פתרון תרגיל בית 2 בתורת החבורות
88-218 סמסטר א' תש"ף

שאלה 1. (חימום) תהי G חבורה, ו-$a \in G$ איבר. הוכיחו:

א. אם $aa = a$, אזי $a = e$.

ב. אם יש $b \in G$ כך ש-$ab = e$ אזי $ba = e$ ו-$b = a^{-1}$.

פתרון.

א. מפני ש-$a \in G$ איבר בחבורה, אזי קיים לו הופכי a^{-1}. נכפול את שני אגפי המשוואה ב-a^{-1} מימין (אותה תוצאה תתקבל בכפל משמאל) ונקבל

$$a = aaa^{-1} = aa^{-1} = e$$

ב. בחבורה כל איבר הוא הפיך. אם $ab = e$, אזי b הופכי ימני של a. אם c הוא הופכי שמאלי כלשהו של a, אזי

$$b = e \cdot b = (ca)b = c(ab) = c \cdot e = c$$

כלומר $c = b$. לכן $b = a^{-1}$ הוא ההופכי של a ו-$ba = e$.

שאלה 2. (חימום) 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:

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

ב. $(a^n)^m = a^{nm}$ 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-$a^{-n} = \left(a^{-1}\right)^n$. הוכיחו כי $(a_1 \dots a_k)^{-1} = a_k^{-1} \dots a_1^{-1}$ לכל $a_1, \dots, a_k \in S$. הסיקו כי $(a^n)^{-1} = \left(a^{-1}\right)^n$ לכל $n \in \mathbb{Z}$.

פתרון.

א. לפי ההגדרה $a^n a^m = (\underbrace{a \cdots a}_{n})(\underbrace{a \cdots a}_{m})$ ולפי קיבוציות הפעולה זה שווה ל-$a^{n+m} = \underbrace{a \cdots a}_{m+n}$.

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

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

$$a_k^{-1}\dots a_2^{-1}a_1^{-1}a_1a_2\dots a_k = a_k^{-1}\dots a_2^{-1}a_2\dots a_k = \dots = a_k^{-1}a_k = e$$
$$a_1\dots a_{k-1}a_ka_k^{-1}a_{k-1}^{-1}\dots a_1^{-1} = a_1\dots a_{k-1}a_{k-1}^{-1}\dots a_1^{-1} = \dots = a_1^{-1}a_1 = e$$

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

שאלה 3. בחרו כמה סעיפים וענו עבור המערכת האלגברית המופיעה בו:
האם היא אגודה?
האם היא מונואיד? אם כן, מי הוא איבר היחידה?
האם היא חבורה?
האם הפעולה היא חילופית?

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

ב. $(\mathbb{Q}\setminus\{-1\},*)$, המספרים הרציונלים בלי -1 עם הפעולה $a*b=a+b+ab$.

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

ד. $(\mathbb{Z}\setminus 3\mathbb{Z},\cdot)$, המספרים השלמים פרט לכפולות של 3 עם פעולת הכפל הרגילה.

ה. תהי X קבוצה. $(P(X),\triangle)$, כאשר $P(X)$ היא קבוצת החזקה של X. הפעולה היא ההפרש הסימטרי המוגדר לכל $A,B\in P(X)$ לפי $A\triangle B=(A\cup B)\setminus(A\cap B)$.

ו. הקבוצה הבאה ביחס לחיבור מטריצות

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

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

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 אגודה כי ישנה סגירות והפעולה קיבוצית, שכן מתקיים $(a*b)*c = a+b+c+4 = a*(b*c)$. הפעולה חילופית עקב חילופיות החיבור הרגיל בטבעיים. לא מדובר במונואיד כי אילו היה איבר יחידה, אזי הוא היה -2 שאינו מספר טבעי.

ב. מבנה זה הוא חבורה חילופית. הפעולה קיבוצית כי

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

כאשר אנחנו נעזרים בחילופיות של החיבור בשיוויון בין השורות. בעזרת החילופיות גם של כפל רגיל נראה שהפעולה חילופית:

$$a*b=a+b+ab=b+a+ba=b*a$$

לכל $a\in\mathbb{Q}\setminus\{-1\}$ מתקיים $a*0=a+0+a\cdot 0=a$ ולכן איבר היחידה הוא $e=0$. נמצא שכל איבר הפיך כי $a*b=a+b+ab=0$ אם ורק אם $b(1+a)=-a$, כלומר $b=\frac{-a}{1+a}$ והקבוצה לא כוללת את -1, ולכן אין חלוקה באפס ובנוסף ברור כי $b\neq -1$ (אחרת $-1=\frac{-a}{1+a}$ ונסיק $1=0$).

ג. 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 $\max\{1,n\} = \max\{n,1\} = n$. אין הפיך לאף איבר פרט ל-1, ולכן מדובר במונואיד. הפעולה חילופית.

ד. הפעולה סגורה כי מכפלה של מספרים שלמים שאינם כפולה של 3 היא מספר שלם שאינו כפולה של 3. הפעולה קיבוצית כי פעולת הכפל הרגילה של מספרים היא קיבוצית. קיים איבר יחידה, שהוא $1 \in \mathbb{Z}\setminus 3\mathbb{Z}$. אין הפיך לכמעט כל האיברים, למשל לאיבר 2 אין הפיך. לכן מבנה זה הוא מונואיד.

ה. מבנה זה הוא חבורה. סגירות נובעת מכך שאם $A,B \in P(X)$, אז גם $A\triangle B$ היא תת קבוצה של X. קיבוציות הפעולה ידועה ממתמטיקה בדידה. איבר היחידה הוא הקבוצה הריקה. קל לבדוק שכל איבר הוא ההופכי של עצמו. הפעולה (כפי ששמה רומז) היא חילופית.

ו. 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.

ז. מבנה זה הוא חבורה. הסגירות לא מיידית, 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.

שאלה 4. תהינה $(G,*)$ ו-$(H,\bullet)$ חבורות. נגדיר על המכפלה הקרטזית $G\times H$ פעולה "רכיב-רכיב":

$$(g_1,h_1)(g_2,h_2) = (g_1 * g_2, h_1 \bullet h_2)$$

לכל $g_1,g_2 \in G, h_1,h_2 \in H$.

א. הוכיחו כי $G\times H$ עם הפעולה לעיל היא חבורה. היא נקראת המכפלה הישרה (החיצונית) של G ו-H.

ב. הוכיחו או הפריכו: החבורה $G\times H$ אבלית אם ורק אם G ו-H אבליות.

ג. תהינה G', H' תת־חבורות של G, H בהתאמה. הוכיחו או הפריכו: $G' \times H'$ היא תת־חבורה של $G \times H$.

פתרון.

א. ההוכחה לכל אחד מהתנאים בהגדרת חבורה (קיבוציות הפעולה, קיום איבר יחידה וקיום הפיך לכל איבר) נובעת מהתנאי המקביל שמתקיים עבור G ו-H שהן חבורות. יהיו $(g_1,h_1),(g_2,h_2),(g_3,h_3) \in G \times H$. אזי

$$\begin{aligned}((g_1,h_1)(g_2,h_2))(g_3,h_3) &= (g_1g_2,h_1h_2)(g_3,h_3) = (g_1g_2g_3,h_1h_2h_3)\\ &= (g_1,h_1)(g_2g_3,h_2h_3) = (g_1,h_1)((g_2,h_2)(g_3,h_3))\end{aligned}$$

כי הפעולות ב-G וב-H הן קיבוציות. איבר היחידה הוא $e_{G\times H} = (e_G, e_H)$, ואכן

$$(g,h)(e_G,e_H) = (ge_G, he_G) = (g,h) = (e_G g, e_H h) = (e_G,e_H)(g,h)$$

לכל איבר $(g,h) \in G \times H$. ההופכי שלו הוא $\left(g^{-1},h^{-1}\right)$ מפני ש-

$$(g,h)\left(g^{-1},h^{-1}\right) = \left(gg^{-1},hh^{-1}\right) = (e_G,e_H) = \left(g^{-1}g,h^{-1}h\right) = \left(g^{-1},h^{-1}\right)(g,h)$$

ב. הוכחה. אם $G \times H$ אבלית, אזי לכל $(g_1,h_1),(g_2,h_2) \in G \times H$ מתקיים

$$(g_1g_2,h_1h_2) = (g_1,h_1)(g_2,h_2) = (g_2,h_2)(g_1,h_1) = (g_2g_1,h_2h_1)$$

ובפרט לכל $g_1,g_2 \in G$ ולכל $h_1,h_2 \in H$ מתקיים $g_1g_2 = g_2g_1$ ו-$h_1h_2 = h_2h_1$, שזו בדיוק ההגדרה לכך ש-G, H אבליות.
אם G, H אבליות, אז נחזור על הטיעון בכיוון השני.

ג. הוכחה. מפני ש-$G' \le G$, אז $e_G \in G'$, ובאופן דומה מפני ש-$H' \le H$, 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

$$(g_1,h_1)(g_2,h_2) = (g_1g_2,h_1h_2) \in G' \times H'$$

שהרי $g_1g_2 \in G'$ ו-$h_1h_2 \in H'$. כך גם לגבי סגירות להופכי, אם $(g,h) \in G' \times H'$, אז $g^{-1} \in G'$ ו-$h^{-1} \in H'$, ולכן $\left(g^{-1},h^{-1}\right) \in G' \times H'$ שהוא האיבר ההופכי של (g,h).

שאלה 5. תהי G חבורה. הוכיחו כי G 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

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

כלומר $ba = ab$.

שאלה 6. תהי $G = \{a_1,a_2,\ldots,a_n\}$ חבורה אבלית סופית. נסמן $b = a_1a_2\cdots a_n$. הוכיחו כי $b^2 = e$. רשות: בעזרת השאלה הבאה מצאו קריטריון מתי $b = e$.

פתרון. כיוון ש-G אבלית, לא משנה סדר המכפלה של האיברים ב-b^2. נשים לב שב-b^2 כל איבר בחבורה מופיע פעמיים. נסדר את המכפלות כך של איבר יהיה ליד ההופכי שלו $b^2 = a_1a_1^{-1}a_2a_2^{-1}\cdots a_na_n^{-1}$. אז נצמצם ונקבל כי $b^2 = e$.

שאלה 7. תהי G חבורה. נסמן $m_2 = \left|\left\{x \in G \,\middle|\, x^2 = e\right\}\right|$.

א. הראו שבכל חבורה סופית מתקיים: $m_2 \equiv |G| \pmod 2$.

ב. הראו שבכל חבורה עם מספר זוגי של איברים קיים איבר $e \neq x$ המקיים $x^2 = e$.

הדרכה לסעיף א: העזרו ביחס השקילות הבא על G: $x \sim y \iff x = y \vee xy = e$. מה הגודל של כל מחלקת שקילות?

פתרון.

א. נסתכל על יחס השקילות שבהדרכה. כלומר כל איבר שקול לעצמו ולהופכי שלו. נשים לב שאיבר הוא ההופכי של עצמו אם ורק אם הוא מקיים $x^2 = e$. לכן מחלקת שקילות של x היא או מגודל 1 (אם $x^2 = e$) או מגודל 2 (אם $x^2 \neq e$). מכיוון שקבוצה היא איחוד מחלקות השקילות שלה: $|G| = m_2 + 2r$ כאשר r הוא מספר המחלקות השונות מגודל 2. מכאן ש-$|G| \equiv m_2 \pmod 2$.

ב. לפי הסעיף הקודם, מכיוון ש-$|G|$ זוגי, כך גם m_2. תמיד מתקיים $m_2 \geq 1$ כי e מקיים את הדרישה ש-$e^2 = e$. לכן אצלנו נסיק כי $m_2 \geq 2$, ולכן חייב להיות עוד איבר חוץ מהיחידה המקיים את התכונה.

שאלה 8. יהי F שדה. קבעו (והוכיחו את קביעתכם) האם תת־הקבוצות הבאות הן תת־חבורות של החבורות הנתונות או לא:

א. $O_n(F) = \left\{A \in GL_n(F) \,\middle|\, A^T = A^{-1}\right\} \subseteq GL_n(F)$ המטריצות האורתוגונליות.

ב. $\{A \in M_n(F) \,|\, \det A = 0\} \subseteq M_n(F)$.

פתרון.

א. כן, זו תת־חבורה. בהוכחה כנראה תעזרו בזהויות מאלגברה לינארית לפיהן $(A^{-1})^T = (A^T)^{-1}$ ו-$(AB)^T = B^TA^T$ לכל $A, B \in GL_n(F)$. ברור ש-$O_n(F) \neq \varnothing$ כי $I^T = I = I^{-1}$ ולכן $I \in O_n(F)$. הסגירות להופכי נובעת מהזהות לעיל, שכן אם $A \in O_n(F)$, אז $(A^{-1})^T = (A^T)^{-1} = (A^{-1})^{-1}$ ולכן $A^{-1} \in O_n(F)$. הסגירות לפעולה נובעת מהזהות השנייה, שכן אם $A, B \in O_n(F)$, אז $(AB)^T = B^TA^T = B^{-1}A^{-1} = (AB)^{-1}$ ולכן $AB \in O_n(F)$.

ב. לא, זו אינה תת־חבורה של $M_n(F)$. נבחר $n = 2$ ועבור כל שדה קל לראות שתת־הקבוצה לא סגורה לפעולה, למשל

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

שאלה 9. תהי G חבורה ו-H, K תת־חבורות שלה. הוכיחו או הפריכו את הטענות הבאות:

א. $H \cap K$ היא תת־חבורה.

ב. $H \cup K$ היא תת־חבורה.

ג. $HK = \{hk \,|\, h \in H, k \in K\}$ היא תת־חבורה.

ד. אם G אבלית אז HK היא תת־חבורה.

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

פתרון.

א. כן, $H \cap K \le G$. החיתוך $H \cap K$ אינו ריק כי H,K הן תת־חבורות G. לכן $e \in H,K$, ולכן $e \in H \cap K$. יהי $g \in H \cap K$. אזי $g^{-1} \in H$ וגם $g^{-1} \in K$ כי H,K סגורות להופכי (כי הן תת־חבורות) ולכן $g^{-1} \in H \cap K$ וקיבלנו סגירות להופכי. יהיו $g_1, g_2 \in H,K$. אזי $g_1 g_2 \in H$ וגם $g_1 g_2 \in K$ כי H,K סגורות לפעולה ולכן גם $g_1 g_2 \in H \cap K$ וקיבלנו סגירות לפעולה.

ב. לא, $H \cup K$ אינה תת־חבורה. נבחר $G = \mathbb{Z}$ ואת תת־החבורות $H = 2\mathbb{Z}$, $K = 3\mathbb{Z}$ (ראינו בכיתה שאלו תת־חבורות של G). אזי $H \cup K$ אינו תת־חבורה כי אינו סגור לפעולה. למשל $2,3 \in H \cup K$, אבל $2+3=5 \notin H \cup K$.
למעשה $H \cup K$ הוא תת־חבורה אם ורק אם $H \subseteq K$ או $K \subseteq H$. לכן כל דוגמה נגדית מחייבת זוג תת־חבורות שלא מוכלות אחת בשנייה.

ג. הפרכה. בדרך כלל זו לא תת־חבורה. נבחר $G = S_3$, ואת תת־החבורות $H = \langle (1\ 2) \rangle$ ו-$K = \langle (1\ 3) \rangle$. נקבל כי

$$HK = \{\mathrm{id}, (1\ 2), (1\ 3), (1\ 3\ 2)\}$$

שהיא לא תת־חבורה, למשל כי אין סגירות להופכי לאיבר $(1\ 3\ 2)$, או כי מספר האיברים ב-HK לא מחלק את $|S_3| = 6$.

ד. הוכחה. הקבוצה HK לא ריקה כי $e \in H$ וגם $e \in K$ ולכן $e \cdot e = e \in HK$. יש סגירות להופכי כי אם $hk \in HK$, אז גם $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}k^{-1} \in HK$ כאשר השתמשנו באבליות של G בשיוויון השני, ובכך ש-H,K הן תת־חבורות ולכן $h^{-1} \in H$ ו-$k^{-1} \in K$. הסגירות לפעולה גם דורשת את האבליות: אם $h_1k_1, h_2k_2 \in HK$, אז גם $h_1k_1h_2k_2 = h_1h_2k_1k_2 \in HK$. שימו לב שהשתמשנו בכך ש-H,K סגורות לפעולה ולכן $h_1h_2 \in H$ ו-$k_1k_2 \in K$.

ה. נוכיח כי $\Delta_H \le G \times G$. 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 $\Delta_H \le G$. שימו לב שזהו לא מקרה פרטי של סעיף 4ג!

שאלות רשות

את שאלות הרשות אין חובה לפתור, אבל אם פתרתם אותן, בבקשה שלחו לנו פתרון שלהן.

שאלה 10. הוכיחו שאם באגודה S יש פתרון לכל משוואה מן הצורה $ax = b$ או $xa = b$, אז זו חבורה. (רמז: לפי ההנחה יש איבר $e \in S$ (התלוי ב-a) כך ש-$ae = a$. לכל $c \in S$ קיים x כך ש-$xa = c$, ואז $ce = xae = xa = c$, ולכן e הוא יחידה מימין. באופן דומה יש יחידה משמאל.)

פתרון. נשתמש ברמז, ולפי הנחה יש פתרון למשוואה $ax = a$. נניח כי e הוא פתרון (התלוי ב-a). נשים לב כי לכל $c \in S$ מתקיים כי קיים פתרון x למשוואה $xa = c$. לכן

$$ce = (xa)e = x(ae) = xa = c$$

וקיבלנו כי e הוא יחידה מימין. באופן דומה יש פתרון e' למשוואה $xa = a$. לכל $c \in S$ קיים פתרון x למשוואה $ax = c$, ומתקיים כי

$$e'c = e'(ax) = (e'a)x = ax = c$$

ולכן e' יחידה משמאל. אבל אם קיימים איברי יחידה מימין ומשמאל, אז יש איבר יחידה יחיד. נסמן אותו ב-e. לפי הנתון יש פתרון למשוואות $cx = e$ ו-$xc = e$, כלומר קיים הופכי משמאל ומימין לכל איבר $c \in S$. לכן כל איבר $c \in S$ הוא הפיך.

בהצלחה!