

# אלגברה מופשטת – פתרון תרגיל 2

## שאלה 1

א. תהי  $G$  חבורה סופית,  $a, b \in G$ . הוכיחו:  $o(ab) = o(ba)$ .  
(רמז: אם  $o(ab) = n, o(ba) = m$ , הסתכלו על  $(ba)^{n+1}$  ועל  $(ab)^{m+1}$ .)  
פתרון:

נסתכל על  $(ba)^{n+1}$ :  
 $(ba)^{n+1} = ba \cdot \dots \cdot ba = b \cdot (ab)^n \cdot a = ba \Leftrightarrow (ba)^n = 1 \Leftrightarrow m \mid n$   
ואם נסתכל על  $(ab)^{m+1}$  נקבל ש-  $n \mid m$ . לכן  $n=m$ .

ב. תהי  $G$  חבורה,  $o(g) = n, g \in G$ . הוכיחו ש-  $g^a = g^b$  אם ורק אם  $a \equiv b \pmod{n}$ .

פתרון:

$$g^a = g^b \Rightarrow g^{a-b} = 1 \Rightarrow n \mid (a-b) \Rightarrow a = b + kn \Rightarrow a \equiv b \pmod{n} : \Leftarrow$$

$$a \equiv b \pmod{n} \Rightarrow a = b + kn \Rightarrow g^a = g^{b+kn} = g^b g^{kn} = g^b : \Rightarrow$$

## שאלה 2

א. נגדיר  $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z}_3 \right\}$ . הוכיחו כי  $G$  חבורה ביחס לפעולת כפל

מטריצות, מצאו את הסדר של  $G$  ואת הסדר של כל איבר ב- $G$ .

ב. תהי  $G$  חבורה. אם לכל  $a, b \in G$  מתקיים  $(ab)^3 = a^3 b^3$  האם  $G$  אבלית?

א)  $G$  מוכלת ב-  $GL_3(\mathbb{Z}_3)$  (חבורת המטריצות ההפיכות מסדר  $3 \times 3$  מעל  $\mathbb{Z}_3$ ). ברור שזוהי קבוצה לא ריקה, לכן נותר לבדוק סגירות לכפל ולהופכי – בדקו זאת ישירות. הסדר של  $G$  הוא  $3 \times 3 \times 3 = 27$  (כי יש שלוש אפשרויות לבחור את  $a$ , שלוש אפשרויות לבחור את  $b$  ושלוש – את  $c$ ).  
בודקים ישירות כי כל איבר ב-  $G$  פרט לאיבר היחידה הוא מסדר 3 (ז"א – עבור כל מטריצה – כשמכפילים אותה בעצמה 3 פעמים – נקבל את האיבר היחידה – מטריצת הזהות. אין הכוונה לבדוק את הסדר של האיברים ב- $\mathbb{Z}_3$ ).

ב) לא. החבורה מסעיף א) מהווה דוגמא נגדית.

### שאלה 3

- א. מצאו את הספרה האחרונה של המספר  $79^{207}$ .
- ב. מצאו את הסדר של  $35 \in (\mathbb{Z}_{75}, +)$ .

פתרון:

א.

$$79^{207} \pmod{10} = 9^{207} \pmod{10} = (9^2)^{103} \cdot 9 \pmod{10} = 1^{103} \cdot 9 \pmod{10} = 9$$

ב.

האיבר הניטרלי הוא 0, והפעולה היא חיבור, לכן צריך למצוא את הסדר k של  $a=35$ :

אזי, על פי הנוסחה:

$$k = 75 / (75, 35) = 75 / 5 = 15$$

### שאלה 4

- א. מצא את תת החבורה הציקלית ב- $S_7$  הנוצרת על-ידי התמורה  $(123)(57)$ .
- ב. בדקו שמתקיים  $S_3 = \langle (12), (123) \rangle = \langle (12), (23) \rangle$ .

פתרון:

$$\begin{aligned}
((123)(57))^1 &= (123)(57) \\
((123)(57))^2 &= (123)^2(57)^2 = (132) \\
((123)(57))^3 &= (123)^3(57)^3 = (57) \\
((123)(57))^4 &= (123)^4(57)^4 = (123) \\
((123)(57))^5 &= (123)^5(57)^5 = (132)(57) \\
((123)(57))^6 &= (123)^6(57)^6 = Id
\end{aligned}$$

.א.

ב. מספיק להראות כי היוצרים של כל קבוצה נמצאים כל אחת מהקבוצות.

$$\begin{aligned}
(12)(23) &= (123) : (123) \in \langle (12), (23) \rangle \\
(123)^2(12) &= (23) : (23) \in \langle (12), (123) \rangle
\end{aligned}$$

## שאלה 5

- א. מצאו תת חבורה ציקלית מסדר 8 ותת חבורה לא ציקלית מסדר 8 של  $U_{32}$ .
- ב. מצאו בתוך  $(\mathbb{Q}, +)$  שרשרת אינסופית (עולה) של תת חבורות ציקליות.
- רמז: הראשונה נוצרת על ידי 1.

פתרון:

$$\langle 3 \rangle = \{3, 9, 27, 17, 19, 25, 11, 1\} \quad \text{א.}$$

$$\langle 9, 15 \rangle = \{1, 7, 9, 15, 17, 23, 25, 31\} \quad \text{לא ציקלית (לדוגמא)}$$

- ב.  $\langle 1 \rangle \leq \langle \frac{1}{2} \rangle \leq \langle \frac{1}{4} \rangle \leq \langle \frac{1}{8} \rangle \dots$  ובאופן כללי, נבחר את האיבר היוצר את הסדרה הנ"ל ע"י  $\frac{1}{2^{(n-1)}}$ .

## שאלה 6

תהי  $G$  חבורה. הראו שאם  $a, b \in G$  מתחלפים (כלומר  $ab = ba$ ) אזי  $\langle a, b \rangle$  היא תת חבורה אבליית של  $G$ .

פתרון: ראינו כי עבור חבורות אבליות מתקיים:

$\langle a, b \rangle = \{a^n b^m \mid n, m \in \mathbb{Z}\}$ . אמנם כאן צריך להוכיח כי  $\langle a, b \rangle$  אבלית בגלל ש  $a$  ו  $b$  מתחלפים הדבר נכון גם כאן. ניקח שני איברים ב  $\langle a, b \rangle$ ,  $x, y \in \langle a, b \rangle$ , הם ניתנים להצגה כך  $x = a^{n_1} b^{m_1}$ ,  $y = a^{n_2} b^{m_2}$ . אזי

$$xy = a^{n_1} b^{m_1} a^{n_2} b^{m_2} \xrightarrow{ab=ba} xy = a^{n_2} b^{m_2} a^{n_1} b^{m_1} = yx$$

מכאן ש  $\langle a, b \rangle$  תת חבורה אבלית.

## שאלה 7

א. הראו ש-  $(\mathbb{Q}, +, 0)$  אינה נוצרת סופית.  
פתרון:

נניח בשלילה כי  $\mathbb{Q}$  כן נוצרת סופית, כלומר

$$\mathbb{Q} = \left\langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_{k-1}}{b_{k-1}}, \frac{a_k}{b_k} \right\rangle$$

כאשר  $\frac{a_i}{b_i}$  הינו שבר מצומצם. נראה כי

$$\frac{1}{lcm(b_1, \dots, b_k) + 1} \notin \left\langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_{k-1}}{b_{k-1}}, \frac{a_k}{b_k} \right\rangle$$

בתרגול ראינו שעבור חבורה אבלית הנוצרת ממספר סופי של איברים כל איבר בקבוצה ניתן לייצג כך

$$n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \dots + n_{k-1} \frac{a_{k-1}}{b_{k-1}} + n_k \frac{a_k}{b_k} = c \quad n_1, \dots, n_k \in \mathbb{Z}$$

מכיוון שהשברים מצומצמים נקבל שניתן להציג את  $c$  כך

$$c = \frac{M}{lcm(b_1, \dots, b_k)} \quad M \in \mathbb{Z}$$

וברור כי

$$\left| \frac{M}{\text{lcm}(b_1, \dots, b_k)} \right| > \frac{1}{\text{lcm}(b_1, \dots, b_k) + 1}$$

מכאן סתירה ונקבל כי

$$\mathbb{Q} \neq \left\langle \frac{a_1}{b_1}, \frac{a_2}{b_2}, \dots, \frac{a_{k-1}}{b_{k-1}}, \frac{a_k}{b_k} \right\rangle$$

ב. הראו ש-  $\mathbb{Z}_n \times \mathbb{Z}_m$  נוצרת סופית. מצאו קבוצת איברים יוצרים.

פתרון:

כל איבר ב-  $\mathbb{Z}_n \times \mathbb{Z}_m$  הינו מהצורה  $(a_1, a_2)$  כאשר  $a_1 \in \mathbb{Z}_n, a_2 \in \mathbb{Z}_m$ . כלומר

$$\begin{aligned} a &= a_1(1,0) + a_2(0,1) \\ \Rightarrow \langle (1,0), (0,1) \rangle &= \mathbb{Z}_n \times \mathbb{Z}_m \end{aligned}$$

### שאלת אתגר

מספר  $n$  נקרא **חופשי מריבועים** אם לא קיים  $p$  ראשוני כך ש-  $p^2$  מחלק את  $n$ . כלומר  $n$  הוא מכפלה של ראשוניים זרים או 1.

- מצאו חבורה  $G$  כך שלכל  $n \in \mathbb{N}$  מתקיים: קיים איבר  $a \in G$  כך ש-  $o(a) = n$ .
  - מצאו חבורה  $G$  כך שהסדר של כל איבר בה הוא חופשי מריבועים.
  - מצאו חבורה  $G$  כך שלכל  $n \in \mathbb{N}$  חופשי מריבועים מתקיים כי קיים איבר  $a \in G$  כך ש-  $o(a) = n$  ושהסדר של כל איבר בחבורה הוא חופשי מריבועים או  $\infty$ .
- (רמז: מכפלה ישרה של חבורות ציקליות מסויימות. מי הם האיברים מסדר  $?\infty$ )

### פתרון

(מבוסס על הפתרון המוצלח של גיא בלשר)

א. נראה שתי חבורות כאלו. הראשונה היא מכפלה ישרה אינסופית של כל החבורות הציקליות הסופיות  $G = \prod_{i=1}^{\infty} \mathbb{Z}_i$ . איבר היחידה בחבורה  $G$  הוא "הוקטור" שכולו אפסים  $(0,0,\dots)$ . עבור כל  $n \in \mathbb{N}$  ישנו האיבר  $(0,\dots,0,1,0,\dots)$  שבו ה-1 הוא במקום ה- $n$ , וסדר איבר זה הוא  $n$ .

החבורה השנייה, שראינו בהרצאה, היא  $\Omega_{\infty} = \bigcup_{i=1}^{\infty} \Omega_i = \bigcup_{i=1}^{\infty} \{z \in \mathbb{C} : z^i = 1\}$

בדומה לשאלה מן התרגול, לכל  $n \in \mathbb{N}$  האיבר  $\omega_n = \text{cis}\left(\frac{2\pi}{n}\right)$  שייך ל- $\Omega_{\infty}$

(שכן  $\omega_n^n = \text{cis}\left(\frac{2\pi}{n}\right)^n = \text{cis}\left(n \cdot \frac{2\pi}{n}\right) = \text{cis}(2\pi) = 1$ ) והוא מסדר  $n$ .

ב. המטרה של סעיף זה הייתה לעזור למצוא תשובה לסעיף הבא. כל חבורה סופית מסדר חופשי מריבועים תספיק. הרי הסדר של איבר מחלק את סדר החבורה, ומספר שמחלק חופשי מריבועים הוא חופשי מריבועים. אפילו החבורה הטריטוריאליית  $\{e\}$  עונה על הדרישה.

ג. נסמן את קבוצת המספרים החופשיים מריבועים ב- $A$ .

טענה שנצטרך להמשך: אם  $m, n$  חופשיים מריבועים, אז גם  $[n, m]$  חופשי מריבועים. נניח בשלילה כי  $[n, m]$  אינו חופשי מריבועים, אזי קיים ראשוני  $p$  כך שמתקיים  $p^2 \mid [n, m]$ . לכן נקבל כי  $p^2 \mid n$  או  $p^2 \mid m$ , שהרי  $[n, m]$  הוא

הכפולה המשותפת המינימלית ולא ייתכן כי  $n \mid \frac{[n, m]}{p}$  וגם  $m \mid \frac{[n, m]}{p}$ . אבל אז

נגיע לסתירה להנחה כי  $n, m$  הם חופשיים מריבועים.

מזכר בטענה לגבי סדר מכפלת איברים  $a, b$  בחבורה אבלית:

$[o(a), o(b)] \mid o(ab)$ . לכן אם סדר האיברים  $a, b$  חופשי מריבועים, אז גם סדר

המכפלה  $ab$  חופשי מריבועים.

נסתכל על החבורה  $\Omega_A = \bigcup_{i \in A} \Omega_i = \bigcup_{i \in A} \{z \in \mathbb{C} : z^i = 1\}$  שהיא תת-חבורה של

$\Omega_{\infty}$ . נראה כי מתקיימת סגירות: יהיו  $a_1, a_2 \in \Omega_A$  ונרצה להראות  $a_1 a_2 \in \Omega_A$ .

לכן קיימים  $n_1, n_2 \in A$  וכמו כן  $k_1, k_2 \in \mathbb{N}$  כך ש-

$$a_1 = \text{cis}\left(\frac{2\pi}{n_1} k_1\right), a_2 = \text{cis}\left(\frac{2\pi}{n_2} k_2\right)$$

$$a_1 a_2 = \text{cis}\left(\frac{2\pi}{n_1} k_1\right) \text{cis}\left(\frac{2\pi}{n_2} k_2\right) = \text{cis}\left(\frac{2\pi}{[n_1, n_2]} k_3\right)$$

לבחור  $k_3 = \frac{n_1}{(n_1, n_2)} k_2 + \frac{n_2}{(n_1, n_2)} k_1$ . הסדר של  $a_1, a_2$  הוא חופשי מריבועים

ולכן הסדר של  $a_1 a_2$  מחלק את  $[n_1, n_2]$ , כלומר הוא חופשי מריבועים. הוכחת קיום איבר יחידה, קיבוציות הפעולה וקיום הופכי היא קלה, כתת־חבורה של  $\Omega_\infty$ .

נשים לב כי לכל  $n \in A$  (מספר חופשי מריבועים) האיבר  $\omega_n = \text{cis}\left(\frac{2\pi}{n}\right)$  הוא

מסדר  $n$  כדרוש. בחבורה זו הסדר של כל איבר הוא סופי.

דוגמה נוספת היא החבורה  $G = \prod_{p \text{ prime}} \mathbb{Z}_p$  שהיא מכפלה ישרה של כל

החבורות הציקליות מסדר ראשוני. האיברים מסדר אינסופי בחבורה זו הם האיברים עם מספר לא סופי של איברים לא אפסיים (הסבירו!). הסדר של כל איבר מסדר סופי הוא חופשי מריבועים. הסדר של איבר  $(0, \dots, 0, a_i, 0, \dots)$

שכולו אפסים פרט ל- $a_i$  במקום ה- $i$  הוא  $p_i$ . איבר מסדר סופי נראה כמו

$$\{p_{i_1}, \dots, p_{i_k}\} \text{ כשיש מספר סופי של ראשוניים } (0, \dots, 0, a_{i_1}, 0, \dots, 0, a_{i_k}, 0, \dots)$$

שברכיב  $\mathbb{Z}_{p_i}$  במכפלה הישרה הוא לא אפסי. הסדר של איבר זה הוא

מסדר  $n$ . שהוא חופשי מריבועים. בדרך זו לכל  $n \in A$  אפשר לבנות איבר

מסדר  $n$ .

לקבוצה של האיברים שיש להם מספר סופי של איברים לא אפסיים

במכפלה ישרה קוראים הסכום הישר, ומשתמשים בדרך כלל בסימון  $\bigoplus$ .

בטענה מן התירגול הראנו כי בחבורה אבלית (כמו  $G$ ) קבוצת האיברים

מסדר סופי מהווה תת־חבורה. במקרה שלנו זה בדיוק הסכום הישר

$$H = \bigoplus_{p \text{ prime}} \mathbb{Z}_p \text{ אפשר לבדוק כי } \Omega_A \cong H \text{ לפי האיזומורפיזם}$$

$$\varphi: (0, \dots, 0, a_{i_1}, 0, \dots, 0, a_{i_k}, 0, \dots) \mapsto \text{cis}\left(2\pi\left(\frac{a_{i_1}}{p_{i_1}} + \frac{a_{i_2}}{p_{i_2}} + \dots + \frac{a_{i_k}}{p_{i_k}}\right)\right)$$

$$\text{מהצורה } (0, \dots, 0, 1, 0, \dots) \text{ ל-} \text{cis}\left(\frac{2\pi}{p_i}\right)$$

אגב, גם החבורה  $\prod_{i \in A} \mathbb{Z}_i$  היא דוגמה שעונה לדרישות השאלה. האיברים

מסדר אינסופי בחבורה זו, הם שוב האיברים עם מספר לא סופי של איברים

לא אפסיים. למה היא לא איזומורפית לאף אחת מהחבורות הקודמות

שהוצגו בשאלה זו?

**בהצלחה!**