

# מבנים אלגבריים 89-214 תשפ"ג

## שעת קבלה 5.1.2023

שלום!

**תרגיל 0.1.** תהינה  $G_1, G_2$  חבורות. האם כל תת-חבורה  $K \leq G_1 \times G_2$  היא בהכרח מן הצורה  $K_1 \times K_2$  כאשר  $K_i \leq G_i$ ?

פתרון. לא! ראינו את הפתרון. אפשר לבחור למשל את  $G_1 = G_2 = \mathbb{Z}_2$  ואת

$$K = \langle (1, 1) \rangle = \{(0, 0), (1, 1)\}$$

ההטלה הטבעית על הרכיב הראשון של  $G_1 \times G_2$  היא הפונקציה (למעשה אפימורפיזם)

$$p_1: G_1 \times G_2 \rightarrow G_1 \\ (g_1, g_2) \mapsto g_1$$

ובאופן דומה ההטלה  $p_2$  על הרכיב השני מוגדרת. נשים לב כי  $p_1(K) = G_1$  וגם  $p_2(K) = G_2$ , אבל  $K$  שהיא מסדר 2 אינה  $G_1 \times G_2$  שהיא מסדר 4. דרך אחרת: לחבורה  $G_1$  (וכך גם ל- $G_2$ ) יש בדיוק שתי תת-חבורות, הראשונה היא  $\{0\}$  והשנייה היא  $\mathbb{Z}_2$ . לכן ל- $G_1 \times G_2$  יש בדיוק ארבע תת-חבורות מן הצורה  $K_1 \times K_2$ . אבל  $K$  שבחרנו למעלה לא שווה לאף אחת מארבע תת-החבורות האלו.

**תרגיל 0.2.** אם  $G$  ציקלית, אז כל תת-חבורה שלה היא ציקלית.

פתרון. עשינו בתרגול. נניח  $H \leq G = \langle a \rangle$ . אם  $H = \{e\}$ , ברור כי  $H$  ציקלית, הרי  $H = \langle e \rangle$ .

אם  $H \neq \{e\}$ , אז קיים  $a^i \in H$ ,  $e \neq a^i$ . נשים לב שמסגירות להופכי גם  $a^{-i} \in H$ . יהי  $s$  המספר הטבעי הקטן ביותר כך ש- $a^s \in H$ . נוכיח  $H = \langle a^s \rangle$  בהכלה דו-כיוונית. (⊇): אם  $(a^s)^k \in \langle a^s \rangle$ , אז מסגירות לפעולה ב- $H$ , בוודאי  $(a^s)^k \in H$ . (⊆): אם  $a^n \in H$  (הרי כל איברי  $H$  הם חזקות כלשהן של  $a$ ), אז לפי חלוקה אוקלידית קיימים  $q, r$  כך ש- $n = qs + r$  וגם  $0 \leq r < s$ . אז

$$a^r = a^{n-qs} = \underbrace{a^n}_{\in H} \cdot \underbrace{(a^s)^{-q}}_{\in H} \in H$$

ולכן  $a^r \in H$ . מהמינימליות של  $s$ , בהכרח  $r = 0$ . לכן  $a^n = (a^s)^q \in \langle a^s \rangle$ . בסך הכל  $H = \langle a^s \rangle$ .

הערה 0.3. אם  $G$  ציקלית ואינסופית, אז גם  $H$  (לא טריוויאלית) היא אינסופית.

הערה 0.4. אם  $a \in G$  איבר מסדר  $n$  בחבורה כלשהי. אז

$$o(a^d) = \frac{n}{(n, d)}$$

**תרגיל 0.5.** נניח  $a_1 \equiv b_1 \pmod{n}$  וגם  $a_2 \equiv b_2 \pmod{n}$ . הוכיחו כי  $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ .

פתרון. לפי הגדרה של שקילות מודולו  $n$ , קיימים  $k_1$  ו- $k_2$  עבורם

$$a_1 = b_1 + k_1 n$$

$$a_2 = b_2 + k_2 n$$

נכפול את המשוואות ונקבל

$$a_1 a_2 = b_1 b_2 + K n$$

עבור  $K \in \mathbb{Z}$  שקל לחשב מפורשות. לכן  $a_1 a_2 \equiv b_1 b_2 \pmod{n}$ .

**תרגיל 0.6.** הוכיחו שלכל  $s > 1$  ו- $m$  טבעיים מתקיים כי  $m | \varphi(s^m - 1)$ .

פתרון. יש פתרון בדף הקורס. תקציר שלו הוא בערך ככה: לפי משפט לגראנז' הסדר של תת-חבורה מחלק את הסדר של החבורה (עבור חבורות סופיות). בפרט, הסדר של איבר מחלק את הסדר של החבורה.

ראינו כבר כי  $|U_{s^m-1}| = \varphi(s^m - 1)$ . אם נמצא איבר  $x \in U_{s^m-1}$  מסדר  $m$ , אז סיימנו.

לפי אינטואיציה, נזכר כי 1 הוא איבר היחידה של  $U_{s^m-1}$  ורוצים איבר שמעלים אותו בחזקת  $m$  ומגיעים ל-1 (ו- $m$  הוא המספר הטבעי הקטן ביותר עבורו זה מתקיים). נחש כי  $x = s$  הוא מסדר  $m$ .

קודם יש להראות כי  $s \in U_{s^m-1}$ . כלומר  $(s, s^m - 1) = 1$ . זה נכון למשל לפי אלגוריתם אוקלידס

$$(s^m - 1, s) = [s^m - 1 = (s^{m-1} - 1) \cdot s + s - 1] = (s, s - 1) = (s - 1, 1) = 1$$

הרי ראינו טענה בכיתה שאם  $n = qm + r$ , אז  $(n, m) = (m, r)$ . כעת נחשב את  $o(s)$ . ברור כי  $s^i < s^m - 1$  לכל  $0 \leq i < m$ . לכן  $s^i \not\equiv 1 \pmod{s^m - 1}$  לכל  $0 \leq i < m$ . אבל

$$s^m - 1 \equiv 0 \pmod{s^m - 1}$$

$$s^m \equiv 1 \pmod{s^m - 1}$$

ולכן  $o(s) = m$ .

**תרגיל 0.7.** הראו כי  $\gcd(m^2, m + n) = \gcd(n^2, m + n)$  לכל  $m, n \in \mathbb{Z}$  שלא שניהם אפס.

פתרון. כמו מקודם, ראינו שאם  $x = qy + r$ , אז  $(x, y) = (y, r)$ . ידוע לנו כי

$$(m+n)(m-n) = m^2 - n^2$$

אז  $m^2 = (m-n) \cdot (m+n) + n^2$  אז

$$\gcd(m^2, m+n) = \gcd(m+n, n^2) = \gcd(n^2, m+n)$$

דרך אחרת: אפשר להניח  $n \geq m$ , ואז  $n^2 \geq m^2$  אז

$$n^2 \geq 2n \geq n+m$$

לכל  $n > 2$ . זה לא כל כך יעבוד עם אלגוריתם אוקלידס, אז ננסה שימוש כפול בטענה לגבי  $x = qy + r$ :

$$(n^2, n+m) = [n^2 = n \cdot (n+m) - nm] = (n+m, -nm)$$

$$(m^2, n+m) = [m^2 = m \cdot (n+m) - nm] = (n+m, -nm)$$

וקיבלנו שיוויון.

הערה 0.8. באופן כללי  $(x, y) = (-x, y) = (x, -y) = (-x, -y) = (y, x)$ .

**תרגיל 0.9.** תהי  $G$  חבורה אבלית סופית שיש לה את האיברים  $a_1, a_2, \dots, a_n$ . יהי  $b = \prod_{i=1}^n a_i$ . הוכיחו כי  $b^2 = e$ .

פתרון. נגדיר  $f: G \rightarrow G$  לפי  $f(g) = g^{-1}$ . לכל  $a_i \in G$  קיים הופכי, כלומר קיים  $1 \leq j \leq n$  כך ש- $a_i^{-1} = a_j$ . במילים אחרות  $f(a_i) = a_j$ . מפני שקיים הופכי (יחיד) לכל איבר, הפונקציה  $f$  היא חח"ע ועל. אז

$$b^2 = \left( \prod_{i=1}^n a_i \right)^2 \stackrel{\text{אבליות}}{=} \prod_{i=1}^n a_i \cdot f(a_i) = \prod_{i=1}^n a_i \cdot a_i^{-1} = \prod_{i=1}^n e = e$$

באופן כללי בחבורה אבלית  $a_1 \cdot a_2 \cdots a_n = a_{\sigma(1)} \cdot a_{\sigma(2)} \cdots a_{\sigma(n)}$  לכל תמורה  $\sigma \in S_n$ , כמו למשל התמורה ששולחת את  $a_i$  להופכי שלו.

**תרגיל 0.10.** הוכיחו שכל זוג תמורות זרות  $\sigma, \tau \in S_n$  מתחלפות.

פתרון. נזכר בהגדרה של תומץ של תמורה

$$\text{supp}(\sigma) = \{i \mid \sigma(i) \neq i\}$$

בשאלה נתון כי  $\text{supp}(\sigma) \cap \text{supp}(\tau) = \emptyset$ . רוצים להוכיח כי  $\sigma\tau = \tau\sigma$ . נחלק למקרים:

• אם  $i \notin \text{supp}(\sigma)$  וגם  $i \notin \text{supp}(\tau)$ , אז  $\sigma(i) = i$  וגם  $\tau(i) = i$ . אז נחשב

$$\sigma\tau(i) = \sigma(\tau(i)) = \sigma(i) = i = \tau(i) = \tau\sigma(i)$$

- אם  $i \notin \text{supp}(\sigma)$  וגם  $i \in \text{supp}(\tau)$  אז עדיין  $\sigma(i) = i$ . בהכרח גם  $\tau(i) \in \text{supp}(\tau)$  לכן

$$\sigma\tau(i) = \sigma(\tau(i)) = \tau(i) = \tau(\sigma(i)) = \tau\sigma(i)$$

- אם  $i \in \text{supp}(\sigma)$  וגם  $i \notin \text{supp}(\tau)$ , נקבל חישוב דומה לסעיף ה
- קודם.

וסיימנו כי לפי הנתון אין  $1 \leq i \leq n$  ששייך לתומכים של שתי התמורות.