פתרון תרגיל בית 2 במבוא לתורת החבורות
סמסטר א' תש"ף

שאלה 1. כתבו את לוח הכפל של S_3.

פתרון. כתבו את כל איברי S_3 (רצוי בכתיב מחזורים) בשורות ובעמודות והכפילו בזהירות להנאתכם.

שאלה 2. תהי $\sigma = (257)(423)(57)(3416) \in S_8$. מצאו את σ^3 ואת σ^{-1} (אזהרה: המחזורים אינם זרים).

א. כפי שראינו בכיתה, לכל תמורה יש ייצוג כמכפלת מחזורים זרים. חישוב זריז יגלה כי

$$\sigma = (1\ 6\ 4)(2\ 3\ 5)$$

וכי $\sigma^3 = \mathrm{id}$. לכן $\sigma^{-1} = \sigma^2 = (1\ 4\ 6)(2\ 5\ 3)$.

שאלה 3. 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 4. בכל סעיף, קבעו והוכיחו 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. $\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z}_p \right\} \subseteq GL_3(\mathbb{Z}_p)$. תזכורת: $GL_3(\mathbb{Z}_p)$ היא חבורת המטריצות ההפיכות בגודל 3×3 מעל השדה $\mathbb{Z}_p$, עם הפעולה של כפל מטריצות.

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

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

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

(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

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

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

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

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 5. הוכיחו ש-A_n היא תת־חבורה של S_n ושיש בה $\frac{n!}{2}$ איברים (רמז: הגדירו $f : S_n \to S_n$ לפי $f(\sigma) = (12)\sigma$).

פתרון. נשים לב כי f שולחת תמורות זוגיות לאי-זוגיות ולהיפך, לכן ניתן לחשוב עליה כעל שתי פונקציות:
$f_1 : A_n \to S_n \setminus A_n$ ו-$f_2 : S_n \setminus A_n \to A_n$ המוגדרות באותו אופן: $f_i(\sigma) = (12)\sigma$ עבור $i = 1, 2$.
אלה בבירור פונקציות הופכיות זו לזו, בפרט הפיכות (ניתן גם להגדיר רק אחת שהיא צמצום של המקורית ולהראות שהיא חח"ע ועל),
ולכן: $|A_n| = |S_n \setminus A_n|$, כלומר: $|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

שאלה 6. 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.

פתרון.

(א) הטענה נכונה. נוכיח עם הקריטריון המקוצר:

i. $H, K \leq G$, ולכן $e \in H$ וגם $e \in K$, כלומר $e \in H \cap K$.

ii. 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.

שאלה 7 (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:

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

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

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

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

בהצלחה!