

# מבנים אלגבריים למדעי המחשב 89-214-05

חיים שרגא רוזנר

השלמה לשיעור תרגיל 4

**משפט 0.1** תהי  $G$  חבורה ציקלית, ותהי  $H$  תת-חבורה. אזי  $H$  ציקלית.

**הוכחה:**  $G$  ציקלית, ולכן יש לה יוצר  $g$ . מתקיים  $\langle g \rangle = \{g^i : i \in \mathbb{Z}\} = G$ . לכן, כל האיברים ב- $G$  הם מהצורה  $g^i$ , ובפרט גם כל איברי  $H$  הם מצורה זו. אנו נביט בחזקות החיוביות של  $g$  שנמצאות ב- $H$ .

**מקרה I:** יש חזקות חיוביות של  $g$  שנמצאות ב- $H$ . נביט בחזקה הטבעית המינימלית של  $g$  שמחזירה איבר ב- $H$ . נסמן אותה

$$s = \min \{i \in \mathbb{N} : g^i \in H\}$$

אנו רוצים לטעון כי  $H = \langle g^s \rangle$ , על ידי הכלה דו-כיוונית.

• ( $\supseteq$ ) ברור שמתקיים  $g^s \in H$ , מהגדרת  $H$ . כעת, מכיוון ש- $H$  סגורה לפעולה, גם כל החזקות של  $g^s$  שייכות ל- $H$ , ולכן  $H \supseteq \langle g^s \rangle$ .

• ( $\subseteq$ ) נניח  $g^k \in H$ . לפי משפט החילוק יש  $q, r$  שלמים יחידים כך  $k = qs + r$ . כאשר  $0 \leq r < s$ . כל החזקות של  $g^s$  נמצאות ב- $H$ , ובפרט גם החזקה  $g^{-qs}$ . אם כן,  $g^{qs} \in H$ . אז גם ההופכי שלו,  $g^{-qs} \in H$ . נכפיל אותו ב- $g^k$ , ונקבל

$$g^k \cdot g^{-qs} = g^{qs+r} \cdot g^{-qs} = g^{qs+r-qs} = g^r \in H$$

מצאנו כאן ש- $g^r \in H$ . כעת, אם  $0 < r < s$  אז זו סתירה להגדרה של  $s$  כמינימלי. לכן  $r = 0$ . מצאנו כאן שכל איבר ב- $H$  הוא מהצורה  $g^{qs}$  עבור  $q$  שלם, ולכן  $H \subseteq \langle g^s \rangle$ .

אם כן, הראנו הכלה דו-כיוונית, וכתוצאה מכך הראנו שויון. מצאנו ש- $H$  היא החבורה הציקלית הנוצרת על ידי  $g^s$ .

**מקרה II:** אין חזקות חיוביות של  $g$  ב- $H$ . לפיכך גם אין חזקות שליליות של  $g$  ב- $H$ , כי אם  $a$  איבר בחבורה א.ס.ס.  $a^{-1}$  איבר בה. אם כן החזקה היחידה של  $g$  שנמצאת ב- $H$  היא החזקה השלמה שאיננה חיובית ולא שלילית, דהיינו  $g^0 = e$ . אם כן,  $H = \{e\} = \langle e \rangle$ . מצאנו כאן כי במקרה זה, החבורה  $H$  היא טריוויאלית, ולכן היא ציקלית.

■

**תרגיל** נניח  $a \mid b$  וגם  $a \mid a$ . מה אנחנו יודעים על  $a$  ועל  $b$ ?

**פתרון** לפי הגדרת **מחלק** קיימים מספרים שלמים  $c, d$  כך ש-

$$ac = b \quad bd = a$$

נציב את הנוסחאות זו בזו, ונקבל

$$acd = a \quad bdc = b$$

לאחר צמצום מקבלים  $cd = 1$ . כעת,  $c$  ו- $d$  שלמים, ולכן יש לנו שני פתרונות בלבד:

$$\begin{aligned} c = d = 1 \\ c = d = -1 \end{aligned}$$

לפיכך, מתקיים אחד היחסים הבאים בין  $a$  ל- $b$ :  $a = b$  או  $a = -b$ .

**הערה 0.2** לפיכך, אם  $a \mid b$  **לא ניתן** להסיק ש- $a = b$ , אלא אם נתון ששניהם חיוביים או ששניהם שליליים.