תרגיל 3 מבוא לתורת החבורות

שאלה 3.1 חשבו את ההופכי של האיברים הבאים:

1. -11 ב U_{27}

פתרון: קודם כל נשים לב ש $-11 = 16$ נשתמש באלגוריתם אוקלידס

$$\begin{aligned} 27 &= 16 + 11 \\ 16 &= 11 + 5 \\ 11 &= 2 \cdot 5 + 1 \end{aligned}$$

ולכן

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 = 11 - 2 \cdot (16 - 11) = -2 \cdot 16 + 3 \cdot 11 \\ &= -2 \cdot 16 + 3 \cdot (27 - 16) = 3 \cdot 27 - 5 \cdot 16 \end{aligned}$$

ולכן ההופכי של 16 הוא $-5 = 22$

2. 34 ב U_{117}

פתרון: שוב. אלגוריתם אוקלידס.

$$\begin{aligned} 117 &= 3 \cdot 34 + 15 \\ 34 &= 2 \cdot 15 + 4 \\ 15 &= 3 \cdot 4 + 3 \\ 4 &= 3 + 1 \end{aligned}$$

ולכן בחישוב לאחור מקבלים

$$\begin{aligned} 1 &= 4 - 3 = 4 - (15 - 3 \cdot 4) = -15 + 4 \cdot 4 \\ &= -15 + 4(34 - 2 \cdot 15) = 4 \cdot 34 - 9 \cdot 15 \\ &= 4 \cdot 34 - 9(117 - 3 \cdot 34) = -9 \cdot 117 + 31 \cdot 34 \end{aligned}$$

ולכן ההופכי הוא 31.

שאלה 3.2 כתבו את טבלת הכפל של U_8 ושל U_{10}. בנוסף עבור כל איבר חשבו את הסדר שלו.

פתרון: עבור U_8. זאת טבלת הכפל:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

כמו שרואים מייד מהטבלה. כל האיברים (פרט ליחידה) הם מסדר 2.

עבור U_{10}. זאת טבלת הכפל:

$\cdot$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

קל לבדוק ש $\mathrm{o}(1) = 1$ $\mathrm{o}(9) = 2$ $\mathrm{o}(3) = \mathrm{o}(7) = 4$.

שאלה 3.3 הגדירו פעולה (סבירה) על $\mathbb{Z}_n$ באמצעות נציגים ש**אינה** מוגדרת היטב והדגימו שהיא אינה מוגדרת היטב.
פתרון: אפשר למשל להגדיר:

$$[a] * [b] = [\gcd(a, b)]$$

נראה שזה לא מוגדר היטב על ידי דוגמא נגדית. נניח $n = 5$ אז

$$[2] * [4] = [2]$$

אבל

$$[7] * [9] = [1]$$

וכמובן $[2] \neq [1]$.

שאלה 3.4 תהי G חבורה סופית.

1. הוכיחו כי לכל $a, b \in G$ מתקיים $\mathrm{o}(ab) = \mathrm{o}(ba)$.
פתרון: נניח

$$(ab)^n = e$$

שימו לב שאפשר לכתוב זאת גם ככה:

$$a(ba)^{n-1}b = e$$

ולכן

$$(ba)^{n-1}b = a^{-1}$$

ועל ידי כפל מימין ב a נקבל

$$(ba)^{n-1}ba = e$$

כלומר

$$(ba)^n = e$$

באופן דומה מוכיחים שאם $(ba)^n = e$ אז $(ab)^n = e$. ולכן

$$\{k \in \mathbb{N} \mid (ab)^k = e\} = \{k \in \mathbb{N} \mid (ba)^k = e\}$$

ממילא

$$\mathrm{o}(ab) = \min\{k \in \mathbb{N} \mid (ab)^k = e\} = \min\{k \in \mathbb{N} \mid (ba)^k = e\} = \mathrm{o}(ba)$$

2. הוכיחו כי לכל $a,b,c \in G$ מתקיים $\mathrm{o}(abc)=\mathrm{o}(bca)$.
פתרון: לפי הסעיף הקודם

$$\mathrm{o}(abc)=\mathrm{o}(a(bc))=\mathrm{o}((bc)a)=\mathrm{o}(bca)$$

3. מצאו $a,b,c \in S_3$ כך ש $\mathrm{o}(abc)\neq \mathrm{o}(bac)$
פתרון: ניקח

$$a=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\quad b=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad c=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

ואז

$$abc=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

$$bac=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$$

שהם כמובן מסדרים שונים.

שאלה 3.5 נגדיר

$$G=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\mid a,b,c\in\mathbb{Z}_3\right\}$$

זאת חבורה ביחס לפועלה של כפל מטריצות (מומלץ להוכיח כדי להיווכח). חשבו את הסדר של כל איבר ב G.
פתרון: הסדר של איבר היחידה הוא כמובן 1. הסדר של כל איבר אחר הוא 3. אפשר לעבור איבר איבר ולחשב אבל אנחנו נעשה את זה ככה: נשים לב ש

$$\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}=I+N$$

כאשר

$$N=\begin{pmatrix}0&a&b\\0&0&c\\0&0&0\end{pmatrix}$$

עכשיו, נשים לב ש $N^3=0$. כעת,

$$(I+N)^3=I+3N+3N^2+N^3$$

היות ש $N^3=0$ ואנחנו עובדים מעל $\mathbb{Z}_3$ אז זה שווה ל I. ולכן הסדר הוא לכל היותר 3. עכשיו, האם יכול להיות ש $\mathrm{o}(I+N)=2$? לא. כי אם הסדר היה 2 אז לפי משפט מהכיתה $2\mid 3$ וזה לא קורה. ולכן אם $N\neq 0$ מתקיים

$$\mathrm{o}(I+N)=3$$

כלומר הסדר של כל איבר פרט לאיבר היחידה הוא 3.

שאלה 3.6 תהי K חבורה שבה מתקיים

$$(ab)^3 = a^3b^3$$

הוכיחו או הפריכו: K אבלית. רמז: התשובה נמצאת כבר בתרגיל אחר בדף הזה.
פתרון: בתרגיל הקודם יש חבורה שבה הסדר של כל איבר הוא 1 או 3 ולכן ממילא מתקיים

$$(ab)^3 = e = a^3b^3$$

מצד שני החבורה לא אבלית. למשל ברור ש

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

שאלה 3.7 תהי G חבורה אבלית ותהי H תת הקבוצה שמכילה את כל האיברים עם סדר סופי. הוכיחו כי H תת חבורה.
פתרון: קודם כל H לא ריקה כי $e \in H$. נוכיח ש H סגורה לכפל. יהיו $a, b \in H$ ונניח

$$\mathrm{o}(a) = n, \quad \mathrm{o}(b) = m$$

אז בוודאי

$$(ab)^{nm} = a^{nm}b^{nm} = e$$

ולכן

$$\mathrm{o}(ab) \leq nm$$

ולכן

$$ab \in H$$

כמו כן כבר ראינו ש $\mathrm{o}(a) = \mathrm{o}(a^{-1})$ ולכן אם $a \in H$ אז בוודאי $a^{-1} \in H$. זה מוכיח ש H תת חבורה.

שאלה 3.8 מצאו איבר מסדר 6 ב S_5. רמז/הדרכה: מצאו איבר מסדר 2 ב S_2. מצאו איבר מסדר 3 ב S_3.
פתרון: הנה האיבר:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 6 \end{pmatrix}$$

אפשר לבדוק שהוא מסדר 6.