

# מבנים דיסקרטיים – תרגיל 3 – פתרון

## שאלה 1

בשיעור הגדרנו לכל  $n \in \mathbb{N}$  את  $U_n = \{0 < k < n \mid \gcd(k, n) = 1\}$  ואמרנו (בלי להוכיח) שהיא חבורה ביחס לפעולה  $a \cdot b = (ab) \bmod n$  (החבורה  $(U_n, \cdot)$  נקראת חבורת אוילר של  $n$ ).

- מצאו את האיברים של  $U_{10}, U_{12}$ .
- הראו כי  $U_{10}$  ציקלית ו- $U_{12}$  לא ציקלית.
- מצאו איבר מסדר 3 ב- $U_7$ . הראו כי הוא אכן מסדר 3.

## פתרון

**סעיף א:**  $U_{10} = \{1, 3, 7, 9\}$ ,  $U_{12} = \{1, 5, 7, 11\}$

**סעיף ב:** ב- $U_{10}$  מתקיים  $\langle 3 \rangle = \{1, 3, 9, 7\} = U_{10}$  ולכן  $U_{10}$  ציקלית.

לעומת זאת ב- $U_{12}$  מתקיים  $\langle 1 \rangle = \{1\} \neq U_{12}$ ,  $\langle 7 \rangle = \{1, 7\} \neq U_{12}$ ,  $\langle 5 \rangle = \{1, 5\} \neq U_{12}$ ,  $\langle 11 \rangle = \{1, 11\} \neq U_{12}$  ולכן  $U_{12} \neq \langle g \rangle$  לכל  $g \in U_{12}$ , כלומר  $U_{12}$  לא ציקלית.

## שאלה 2

תהי  $(G, \cdot)$  חבורה ויהי  $g \in G$ . הוכיחו:

- $o(g) = o(g^{-1})$ .
- אם  $G$  סופית אז  $o(g) < \infty$ .

## הוכחה

**סעיף א:**  $o(g^{-1}) = \min \{n \in \mathbb{N} : g^n = e\} \cup \{\infty\} = \min \{n \in \mathbb{N} : (g^n)^{-1} = e^{-1}\} \cup \{\infty\} = \min \{n \in \mathbb{N} : g^{-n} = e\} \cup \{\infty\} = o(g)$ . **מש"ל.**

**סעיף ב:** נתבונן בסדרה  $g, g^2, g^3, g^4, \dots$ . היות ו- $G$  סופית חייבים להיות  $n, m \in \mathbb{N}$  שונים כך ש- $g^n = g^m$  (אחרת,  $\{g, g^2, g^3, g^4, \dots\}$  קבוצה אינסופית ונקבל סתירה לסופיות  $G$ ). בה"כ  $m > n$ . אזי  $e = g^n g^{-n} = g^m g^{-n} = g^{m-n}$ . **מש"ל.**  $o(g) \leq m - n < \infty$  ולכן  $e = g^n g^{-n} = g^{m-n} = g^{m-n}$ .

## שאלה 3

תהי  $(G, \cdot)$  חבורה סופית ואבלית. נגדיר  $b = \prod_{g \in G} g$ .

- הראו כי  $b^2 = e$ .
- ניח שב- $G$  אין איברים מסדר 2. הראו כי  $b = e$ .
- רשומ:** יהי  $p$  ראשוני. השתמשו בסעיף א עם  $G = U_p$  כדי להראות ש- $1 - (p-1)!$  מתחלק ב- $p$ .

## הוכחה

**סעיף א:** היות והפונקציה  $g \mapsto g^{-1}$  היא תמורה (=חח"ע ועל) על  $G$  (מדוע?), והיות ו- $G$  אבלית, מתקיים  $b = \prod_{g \in G} g = \prod_{g \in G} g^{-1} = \prod_{g \in G} g g^{-1} = \prod_{g \in G} e = e$ , לכן,  $b = e$ . **מש"ל.**

**סעיף ב:** לפי סעיף א,  $b^2 = e$  ולכן  $o(b) = 2$  או  $o(b) = 1$ . נתון שאין איברים מסדר 2 ב- $G$  ולכן  $o(b) = 1$ , כלומר  $b = e$ . **מש"ל.**

**סעיף ג:** היות ו- $p$  ראשוני  $U_p = \{1, 2, \dots, p-1\}$ . נבחר בסעיף א  $G = U_p$ , אזי  $b = \prod_{g \in G} g = ((p-1)!) \pmod{p}$ . לפי סעיף א,  $b^2 = ((p-1)!)^2 \pmod{p} = 1$ , לכן,  $((p-1)!)^2 - 1 \pmod{p} = 0$ . **מש"ל.** וזה בדיוק מה שרצינו להוכיח.

## שאלה 4

תהי  $(G, \cdot)$  חבורה ו- $g \in G$ . נניח ש- $o(g) = 6$ . מה הסדר של  $g^2$ ? של  $g^3$ ? של  $g^4$ ? מדוע?

## פיתרון

היות ו- $o(g) = 6$  אז  $g, g^2, g^3, g^4, g^5 \neq e$  ו- $g^6 = e$ .

לכן:

$$o(g^2) = 3 \text{ ולכן } (g^2)^3 = g^6 = e, (g^2)^2 = g^4 \neq e, g^2 \neq e$$

$$o(g^3) = 2 \text{ ולכן } (g^3)^2 = g^6 = e, g^3 \neq e$$

$$o(g^4) = 3 \text{ ולכן } (g^4)^3 = g^{12} = (g^6)^2 = e, (g^4)^2 = g^8 = g^6 \cdot g^2 = g^2 \neq e, g^4 \neq e$$

## שאלה 5

תהי  $(G, \cdot)$  חבורה ציקלית עם  $k$  איברים.

א. הוכיחו כי  $G$  חילופית.

ב. הוכיחו כי לכל  $g \in G$  מתקיים  $g^k = e$ .

ג. נניח כי  $k$  ראשוני. הראו כי לכל  $g \in G$  מתקיים  $o(g) = k$ .

[בפתרון השאלה אתם יכולים להשתמש בטענה הבאה שהוכחנו בכיתה: עבור  $n \in \mathbb{N}$  מתקיים  $g^n = e$  אם  $n \mid o(g)$ .]

## הוכחה

יהי  $x \in G$  כך ש- $G = \langle x \rangle$  (קיים  $x$  כזה כי  $G$  ציקלית). אזי  $k = |G| = |\langle x \rangle| = o(x)$ .

**סעיף א:** יהיו  $a, b \in G$ . אזי קיימים  $n, m \in \mathbb{Z}$  כך ש- $a = x^n, b = x^m$  (כי  $a, b \in G = \langle x \rangle$ ). כעת:  $ab = x^n x^m = x^{n+m} = x^m x^n = ba$ . **מש"ל.**

**סעיף ב:** יהי  $g \in G$ . אזי קיים  $n \in \mathbb{Z}$  כך ש- $g = x^n$ . היות ו- $o(x) = k$  מתקיים  $g^k = (x^n)^k = x^{nk} = (x^k)^n = e^n = e$ . **מש"ל.**

סעיף ג: יהי  $e \neq g \in G$ . לפי סעיף ב  $g^k = e$ . לפי טענה שהוכחנו בכיתה, זה אומר ש- $o(g)$  מחלק את  $k$ . היות ו- $k$  ראשוני, נובע ש- $o(g) \in \{1, k\}$ . ולכן  $g \neq e$  ולכן  $o(g) \neq 1$ . לכן בהכרח  $o(g) = k$ .  
**מש"ל.**