

תרגיל 1 – אלגברה מופשטת 1

1. מצא  $a$  ו  $b$  המקיימים  $\gcd(r, s) = ar + bs$ , כאשר

א.  $r = 11, s = 17$

ב.  $r = 8, s = 12$

**פתרון**

א.  $\gcd(r, s) = 1 = 2 \cdot 17 - 3 \cdot 11$

ב.  $\gcd(r, s) = 4 = 1 \cdot 12 - 1 \cdot 8$

2. יהיו  $a, b, c \in \mathbb{Z}$  כך ש  $a|bc$  ו  $\gcd(a, b) = 1$  הוכח ש  $a|c$ .

**פתרון**

נתון ש  $\gcd(a, b) = 1$  על פי משפט ה  $\gcd$  קיימים  $m, n$  כך ש  $ma + nb = 1$ . נניח ש  $c \in \mathbb{Z}$  כך ש

$a|bc$  ז"א קיים  $q \in \mathbb{Z}$  כך ש  $bc = aq$ . מכיוון ש  $ma + nb = 1$  נקבל  $c = mac + nbc$  ומכיוון ש

$bc = aq$  נקבל  $c = mac + naq = a(mc + nq)$  ז"א  $a|c$ .

3. א. הוכח ש  $\Omega_\infty = \{w \in \mathbb{C} \mid w^m = 1 \text{ ש } m \in \mathbb{Z} \text{ קיים}\}$  חבורה אבלית ביחס לפעולת הכפל של

מספרים מרוכבים.

ב. הוכח ש  $\Omega = \{z \in \mathbb{C} \mid |z| = 1\}$  חבורה אבלית ביחס לפעולת הכפל של מספרים מרוכבים.

**פתרון**

א.

**סגירות לכפל**

יהיו  $\omega, \rho \in \Omega_\infty$  אזי קיימים  $m, n \in \mathbb{Z}$  כך שמתקיים:  $\omega^m = \rho^n = 1$ .

$$(\omega\rho)^{mn} = \omega^{mn} \cdot \rho^{mn} = \omega^{mn} \cdot \rho^{nm} = (\omega^m)^n \cdot (\rho^n)^m = 1^n \cdot 1^m = 1$$

השוויון הראשון נובע מהקומוטטיביות ב  $\mathbb{C}$ , השוויון השני נובע מהקומוטטיביות ב  $\mathbb{Z}$ , השוויון השלישי

נובע מהגדרת החזקה ומכיוון ש  $(\mathbb{C}^*, \cdot)$  חבורה.

**קיום איבר הופכי**

יהי  $\omega \in \Omega_\infty$  ולכן  $\omega \in \mathbb{C}^*$  (לא קיים  $n \in \mathbb{Z}$  כך ש  $0^n = 1$  ולכן  $0 \notin \Omega_\infty$  ז"א  $\Omega_\infty \subseteq \mathbb{C}^*$ ) אז קיים  $n$

שלם כך ש  $\omega^n = 1$ .  $\omega \in \mathbb{C}^*$  ולכן קיים ל  $\omega$  איבר הופכי  $\omega^{-1}$ . נראה ש  $\omega^{-1} \in \Omega_\infty$ .

$$(\omega^{-1})^n = \omega^{-1 \cdot n} = \omega^{n \cdot (-1)} = (\omega^n)^{-1} = 1^{-1} = 1$$

מכיוון ש  $\Omega_\infty \subseteq \mathbb{C}^*$  וש  $(\mathbb{C}^*, \cdot)$  חבורה נקבל מהקריטריון המקוצר ש  $\Omega_\infty$  תת חבורה של  $\mathbb{C}^*$ .

ב.

מכיוון ש  $\Omega \neq 0$  כי  $|0| = 0 \neq 1$  אז  $\Omega \subseteq \mathbb{C}^*$ . נוכיח שוב ש  $\Omega$  תת חבורה על פי הקריטריון המקוצר.

**סגירות לכפל**

יהיו  $z, u \in \Omega$ .  $|z \cdot u| = |z| \cdot |u| = 1 \cdot 1 = 1$  ולכן  $z \cdot u \in \Omega$ .

**קיום איבר הופכי**

יהי  $\Omega$ ,  $z \in \Omega$ ,  $z^{-1} = (\overline{z \cdot \bar{z}})^{-1} \cdot \bar{z}$ , מכיוון ש  $|z|=1$  אז  $z \cdot \bar{z} = 1$  ואז  $z^{-1} = \bar{z}$  ו  $|z^{-1}| = |\bar{z}| = |z| = 1$ .

4. תהיי  $G$  חבורה הוכח את הטענות הבאות:

א. אם לכל  $a \in G$  מתקיים  $a^2 = e$  אז  $G$  אבלית.

ב. אם לכל  $a, b \in G$  מתקיים  $(ab)^2 = a^2 b^2$  אזי  $G$  חבורה אבלית.

#### פתרון

א.

צריך להוכיח שלכל  $b, c \in G$  מתקיים  $bc = cb$ . נתון שלכל  $a \in G$  מתקיים  $a \cdot a = e$  ולכן

$$.a = a \cdot (a \cdot a^{-1}) = (a \cdot a) \cdot a^{-1} = e \cdot a^{-1} = a^{-1} \Rightarrow a = a^{-1}$$

בפרט לכל  $b, c \in G$  מתקיים  $(bc)^{-1} = bc$ . ראינו ש  $(bc)^{-1} = c^{-1} b^{-1}$  ומכיוון שלכל  $a \in G$  מתקיים

$$.bc = (bc)^{-1} = c^{-1} b^{-1} = cb$$

ב.

יהיו  $a, b \in G$

$$.ba = (a^{-1} a)(ba)(bb^{-1}) = a^{-1}(ab)(ab)b^{-1} = a^{-1}(ab)^2 b^{-1} = a^{-1} a^2 b^2 b^{-1} = ab$$

5. א. הוכח שהקבוצה  $\mathbb{R}^3$  עם הפעולה הבאה:

$$(x_1, y_1, z_1) \cdot (x_2, y_2, z_2) = (x_1 + x_2 + z_1 y_2, y_1 + y_2, z_1 + z_2)$$

ב. את האיבר ההופכי ל  $(30, 7, 2012)$ .

#### פתרון

א.

#### סגירות

יהיו  $(x_1, y_1, z_1), (x_2, y_2, z_2) \in \mathbb{R}^3$  מכיוון שהקבוצה  $\mathbb{R}$  סגורה לכפל וחיבור נקבל ש

$$.(x_1 + x_2 + z_1 y_2, y_1 + y_2, z_1 + z_2) \in \mathbb{R}^3 \Leftarrow x_1 + x_2 + z_1 y_2 \in \mathbb{R} \wedge y_1 + y_2 \in \mathbb{R} \wedge z_1 + z_2 \in \mathbb{R}$$

#### אסוציאטיביות

יהיו  $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) \in \mathbb{R}^3$

$$((x_1, y_1, z_1) \cdot (x_2, y_2, z_2)) \cdot (x_3, y_3, z_3) = (x_1 + x_2 + z_1 y_2, y_1 + y_2, z_1 + z_2) \cdot (x_3, y_3, z_3) =$$

$$= (x_1 + x_2 + z_1 y_2 + x_3 + (z_1 + z_2) y_3, (y_1 + y_2) + y_3, (z_1 + z_2) + z_3)$$

$$(x_1, y_1, z_1) \cdot ((x_2, y_2, z_2) \cdot (x_3, y_3, z_3)) = (x_1, y_1, z_1) \cdot (x_2 + x_3 + z_2 y_3, y_2 + y_3, z_2 + z_3) =$$

$$= (x_1 + x_2 + x_3 + z_2 y_3 + z_1 (y_2 + y_3), y_1 + (y_2 + y_3), z_1 + (z_2 + z_3))$$

מכיוון ש  $\mathbb{R}$  שדה נקבל ש

$$x_1 + x_2 + x_3 + z_2 y_3 + z_1 (y_2 + y_3) = x_1 + x_2 + z_1 y_2 + x_3 + (z_1 + z_2) y_3$$

$$. y_1 + (y_2 + y_3) = (y_1 + y_2) + y_3$$

$$z_1 + (z_2 + z_3) = (z_1 + z_2) + z_3$$

#### קיום איבר יחידה

איבר היחידה הוא  $(0, 0, 0)$  מכיוון ש

$$(x_1, y_1, z_1) \cdot (0, 0, 0) = (x_1 + 0 + z_1 \cdot 0, y_1 + 0, z_1 + 0) = (x_1, y_1, z_1)$$

$$(0, 0, 0) \cdot (x_1, y_1, z_1) = (0 + x_1 + 0 \cdot y_1, 0 + y_1, 0 + z_1) = (x_1, y_1, z_1)$$

### איבר הופכי

$$(x, y, z) \cdot (zy - x, -y, -z) = (x + zy - x + z \cdot (-y), y - y, z - z) = (0, 0, 0)$$

$$(zy - x, -y, -z) \cdot (x, y, z) = (zy - x + x - zy, -y + y, -z + z) = (0, 0, 0)$$

האיבר ההופכי של  $(x, y, z)$  הוא  $(zy - x, -y, -z)$ .

### לא קומוטטיבי

$$(1, 2, 3) \cdot (4, 5, 6) = (1 + 4 + 3 \cdot 5, 2 + 5, 3 + 6) = (20, 7, 9)$$

$$(4, 5, 6) \cdot (1, 2, 3) = (4 + 1 + 6 \cdot 2, 5 + 2, 6 + 3) = (17, 7, 9)$$

קיבלנו שני איברים  $a, b \in \mathbb{R}^3$  כך ש  $ab \neq ba$ .

ב.

ראינו בסעיף א שהאיבר ההופכי ל  $(x, y, z)$  הוא  $(zy - x, -y, -z)$ , ולכן האיבר ההופכי ל  $(30, 7, 2012)$

הוא  $(14054, -7, -2012)$ .

6. כמה מבנים אלגבריים בינריים קיימים מעל קבוצה עם 5 איברים כך שהפעולה היא:

א. קומוטטיבית.

ב. קומוטטיבית ובעלת איבר נטרלי.

### פתרון

א.

	a	b	c	d	e
a	11	1	2	3	4
b	1	12	5	6	7
c	2	5	13	8	9
d	3	6	8	14	10
e	4	7	9	10	15

לכל אחד מהמשבצות הממוספרות יש 5 אופציות ולכן מספר האפשרויות הוא  $5^{15}$ .

ב.

	e	a	b	c	d
e	e	a	b	c	d
a	a	7	1	2	3
b	b	1	8	4	5
c	c	2	4	9	6
d	d	3	5	6	10

לכל אחד מהמשבצות הממוספרות יש 5 אופציות ולכן מספר האפשרויות הוא  $5^{10}$ . כל אחד מהאיברים יכול להיות איבר יחידה ולכן סה"כ יש  $5^{11}$  אופציות.

7. נביט בקבוצה  $(\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$  ונגדיר פעולה \* על הקבוצה המקיימת:

$$(a,b)*(c,d) = \begin{cases} (a+c-b,d) & c > b \\ (a,b-c+d) & \text{otherwise} \end{cases}$$

א. הראו כי הקבוצה יחד עם הפעולה הנ"ל מהווה מונואיד.  
 ב. מהי קבוצת האיברים ההפיכים משמאל? האם היא חבורה?

### פתרון

א.

### סגירות

יהיו  $(a,b), (c,d) \in (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$

מקרה 1  $c > b$  ולכן

$$(a+c-b,d) \in (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\}) \Leftrightarrow a+c-b \in \mathbb{N} \cup \{0\} \Leftrightarrow a+c-b > 0 \Leftrightarrow c-b > 0$$

מקרה 2  $c \leq b$  ולכן

$$(a,b-c+d) \in (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\}) \Leftrightarrow b-c+d \in \mathbb{N} \cup \{0\} \Leftrightarrow b-c+d \geq 0 \Leftrightarrow b-c \geq 0$$

### אסוציאטיביות

יהיו  $(a,b), (c,d), (e,f) \in (\mathbb{N} \cup \{0\}) \times (\mathbb{N} \cup \{0\})$

מקרה 1  $c > b$

$$((a,b)*(c,d))*(e,f) = (a+c-b,d)*(e,f) = \begin{cases} (a+c-b+e-d,f) & e > d \\ (a+c-b,d-e+f) & \text{otherwise} \end{cases}$$

נשים לב שאם  $c > b \wedge e > d$  אז  $c+e-d > b$  ולכן:

$$(a,b)*((c,d),(e,f)) = \begin{cases} (a,b)*(c+e-d,f) = (a+c+e-d-b,f) & e > d \\ (a,b)*(c,d-e+f) = (a+c-b,d-e+f) & \text{otherwise} \end{cases}$$

מקרה 2  $c \leq b$

$$((a,b)*(c,d))*(e,f) = (a,b-c+d)*(e,f) = \begin{cases} (a+e-(b-c+d),f) & e > b-c+d \\ (a,b-c+d-e+f) & \text{otherwise} \end{cases}$$

שימו לב  $e > d \Leftrightarrow c \leq b \wedge e > b-c+d$  נקבל

$$(a,b)*((c,d),(e,f)) = \begin{cases} (a,b)*(c+e-d,f) = (a+c+e-d-b,f) & e > b-c+d \\ (a,b)*(c+e-d,f) = (a,b-(c+e-d)+f) & d < e \leq b-c+d \\ (a,b)*(c,d-e+f) = (a,b-c+d-e+f) & \text{otherwise} \end{cases}$$

ובסה"כ נקבל ש

$$(a,b)*((c,d),(e,f)) = \begin{cases} (a+e-(b-c+d),f) & e > b-c+d \\ (a,b-c+d-e+f) & \text{otherwise} \end{cases}$$

### קיום איבר יחידה

$(0,0)$  הוא איבר יחידה מכיוון ש

$$(a,b)*(0,0) = (a,b-0+0) = (a,b)$$

$$(0,0)*(a,b) = (0+a-0,b) = (a,b)$$

ב.

קבוצת האיברים ההפיכים משמאל היא  $\{(a,0) : a \in \mathbb{N} \cup \{0\}\}$

מכיוון ש  $(0,a)*(a,0) = (0,a-a+0) = (0,0)$  קבוצת ההפיכים משמאל לא חבורה מכיוון שהאיברים ההופכים אינם בקבוצה.  $(0,a)$  לא נמצא בקבוצה האיברים ההפיכים משמאל.

8. תהיינה  $H_1, H_2$  תת חבורות של  $G$ . הוכח כי  $H_1 \cup H_2$  תת חבורה של  $G$  אם ורק אם

$$H_2 \subseteq H_1 \text{ או } H_1 \subseteq H_2$$

### פתרון

$\Rightarrow$  נתון ש  $H_1 \subseteq H_2$  או  $H_2 \subseteq H_1$ . נניח ב.ה.ג.כ ש  $H_1 \subseteq H_2$  ואז  $H_1 \cup H_2 = H_2$  נתון ש  $H_2$  תת חבורה של  $G$  ולכן  $H_1 \cup H_2$  תת חבורה של  $G$ .

$\Leftarrow$

נניח ש  $H_1 \cup H_2$  תת חבורה של  $G$ .

נניח בשלילה ש  $H_1$  לא מוכל ב  $H_2$  וגם  $H_2$  לא מוכל ב  $H_1$ .

ז"א קיים  $a \in H_1 \wedge a \notin H_2$  וכן קיים  $b \in H_2 \wedge b \notin H_1$  נשים לב ש  $a, b \in H_1 \cup H_2$  מכיוון ש

$$H_1 \cup H_2 \text{ תת חבורה אז } a \cdot b \in H_1 \cup H_2 \text{ ז"א } ab \in H_1 \vee ab \in H_2$$

אם  $ab \in H_1 \Leftrightarrow a^{-1}ab \in H_1 \Leftrightarrow b \in H_1$  וקיבלנו סתירה.

אם  $ab \in H_2 \Leftrightarrow abb^{-1} \in H_1 \Leftrightarrow a \in H_2$  וקיבלנו סתירה.

ולכן  $H_2 \subseteq H_1$  או  $H_1 \subseteq H_2$ .

9. רשמו את כל האיברים שבהבורה  $U_{10}$  רשמו את טבלת הכפל שלה ומצאו את כל תתי החבורות שלה.

### פתרון

$$U_{10} = \{1, 3, 7, 9\} \text{ ז"א } U_{10} = \{a \in \mathbb{Z}_{10} \mid 1 \leq a \leq 10, \gcd(a, 10) = 1\}$$

לוח הכפל

	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

תתי החבורות הם:  $\{1\}, \{1, 9\}$ .

10. תהיי  $A \in \mathbb{R}^{n \times n}$  מטריצה כך ש  $n > 1$  נגדיר  $V_A = \{B \in \mathbb{R}^{n \times n} \mid AB = BA\}$  האם  $V_A$  אגודה,

מונואיד, חבורה או חבורה אבלית. הוכח את תשובתך.

### פתרון

תהיי  $A \in \mathbb{R}^{n \times n}$  מטריצה כך ש  $n > 1$ .

### סגירות

יהיו  $B, C \in V_A$  ז"א  $AB = BA \wedge AC = CA$ .  
 $BC \in V_A$  ולכן  $A(BC) = (AB)C = (BA)C = B(AC) = B(CA) = (BC)A$ .

### אסוציאטיביות

נובע מאסוציאטיביות בכפל מטריצות.

### איבר יחידה

מכיוון ש  $AI = IA$  נקבל ש  $I \in V_A$  ולכל מטריצה  $B \in \mathbb{R}^{n \times n}$  מתקיים  $B = BI = IB$  ובפרט לכל  $B \in V_A$  מתקיים  $B = BI = IB$  ולכן  $I$  איבר יחידה.

### קיום הופכי

לא לכל מטריצה ב  $V_A$  קיים הופכי. מטריצת האפס שייכת ל  $V_A$  אבל אין לה הופכי.

הקבוצה  $V_A$  היא מונואיד.

11. הוכח כי בחבורה  $G$  מסדר סופי כל  $e \neq a \in G$  הוא מסדר סופי.

### פתרון

מכיוון ש  $G$  מסדר סופי קיימים  $m \neq n \in \mathbb{N}$  כך ש  $a^m = a^n$  נניח ב.ה.ג.כ ש  $n < m$ . מכיוון ש  $G$  חבורה קיים  $a^{-1} \in G$  כך ש  $a \cdot a^{-1} = e$   $a^m \cdot (a^{-1})^n = a^n \cdot (a^{-1})^n = e$   $a \cdot a^{-1} = e$  ולכן  $a^{m-n} = e$  ולכן  $a$  מסדר סופי.

12. הוכח שהחבורה  $U_8$  לא ציקלית והחבורה  $U_9$  ציקלית.

### פתרון

$$U_8 = \{1, 3, 5, 7\}$$

נביט בתת החבורות שכל אחד מאברי  $U_8$  יוצר:

$$\langle 1 \rangle = \{1\}, \langle 3 \rangle = \{1, 3\}, \langle 5 \rangle = \{1, 5\}, \langle 7 \rangle = \{1, 7\}$$

אף אחד מאברי הקבוצה לא יוצר אותה ולכן  $U_8$  לא ציקלית.

$$U_9 = \{1, 2, 4, 5, 7, 8\}$$

$\langle 2 \rangle = \{2, 4, 8, 7, 5, 4\}$  ז"א 2 יוצר את  $U_9$  ולכן  $U_9$  חבורה ציקלית.

### תרגיל בונוס

הוכח שיש אינסוף ראשוניים מהצורה  $6n - 1$ . הדרכה: יש דמיון עם הוכחת אוקלידס לקיומם של אינסוף מספרים ראשוניים.

### פתרון:

### שלב א (טריוויאלי)

כל מספר שלם הוא אחד (ורק אחד) מהטיפוסים הבאים:

$$6n, 6n + 1, 6n + 2, 6n + 3, 6n + 4, 6n + 5 \quad n \in \mathbb{Z}$$

לכן כל ראשוני אי-זוגי הגדול מ 3 הוא מהטיפוס  $6n + 1$  או  $6n - 1$

$$(\text{כמובן } \{6n + 5\}_{n \in \mathbb{Z}} = \{6n - 1\}_{n \in \mathbb{Z}})$$

### שלב ב (לא טריוויאלי)

הערה: רעיון בהוכחת שלם ב דומה להוכחה של העובדה שיש אינסוף מספרים ראשוניים (אוקלידס).

תזכורת: נניח בשלילה שיש מספר סופי  $p_1, \dots, p_m$  ראשוניים. אז מוגדרת מכפלה סופית  $a = p_1 \cdots p_m - 1$ . ניקח פירוק  $a = q_1 \cdots q_r$  דרך ראשוניים. אזי כל  $q_j$  שווה לאחד מ  $p_i$  הנ"ל. מכאן נקבל  $1 | p_i$ , סתירה.

נניח בשלילה שיש מספר סופי  $p_1, \dots, p_m$  ראשוניים מהטיפוס  $6n - 1$ .

ניקח מספר טבעי  $a = 6p_1 \cdots p_m - 1$ . אז  $a$  מספר טבעי אי-זוגי מהטיפוס  $6n - 1$  כך ש  $p_i < a \quad \forall 1 \leq i \leq m$ .

בפירוק  $a = q_1 \cdots q_r$  דרך ראשוניים יש רק ראשוניים אי-זוגיים. אפשר גם להניח שהם גדולים מ 3 (אחרת 3 מחלק את 1, סתירה).

לפי שלב א כל  $q_1, \dots, q_r$  הוא מהטיפוס  $6n - 1$  או  $6n + 1$ .

מקרה 1: יש ביניהם  $q_j$  מהטיפוס  $6n - 1$ .

אזי  $q_j$  שווה לאחד מ  $p_i$  הנ"ל. אבל זה גורר  $a | p_i$  ואז נקבל  $1 | p_i$  (כי  $a = 6p_1 \cdots p_m - 1$ ), סתירה !

מקרה 2: כל הגורמים  $q_1, \dots, q_r$  הם מהטיפוס  $6n + 1$ . אבל אז גם המכפלה  $a = q_1 \cdots q_r$  מאותו טיפוס.

ז"א קבלנו ש  $a$  מהטיפוס  $6n + 1$ . אבל זה בסתירה עם העובדה ש  $a$  מהטיפוס  $6n - 1$ .