

## אלגברה מופשטת – פתרון תרגיל 2

### שאלה 1

- א. מצאו את המחלק המשותף המקסימלי: (5614, 1260).  
ב. מצאו  $\alpha, \beta \in \mathbb{Z}$  כך ש-  $1525\alpha + 927\beta = 1$ .

### פתרון

שני התרגילים נפתרים עם אוקלידס. ניתן רק את התשובות הסופיות:

- א. 14;  
ב.  $\alpha = 448, \beta = -737$ .

### שאלה 2

- א) תהי  $G$  חבורה סופית,  $a, b \in G$ . הוכיחו:  $ord(ab) = ord(ba)$   
(רמז: אם  $ord(ab) = n, ord(ba) = m$ , הסתכלו על  $(ba)^{n+1}$  ועל  $(ab)^{m+1}$ .)  
ב) תהי  $G$  חבורה,  $ord(g) = n, g \in G$ . הוכיחו ש-  $g^a = g^b$  אם  $a \equiv b \pmod{n}$ .

### פתרון

- א) נסתכל על  $(ba)^{n+1}$ :  
 $(ba)^{n+1} = ba \cdot \dots \cdot ba = b(ab)^n a = ba \rightarrow (ba)^n = 1 \rightarrow m|n$   
ואם נסתכל על  $(ab)^{m+1}$ , נקבל ש-  $n|m$  ולכן  $m = n$ .  
ב) יישום ישיר של המשפט הבא: אם  $g^m = 1$  אזי  $o(g)$  מחלק את  $m$ .

ביתר פירוט:

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

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

מש"ל

### שאלה 3

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?

### פתרון

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  $3 \cdot 3 \cdot 3 = 27$  (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 איבר היחידה – מטריצת הזהות. אין הכוונה לבדוק את הסדר של האיברים ב- $\mathbb{Z}_3$ ).

ב. לא. החבורה מסעיף א' מהווה דוגמה נגדית, שכן כל איבר (פרט ליחידה) הוא מסדר 3, אך החבורה אינה אבלית.

מש"ל

### שאלה 4

אילו מן החבורות הבאות הן ציקליות? עבור החבורות הציקליות מצאו יוצר, אחרת הסבירו מדוע החבורה אינה ציקלית.

א.  $\mathbb{Z}_{10} \times \mathbb{Z}_{15}$ ;

ב.  $\mathbb{Z}_5 \times \mathbb{Z}_2$ ;

ג.  $U_{20}$ ;

ד.  $U_8 \times U_9$ .

### פתרון

א. אינה ציקלית כי אין איבר מסדר 150. אכן, לכל  $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{15}$  מתקיים:

$$30(a, b) = (0, 0)$$

ב. החבורה ציקלית ונוצרת על ידי  $(1, 1)$ .

- ג.  $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$  ולכן  $|U_{20}| = 8$ . החבורה אינה ציקלית שכן אין בה איבר מסדר 8 (בדקו!).
- ד.  $U_8 = \{1, 3, 5, 7\}$ ,  $U_9 = \{1, 2, 4, 5, 7, 8\}$  יהי  $(a, b) \in U_8 \times U_9$ , אזי  $(a, b)^{12} = (a^{12}, b^{12}) = (1, 1)$  ולכן  $o((a, b)) \leq 12$  ולכן החבורה אינה ציקלית.

מש"ל

## שאלה 5

- א. תהיינה  $H, G_1, G_2$  תת-חבורות של  $G$ . הוכיחו: אם  $H \subseteq G_1 \cup G_2$  אזי  $H \subseteq G_1$  או  $H \subseteq G_2$ .
- ב. מצאו דוגמה לחבורה  $G$  ולתת חבורות  $H, G_1, G_2, G_3 \leq G$  כך ש-  
 $H \subseteq G_1 \cup G_2 \cup G_3$  אבל  $H$  אינה מוכלת בשום איחוד מהצורה  $G_i \cup G_j$ .

## פתרון

- א. תהי  $H \subseteq G_1 \cup G_2$ . נניח בשלילה שקיימים  $t \in H \setminus G_2$ ,  $h \in H \setminus G_1$  (מ) שבפרט אומר  $(t \in G_1, h \in G_2)$ . מכיוון ש- $t, h \in H$  מתקיים  $th \in H$  ולכן  $th \in G_1 \vee th \in G_2$ . נניח ש- $th \in G_1$ , מכיון ש- $t \in G_1$  גם  $t^{-1} \in G_1$  ולכן  $t^{-1}(th) = (t^{-1}t)h = 1h = h \in G_1$  לסתירה במקרה בו  $th \in G_2$ .
- ב. נתבונן ב- $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ , ובתת החבורות  
 $G_1 = \{0\} \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0, 0), (0, 1, 0), (0, 0, 1), (0, 1, 1)\}$   
 $G_2 = \mathbb{Z}_2 \times \{0\} \times \mathbb{Z}_2 = \{(0, 0, 0), (1, 0, 0), (0, 0, 1), (1, 0, 1)\}$   
 $G_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \{0\} = \{(0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 0)\}$   
נגדיר:  $H = \{(0, 0, 0), (0, 1, 1), (1, 1, 0), (1, 0, 1)\}$  קל לראות שזו אכן תת חבורה. מתקיים  $H \subseteq G_1 \cup G_2 \cup G_3$ , ושימו לב שהיא אכן אינה מוכלת באף איחוד של שניים.  
הערה: מכיוון שכבר ראיתם הגדרה של חבורה נוצרת סופית, שימו לב שיכולנו לכתוב  $H = \langle (1, 1, 0), (0, 1, 1) \rangle$ , במקום לתת את ההצגה המפורשת.

מש"ל

## שאלה 6

- 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

- א. החבורה הציקלית (יש יותר מאחת) היא  $\langle 3 \rangle = \{3, 9, 27, 17, 19, 25, 11, 1\}$ . תת חבורה לא ציקלית (לדוגמה)  $\langle 9, 15 \rangle = \{1, 7, 9, 15, 17, 23, 25, 31\}$ .
- ב. הנה שרשרת כזאת לדוגמה:  $\mathbb{Z} \leq \frac{1}{2}\mathbb{Z} \leq \frac{1}{4}\mathbb{Z} \leq \dots \leq \frac{1}{2^n}\mathbb{Z} \leq \frac{1}{2^{n+1}}\mathbb{Z} \leq \dots$ .

מש"ל

## שאלה 7

תהי  $G$  חבורה. נסמן  $m_2(G) = |\{x \in G : x^2 = 1\}|$ , כלומר  $m_2(G)$  הוא מספר הפתרונות של המשוואה  $x^2 = 1$  בחבורה  $G$ .

- א. הראו שבכל חבורה סופית  $G$  מתקיים  $m_2(G) \equiv |G| \pmod{2}$ ;
- [שימו לב שהחבורה לא בהכרח אבלית!]
- ב. הראו שבכל חבורה עם מספר **זוגי** של איברים קיים איבר מסדר 2. רמז לסעיף א': הגדירו על  $G$  את יחס השקילות הבא:  
 $x \equiv y \Leftrightarrow (x = y \vee xy = 1)$  ושימו לב שהאיברים שריבועם אינו 1 שייכים למחלקות שקילות בגודל 2.
- הערה: הרמז מציע דרך פתרון אלגנטית. כדאי שלפני זה תנסו להגיע לאיזשהו פתרון אינטואיטיבי על סמך הרעיונות שכבר ראינו בכיתה.

## פתרון

- א. נגדיר את היחס המוצע ברמז. זהו אכן יחס שקילות (בדקו!). מה הן מחלקות השקילות? אם  $a \in G$  מקיים  $a^2 = 1$  אזי הוא הופכי לעצמו, כלומר,  $a = a^{-1}$ , ולכן  $[a] = \{a\}$ . אכן, אם היה איבר נוסף במחלקת שקילות זו, נניח  $a \neq x \in [a]$  אזי היה מתקיים  $xa = 1$  ואז  $x = a^{-1} = a$ . מחלקת השקילות של איבר היחידה היא מגודל 1:  $[1] = \{1\}$ .
- מה לגבי שאר האיברים? אם  $1 \neq b \in G$  אינו מסדר 2, אזי  $[b] = \{b, b^{-1}\}$  (מדוע אין שם עוד איברים? כי ההופכי הינו יחיד). כעת, האיחוד של כל מחלקות השקילות נותן את החבורה כולה, לכן

$$G = \{1\} \cup \left( \bigcup_{o(a)=2} [a] \right) \cup \left( \bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b] \right)$$

(שימו לב שזה איחוד זר!). נשים לב ש-

$$\text{ולכן } m_2(G) = \left| \{1\} \cup \left( \bigcup_{o(a)=2} [a] \right) \right|$$

$$|G| = \left| \{1\} \cup \left( \bigcup_{o(a)=2} [a] \right) \cup \left( \bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b] \right) \right| = m_2(G) + 2k$$

מחלקות השקילות באיחוד  $\bigcup_{\substack{o(b) \neq 2 \\ b \neq 1}} [b]$ . מכיוון ש-  $|G| = m_2(G) + 2k$  נקבל ש-

$$|G| \equiv m_2(G) \pmod{2}, \text{ כנדרש.}$$

ב. תהא  $G$  חבורה עם מספר זוגי של איברים, נניח  $2k$ . נניח בשלילה שאין איבר מסדר 2, ולכן  $m_2(G) = 1$ . לפי הסעיף הקודם נקבל  $1 \equiv 2k \pmod{2}$ , וזאת כמובן סתירה. לכן קיים ב- $G$  איבר מסדר 2.

מש"ל