

פתרון תרגיל בית 2 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 כ"ז חשוון ה'תשע"ו, 8.11.2015.

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

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

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

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

ה. הקבוצה הבאה ביחס לחיבור מטריצות

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

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

ז. $(\mathbb{R} \setminus \{-1\}, \circ)$, 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. הסגירות של הפעולה ברורה. הפעולה קיבוצית כי

$$\max\{\max\{a, b\}, c\} = \max\{a, b, c\} = \max\{a, \max\{b, c\}\}$$

איבר היחידה הוא 1 כי לכל $n \in \mathbb{N}$ מתקיים $\max\{n, 1\} = \max\{1, n\} = n$. אין הפיך לאף איבר פרט ל-1, ולכן מדובר במונואיד. הפעולה חילופית.

ג. הפעולה סגורה כי כפל של מספרים שלמים זוגיים הוא שלם זוגי. הפעולה קיבוצית כי פעולת הכפל הרגילה של מספרים היא קיבוצית. לא קיים איבר יחידה, שכן אם $a \in 2\mathbb{Z}$ היה איבר יחידה אז יתקיים $2 \cdot a = 2$, ונקבל כי $a = 1 \notin 2\mathbb{Z}$. לכן מבנה זה הוא אגודה.

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

ה. 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.

ו. 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.

ז. 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 $a \circ b = -1$, 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 2. 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 $a^2b^2 = aabb = abab = (ab)^2$. נכפיל משמאל ב- a^{-1} ומימין ב- b^{-1} ונקבל

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

כלומר $ba = ab$

שאלה 3. יהי M מונואיד שבו כל איבר הפיך מימין. הוכיחו או הפריכו: M הוא חבורה. פתרו. כדי להוכיח מספיק להראות כי כל איבר ב- M הוא הפיך. יהי $a \in M$, ולפי הנתון בשאלה הוא הפיך מימין. כלומר קיים $b \in M$ כך ש- $ab = e$. גם b הפיך מימין, ולכן קיים $c \in M$ כך ש- $bc = e$. נשים לב כי

$$a = a \cdot e = a \cdot (b \cdot c) = (a \cdot b) \cdot c = e \cdot c = c$$

וקיבלנו כי $ab = bc = ba = e$. כלומר b הוא ההופכי של a .

שאלה 4. הוכיחו כי בלוח כפל של חבורה סופית בכל שורה מופיעים כל איברי החבורה, וכל איבר מופיע פעם אחת.

פתרו. נסתכל בשורה של איבר כללי a . בשורה זו יופיעו האיברים בקבוצה $\{ag : g \in G\}$. יהי b איבר בחבורה, ונראה שיש $g \in G$ כך ש- $b = ag$. נקח את $b = a^{-1}g$. לכן b מופיע בשורה של a ובעמודה של $a^{-1}b$.

כדי לראות שאף איבר לא מופיע פעמיים בשורה, נשים לב כי ההתאמה של $a \mapsto ag$ היא על מקבוצה סופית לעצמה, ולכן ח"ע. דרך אחרת לראות זאת: לו האיבר b מופיע בלפחות שתי עמודות שונות, נניח העמודות של x ושל y , אז נקבל כי $ax = b = ay$. נצמצם ונקבל $x = y$, שזו סתירה להנחה שמדובר בעמודות שונות.

שאלה 5. 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?

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

$$\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ \hline b & a & a \end{array}$$

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

$$\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ \hline b & b & b \end{array}$$

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

ב.

$$\begin{array}{c|cc} * & a & b \\ \hline a & a & a \\ \hline b & a & b \end{array}$$

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.

$$\begin{array}{c|cc} * & a & b \\ \hline a & a & b \\ \hline b & b & a \end{array}$$

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 6. 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), וכך 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 $x - y = nm \cdot k$ 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 $1 = 3 \cdot 11 - 4 \cdot 8 = (11, 8)$ ולפי האמור לעיל נסתכל על $-63 = 1 \cdot 3 \cdot 11 + 3 \cdot (-4) \cdot 8 = -63 \equiv 25 \pmod{88}$. נדרש מספר טבעי, ולכן נקח את 25 .

שאלה 7 (אתגר רשות). 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 $g(1000000) = 2624152$. 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 $g(1000000)$ 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>.