

# תרגול מס' 5 במבנים אלגבריים 1

## קוסטים וקבוצות מנה

תהא חבורה  $G$  ות"ח  $H$ . הקוסט השמאלי של  $a \in G$  לגבי  $H$  הוא הקבוצה:  $aH = \{ah : h \in H\}$ .

קבוצת המנה של החלוקה משמאל היא קבוצת הקוסטים השמאליים:  $G/H = \{gH : g \in G\}$ .

באותו האופן קוסט ימני הוא  $Ha$ , וקבוצת המנה מימין היא:  $H \backslash G = \{Hg : g \in G\}$ .

הקוסטים הם מחלקות שקילות בתוך  $G$  לכן היא איחוד זר של הקוסטים. גודל כל קוסט הוא  $|H|$ , ולכן הוא מחלק את סדר החבורה. גודלה של קבוצת המנה (לא משנה מאיזה צד) הוא מספר הקוסטים. הגודל הזה נקרא "האינדקס של  $H$  ב- $G$ ".

משפט לגרנז': אם  $G$  סופית אזי:  $\forall H \leq G: |G/H| = [G:H] = \frac{|G|}{|H|}$ .

מסקנה:  $\forall g \in G: o(g) \mid |G|$ .

הגדרה: אם מתקיים:  $\forall g \in G: gH = Hg$  אזי  $H$  היא תת-חבורה נורמלית ונסמן:  $H \triangleleft G$ .

(אם חבורת האם היא אבלית אז כמובן שכל תת-חבורה שלה היא נורמלית).

## דוגמאות:

$$1. \forall n: \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n, [\mathbb{Z}:n\mathbb{Z}] = n$$

$$2. \text{ תהא } G = U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\} \text{ ות"ח: } H = \langle 3 \rangle = \{1, 3, 9, 11\} \leq G$$

כיוון שהחבורה היא אבלית אין הבדל בין קוסטים ימניים לשמאליים ואלו הם:

$$G/H = \{H, 5H\} \text{ ובסה"כ: } eH = \langle 3 \rangle = \{1, 3, 9, 11\}, 5H = 5 \cdot \langle 3 \rangle = \{5, 15, 13, 7\}$$

3. תת-החבורה  $\langle b \rangle$  הנוצרת משיקוף ב-  $D_3 = \langle a, b : a^3 = b^2 = 1, ab = ba^2 \rangle$  אינה נורמלית אבל  $\langle a \rangle$  כן.

**טענה:** תהא  $G$  חבורה ו- $H$  תת-חבורה. אם:  $[G:H] = 2$  אזי:  $H \triangleleft G$ .

**הוכחה:** כיוון ש- $[G:H] = 2$  יש רק שני קוסטים:  $G/H = \{H, H^c\}$ .

לכן ישנן שתי אפשרויות ל- $g \in G$ :  
 $g \in H \Rightarrow gH = H = Hg$ ,  
 $g \notin H \Rightarrow gH = H^c = Hg$   
 בכל מקרה:  $gH = Hg$ .  $\forall g \in G$ .

**תרגיל:** תאר את  $G/H$  עבור:  $G = (\mathbb{R}^2, +)$  ו- $H = \{(t, 5t)\}$ .

**פתרון:** מבחינה גאומטרית,  $H$  הוא ישר עם שיפוע 5 העובר דרך ראשית הצירים.

קודם כל נוודא שאכן  $H \leq G$ :

$$1. e = (0, 0) \in H$$

$$2. \forall x, y \in H : x = (t_1, 5t_1), y = (t_2, 5t_2) : x \cdot y^{-1} = (t_1, 5t_1) - (t_2, 5t_2) = (t_1 - t_2, 5(t_1 - t_2)) \in H$$

נבדוק מהי קבוצת המנה:

$$G/H = \{(a, b) + (t, 5t)\} = \{(a+t, b+5t)\} = \{(x, y) : y = b + 5t, x = a + t\} = \left\{ (x, y) : y = 5x + \underbrace{b - 5a}_{t \in \mathbb{R}} \right\}$$

כלומר קבוצת המנה היא כל הישרים במישור עם שיפוע 5.

**טענה:** כל חבורה מסדר ראשוני היא ציקלית.

**פתרון:** אפשר להגיד יותר מזה: כל איבר  $e \neq g \in G$  הוא עפ"י לגרנז' מסדר  $p$  ולכן יוצר לבד את כל  $G$ .

**משפט אוילר:**  $\forall a \in \mathbb{Z}^\times, n \in \mathbb{N} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**הוכחה:**  $a \in \mathbb{Z}^\times, (a, n) = 1 \Rightarrow a \equiv \bar{a} \in U_n \Rightarrow a^{\varphi(n)} = \bar{a}^{|U_n|} = 1$ .

מקרה פרטי של משפט אוילר: **משפט פרמה (הקטן)**:  $\forall a \in \mathbb{Z}^\times, p \nmid a: a^{p-1} \equiv 1 \pmod{p}$ .

**דוגמה**: חשב את שתי הספרות האחרונות של המספר  $9^{121}$ .

**פתרון**: כיוון ש:  $(9, 100) = 1$  עפ"י אוילר:  $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$ .

מכאן ש:  $9^{121} = (9^{40})^3 \cdot 9 \equiv 1^3 \cdot 9 \equiv 9 \pmod{100}$ .

**תרגיל**: חשב את  $197^{81}$  מודולו 34.

**פתרון**: לצורך פשטות נשים לב כי:  $197 \equiv 27 \pmod{34}$  וגם ש:  $(27, 34) = 1$ .

לכן עפ"י משפט אוילר:  $197^{\varphi(34)} = 27^{\varphi(34)} \equiv 1 \pmod{34}$ .

נחשב:  $\varphi(34) = \varphi(2) \cdot \varphi(17) = 16$ .

לכן בסיסה"כ:  $197^{81} = 27^{81} = \underbrace{(27^{16})^5}_{\equiv 1 \pmod{34}} \cdot 27 \equiv 27 \pmod{34}$ .