פתרון תרגיל בית 4 בתורת החבורות
88-218 סמסטר א' תשע"ח

הוראות בהגשת הפתרון יש לרשום שם מלא, מספר ת"ז ומספר קבוצת תרגול. הגישו את התרגיל בתרגול שלכם בשבוע המתחיל בתאריך 3.12.2017.

שאלות חימום

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

שאלה 1. תארו את כל המחלקות השמאליות ב-$\mathbb{Z}_{30}/\langle 3\rangle$.

פתרון. האיבר 3 הוא מסדר 10, ולכן $|\langle 3\rangle| = 10$. לפי משפט לגראנז' נקבל

$$|\mathbb{Z}_{30}/\langle 3\rangle| = \frac{|\mathbb{Z}_{30}|}{|\langle 3\rangle|} = \frac{30}{10} = 3$$

והמחלקות, עד כדי בחירת נציגים, הן $\{\langle 3\rangle, 1+\langle 3\rangle, 2+\langle 3\rangle\}$.

שאלה 2. תהי קבוצה $X=\{a,b\}$. הוכיחו שיש שתי פעולות שונות של $\mathbb{Z}_2$ על X. מי מהן טרנזיטיבית?

פתרון. ישנן בדיוק שתי פעולות. האחת, הפעולה הטריוויאלית המוגדרת לפי $g*a=a$, $g*b=b$ לכל $g\in\mathbb{Z}_2$. היא לא טרנזיטיבית, כי המסלול של a כולל רק את a.
הפעולה השנייה היא "הפעולה שהופכת", המוגדרת לפי

$$0*a=a,\quad 0*b=b,\quad 1*a=b,\quad 1*b=a$$

והיא כן טרנזיטיבית.

שאלות להגשה

שאלה 3. רמז: הסעיפים הבאים דורשים קצת קומבינטוריקה.

א. מצאו כמה איברים מסדר 6 יש בחבורה S_6.

ב. מצאו כמה איברים מסדר 2 יש בחבורה S_6.

פתרון. האם אתם יודעים מהו הקשר של (איחוד של) מחלקות צמידות לשאלה?

א. כל תמורה ניתן להציג כמכפלת מחזורים זרים, והסדר של התמורה יהיה הכמ"מ (lcm) של אורכי המחזורים בהצגה זו. הסבירו מדוע ב-S_6 ניתן לקבל כמ"מ 6 בשני אופנים בדיוק: מחזורים מאורך 6 $(a_1,\dots,a_6)$ שישנם $\binom{6}{6}(6-1)! = 5! = 120$ כאלו; ומכפלה של מחזור מאורך 3 עם חילוף $(a_1,a_2)(a_3,a_4,a_5)$ ויש $\binom{6}{2}\binom{6-2}{3}(3-1)! = 120$ כאלו. בסך הכל יש 240 איברים מסדר 6.
ודאו שאתם מבינים את החישובים הקומבינטוריים לעיל ויודעים כיצד להגיע אליהם.

ב. באופן דומה לסעיף הקודם, כאן יהיו לנו שלושה סוגי איברים מסדר 2: חילופים, מכפלה של שני חילופים ומכפלה של שלושה חילופים. בסך הכל ישנם

$$\binom{6}{2}+\binom{6}{2}\binom{4}{2}\frac{1}{2!}+\binom{6}{2}\binom{4}{2}\binom{2}{2}\frac{1}{3!}=15+45+15=75$$

איברים מסדר 2 בחבורה S_6.

שאלה 4. מצאו את האינדקסים הבאים:

א. $[U_{14}:\langle 11\rangle]$ רמז: משפט לגראנז'.

ב. $[\mathbb{Z}_8\times\mathbb{Z}_8:\langle(2,2)\rangle]$ רמז: משפט לגראנז'.

ג. $[\mathbb{Z}\times\mathbb{Z}:\langle(2,2)\rangle]$ רמז: קודם תארו את המחלקות השמאליות.

פתרון.

א. איברי U_{14} הם הטבעיים שקטנים וזרים ל-14. כלומר $U_{14}=\{1,3,5,9,11,13\}$. חישוב קצר יראה כי $\langle 11\rangle=\{1,9,11\}$, ואז לפי משפט לגרנז' נקבל שיש בדיוק שתי מחלקות שמאליות. כלומר $[U_{14}:\langle 11\rangle]=2$.

ב. הסדר של החבורה $\mathbb{Z}_8\times\mathbb{Z}_8$ הוא $8\cdot 8=64$, והסדר של תת־החבורה $\langle(2,2)\rangle$ הוא כסדר של האיבר $(2,2)$, שהוא 4. לכן לפי משפט לגראנז' $[\mathbb{Z}_8\times\mathbb{Z}_8:\langle(2,2)\rangle]=64/4=16$.

ג. נוכיח כי $[\mathbb{Z}\times\mathbb{Z}:\langle(2,2)\rangle]=\infty$ לפי זה שנראה ש-$\{(0,n)+\mathbb{Z}\times\mathbb{Z}\}$ היא קבוצה אינסופית של מחלקות שמאליות שונות (אלו לא כל המחלקות). אם $(0,n)+\mathbb{Z}\times\mathbb{Z}=(0,m)+\mathbb{Z}\times\mathbb{Z}$ זה אומר

$$(0,n)-(0,m)\in\langle(2,2)\rangle$$

כלומר ש-$(2k,2k)=(0,n-m)$ לאיזשהו $k\in\mathbb{Z}$. לכן $n-m=0$, ולכן $n=m$. כלומר יש אינסוף מחלקות שמאליות שונות.

שאלה 5. תהי G חבורה ותהינה $H,K\leq G$ תת־חבורות סופיות שלה.

א. הוכיחו שאם $(|H|,|K|)=1$, אז $H\cap K=\{e\}$.

ב. יהי p מספר ראשוני. הוכיחו שאם $|H|=|K|=p$ וגם $H\neq K$, אז $H\cap K=\{e\}$.

פתרון.

א. ידוע לנו כי $H\cap K$ היא תת־חבורה של H ושל K. לכן לפי משפט לגראנז' מתקיים כי $|H\cap K|$ מחלק את $|H|$ ואת $|K|$. אך לפי הנתון הממ"מ של $|H|$ ו-$|K|$ הוא 1. לכן $|H\cap K|\leq 1$. אבל תמיד $|H\cap K|\geq 1$ כי איבר היחידה שייך אליו, ולכן קיבלנו כי $H\cap K=\{e\}$.

ב. יהי $x\in H\cap K$ איבר כלשהו. נניח בשלילה כי $x\neq e$. לכן $o(x)>1$. אנחנו יודעים כי $o(x)$ מחלק את $|H|$ ואת $|K|$, ולכן בהכרח $o(x)=p$. כלומר $|\langle x\rangle|=p$ ומפני ש-H,K הן חבורות אז הן סגורה לפעולה ונסיק $\langle x\rangle\subseteq H,K$. מהנתון $|H|=|K|=p$ נקבל $\langle x\rangle=H=K$ כי ב-$\langle x\rangle$ יש בדיוק p איברים שונים. אך זו סתירה לנתון, ונסיק כי $x=e$.

שאלה 6. תהי G חבורה סופית מסדר אי זוגי. הוכיחו שלכל איבר $e\neq x\in G$ מתקיים $x^{-1}\notin\operatorname{conj}(x)$ (כלומר ההופכי של x לא שייך למחלקת הצמידות של x).

פתרון. נניח בשלילה כי $x^{-1} \notin \mathrm{conj}(x)$. כלומר x צמוד להופכי שלו, ולכן קיים $g \in G$ כך ש-$gxg^{-1} = x^{-1}$. נצמיד את המשוואה האחרונה שוב ב-g ונקבל

$$g^2xg^{-2} = gx^{-1}g^{-1} = \left(gxg^{-1}\right)^{-1} = x$$

ולכן $g^2x = xg^2$. החבורה G היא סופית מסדר אי זוגי, ולכן הסדר של g הוא אי זוגי, נניח $o(g) = 2m + 1$. לכן $e = g^{2m+1} = g\left(g^2\right)^m$, וקיבלנו כי $g^{-1} = \left(g^2\right)^m$. נציב זאת במשוואה $gxg^{-1} = x^{-1}$ ונקבל

$$x = g\left(g^2\right)^m x = gx\left(g^2\right)^m = x^{-1}$$

ולכן $x = x^{-1}$, שזו סתירה כי x אינו איבר היחידה ואין בחבורה איברים מסדר 2.

שאלה 7. תהי G חבורה ותהי $S \subseteq G$ תת־קבוצה לא ריקה. נגדיר את המְרַכֵּז של S ב-G להיות

$$C_G(S) = \{g \in G \,|\, \forall s \in S, gs = sg\}$$

זו הכללה למושג מְרַכֵּז של איבר $s \in G$ שבכיתה סימנו $C_G(s)$.

א. הוכיחו שאם $S \subseteq T \subseteq G$, אז $C_G(T) \subseteq C_G(S)$.

ב. הוכיחו

$$C_G(S) = \bigcap_{s\in S} C_G(s) = \bigcap_{s\in\langle S\rangle} C_G(s) = C_G(\langle S\rangle)$$

והסיקו כי $C_G(S) \leq G$.

ג. תנו דוגמה לחבורה G ותת־קבוצה S כך ש-$|S| \geq 2$ וגם $S \subsetneqq C_G(S) \subsetneqq G$. רמז: אפשר להסתפק ב-$G = S_3$ (אבל לא חייבים!)

ד. תנו דוגמה לחבורה G ותת־קבוצה S כך ש-$|S| \geq 2$ וגם $C_G(S) \subsetneqq S \subsetneqq G$. רמז: אפשר להסתפק ב-$G = S_3$ (אבל לא חייבים!)

פתרון.

א. יהי $g \in C_G(T)$. אזי לכל $t \in T$ מתקיים $gt = tg$. מפני ש-$S \subseteq T$, אז בפרט לכל $t \in S$ מתקיים $gs = sg$. כלומר $g \in C_G(S)$, ולכן $C_G(T) \subseteq C_G(S)$.

ב. נתחיל בהוכחת $C_G(S) = \bigcap_{s\in S} C_G(s)$:

$$g \in C_G(S) \Leftrightarrow \forall s \in S, gs = sg \Leftrightarrow \forall s \in S, g \in C_G(s) \Leftrightarrow g \in \bigcap_{s\in S} C_G(s)$$

וראינו בכיתה כי $C_G(s)$ הוא תת־חבורה, ושחיתוך תת־חבורות הוא תת־חבורה. לכן $C_G(S) \leq G$.
הוכחת $\bigcap_{s\in\langle S\rangle} C_G(s) = C_G(\langle S\rangle)$ נובעת ישירות מהחישוב הקודם כאשר מחליפים את S ב-$\langle S\rangle$ (שהרי גם $\langle S\rangle$ היא תת־קבוצה לא ריקה של G). מפני ש-$S \subseteq \langle S\rangle$, אז לפי הסעיף הקודם $C_G(\langle S\rangle) \subseteq C_G(S)$ ונותר לנו להוכיח את ההכלה בכיוון השני. יהי $g \in C_G(S)$, אזי הוא מתחלף עם כל איברי S. מכאן ש-g גם מתחלף עם כל חזקה של איברי S, כולל חזקות שליליות. יהי $s_1^{\pm1}\dots s_n^{\pm1} \in \langle S\rangle$ איבר כלשהו כאשר $s_1, \dots, s_n \in S$. אזי

$$gs_1^{\pm1}s_2^{\pm1}\dots s_n^{\pm1} = s_1^{\pm1}gs_2^{\pm1}\dots s_n^{\pm1} = \dots = s_1^{\pm1}\dots s_n^{\pm1}g$$

כי g מתחלף עם כל s_i או s_i^{-1}. לכן $g \in C_G(\langle S\rangle)$ וקיבלנו $C_G(S) = C_G(\langle S\rangle)$.

ג. יש אינסוף תשובות אפשרויות כאן. כדי להבטיח $S \subsetneqq C_G(S)$ צריך לדאוג שכל איברי S מתחלפים עם כל איברי S (אם S הייתה תת־חבורה היינו אומרים כי S אבלית). נבחר $G = S_3$. אז אפשר לבחור $S = \{(123), (132)\}$. נשים לב כי $\langle S\rangle = \langle (123)\rangle$, וחישוב קצר יראה כי $C_G(S) = \langle (123)\rangle \neq S_3$. לכן $S \subsetneqq C_G(S) \subsetneqq G$.

ד. גם כאן נבחר $G = S_3$. אפשר לבחור $S = \{(123), (12)\}$ או $S = S_3\backslash\{\mathrm{id}\}$. במקרה זה $\langle S\rangle = G$. אז ראינו כי $C_G(S) = Z(G) = \{\mathrm{id}\}$. לכן $C_G(S) \subsetneqq S \subsetneqq G$.

שאלה 8. תזכורת: דגל מלא של $V = \mathbb{R}^n$ הוא שרשרת של מרחבים וקטוריים

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

כאשר $\dim V_i = i$. נסמן ב-$\mathcal{B}$ את אוסף הדגלים המלאים של V.

א. הוכיחו כי החבורה $GL_n(\mathbb{R})$ פועלת על $\mathcal{B}$ לפי

$$A * (V_0 \subset V_1 \subset \cdots \subset V_n) = A\cdot V_0 \subset A\cdot V_1 \subset \cdots \subset A\cdot V_n$$

כאשר $A\cdot V_i = \{Av \,|\, v \in V_i\}$. בנוסף הראו שהפעולה הזו טרנזיטיבית.

ב. מצאו את המייצב של הדגל הסטנדרטי $\{0\} \subset \langle e_1\rangle \subset \langle e_1, e_2\rangle \subset \cdots \subset \langle e_1, \ldots, e_n\rangle$ כאשר $\{e_1, e_2, \ldots, e_n\}$ הוא הבסיס הסטנדרטי. רמז: אינדוקציה על i.

פתרון.

א. יהי $\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$ דגל ב-$\mathcal{B}$. לכל מרחב וקטורי V_i בדגל ולכל $v \in V_i$, איבר היחידה $I_n \in GL_n(\mathbb{R})$ מקיים כי $I_n v = v$. לכן $I_n \cdot V_i = V_i$. אנחנו יודעים שכפל מטריצות (כאשר הגדלים מתאימים) הוא קיבוצי ולכן לכל $A_1, A_2 \in GL_n(\mathbb{R})$ מתקיים $A_1(A_2 v) = (A_1A_2)v$. לכן גם $A_1(A_2\cdot V_i) = (A_1A_2)\cdot V_i$. לכן

$$\begin{aligned} A_1 * (A_2 * (V_0 \subset V_1 \subset \cdots \subset V_n)) &= A_1 * (A_2\cdot V_0 \subset A_2\cdot V_1 \subset \cdots \subset A_2\cdot V_n) \\ &= A_1(A_2\cdot V_0) \subset A_1(A_2\cdot V_1) \subset \cdots \subset A_1(A_2\cdot V_n) \\ &= (A_1A_2)\cdot V_0 \subset (A_1A_2)\cdot V_1 \subset \cdots \subset (A_1A_2)\cdot V_n \\ &= (A_1A_2) * (V_0 \subset V_1 \subset \cdots \subset V_n) \end{aligned}$$

וקיבלנו שאכן מדובר בפעולת חבורה על קבוצה. נותר להראות שהפעולה טרנזיטיבית. נסמן ב-F_e את הדגל הסטנדרטי

$$\{0\} \subset \langle e_1\rangle \subset \langle e_1, e_2\rangle \subset \cdots \subset \langle e_1, \ldots, e_n\rangle$$

מספיק להראות שלכל דגל $F \in \mathcal{B}$ יש $A \in GL_n(\mathbb{R})$ השולחת את F_e אל F (זה נכון לכל פעולה של חבורה, שאם ישנו איבר שהמסלול שלו הוא כל הקבוצה, אז המסלול של כל איבר הוא כל הקבוצה). יהי דגל

$$\{0\} = V_0 \subset V_1 \subset \cdots \subset V_n = V$$

ב-$\mathcal{B}$ כך שלמרחב V_1 יש בסיס $\{b_1\}$ של וקטור עמודה, שאותו נשלים לבסיס $\{b_1, b_2\}$ של V_2, וכן הלאה באינדוקציה עד שנקבל בסיס $\{b_1, \ldots, b_n\}$ של V. הרי לפי הגדרה $\dim V_i = i$ ואנחנו יודעים שאפשר להשלים קבוצה בלתי תלויה לינארית של $i-1$ וקטורים ב-V_i לבסיס בן i איברים. המטריצה A המבוקשת היא מטריצת מעבר בין הבסיס הסטנדרטי לבסיס $\{b_1, \ldots, b_n\}$. באופן מפורש

$$A = \begin{pmatrix} | & | & & | \\ b_1 & b_2 & \cdots & b_n \\ | & | & & | \end{pmatrix}$$

ונקבל $A\cdot\langle e_1, \ldots, e_i\rangle = \langle b_1, \ldots, b_i\rangle = V_i$ לכל i.

ב. תהי $A \in \mathrm{stab}(F_e)$. לכן $A \cdot \langle e_1, \dots, e_i \rangle = \langle e_1, \dots, e_i \rangle$ לכל i. הדרישה $A \cdot \langle e_1 \rangle = \langle e_1 \rangle$ משמעה שהעמודה הראשונה של A היא $(r_1, 0, \dots, 0)$ עבור $r_1 \in \mathbb{R}^*$ (למה $r_1 \neq 0$? כי A הפיכה). כעת מהדרישה $A \cdot \langle e_1, e_2 \rangle = \langle e_1, e_2 \rangle$ נקבל שהעמודה השנייה של A היא מן הצורה $(r_2', r_2, 0, \dots, 0)$ עבור $r_2 \in \mathbb{R}^*$ ו-$r_2' \in \mathbb{R}$. מכאן ברור שצריך להמשיך באינדוקציה על n, המימד של V.

נוכיח באינדוקציה על n ש-$\mathrm{stab}(F_e)$ הוא תת־החבורה של המטריצות המשולשיות העליונות ההפיכות. בסיס האינדוקציה עשינו לעיל. נניח את נכונות הטענה עבור $n-1$. כלומר לכל $1 \leq i \leq n-1$ מתקיים $A \cdot V_i = V_i$. נשאר להוכיח $A \cdot V_n = V_n$. ניתן להניח כי

$$A = \left(\begin{array}{cccc|c} r_1 & * & * & * & a_1 \\ 0 & r_2 & * & * & \vdots \\ \vdots & \ddots & \ddots & * & \vdots \\ 0 & \cdots & 0 & r_{i-1} & a_{n-1} \\ \hline b_1 & \cdots & \cdots & b_{n-1} & r_n \end{array}\right)$$

כאשר $r_i \in \mathbb{R}^*$, $* \in \mathbb{R}$ לפי הנחת האינדוקציה, ואנו נדרשים למצוא את איברי השורה והעמודה האחרונות. אם $b_i \neq 0$ נקבל סתירה לכך ש-$A \cdot \langle e_1, \dots, e_i \rangle = \langle e_1, \dots, e_i \rangle$. לכן $b_i = 0$ לכל i, וכדי להבטיח ש-A הפיכה נדרוש $r_n \in \mathbb{R}^*$. עבור כל $1 \leq i \leq n-1$ אין שום מגבלה על a_i, שכן אם $v \in V_n$, אז $Av \in \mathbb{R}^n = V_n$, ואם $v \in V_j$ עבור $j < n$, אז $Av \in V_j$ כי בפיתוח המכפלה Av נקבל כי $n - j$ האיברים התחתונים הם 0 (כלומר $a_{n-j}, \dots, a_n$ לא משפיעים כאן כלל). ביתר פירוט: אם $v = \alpha_1 e_1 + \cdots + \alpha_j e_j$, אז אפשר לבדוק לכל מחובר $A\alpha_i e_i \in V_j$ בנפרד. מכאן ש-A מטריצה משולשית עליונה והפיכה, כדרוש.

שאלות רשות

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

שאלה 9. תהי I קבוצה מכוונת (כלומר I היא קבוצה סדורה חלקית כך שלכל $i, j \in I$ קיים $k \in I$ כך ש-$k > i, j$). מערכת של חבורות $\{G_i\}_{i \in I}$ נקראת רשת עולה אם לכל $i < j$ מתקיים $G_i \subseteq G_j$.
הוכיחו שבמקרה זה $\bigcup_{i \in I} G_i$ היא חבורה. בפרט, אם ישנה שרשרת עולה של חבורות $G_1 \subseteq G_2 \subseteq \dots$, אז גם איחוד השרשרת הוא חבורה.

שאלה 10. יהי $\Psi : \mathcal{L} \to \mathcal{L}$ אופרטור מקבוצה סדורה חלקית $(\mathcal{L}, \leq)$ לעצמה.

א. הוכיחו שאם Ψ מקיים את שני התנאים:

- לכל $A, B \in \mathcal{L}$, אם $A \leq B$ אז $\Psi(B) \leq \Psi(A)$.
- לכל $A \in \mathcal{L}$ מתקיים $A \leq \Psi^2(A)$.

אז $\Psi^3 = \Psi$. כלומר שלכל $A \in \mathcal{L}$ מתקיים $\Psi(\Psi(\Psi(A))) = \Psi(A)$.

ב. הסיקו שלכל תת־חבורה $H \leq G$ מתקיים $C_G(C_G(C_G(H))) = C_G(H)$.

בהצלחה!