

פתרון תרגיל בית 2 במבנים אלגבריים 89-214 סמסטר א' תשע"ז

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. תאריך הגשת התרגיל הוא לתרגול בשבוע המתחיל בתאריך י"א כסלו ה'תשע"ז, 11/12/16.

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. ענו עבור כל אחת מן המערכות האלגבריות הבאות: האם היא אגודה? האם היא מונואיד? אם כן, מי הוא איבר היחידה? האם היא חבורה? האם הפעולה היא חילופית?

א. (\mathbb{N}, \max) , המספרים הטבעיים עם הפעולה של בחירת המקסימום.

ב. $(2\mathbb{Z}, \cdot)$, המספרים השלמים הזוגיים עם פעולת הכפל הרגילה.

שאלה 2. קבעו האם תת הקבוצה הנתונה הינה תת חבורה:

א. $n\mathbb{Z} \subseteq \mathbb{Z}$ (עם חיבור).

ב. $\mathbb{N} \subseteq \mathbb{Z}$ (עם חיבור).

שאלה 3. הוכיחו או הפריכו:

א. כל חבורה ציקלית היא חבורה אבלית.

ב. כל חבורה אבלית היא ציקלית.

שאלות להגשה

שאלה 4. ענו עבור כל אחת מן המערכות האלגבריות הבאות: האם היא אגודה? האם היא מונואיד? אם כן, מי הוא איבר היחידה? האם היא חבורה? האם הפעולה היא חילופית?

א. $(\mathbb{Z}, *)$, המספרים השלמים עם הפעולה $a * b = a + b + 2$.

ב. $(\mathbb{R}, *)$, המספרים הממשיים עם הפעולה $a * b = \sqrt{a+b}$.

ג. הקבוצה הבאה ביחס לחיבור מטריצות

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 > 0 \right\}$$

ד. (A, \cdot) , הקבוצה מן הסעיף הקודם ביחס לכפל מטריצות.

ה. $(\mathbb{R} \setminus \{-1\}, \circ)$, המספרים הממשיים עם הפעולה $a \circ b = a + b + ab$. רמז: קודם הוכיחו שזו פעולה סגורה.

פתרון. לא נציין מפורשות בכל סעיף שאם מבנה אלגברי הוא חבורה, אז הוא גם מונואיד, ולכן גם אגודה. ולהפך, אם הוא לא אגודה, אז ודאי שהוא גם לא מונואיד וכו'.

א. מבנה זה הוא חבורה. ישנה סגירות, כי לכל $a, b \in \mathbb{Z}$ מתקיים $a + b + 2 \in \mathbb{Z}$. הפעולה קיבוצית כי $(a * b) * c = a + b + c + 4 = a * (b * c)$. הפעולה חילופית עקב חילופיות החיבור הרגיל בטבעיים. איבר היחידה הוא $e = -2$. האיבר ההופכי של a הוא $-a - 4$.

ב. הפעולה לא סגורה, למשל $0 * -1 = \sqrt{0-1} \notin \mathbb{R}$. גם אילו הקבוצה הייתה \mathbb{C} , אפשר לשים לב שהפעולה אינה קיבוצית. לכן $(\mathbb{R}, *)$ אינה אגודה. הפעולה חילופית.

ג. הפעולה לא סגורה, למשל

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin A$$

ולכן לא מדובר באגודה. הפעולה חילופית.

ד. מבנה זה הוא חבורה. הסגירות לא מיידיית, שכן לא מספיק להראות שמכפלת שני איברים הוא מטריצה, אלא מטריצה ששייכת ל- A :

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & bc + ad \\ -(bc + ad) & ac - bd \end{pmatrix}$$

ולשים לב כי $(ac - bd)^2 + (bc + ad)^2$ שהיא הדטרמיננטה של המכפלה היא מכפלה של דטרמיננטות חיוביות, ולכן חיובית בעצמה. הפעולה קיבוצית כי כפל מטריצות הוא קיבוצי. איבר היחידה הוא מטריצת היחידה I_2 . כל מטריצה במבנה זה היא הפיכה מפני שמתקיים $a^2 + b^2 > 0$ שהיא הדטרמיננטה, כשהאיבר ההופכי הוא

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2 + b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

ודאו למה מטריצה זו שייכת למבנה. בדיקה ישירה תראה שהפעולה חילופית.

ה. ברור שעבור $a, b \in \mathbb{R} \setminus \{-1\}$ נקבל $a \circ b \in \mathbb{R}$. כדי להוכיח סגירות צריך להראות כי $a \circ b \neq -1$. נניח בשלילה $a + b + ab = -1$, ואז נעביר אגפים לקבל $a(1+b) = -1 - b$ נצמצם את $1 + b$ (שהרי $b \neq -1$) ונקבל $a = -1$ וזו סתירה. את קיבוציות הפעולה נוכיח באופן ישיר

$$\begin{aligned} (a \circ b) \circ c &= (a + b + ab) \circ c = (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + ab + bc + ac + abc \\ &= a + (b + c + bc) + a(b + c + bc) = a \circ (b + c + bc) = a \circ (b \circ c) \end{aligned}$$

הפעולה היא חילופית

$$a \circ b = a + b + ab = b + a + ba = b \circ a$$

ולכן כדי למצוא איבר יחידה מספיק למצוא איבר e כך ש- $a \circ e = a$. כלומר $a + e + ae = a$, לכן $e(1+a) = 0$, נחלק ב- $(1+a)$ שהרי $a \neq -1$ ונקבל כי $e = 0$ הוא איבר היחידה.

לכל איבר $a \in \mathbb{R} \setminus \{-1\}$ נמצא הופכי לפי $a \circ x = a + x + ax = 0$. נפתור עבור x ונקבל $x = \frac{-a}{1+a}$ (שוב החלוקה מותרת כי $a \neq -1$). כלומר כל איבר הוא הפיך וקיבלנו כי $(\mathbb{R} \setminus \{-1\}, \circ)$ היא חבורה.

שאלה 5. תהי G חבורה. הוכיחו כי G היא אבלית אם ורק אם לכל $a, b \in G$ מתקיים כי $(ab)^2 = a^2b^2$.

פתרון. לכל זוג איברים $a, b \in G$ מתקיים $(ab)^2 = abab = aabb = a^2b^2$. נכפיל משמאל ב- a^{-1} ומימין ב- b^{-1} ונקבל

$$a^{-1}ababb^{-1} = ba = ab = a^{-1}aabb^{-1}$$

כלומר $ba = ab$.

שאלה 6. תהי קבוצה $S = \{a, b\}$. רשמו לוחות כפל עם פעולה $*$ כך שהמערכת האלגברית $(S, *)$ היא:

א. אגודה שאינה מונואיד.

ב. מונואיד שאינו חבורה.

ג. חבורה. למה בהכרח מתקבלת חבורה חילופית?

פתרון. א. ניתן שתי אפשרויות (שהן היחידות עד כדי שקילות): האחת היא

*	a	b
a	a	a
b	a	a

שלעיתים נקראת "אגודת האפס" (Null semigroup) על שני איברים. השנייה היא

*	a	b
a	a	a
b	b	b

אגודת אפס משמאל (left zero semigroup), כלומר לכל $x, y \in S$ מתקיים $xy = x$.

ב.

*	a	b
a	a	a
b	a	b

זו טבלת הכפל של (\mathbb{Z}_2, \cdot) כאשר $a = 0, b = 1$. זו למעשה גם טבלת האמת של הקשר הלוגי "וגם", כאשר $a = F, b = T$. איבר היחידה הוא b .

ג.

*	a	b
a	a	b
b	b	a

במקרה זה a הוא איבר היחידה. האיבר b הוא ההופכי של עצמו. זו בדיוק טבלת הכפל של $(\mathbb{Z}_2, +)$ כאשר $a = 0, b = 1$.

שאלה 7. בכל סעיף, קבעו האם תת-הקבוצה הנתונה היא תת-חבורה:

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

ב. $k\mathbb{U}_n \subseteq \mathbb{U}_n$ כאשר $(k, n) = 1$ (\mathbb{U}_n הינה חבורת אויילר ה- n).

$$g. \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_p \right\} \subseteq GL_3(\mathbb{Z}_p)$$

תזכורת: $GL_3(\mathbb{Z}_p)$ היא חבורת המטריצות ההפיכות מעל \mathbb{Z}_p מסדר 3×3 .

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

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

(בשני הסעיפים האחרונים הפעולה היא הרכבת פונקציות).

פתרון.

א. ניעזר בקריטריון המקוצר. 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. גם פה זו תת-חבורה, וההוכחה זהה להוכחה בסעיף הראשון (רק שמחליפים את 8 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 $\begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \in H$, 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 לא תת-חבורה, כי אין סגירות; למשל, נסתכל על $f(x) = x - \frac{1}{2}$. ודאי ש- f הפיכה

$$f(1) = \frac{1}{2} > 0 \text{ אבל}$$

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

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, $\text{Id} \in H$ כי היא הפיכה וכן $\text{Id}(1) = 1$. 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. כמו כן,

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

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

שאלה 8. 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 $g_1 g_2^{-1} \in H$ 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 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 9. 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.

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, 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.

i. 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 $n = o(ab) \leq o(ba)$. בפרט, $o(ab) < \infty$. אם נפעיל את אותו הנימוק עבור ba במקום ab , נקבל $o(ab) \leq o(ba)$, ובסך הכל, $o(ab) = o(ba)$.

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

שאלה 10. תהי $G = \{a_1, a_2, \dots, a_n\}$ חבורה אבלית סופית. יהי איבר $b = a_1 a_2 \dots a_n$.

א. הוכיחו $b^2 = e$.

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

הוכחה.

א. לפי ההגדרה של העלאה בריבוע,

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

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,

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

לכן מקבלים $b^2 = e$.

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

□

שאלות רשות

שאלה 11. נזכיר שמשפט השאריות הסיני אומר שאם n, m זרים, אזי לכל $a, b \in \mathbb{Z}$ קיים x יחיד עד כדי שקילות מודולו nm כך ש- $x \equiv a \pmod{n}$, $x \equiv b \pmod{m}$. הוכחנו כי $x = bsn + atm$ מקיים את הדרוש. הוכיחו שזה הפתרון היחיד עד כדי שקילות מודולו nm .
רשות למי שרוצה לתרגל: מצאו $y \in \mathbb{N}$ כך ש- $y \equiv 3 \pmod{11}$ וגם $y \equiv 1 \pmod{8}$.

פתרון. כדי להראות יחידות של x מודולו nm נשתמש בטיעון קומבינטורי. לכל זוג (a, b) יש x (לפחות אחד) המתאים לו מודולו nm . ישנם בסה"כ nm זוגות שונים (a, b) (מודולו nm), וכן רק nm ערכים אפשריים ל- x (מודולו nm). ההתאמה הזו היא פונקציה על בין קבוצות סופיות שוות עוצמה, ולכן ההתאמה היא גם חח"ע. דרך אחרת: אם קיים מספר y המקיים את הטענה, אז $x - y \equiv 0 \pmod{n}$, $x - y \equiv 0 \pmod{m}$, כלומר $n|x - y$ וגם $m|x - y$. מהנתון $(n, m) = 1$ נקבל כי $[n, m] = nm|x - y$ ולכן $x \equiv y \pmod{nm}$. (בהמשך הקורס נראה גם $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.)
למי שרצה לתרגל, נשים לב כי $(11, 8) = 1 = 3 \cdot 11 - 4 \cdot 8$ ולפי האמור לעיל נסתכל על $-63 = 1 \cdot 3 \cdot 11 + 3 \cdot (-4) \cdot 8 = -63 \pmod{88}$.
נדרש מספר טבעי, ולכן נקח את $y = 25 \equiv -63 \pmod{88}$.

שאלה 12. פתרו את בעיה 443 מפרוייקט אוילר¹ (מומלץ לתכנת).
תהי $g(n)$ הסדרה המוגדרת לפי

$$g(4) = 13$$

$$g(n) = g(n-1) + \gcd(n, g(n-1)) \quad \forall n > 4$$

הערכים הראשונים של הסדרה הם

n	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$g(n)$	13	14	16	17	18	27	28	29	30	31	32	33	34	51	54	55	60

נתון כי $g(1000) = 2524$ וכי $g(1\,000\,000) = 2624152$. מצאו את $g(10^{15})$.
פתרון. ניתן רק כמה עצות: אם מתכנתים את הפונקציה בצורה הנאיבית, אז נקבל זמן ריצה מעריכי, כי קוראים פעמיים ל- $g(n-1)$ בכל קריאה. אנו יודעים שקיימים s, t כך ש- $\gcd(n, g(n-1)) = sn + tg(n-1)$. לכן עבור $n > 4$ אפשר לחשב באופן שקול את $g(n) = sn + (t+1)g(n-1)$. כך נקבל זמן ריצה בערך $O(n \log n)$, שיאפשר לחשב את $g(1\,000\,000)$ בשניות ספורות. כעת נשאר לחפש תבנית בערכי $g(n)$, שהיא תאפשר לממש חישוב בזמן ריצה בערך $O(\log^2 n)$.

בהצלחה!

¹המקור נמצא בדף <https://projecteuler.net/problem=443>