

## אלגברה מופשטת 2 - תרגיל

אתר הקורס: [www.math-wiki.com](http://www.math-wiki.com) - "מופשטת"

### משפט אוקלידס

בהינתן שני מספרים שלמים  $a, b \in \mathbb{Z}$  כך ש  $b \neq 0$  ניתן לחלק את  $a$  ב  $b$  עם שארית: כלומר קיימים  $r, q \in \mathbb{Z}$  כך ש  $0 \leq r < |b|$  ומתקיים  $a = qb + r$ . שארית  $r$ .

### דוגמאות

א. אם מחלקים את 7 ב 2  $7 = 3 \cdot 2 + 1$ . אם מחלקים את 7 ב 2:  $7 = (-3) \cdot (-2) + 1$ ,  $0 \leq 1 < (-2)$ .  
תרגיל: הראו ש  $r$  ו  $q$  נקבעים ביחידות.

### הגדרה

$a, b \in \mathbb{Z}$ . נאמר כי  $b$  מחלק את  $a$  או לחילופין  $a$  מתחלק ב  $b$  אם  $a = c \cdot b$  לאיזשהו  $c \in \mathbb{Z}$ , או לחילופין אם שארית החלוקה של  $a$  ב  $b$  היא אפס.

### הגדרה

1. בהינתן  $a, b \in \mathbb{Z}$  (כך שלא שניהם אפס) נגדיר את המחלק המשותף המקסימלי  $c = \gcd(a, b)$  להיות המספר השלם החיובי הגדול ביותר שמחלק את שניהם.

2. מכפלה משותפת מינימלית  $\text{lcm}(a, b)$  היא המספר השלם החיובי הקטן ביותר במחלק

$$\text{lcm}(a, b) = \frac{a \cdot b}{\gcd(a, b)} \text{ ב } a \text{ ו } b.$$

### הגדרה

$a, b \in \mathbb{Z}$  נקראים זרים אם  $\gcd(a, b) = 1$ .

### משפט

לכל  $a, b \in \mathbb{Z}$  (כך שלא שניהם אפס) קיימים  $u, v \in \mathbb{Z}$  כך ש  $au + bv = \gcd(a, b)$ .

## אלגוריתם אוקלידס

נתונים:  $a, b \in \mathbb{Z}$ ,  $a \geq b$ . רוצים למצוא:  $\gcd(a, b)$

$$a = q_1 b + r_1, 0 \leq |r_1| < |b|$$

$$b = q_2 r_1 + r_2, 0 \leq |r_2| < |r_1|$$

$$r_1 = q_3 r_2 + r_3$$

$\vdots$

$$r_{k+1} = 0$$

$$r_k | r_{k-1}$$

$$r_k = \gcd(a, b)$$

## דוגמה

$$\gcd(234, 61)$$

$$234 = 3 \cdot 61 + 51$$

$$61 = 1 \cdot 51 + 10$$

$$51 = 5 \cdot 10 + 1$$

$$\gcd(234, 61) = 1$$

עכשיו נמצא את  $u, v$ :

$$51 - 5 \cdot 10 = 234 - 3 \cdot 61 - 5(61 - 1 \cdot 51) = 1 \cdot 234 - 3 \cdot 61 - 5 \cdot 61 + 6 \cdot 51 = 6 \cdot 234 - 23 \cdot 61$$

## תרגילי בית

1. אם  $c$  מחלק את  $a$  ו $b$  אזי  $c$  מחלק את  $\gcd(a, b)$ .

2. אם  $c$  מחלק את  $a$  ו $b$  אזי  $\text{lcm}(a, b)$  מתחלק ב $c$ .

$$3. \text{ אם } b = \prod_{i=1}^m p_i^{\beta_i} \text{ ו-} a = \prod_{i=1}^m p_i^{\alpha_i}$$

$$\gcd(a, b) = \prod_{i=1}^m p_i^{\min\{\alpha_i, \beta_i\}}$$

$$\text{lcm}(a, b) = \prod_{i=1}^m p_i^{\max\{\alpha_i, \beta_i\}}$$

$$4. \text{ lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

$$5. \gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1$$

$$6. \text{ אם } a|bc \text{ וגם } \gcd(a, b) = 1 \text{ אזי } a|c$$

## הגדרה

קבוצה  $G$  עם פעולה  $\otimes$  בינארית  $G \otimes G \rightarrow G$  היא "חבורה" אם מתקיימים התנאים הבאים:

1. סגירות (מוגדרות?)

$$\text{לכל } a, b \in G \text{ קיים יחיד } c \in G \text{ כך ש-} a \otimes b = c$$

2. אסוציאטיביות

$$a \otimes (b \otimes c) = (a \otimes b) \otimes c$$

3. קיום איבר יחידה  $e \in G$

$$\forall a \in G, a \otimes e = e \otimes a = a$$

4. קיום איבר הופכי

$$\text{לכל } a \in G \text{ קיים } b \in G \text{ (יחיד) כך ש-} a \otimes b = b \otimes a = e$$

אם בנוסף לתנאים הקודמים מתקיים:

5. חילופיות \אבליות

$$\forall a, b \in G, a \otimes b = b \otimes a$$

אז  $G$  נקראת אבלית.

## הערות

1. אם מתקיימים תנאים 1-3 אך לא דווקא 4, אזי  $G$  נקראת מונויד.

2. אם מתקיימים 1-2 ולא דווקא 3 ו-4 אזי  $G$  נקראת אגודה (או חבורה למחצה)

## הערה

1. לעיתים רבות משמיטים את  $\otimes$  ורושמים פשוט  $ab$ .
2. כאשר מתייחסים לחבורה מקובל לרשום  $(G, \otimes, e)$ .

## דוגמאות

1.  $S = (\mathbb{N}, *)$  כאשר  $*$  מוגדר לפי  $a * b = b^a$ .  
סגירות?  $\checkmark$   
האם יש איבר יחידה?  $\chi$ . אם ננסה לקחת את 1 (המועמד היחיד, שכן  $\forall a \neq 1, b^a \neq b$ ), אזי  $b * 1 = 1^b \neq b$ .  
אסוציאטיביות?  $\chi$ . אבל  $(3 * 3) * 3 = (27) * 3 = 3^{27}$  אבל  $3 * (3 * 3) = 27^3 = 3^9$ .
2. תהי קבוצה  $X$  כלשהי. נביט במועמדת לחבורה  $(P(X), \cup, \emptyset)$ .  
סגירות?  $\checkmark$   
איבר יחידה?  $\checkmark$   
אסוציאטיביות?  $\checkmark$   
הפכי?  $\chi$ : אם  $A \neq \emptyset$  אזי  $A \cup B \neq \emptyset$  לכן זוהי אינה חבורה, אלא מונויד.

## הערה

דוגמה 2 היא דוגמה למונויד שלא יכולה להתרחב לחבורה. לעומת זאת,  $(\mathbb{N}, \cdot, 1)$  היא מונויד שמתרחב לחבורה אם מחליפים את  $\mathbb{N}$  ב  $\mathbb{Q} \setminus \{0\}$ .

4.  $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$  ונגדיר פעולה  $*$ :  
 $(x, y) * (z, w) = (x \cdot z - y \cdot w, x \cdot w + y \cdot z)$ . האם  $C$  חבורה ביחס ל  $*$ ?  
נביט במרכיבים:

$$(x + iy)(z + iw) = xz - yw + i(yz + xw)$$

$$x^2 + y^2 = |x + iy|^2 = 1 \Rightarrow x + iy = \text{cis } \alpha$$

$C$  עם הפעולה  $*$  היא מתנהגת כמו  $D = \{\text{cis } \alpha : 0 \leq \alpha < 2\pi\}$  עם פעולת כפל.

האם  $D$  חבורה?

$$\text{cis } (\alpha) \text{cis } (\beta) = \text{cis } (\alpha + \beta) \in D \quad \checkmark \text{ סגירות?}$$

$$\text{cis } (\alpha) \text{cis } (\beta) \text{cis } (\gamma) = \text{cis } (\alpha + \beta + \gamma) \quad \checkmark \text{ אסוציאטיביות?}$$

$$\text{cis } (0) = 1 \quad \checkmark \text{ איבר יחידה?}$$

$$\text{cis } (\alpha) \text{cis } (2\pi - \alpha) = \text{cis } (0) \quad \checkmark \text{ הופכי?}$$

$C$  היא חבורה אבלית.

## הגדרה

"סדר" של חבורה הוא פשוט העוצמה שלה כקבוצה (כמו בדידה).

### טבלאות כפל

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	6	8
3	0	3	6	9	12

$(\mathbb{Z}_4, +, 0)$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	4
2	2	3	0	1
3	3	0	1	2

$(\mathbb{Z}_2 \times \mathbb{Z}_2, +, (0,0))$

+	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,1)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

הסימטריות נובעת מחילופיות