

# תרגול מס' 4 במבנים אלגבריים 1

## סדר של איבר ושל חבורה, חבורות ציקליות

הגדרה: סדר של חבורה הוא מספר האיברים בה.

$$o(g) := \begin{cases} \min\{k \in \mathbb{N} \mid g^k = e\} & \text{הסדר של איבר } g \text{ בחבורה מוגדר כ:} \\ \infty & \text{if there is no such } k \end{cases}$$

דוגמה: ב-  $U_{10} = \{1, 3, 7, 9\}$  :  $o(3) = 4, o(9) = 2$ .

**תרגיל:** תהא חבורה  $G$  מסדר זוגי. הוכח כי קיים לפחות איבר אחד לא ניטרלי מסדר 2.

**פתרון:** נניח בשלילה כי לכל איבר לא ניטרלי יש איבר הופכי אחר. נסדר את האיברים בזוגות: כל אחד עם ההופכי שלו (הזוגות הם זרים שכן קיים רק הופכי אחד לכל איבר). האיבר הניטרלי יישאר לבד. איחוד הזוגות עם האיבר הניטרלי ייתן קבוצה בת מספר אי-זוגי של איברים. סתירה.

**הגדרה:** חבורה ציקלית היא חבורה שנוצרת מאיבר אחד בה:  $\exists g \in G: G = \langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$

**טענה:** כל חבורה ציקלית היא בהכרח אבלית.

**הוכחה:** אם  $G = \langle a \rangle$  אז:  $\forall g_1, g_2 \in G: g_1 g_2 = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = g_2 g_1$  □

## דוגמאות:

$(\mathbb{Z}, +)$  חבורה ציקלית אינסופית הנוצרת מ-1.

קבוצת שורשי היחידה:  $x^n = 1$  מעל  $\mathbb{C}$  היא:  $\Omega_n = \left\{ \text{cis}\left(\frac{2\pi k}{n}\right) : k = 0, 1, 2, \dots, n-1 \right\}$ .

אם נסמן:  $\omega_n = \text{cis}\left(\frac{2\pi}{n}\right)$  נקבל ש:  $\Omega_n = \langle \omega_n \rangle$ , כלומר זו חבורה ציקלית.

באופן יותר כללי, החבורה  $G = \langle z = r \cdot cis\theta \rangle$  תהא סופית אם"ם:

1.  $r = 1$ ,

2.  $\frac{\theta}{\pi} \in \mathbb{Q}$  שכן אם:  $\theta = \frac{a}{b}\pi$ ,  $a, b \in \mathbb{Z} - \{0\}$  אזי:  $cis\left(\frac{a\pi}{b}\right)^{2b} = 1$ .

למשל:  $G = \left\langle cis\left(\frac{\pi}{4}\right) \right\rangle = \left\langle \frac{1+i}{\sqrt{2}} \right\rangle$  היא חבורה מסדר 8 אבל:  $G = \langle 1+i \rangle$  אינסופית.

**תרגיל:** נסמן:  $\Omega_\infty = \bigcup_{i \in \mathbb{N}} \Omega_i$ . הוכח:

א.  $\Omega_\infty \leq \mathbb{C} \setminus \{0\}$

ב.  $\forall x \in \Omega_\infty : o(x) < \infty$

ג.  $\Omega_\infty$  אינה ציקלית.

**פתרון:**

א. תת-חבורה:  $\forall a, b \in \Omega_\infty : a \in \Omega_i = \left\langle cis\left(\frac{2\pi}{i}\right) \right\rangle \Rightarrow a = cis\left(\frac{2\pi k_1}{i}\right)$

$b \in \Omega_j = \left\langle cis\left(\frac{2\pi}{j}\right) \right\rangle \Rightarrow b = cis\left(\frac{2\pi k_2}{j}\right)$

$a \cdot b^{-1} = cis\left(\frac{2\pi k_1}{i}\right) \cdot cis\left(-\frac{2\pi k_2}{j}\right) = cis\left(\frac{2\pi k_1}{i} - \frac{2\pi k_2}{j}\right) = cis\left(2\pi \frac{k_1 j - k_2 i}{ij}\right)$   
 ולכן:  
 $= cis\left(\frac{2\pi}{ij}\right)^{k_1 j - k_2 i} \in \left\langle cis\left(\frac{2\pi}{ij}\right) \right\rangle = \Omega_{ij} \subset \Omega_\infty$

ב.  $\forall x \in \Omega_\infty : \exists n | x \in \Omega_n \Rightarrow o(x) \leq n$

ג. נניח בשלילה כי  $G = \langle a \rangle$  אזי בהכרח:  $o(a) = \aleph_0$  בסתירה לסעיף הקודם.

**טענה:** תהא חבורה  $G$  ואיבר:  $a \in G$  כך ש:  $o(a) = n$ . אזי:  $o(a^d) = \frac{n}{(d,n)}$ .  $\forall d \leq n$ .

**הוכחה:** היתכנות:  $1 = (a^n)^{\frac{d}{(d,n)}} = (a^d)^{\frac{n}{(d,n)}}$  (כמוכן ש:  $d \mid (d,n)$ ).

**מינימאליות:** נניח  $(a^d)^t = 1$ . כלומר:  $a^{dt} = 1$  ידוע כי:  $o(a) = n$  לכן:  $n \mid dt$ .

מכאן גם ש:  $\frac{dt}{(d,n)} \mid \frac{n}{(d,n)}$ . אבל:  $1 = \left( \frac{n}{(d,n)}, \frac{d}{(d,n)} \right)$  ולכן:  $\frac{n}{(d,n)} \mid t \Leftrightarrow \frac{n}{(d,n)} \leq t$ .

**תרגיל:** תהא  $G = \langle a \rangle$  חבורה ציקלית מסדר  $n$ . כמה איברים יכולים ליצור את  $G$  כ"א לבדו?

**פתרון:**  $1 = (n,k) \Leftrightarrow o(a^k) = \frac{n}{(n,k)} = n \Leftrightarrow G = \langle a^k \rangle$ . כלומר מס' היוצרים הוא  $\varphi(n)$ .

**דוגמה:**  $\langle 7 \rangle = \{1, 7, 9, 3\}$   $U_{10} = \{1, 3, 9, 7\} = \langle 3 \rangle$ .  $7 = 3^3, (3,4) = 1 \Rightarrow$

**תרגיל:** נניח שהחבורה  $U_n$  ציקלית. כמה איברים יכולים ליצור כ"א לבדו את החבורה כולה?

**פתרון:**  $\varphi(\varphi(n))$ .

**משפט:** תהא  $G = \langle g \rangle$  חבורה ציקלית. אזי:  $H = \langle a \rangle \Leftrightarrow H \leq G$

**הוכחה:** הכיוון  $(\Leftarrow)$ : הוא ברור.

בכיוון ההפוך: נניח  $H \leq G$ . ניקח את החזקה המינימלית  $m$  כך ש:  $g^m \in H$  אזי:

$$\forall b \in G: b = g^k \mid k \geq m \Rightarrow k = ms + t \quad 0 \leq t < m \Rightarrow g^t = g^{-ms} \cdot g^k = \underbrace{(g^m)^{-s}}_{\in H} \cdot \underbrace{g^k}_{\in H} \in H$$

אבל  $m$  היא מינימלית, לכן בהכרח  $t = 0$ . מכאן ש:  $H = \langle g^m \rangle \Rightarrow \forall b \in H: b = (g^m)^s$ .

**מקרה פרטי:**  $G = (\mathbb{Z}, +) = \langle 1 \rangle$  : כל תת החבורות הן מהצורה:  $\langle k \rangle = k\mathbb{Z}$ .

**טענה:**  $\forall m, n \in \mathbb{Z}: \langle m \rangle \cap \langle n \rangle = \langle [m, n] \rangle$

**הוכחה:**  $h \in \langle m \rangle \cap \langle n \rangle \Leftrightarrow m|h \wedge n|h \Leftrightarrow [m, n]|h \Leftrightarrow h \in \langle [m, n] \rangle$

**טענה:** נגדיר:  $\langle m \rangle + \langle n \rangle = \{a+b \mid a \in \langle m \rangle, b \in \langle n \rangle\}$ .  $\forall m, n \in \mathbb{Z}$ . אזי:  $\langle m \rangle + \langle n \rangle = \langle (m, n) \rangle$ .

**הוכחה:** ( $\Leftarrow$ ) צ"ל:  $\langle m \rangle + \langle n \rangle \subseteq \langle (m, n) \rangle$ .

$\forall h \in \langle m \rangle + \langle n \rangle: h = a + b: m|a \wedge n|b$   
הוכחה:  
 $\Rightarrow (m, n)|a \wedge (m, n)|b \Rightarrow (m, n)|a + b = h \Rightarrow h \in \langle (m, n) \rangle$

( $\Rightarrow$ ) צ"ל:  $\langle m \rangle + \langle n \rangle \supseteq \langle (m, n) \rangle$ .

$d = (m, n) \Rightarrow \exists k_1, k_2 \in \mathbb{Z} \mid k_1 m + k_2 n = d$  הוכחה:

$\forall h \in \langle (m, n) \rangle: (m, n)|h \Rightarrow h = q(k_1 m + k_2 n) = qk_1 m + qk_2 n \in \langle m \rangle + \langle n \rangle$