספר רציונלי) שלא נמצא בתת־חבורה $\langle x_1, \ldots, x_n \rangle$ שנוצרת על ידי מספר סופי של איברים $x_1, \ldots, x_n$.

פתרון. בכל תת־חבורה נוצרת סופית $\langle x_1, \ldots, x_n \rangle$ של $\mathbb{Q}^*$ אין את כל האיברים של $\mathbb{Q}^*$. נניח כי $x_i = \frac{a_i}{b_i}$ הוא שבר מצומצם לכל $1 \leq i \leq n$. ישנו מספר סופי של ראשוניים בפירוק של כל המכנים $\{b_1, \ldots, b_n\}$ לגורמים ראשוניים, אז נוכל לבחור ראשוני p שלא נמצא שם. אזי $\frac{1}{p} \notin \langle x_1, \ldots, x_n \rangle$, אבל $\frac{1}{p} \in \mathbb{Q}^*$, ולכן $\mathbb{Q}^*$ לא נוצרת סופית.

שאלה 3. בסעיפים הבאים תנו דוגמה שמפריכה את הטענות השגויות הבאות:

1. תהי G חבורה ותהינה $A, B \lhd G$ תת־חבורות נורמליות. אם $G/A \cong B$, אז $A \cong G/B$.

2. תהי G חבורה ותהינה $A, B \lhd G$ תת־חבורות נורמליות. $G/A \cong G/B$ אם ורק אם $A \cong B$.

3. כל זוג חבורות לא אבליות G, H מסדר 24 הן איזומורפיות.

פתרון.

1. ניתן כמה דוגמאות: נבחר את החבורה האבלית $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, ותת־החבורות $A = \mathbb{Z}_4 \times \{0\}$ ו-$B = \{0, 2\} \times \{0\}$. קל לבדוק כי $G/A \cong \{0\} \times \mathbb{Z}_2 \cong B$, אבל $G/B \cong \{0, 2\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \ncong A$.
דוגמה נוספת היא $G = (\mathbb{C}^*, \cdot)$. נגדיר הומומורפיזם $f : G \to G$ לפי $f(x) = x^2$. נבחר $A = \ker f = \{1, -1\}$. ההעתקה f היא אפימורפיזם (בדקו!) ולכן $G/A \cong \mathbb{C}^*$. כך נוכל לבחור $B = \mathbb{C}^*$, אבל $G/B \cong \{1\}$ היא החבורה הטריוויאלית שאינה איזומורפית לתת־החבורה A שהיא מסדר 2.
דוגמה נוספת שאפשר לבחור היא $G = D_4$ ושתי תת־חבורות נורמליות שלה $A = \langle \sigma \rangle$ ואת $B = Z(G) = \langle \sigma^2 \rangle$. אכן מתקיים $G/A \cong B$, אבל G/B אינה ציקלית ולכן לא איזומורפית ל-A.

2. נבחר שוב את $G = \mathbb{Z}_4 \times \mathbb{Z}_2$, הפעם עם תת־החבורות $A = \mathbb{Z}_4 \times \{0\}$ ו-$B = \{0, 2\} \times \mathbb{Z}_2$. נקבל כי

$$G/A \cong \{0\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \cong \{0, 2\} \times \{0\} \cong G/B$$

אבל A היא ציקלית ואילו B לא ציקלית ולכן $A \ncong B$.

3. נבחר למשל את החבורות D_{12} ואת S_4. בחבורה D_{12} יש איבר מסדר 12, אבל אין איבר מסדר זה בחבורה S_4.

שאלה 4. יהי F שדה. נזכיר כי חבורת הייזנברג מעל F היא חבורת המטריצות

$$H(F) = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in F \right\}$$

עם הפעולה של כפל מטריצות.

1. מצאו את המרכז $Z(H(F))$.

2. נניח כי F שדה סופי, כלומר מסדר $|F| = q \in \mathbb{N}$. מצאו את $[H(F) : Z(H(F))]$.
הערה: למרות שזה לא דרוש לפתרון השאלה, זה "טוב לדעת" שכל שדה סופי הוא מסדר חזקת ראשוני, כלומר קיים p ראשוני כך ש-$q = p^k$.

פתרון.

1. יש למצוא את האיברים שמתחלפים עם כל איבר של $H(F)$. יהא איבר

$$g = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

אנחנו נחפש את כל האיברים מן הצורה

$$h = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}$$

כך שייתקיים $gh = hg$. נבדוק מתי:

$$gh = \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} = hg$$

כלומר מתי

$$gh = \begin{pmatrix} 1 & a+x & z+ay+c \\ 0 & 1 & b+y \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & c+xb+z \\ 0 & 1 & y+b \\ 0 & 0 & 1 \end{pmatrix} = hg$$

עקב חילופיות הפעולות בשדה, מספיק לבדוק מתי $z+ay+c = c+xb+z$. כלומר מתי $ay = xb$. כזכור a,b,c הם פרמטרים "קבועים", ולכן המשתנים הם רק x,y. נשים לב כי אין חשיבות מהו הערך של z ולכן כל האיברים מן הצורה

$$\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ודאי במרכז של $H(F)$. מסתבר כי אלו הם האיברים היחידים במרכז. אם נבחר $x \neq 0$, אזי בסך הכל כדי ש-h לא יתחלף עם g נבחר y כך שיתקיים $ay \neq xb$, כלומר $y \neq a^{-1}xb$. כל עוד יש לפחות שני איברים בשדה (ויש לפי הגדרה), נוכל למצוא y כזה.
הערה: מכאן גם אפשר להראות כי המרכז $Z(H(F))$ איזומורפי למבנה החיבורי של השדה F.

2. אם $q = |F|$, אז בחבורה $H(F)$ ישנם q^3 איברים, לפי האפשריות הבלתי תלויות לבחירת a,b,c. במרכז $Z(H(F))$ ישנם q איברים, לפי מספר האפשריות לבחירת z בסעיף הקודם. האינדקס בחבורה סופית הוא פשוט חלוקת סדר החבורה בסדר תת־החבורה, ולכן $[H(F) : Z(H(F))] = q^2$.

שאלה 5. תהי חבורה G ותהי $H \leq G$ תת־חבורה. הוכיחו כי מתקיים $H \cap Z(G) \subseteq Z(H)$.

פתרון. יהי $x \in H \cap Z(G)$. אזי $x \in H$ וצריך להוכיח שלכל $h \in H$ מתקיים $xh = hx$. נתון כי $x \in Z(G)$ ולכן הוא מתחלף עם כל איברי G, ובפרט עם כל איברי H.

שאלה 6. בסעיפים הבאים תנו דוגמה לחבורה G ולתת־חבורה $H \leq G$ שמקיימות את התנאי הרשום.

1. הכלה ממש $H \cap Z(G) \subset Z(H)$ (בשאלה הקודמת הוכחתם הכלה חלשה). רמז: חבורה דיהדרלית.

2. הכלה ממש $Z(H) \subset Z(G)$.

3. הכלה ממש $Z(G) \subset Z(H)$.
4. $Z(G)$ לא מכיל את $Z(H)$ ולא מוכל בו.

פתרון.

1. נבחר $G = D_4$ ו-$H = \langle \sigma \rangle$. מתקיים $Z(G) = \langle \sigma^2 \rangle$ וגם $Z(H) = H$.
דוגמה נוספת היא $G = S_3$ ו-$H = A_3$. ידוע לנו כי המרכז $Z(G)$ הוא טריוויאלי. כמו כן ידוע לנו כי H היא מסדר 3 ולכן ציקלית, ולכן אבלית. כלומר $Z(H) = H$.
2. נבחר $G = \mathbb{Z}$ ו-$H = 2\mathbb{Z}$.
3. הדוגמאות מן הסעיף הראשון.
4. נבחר $G = D_4$ ו-$H = \langle \tau \rangle$.

שאלה 7. תהי G חבורה ותהי $A = \{a \in G : \exists n \in \mathbb{N}, a^n = e\}$ קבוצת האיברים מסדר סופי בחבורה G. הוכחנו בכיתה כי אם G אבלית, אז $A \leq G$ תת־חבורה (שנקראת תת־חבורת הפיתול של G).

1. נניח כי G אינה בהכרח אבלית, אבל בכל זאת A היא תת־חבורה של G. הוכיחו כי $A \lhd G$ היא תת־חבורה נורמלית.
2. תחת ההנחה של הסעיף הקודם, הוכיחו שבחבורת המנה G/A אין איברים מסדר סופי פרט לאיבר היחידה. רמז: הניחו בשלילה כי קיים איבר מסדר סופי בחבורה G/A, כלומר כי קיימים $x \notin A$ ו-$n \in \mathbb{N}$ כך שמתקיים $(xA)^n = e_{G/A} = A$, והגיעו לסתירה.

פתרון.

1. יהי $a \in A$ כך ש-$a^n = e$ עבור $n \in \mathbb{N}$ כלשהו. קל לראות כי לכל $g \in G$ מתקיים $\left(gag^{-1}\right)^n = e$ ולכן $gag^{-1} \in A$.
2. נשתמש ברמז: נניח וקיים איבר $x \in G$ שאינו ב-A כך שמתקיים $(xA)^n = A$. כלומר $x^n \in A$. לכן קיים m כך ש-$\left(x^n\right)^m = e$ ולכן $x^{nm} = e$, שזו סתירה כי $x \notin A$.

שאלה 8. תהי G חבורה לא אבלית מסדר 8. הוכיחו כי קיימת תת־חבורה ציקלית של G מסדר 4. רמז: הסתכלו על הסדרים האפשריים לאיברי החבורה והוכיחו שקיים לפחות איבר אחד מסדר 4.

פתרון. תהא G חבורה לא אבלית. אנו מסתמכים בסעיף זה על הטענה שסדר איבר בחבורה סופית מחלק את סדר החבורה. לכן הסדרים האפשריים היחידים בחבורה מסדר 8 הם 1, 2, 4 או 8 (לא בהכרח כל הסדרים משתתפים).
יש רק איבר אחד מסדר 1 והוא איבר היחידה. לא ייתכן כי כל שאר האיברים הם מסדר 2, שכן לפי תרגיל שראינו נקבל כי G אבלית. אין בחבורה איבר מסדר 8, שכן אז היא תהיה ציקלית וכל חבורה ציקלית היא אבלית. מכאן קיים איבר, נאמר $a \in G$, שהוא מסדר 4. הסדר של איבר הוא הסדר של תת־החבורה הציקלית $\left\{e, a, a^2, a^3\right\}$ שהוא יוצר.

שאלת אתגר (רשות) הכלילו את השאלה האחרונה: תהא G חבורה לא אבלית מסדר 2^t עבור $t > 2$. אזי קיימת ב-G תת־חבורה ציקלית מסדר 4.

פתרון. באופן דומה לשאלה האחרונה, הסדרים האפשריים היחידים בחבורה מסדר 2^t (כאשר $t > 2$) הם רק מן הצורה 2^k עבור $k \in \{0, 1, 2, \ldots, t\}$. ישנו רק איבר אחד מסדר 1. הסדר של כל שאר האיברים לא יכול להיות 2, כי אז G אבלית. אין איבר מסדר 2^t, שכן אז החבורה ציקלית ולכן אבלית. לכן קיים איבר, נאמר $a \in G$ מסדר $o(a) = 2^k$ עבור $2 \leq k < t$.
אנו יודעים כי סדר תת־החבורה הציקלית שנוצרת על ידי a הוא $|\langle a \rangle| = 2^k$. תת־חבורה של תת־חבורה של G היא שוב תת־חבורה של G (זה נכון לכל חבורה). אנו טוענים כי בתת־החבורה $\langle a \rangle$ ישנו איבר מסדר 4, והוא ישאר מסדר 4 גם בחבורה G. מדובר באיבר $b = a^{2^{k-2}} \in \langle a \rangle$. בחרנו אותו כך שיתקיים $b^4 = e$. תת־החבורה שהוא יוצר היא

$$\langle b \rangle = \left\{ b^0 = b^4 = e = a^{2^k}, b^1 = a^{2^{k-2}}, b^2 = a^{2^{k-1}}, b^3 = a^{3 \cdot 2^{k-2}} \right\}$$

וזו כמובן חבורה ציקלית מסדר 4.

בהצלחה!