

פתרון תרגיל בית 2 במבנים אלגבריים 89-214 סמסטר א' תש"ף

שאלה 1. 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 2. בכל סעיף, קבעו והוכיחו האם תת־הקבוצה הנתונה היא תת־חבורה:

א. $8\mathbb{Z}_{12} = \{8k \mid k \in \mathbb{Z}_{12}\} \subseteq \mathbb{Z}_{12}$

ב. $\{5^k \mid k \in \mathbb{Z}\} \subseteq \mathbb{Q}^*$. תזכורת: הפעולה היא כפל.

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

ד. $\{a + b\sqrt{7} \mid a, b \in \mathbb{Q}, a \neq 0 \vee b \neq 0\} \subseteq \mathbb{R}^*$.

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

ו. $\{f: \mathbb{R} \rightarrow \mathbb{R} \mid f(1) > 0, \text{ הפיכה } f\} \subseteq \{f: \mathbb{R} \rightarrow \mathbb{R} \mid \text{ הפיכה } f\}$.

ז. $\{f: \mathbb{R} \rightarrow \mathbb{R} \mid f(1) = 1, \text{ הפיכה } f\} \subseteq \{f: \mathbb{R} \rightarrow \mathbb{R} \mid \text{ הפיכה } f\}$.

(בשני הסעיפים האחרונים הפעולה היא הרכבת פונקציות).

פתרון.

א. נעזר בקריטריון המקוצר לתת־חבורה. ראשית, ברור ש- $0 \in 8\mathbb{Z}_{12}$. כעת, אם $8m, 8n \in 8\mathbb{Z}_{12}$ אזי גם

$$8m + (-8n) = 8m - 8n = 8(m - n) \in 8\mathbb{Z}_{12}$$

ולכן זו תת־חבורה.

ב. נעזר בקריטריון המקוצר לתת־חבורה. ברור שתת־הקבוצה לא ריקה כי $5^0 = 1 \in \{5^k \mid k \in \mathbb{Z}\}$. הפעולה היא כפל ולכל זוג איברים $5^s, 5^t$ ששייכים לתת־הקבוצה מתקיים $5^s \cdot (5^t)^{-1} = 5^{s-t} \in \{5^k \mid k \in \mathbb{Z}\}$. 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 $a + b\sqrt{7} = 1 \in S$. אם $a + b\sqrt{7}, c + d\sqrt{7} \in S$, אז כדי להוכיח סגירות לפעולה נחשב

$$(a + b\sqrt{7})(c + d\sqrt{7}) = (ac + 7bd) + (ad + bc)\sqrt{7} \in S$$

הכפל הוא של מספרים ממשיים ששונים מאפס, ולכן מכפלתם שונה מאפס. לכן לפחות אחד מהמקדמים הרציונליים $ac + 7bd$ ו- $ad + bc$ אינו אפס. כדי להוכיח סגירות להופכי (שהוא ההופכי של מספרים ממשיים) נחשב

$$\begin{aligned} (c + d\sqrt{7})^{-1} &= \frac{1}{c + d\sqrt{7}} = \frac{1}{c + d\sqrt{7}} \cdot \frac{c - d\sqrt{7}}{c - d\sqrt{7}} \\ &= \frac{c - d\sqrt{7}}{c^2 - 7d^2} = \frac{c}{c^2 - 7d^2} - \frac{d}{c^2 - 7d^2} \sqrt{7} \in S \end{aligned}$$

צריך להקפיד להוכיח שלפחות אחד מהמקדמים בביטוי האחרון שונים מאפס. נשים לב ש- $(c + d\sqrt{7})^{-1} \neq 0$ כי $\sqrt{7}$ אי רציונלי ונתון כי $c \neq 0$ או $d \neq 0$. החלק החשוב הוא שמפני ש- $\sqrt{7}$ אי רציונלי, אז גם $c^2 - 7d^2 \neq 0$. 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

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

ו. לא, זו אינה תת־חבורה, כי אין סגירות לפעולה. למשל, נסתכל על $f(x) = x - \frac{1}{2}$.

ודאי ש- f הפיכה ו- $f(1) = \frac{1}{2} > 0$, אבל

$$(f \circ f)(1) = f(f(1)) = f\left(\frac{1}{2}\right) = 0 \neq 1$$

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, $\text{id} \in H$ כי היא הפיכה וכמו כן $\text{id}(1) = 1$ 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 כהרכבת פונקציות הפיכות. נחשב

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

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

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 $(e_G, e_H) \in G' \times H'$ ולא 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 $(g^{-1}, h^{-1}) \in G' \times H'$ 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. $H \cap K$ היא תת־חבורה של G .

ב. $H \cup K$ היא תת־חבורה של G .

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

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

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

ב. 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.

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 $(h^{-1}, h^{-1}) \in \Delta_H$ ולכן Δ_H סגורה להופכי. מהסגירות לפעולה של H , אם $(h_1, h_1), (h_2, h_2) \in \Delta_H$, אז גם

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

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

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

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 $o(ba) < \infty$ ו- $o(ab) = \infty$. 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 $o(ab) = \infty$.

הפרכה אחרת: תהי $G = \mathbb{Z}_2$ ונבחר $a = b = 1$. אזי $o(a) = o(b) = 2$, כלומר $o(a)o(b) = 4$. אבל $o(a) = o(0) = 1$ (וכמובן $1 \neq 0$). מי שמתעקש לבחור איברים לא טריוויאליים שונים, יכול לעשות זאת בחבורה $\mathbb{Z}_2 \times \mathbb{Z}_2$.

שאלה 6 (חזרה לא להגשה). תהי S אגודה ו- $a \in S$ איבר. נגדיר את פעולת החזקה לפי $a^1 = a$, ולכל $n > 1$ נגדיר $a^{n+1} = a^n \cdot a$. הוכיחו כי מתקיים:

$$a^n a^m = a^{n+m} \text{ לכל } n, m \in \mathbb{N}.$$

$$(a^n)^m = a^{nm} \text{ לכל } n, m \in \mathbb{N}.$$

ג. נניח כי S היא חבורה עם איבר יחידה e ונרחיב את ההגדרה לכל חזקה שלמה לפי $a^0 = e$ ו- $a^{-n} = (a^{-1})^n$. הוכיחו כי $a_k^{-1} \dots a_1^{-1} = (a_1 \dots a_k)^{-1}$ לכל $a_1, \dots, a_k \in S$ הסיקו כי $(a^n)^{-1} = (a^{-1})^n$ לכל $n \in \mathbb{Z}$.

פתרון. בכל הסעיפים יש להשתמש באינדוקציה עבור הוכחה מלאה.

א. לפי ההגדרה $a^n a^m = (\underbrace{a \dots a}_n)(\underbrace{a \dots a}_m) = \underbrace{a \dots a}_{m+n}$. לפי ההגדרה זה שווה ל- a^{n+m} .

ב. באופן דומה $(a^n)^m = \underbrace{a^n a^n \cdots a^n}_m = (\underbrace{a \cdots a}_n) \cdots (\underbrace{a \cdots a}_n) = \underbrace{a \cdots a}_{mn} = a^{mn}$.

ג. כפל משמאל וכפל מימין של $a_1 \dots a_k$ ב- $a_k^{-1} \dots a_1^{-1}$ הוא איבר היחידה:

$$a_k^{-1} \dots a_2^{-1} a_1^{-1} a_1 a_2 \dots a_k = a_k^{-1} \dots a_2^{-1} a_2 \dots a_k = \dots = a_k^{-1} a_k = e$$

$$a_1 \dots a_{k-1} a_k a_k^{-1} a_{k-1}^{-1} \dots a_1^{-1} = a_1 \dots a_{k-1} a_{k-1}^{-1} \dots a_1^{-1} = \dots = a_1^{-1} a_1 = e$$

אם נבחר $k = n$ ו- $a_1 = a_2 = \dots = a_k = a$, אז נקבל $(a^n)^{-1} = a^{-n}$.

שאלה 7 (רשות). 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 $\aleph_0$?

בהצלחה!