פתרון תרגיל בית 3 במבנים אלגבריים
89-214 סמסטר א' תשע"ו

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך ג' כסלו ה'תשע"ו, 15.11.2015.

שאלה 1. בכל סעיף, קבעו האם תת-הקבוצה הנתונה היא תת-חבורה:

א. $6\mathbb{Z}_8 = \{6k | k \in \mathbb{Z}_8\} \subseteq \mathbb{Z}_8$.

ב. $k\mathbb{Z}_n \subseteq \mathbb{Z}_n$ כאשר $(k,n) = 1$.

ג. $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z}_p \right\} \subseteq GL_3(\mathbb{Z}_p)$.
תזכורת: $GL_3(\mathbb{Z}_p)$ היא חבורת המטריצות ההפיכות מעל $\mathbb{Z}_p$ מסדר 3×3.

ד. $\{f : \mathbb{R} \to \mathbb{R} | f \text{ is invertible and } f(1) > 0\} \subseteq \{f : \mathbb{R} \to \mathbb{R} | f \text{ is invertible}\}$.

ה. $\{f : \mathbb{R} \to \mathbb{R} | f \text{ is invertible and } f(1) = 1\} \subseteq \{f : \mathbb{R} \to \mathbb{R} | f \text{ is invertible}\}$.

(בשני הסעיפים האחרונים הפעולה היא הרכבת פונקציות)

פתרון.

א. ניעזר בקריטריון המקוצר. ראשית, ברור ש-$0 \in 6\mathbb{Z}_8$. כעת, אם $6m, 6n \in 6\mathbb{Z}_8$, אזי גם
$$6m + (-6n) = 6m - 6n = 6(m-n) \in 6\mathbb{Z}_8$$
ולכן זו תת-חבורה.

ב. גם פה זו תת-חבורה, וההוכחה זהה להוכחה בסעיף הראשון (רק שמחליפים את 6 ב-k; למעשה, זה נכון לכל k, ולא רק כאשר $(k,n) = 1$).

ג. זו תת-חבורה, הנקראת **חבורת הייזנברג**. נוכיח שזו תת-חבורה לפי הקריטריון המקוצר. נסמן את הקבוצה הזו H.
אכן, קודם כל $I \in H$, אם נבחר $a = b = c = 0$.
כעת, נניח כי $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in H$. רוצים לבדוק האם
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}^{-1} \in H$$

קודם, צריך לחשב את ההופכית של $\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}$; על ידי דירוג, למשל, מקבלים

$$\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&-d&df-e\\0&1&-f\\0&0&1\end{pmatrix}$$

לכן,

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&d&e\\0&1&f\\0&0&1\end{pmatrix}^{-1}=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\begin{pmatrix}1&-d&df-e\\0&1&-f\\0&0&1\end{pmatrix}=\begin{pmatrix}1&a-d&df-e-af+b\\0&1&c-f\\0&0&1\end{pmatrix}\in H$$

פה מסתמכים על הסגירות לחיבור ולכפל של $\mathbb{Z}_p$.

ד. זו <u>לא</u> תת-חבורה, כי אין סגירות; למשל, נסתכל על $f(x)=x-\frac{1}{2}$. ודאי ש-f הפיכה ו-$f(1)=\frac{1}{2}>0$, אבל

$$(f\circ f)(1)=f(f(1))=f\left(\frac{1}{2}\right)=0\not>0$$

כלומר $f\circ f$ אינה בתת-הקבוצה הזו, ולכן זו לא תת-חבורה.

ה. פה נוכיח שזו כן תת-חבורה. נסמן אותה H. שוב, לפי הקריטריון המקוצר.
ראשית, $\mathrm{Id}\in H$ כי היא הפיכה וכן $\mathrm{Id}(1)=1$.
כעת, נניח $f,g\in H$. רוצים להראות כי $f\circ g^{-1}\in H$. ראשית, כיוון ש-f ו-g הפיכות, גם $f\circ g^{-1}$ הפיכה. כמו כן,

$$\left(f\circ g^{-1}\right)(1)=f\left(g^{-1}(1)\right)=f(1)=1$$

ולכן בסך הכל $f\circ g^{-1}\in H$, כדרוש.

שאלה 2. תהי G חבורה, ויהיו $H,K\leq G$ תתי-חבורות של G. הוכיחו או הפריכו את הטענות הבאות:

א. $H\cap K\leq G$ היא תת-חבורה של G.

ב. $H\cup K\leq G$ היא תת-חבורה של G.

פתרון.

א. הטענה נכונה. נוכיח עם הקריטריון המקוצר:

(א) $H,K\leq G$, ולכן $e\in H$ וגם $e\in K$, כלומר $e\in H\cap K$.

(ב) כעת, נניח $g_1,g_2\in H\cap K$. לכן $g_1,g_2\in H$ וגם $g_1,g_2\in K$. כיוון ש-$H,K\leq G$, מתקיים $g_1g_2^{-1}\in H$ וגם $g_1g_2^{-1}\in K$; לכן, $g_1g_2^{-1}\in H\cap K$.

לפי הקריטריון המקוצר, $H\cap K\leq G$.

ב. הטענה אינה נכונה. למשל, ניקח $G=\mathbb{Z}$, $H=2\mathbb{Z}$, $K=3\mathbb{Z}$. קל לוודא כי

$$H\cup K=\{0,\pm2,\pm3,\pm4,\pm6,\pm8,\pm9,\dots\}$$

אבל אין סגירות לחיסור – למשל, $3-2=1\notin H\cup K$.
באופן כללי, $H\cup K\leq G$ אם ורק אם $H\subseteq K$ או $K\subseteq H$; לכן, כל דוגמה של שתי תתי-חבורות שאף אחת אינה מוכלת בשנייה תעבוד.

שאלה 3. תהי G חבורה, ויהיו $a,b\in G$. הוכיחו או הפריכו את כל אחת מהטענות הבאות:

א. אם $o(a),o(b)<\infty$, אזי $o(ab)<\infty$ וכן $o(ab)=o(a)\,o(b)$.

ב. $o(ab)=o(ba)$ (יש להתייחס גם למקרה שבו הסדר אינסופי).

פתרון.

א. הפרכה: ב-$GL_n(\mathbb{R})$, נסתכל על $a=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ ועל $b=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$. על ידי חישוב, מקבלים כי $o(a)=4$, $o(b)=3$. אבל $ab=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, ומתקיים $o(ab)=\infty$.
הפרכה אחרת: ניקח $G=U_8$ (למשל), $a=b=3$. אזי $o(a)=o(b)=2$, כלומר $o(a)\,o(b)=4$; אבל $o(ab)=o(1)=1$ (וכמובן $1\neq 4$).

ב. הוכחה: נוכיח בשני חלקים.

(א) נניח $n=o(ab)<\infty$, כלומר $(ab)^n=e$. על ידי כפל ב-$(ab)^{-1}$ של שני האגפים, מקבלים
$$(ab)^{n-1}=(ab)^{-1}=b^{-1}a^{-1}$$
כעת, נשים לב כי
$$(ba)^n=b\,(ab)^{n-1}\,a=bb^{-1}a^{-1}a=e$$
הוכחנו $(ba)^n=e$, ולכן $o(ba)\leq n=o(ab)$. בפרט, $o(ba)<\infty$. אם נפעיל את אותו הנימוק עבור ba במקום ab, נקבל $o(ab)\leq o(ba)$, ובסך הכל, $o(ab)=o(ba)$.

(ב) נניח $o(ab)=\infty$, ונוכיח $o(ba)=\infty$. נניח בשלילה שזה לא נכון, כלומר $o(ba)<\infty$. לפי החלק הראשון שהוכחנו, נקבל $\infty=o(ab)\leq o(ba)<\infty$, בסתירה. לכן $o(ba)=\infty$, כדרוש.

שאלה 4. נתונות החבורות $\mathbb{Z}_7$, U_{12} ו-U_{14}.

א. חשבו (עם הסבר מפורט) את הסדר של 11 ב-U_{12} וב-U_{14}.

ב. לגבי כל חבורה, קבעו האם היא ציקלית. אם קבעתם שכן – מצאו יוצר מפורש של החבורה, והוכיחו שהוא יוצר את החבורה. אם קבעתם שלא – הסבירו מדוע אין איבר היוצר את החבורה.

פתרון.

א. מתחילים להעלות בחזקות.

- ב-U_{12},
$$11^2=121\equiv 1 \pmod{12}$$
ולכן $o(11)=2$ ב-U_{12}.
- ב-U_{14},
$$\begin{aligned}11^2 &= 121\equiv 9 \pmod{14}\\ 11^3 &= 11^2\cdot 11\equiv 9\cdot 11=99\equiv 1 \pmod{14}\end{aligned}$$
ולכן $o(11)=3$ ב-U_{14}.

ב. נענה לכל חבורה בנפרד:

- כפי שאמרנו בתרגול, כל $\mathbb{Z}_n$ היא ציקלית, ונוצרת על ידי 1; בפרט, גם $\mathbb{Z}_7$ היא ציקלית, וכן $\mathbb{Z}_7 = \langle 1 \rangle$.
- נכתוב את איברי U_{12} במפורש: $U_{12} = \{1, 5, 7, 11\}$. לכן, כדי ש-U_{12} תהיה ציקלית, צריך שיהיה בה איבר מסדר 4 (והוא יהיה היוצר של החבורה). על ידי חישוב ישיר, $o(5) = o(7) = o(11) = 2$, ולכן אין איבר כזה. מכאן ש-U_{12} אינה ציקלית.

- נכתוב את איברי U_{14} במפורש: $U_{14} = \{1, 3, 5, 9, 11, 13\}$. לכן, כדי ש-$U_{14}$ תהיה ציקלית, צריך שיהיה בה איבר מסדר 6 (והוא יהיה היוצר של החבורה). על ידי חישוב ישיר, ניתן לוודא כי $o(3) = 6$, ולכן $U_{14} = \langle 3 \rangle$ היא ציקלית.

שאלה 5. תהי $G = \{a_1, a_2, \ldots, a_n\}$ חבורה אבלית סופית. יהי איבר $b = a_1 a_2 \cdots a_n$.

א. הוכיחו $b^2 = e$.

ב. הוכיחו שאם אין ב-G איבר מסדר 2, אז $b = e$.

ג. בשפת התכנות C הניחו שהיצוג של הטיפוס `unsigned char` הוא של 8 סיביות (כלומר משתנה מטיפוס זה הוא בין 0 לבין 255 כולל). הסבירו מה תהיה התוצאה של קטע הקוד הבא בעזרת בסעיפים הקודמים:

```
unsigned char b=0;
unsigned int i=0;
for (i=0; i <= 255; i++) {
    b += i;
}
printf("%d\n", b);
```

הוכחה.

א. לפי ההגדרה של העלאה בריבוע,

$$b^2 = (a_1 a_2 \ldots a_n)^2 = a_1 a_2 \ldots a_n a_1 a_2 \ldots a_n$$

כיוון ש-G אבלית, אפשר לסדר את האיברים באיזה סדר שאנחנו רוצים. נזכור כי בחבורה כל איבר הוא הפיך, ולכן אפשר לשים כל איבר ליד ההופכי שלו; כלומר,

$$b^2 = a_1 a_1^{-1} a_2 a_2^{-1} \ldots a_n a_n^{-1}$$

לכן מקבלים $b^2 = e$.

ב. נזכור כי איבר $e \neq a \in G$ הוא מסדר 2 אם ורק אם $a^2 = e$, כלומר אם ורק אם $a = a^{-1}$. אם אין ב-G איבר מסדר 2, לכל $a \in G$ שאינו e, גם a וגם a^{-1} מופיעים במכפלה $a_1 a_2 \ldots a_n$. שוב, כיוון ש-G אבלית, אפשר לשים אותם אחד ליד השני, ולצמצם אותם. כך נישאר רק עם איבר היחידה, ונקבל $b = e$.

ג. כיוון שהטיפוס של `unsigned char` יכול להכיל מספרים מהתחום $0, 1, \ldots, 255$, נשים לב שהחיבור שלהם מתנהג בדיוק כמו $\mathbb{Z}_{256}$; למשל, $1 + 255 = 0$, כי בייצוג על ידי ביטים,

$$00000001 + 11111111 = 00000000$$

אז בעצם האיבר b שהוגדר בתוכנית הוא סכום כל האיברים ב-$\mathbb{Z}_{256}$. לכן, הוא בדיוק האיבר b שהוגדר בשאלה עבור $G = \mathbb{Z}_{256}$ (כי אצלנו הפעולה היא חיבור במקום כפל). כמו בהסבר של הסעיף הקודם, כל איבר שאינו מסדר 2 יצטצמם עם הנגדי שלו; לכן, יישארו רק האיברים מסדר 2. קל לוודא שהאיבר היחיד מסדר 2 ב-$\mathbb{Z}_{256}$ הוא 128, ולכן זו התוצאה של החיבור.

□

בהצלחה!