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

שאלה 1. יהיו $n,m \in \mathbb{Z}$. הוכיחו כי $m\mathbb{Z} \le n\mathbb{Z}$ אם ורק אם $n|m$.

פתרון. מצד אחד, אם $m\mathbb{Z} \le n\mathbb{Z}$, 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. 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 3. בכל סעיף, קבעו האם תת־הקבוצה הנתונה היא תת־חבורה:

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

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

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

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

ו. $\{f:\mathbb{R}\to\mathbb{R}\,|\,\text{הפיכה } f\}\supseteq\{f:\mathbb{R}\to\mathbb{R}\,|\,f(1)>0,\text{הפיכה } f\}$.

ז. $\{f:\mathbb{R}\to\mathbb{R}\,|\,\text{הפיכה } f\}\supseteq\{f:\mathbb{R}\to\mathbb{R}\,|\,f(1)=1,\text{הפיכה } f\}$.

(בשני הסעיפים האחרונים הפעולה היא הרכבת פונקציות).

פתרון.

א. לא, כי $\mathbb{N}$ אינה סגורה להופכי. למשל $-3\notin\mathbb{N}$.

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

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

ולכן זו תת־חבורה.

ג. ניעזר 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. 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

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

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

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

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

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

ז. ניעזר בקריטריון המקוצר לתת־חבורה. נסמן את תת־הקבוצה H. ראשית, $\mathrm{Id} \in H$ כי היא הפיכה וכמו כן $\mathrm{Id}(1) = 1$. 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. נחשב

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

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

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

פתרון.

א. הטענה נכונה. נוכיח עם הקריטריון המקוצר:

(א) $H,K\le G$, 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־$H,K\le G$, מתקיים $g_1g_2^{-1}\in H$ וגם $g_1g_2^{-1}\in K$; לכן, $g_1g_2^{-1}\in H\cap K$.

לפי הקריטריון המקוצר, $H\cap K\le G$.

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

$$H\cup K=\{0,\pm2,\pm3,\pm4,\pm6,\pm8,\pm9,\dots\}$$

אבל אין סגירות לפעולה, למשל $3-2=1\notin H\cup K$.
באופן כללי, $H\cup K\le G$ 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 $\Delta_H\le G\times G$. 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 $\Delta_H\le G$.

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

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

ב. הוכיחו $o(ab)=o(ba)$ (גם אם הסדר אינסופי).

פתרון.

א. הפרכה: ב־$GL_n(\mathbb{R})$, נסתכל על $a=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ ועל $b=\left(\begin{smallmatrix}0&1\\-1&-1\end{smallmatrix}\right)$. על ידי חישוב שעשינו בכיתה, מקבלים כי $o(a)=4$, $o(b)=3$. אבל $ab=\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, ומתקיים $o(ab)=\infty$.
הפרכה אחרת: תהי $G=U_8$ ונבחר $a=b=3$. אזי $o(a)=o(b)=2$, כלומר $o(a)o(b)=4$; אבל $o(ab)=o(1)=1$ (וכמובן $1\neq4$).

ב. 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 $o(ba)\le n=o(ab)$. בפרט, $o(ab)<\infty$. אם נפעיל את אותו הנימוק עבור ba במקום ab, נקבל $o(ab)\le o(ba)$, 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 $\infty=o(ab)\le o(ba)<\infty$, בסתירה. לכן $o(ba)=\infty$, כדרוש.

שאלה 6 (חזרה)**.** 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. בכל הסעיפים יש להשתמש באינדוקציה עבור הוכחה מלאה.

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:

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

אם נבחר $k = n$ ו-$a_1 = a_2 = \cdots = a_k = a$, 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!