פתרון תרגיל בית 2 במבנים אלגבריים
89-214 סמסטר א׳ תשפ״ב

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

א. $9\mathbb{Z}_{12} = \{9k \mid k \in \mathbb{Z}_{12}\} \subseteq \mathbb{Z}_{12}$.

ב. $\left\{10^k \,\middle|\, k \in \mathbb{Z}\right\} \subseteq \mathbb{Q}^*$. תזכורת: הפעולה היא כפל.

ג. $\left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) \,\middle|\, a, b, c \in \mathbb{Z}_p \right\} \subseteq GL_3\left(\mathbb{Z}_p\right)$. תזכורת: $GL_3\left(\mathbb{Z}_p\right)$ היא חבורת המטריצות ההפיכות בגודל 3×3 מעל השדה $\mathbb{Z}_p$, עם הפעולה של כפל מטריצות.

ד. $\left\{a + b\sqrt{6} \,\middle|\, a, b \in \mathbb{Q}, a \neq 0 \vee b \neq 0\right\} \subseteq \mathbb{R}^*$.

ה. $\{A \in M_n(\mathbb{R}) \mid \det A = 0\} \subseteq M_n(\mathbb{R})$.

ו. $\{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ הפיכה}\} \subseteq \{f\colon \mathbb{R} \to \mathbb{R} \mid f(0) < 1, f \text{ הפיכה}\}$.

ז. $\{f\colon \mathbb{R} \to \mathbb{R} \mid f \text{ הפיכה}\} \subseteq \{f\colon \mathbb{R} \to \mathbb{R} \mid f(2) = 2, f \text{ הפיכה}\}$.

(בשני הסעיפים האחרונים הפעולה היא הרכבת פונקציות).

פתרון.

א. נעזר בקריטריון המקוצר לתת־חבורה. ראשית, ברור ש-$0 \in 9\mathbb{Z}_{12}$. כעת, אם $9m, 9n \in 9\mathbb{Z}_{12}$, אזי גם

$$9m + (-9n) = 9m - 9n = 9\,(m - n) \in 9\mathbb{Z}_{12}$$

ולכן זו תת־חבורה.

ב. נעזר בקריטריון המקוצר לתת־חבורה. ברור שתת־הקבוצה לא ריקה כי $10^0 = 1 \in \left\{10^k \,\middle|\, k \in \mathbb{Z}\right\}$. הפעולה היא כפל ולכל זוג איברים $10^s, 10^t$ ששייכים לתת־הקבוצה מתקיים $10^s \cdot (10^t)^{-1} = 10^{s-t} \in \left\{5^k \,\middle|\, k \in \mathbb{Z}\right\}$ מפני ש-$s - t \in \mathbb{Z}$.

ג. נעזר בקריטריון המקוצר לתת־חבורה. נסמן את תת־הקבוצה הזו H. אכן, קודם כל איבר היחידה $I_3 \in H$ שייך, כאשר נבחר $a = b = c = 0$. כעת, נניח

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in H$$

ורוצים לבדוק האם

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

נחשב את ההופכי של האיבר השני, למשל על ידי דירוג, ונקבל

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

לכן,

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

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

ד. כן, זו תת־חבורה. נסמן את תת־הקבוצה S. היא לא ריקה כי עבור $a=1,b=0$ נקבל $a+b\sqrt{6}=1\in S$. אם $a+b\sqrt{6},c+d\sqrt{6}\in S$, אז כדי להוכיח סגירות לפעולה נחשב

$$(a+b\sqrt{6})(c+d\sqrt{6})=(ac+6bd)+(ad+bc)\sqrt{6}\in S$$

הכפל הוא של מספרים ממשיים ששונים מאפס, ולכן מכפלתם שונה מאפס. לכן לפחות אחד מהמקדמים הרציונליים $ac+6bd$ ו-$ad+bc$ אינו אפס. כדי להוכיח סגירות להופכי (שהוא ההופכי של מספרים ממשיים) נחשב

$$\begin{aligned}(c+d\sqrt{6})^{-1}&=\frac{1}{c+d\sqrt{6}}=\frac{1}{c+d\sqrt{6}}\cdot\frac{c-d\sqrt{6}}{c-d\sqrt{6}}\\&=\frac{c-d\sqrt{6}}{c^2-6d^2}=\frac{c}{c^2-6d^2}-\frac{d}{c^2-6d^2}\sqrt{6}\in S\end{aligned}$$

צריך להקפיד להוכיח שלפחות אחד מהמקדמים בביטוי האחרון שונים מאפס. נשים לב ש-$(c+d\sqrt{6})^{-1}\neq 0$ כי $\sqrt{6}$ אי רציונלי ונתון כי $c\neq 0$ או $d\neq 0$. החלק החשוב הוא שמפני ש-$\sqrt{6}$ אי רציונלי, אז גם $c^2-6d^2\neq 0$. לכן $S\leq\mathbb{R}^*$.

ה. לא, זו אינה תת־חבורה של $M_n(\mathbb{Q})$. נבחר $n=2$ ואפילו עבור כל שדה (לא רק $\mathbb{Q}$) קל לראות שתת־הקבוצה לא סגורה לפעולה, למשל

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\notin\{A\in M_n(\mathbb{Q})\,|\,\det A=0\}$$

ו. לא, זו אינה תת־חבורה, כי אין סגירות לפעולה. למשל, נסתכל על $f(x)=x+\dfrac{1}{2}$. ודאי ש-f הפיכה ו-$f(0)=\dfrac{1}{2}<1$, אבל

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

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

ז. נעזר בקריטריון המקוצר לתת־חבורה. נסמן את תת־הקבוצה H. ראשית, $\mathrm{id} \in H$ כי היא הפיכה וכמו כן $\mathrm{id}(2) = 2$. 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 כהרכבת פונקציות הפיכות. נחשב

$$\left(f \circ g^{-1}\right)(2) = f\left(g^{-1}(2)\right) = f(2) = 2$$

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

שאלה 2. יהיו $n, m \in \mathbb{Z}$. הוכיחו כי $m\mathbb{Z} \leq n\mathbb{Z}$ אם ורק אם $n|m$.

פתרון. מצד אחד, אם $m\mathbb{Z} \leq n\mathbb{Z}$, אזי בפרט $m = m \cdot 1 \in n\mathbb{Z}$. לכן קיים $k \in \mathbb{Z}$ כך שמתקיים $m = nk$, כלומר $n|m$.

מצד שני, אם $n|m$, אז קיים $d \in \mathbb{Z}$ כך ש-$m = nd$. לכן אם $mk' \in m\mathbb{Z}$, אז $mk' = ndk' \in n\mathbb{Z}$. כלומר $m\mathbb{Z} \subseteq n\mathbb{Z}$. אנחנו כבר יודעים ש-$n\mathbb{Z}$ ו-$m\mathbb{Z}$ הן תת־חבורות של $\mathbb{Z}$, ולכן מספיק להוכיח את ההכלה.

שאלה 3. תהינה $(G, *)$ ו-$(H, \bullet)$ חבורות ותהיינה G', H' תת־חבורות של G, H בהתאמה. הוכיחו או הפריכו: $G' \times H'$ היא תת־חבורה של $G \times H$ (ביחס לפעולה רכיב-רכיב).

פתרון.

א. הוכחה. מפני ש-$G' \leq G$, אז $e_G \in G'$, ובאופן דומה מפני ש-$H' \leq H$, אז $e_H \in H$. לכן $(e_G, e_H) \in G' \times H'$ ולכן $G' \times H'$ לא ריקה.
יש סגירות לפעולה כי G' ו-H' סגורות לפעולה: יהיו $(g_1, h_1), (g_2, h_2) \in G' \times H'$, אזי

$$(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2) \in G' \times H'$$

שהרי $g_1 g_2 \in G'$ ו-$h_1 h_2 \in H'$. כך גם לגבי סגירות להופכי, אם $(g, h) \in G' \times H'$, אז $g^{-1} \in G'$ כי G' חבורה ו-$h^{-1} \in H'$ כי H' חבורה, ולכן $\left(g^{-1}, h^{-1}\right) \in G' \times H'$ שהוא האיבר ההופכי של (g, h).

שאלה 4. תהי G חבורה, ויהיו $H, K \leq G$ תת־חבורות של G. הוכיחו או הפריכו את הטענות הבאות:

א. $H \cup K$ היא תת־חבורה של G.

ב. $H \cap K$ היא תת־חבורה של G.

ג. $\Delta_H = \{(h, h) \,|\, h \in H\}$ היא תת־חבורה של $G \times G$.

פתרון.

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

$$H \cup K = \{0, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 9, \dots\}$$

אבל אין סגירות לפעולה, 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 תת־חבורות שאף אחת אינה מוכלת בשנייה תעבוד.

ב. 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 $g_1 g_2^{-1} \in H$ וגם $g_1 g_2^{-1} \in K$; לכן, $g_1 g_2^{-1} \in H \cap K$.

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

ג. נוכיח כי $\Delta_H \leq G\times G$. היא לא ריקה כי $e\in H$ ולכן $(e,e)\in\Delta_H$. מהסגירות לפעולה של H, אם $(h,h)\in\Delta_H$, אז גם $\left(h^{-1},h^{-1}\right)\in\Delta_H$ ולכן Δ_H סגורה להופכי. מהסגירות לפעולה של H, אם $(h_1,h_1),(h_2,h_2)\in\Delta_H$, אז גם

$$(h_1,h_1)(h_2,h_2)=(h_1h_2,h_1h_2)\in\Delta_H$$

ולכן Δ_H סגורה לפעולה. בסך הכל $\Delta_H\leq G$.

שאלה 5. תהי G חבורה, ויהיו $a,b\in G$.

א. הוכיחו $o(ab)=o(ba)$. זהירות: לא הנחנו שהחבורה אבלית או שהסדרים סופיים.

ב. הפריכו שאם $o(a),o(b)<\infty$, אזי $o(ab)<\infty$ או $o(ab)=o(a)o(b)$.

פתרון.

א. נחלק את ההוכחה לשני חלקים:
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, $o(ab)<\infty$. אם נפעיל את אותו הנימוק עבור ba במקום ab, נקבל $o(ab)\leq o(ba)$, ובסך הכל, $o(ab)=o(ba)$. כעת 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.

ב. 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 שעשינו בכיתה, מקבלים כי $o(a)=4$, $o(b)=3$. אבל $ab=\begin{pmatrix}1&1\\0&1\end{pmatrix}$, ומתקיים $o(ab)=\infty$ לפי בדיקה של $(ab)^i$.

שאלה 6 (אתגר)**.** מצאו חבורה אינסופית שלכל $n\in\mathbb{N}$ קיים בה איבר מסדר n. האם אתם יכולים גם להבטיח שהסדר של כל האיברים הוא סופי?

כמו כן, לכל $m>1$ מצאו חבורה אינסופית G_m שהסדר של כל איבר בה הוא לכל היותר m.

האם אתם יכולים למצוא דוגמאות לשאלות האלו כך שהחבורות הן מעוצמה $\aleph_0$?

פתרון. לחלק הראשון, נתבונן בחבורה Ω_∞, חבורת שורשי היחידה מכל הסדרים. לפי ההגדרה, חבורה זו היא איחוד כל החבורות Ω_n (שורשי היחידה מסדר n), לכן לכל n, קיים בה איבר מסדר n (ניתן לקחת כל איבר ב-Ω_n שלא הופיע ב-Ω_m עבור $m<n$. איברים אלה נקראים שורשי יחידה פרימיטיביים מסדר n). מאותה סיבה, כל אברי Ω_∞ הם מסדר סופי (מספרה של החבורה הראשונה שבה מופיעים). ניתן להשתמש בחבורות אלה גם לחלק השני ולבחור $G_m=\prod_{i=1}^{\infty}\Omega_m$ לכל $m\geq 1$ (שימו לב כי $|G_m|=\aleph$, נסו למצוא חבורות מעוצמת $\aleph_0$). הסדר של כל איבר בהן הוא אכן לכל היותר m (ליתר דיוק מחלק את m). לגבי Ω_∞ כל החבורות באיחוד סופיות ונוספים איברים חדשים בכל שלב, לכן איחודן על פני המספרים הטבעיים הוא בן מניה (אינסופי), כלומר $|\Omega_\infty|=\aleph_0$.

בהצלחה!