

# מבנים אלגבריים תרגול 5 - משפטי חבורות סופיות

19 באפריל 2021

## 1 משפט לגראנז'

תהי  $G$  חבורה סופית עם  $n$  איברים, ותהי  $H \leq G$  תת-חבורה עם  $m$  איברים, אזי:

$$m|n$$

כלומר,

$$\exists a \in \mathbb{Z} : n = m \cdot a$$

מסקנות:

$$1. \forall g \in G : o(g)|n$$

$$2. \forall g \in G : g^n = e$$

תרגילים:

1. תהי  $G$  חבורה סופית עם  $n$  איברים, ותהיינה  $H_1, H_2 \leq G$  תתי חבורות כך ש-:

$$|H_1| = m, |H_2| = k$$

ונניח

$$\gcd(m, k) = 1$$

הוכיחו:

$$H_1 \cap H_2 = \{e\}$$

פתרון: ניזכר שבשיעורי הבית ראינו שחיתוך שלך תתי-חבורות זוהי תת-חבורה. כלומר,

$$H_1 \cap H_2 \leq H_1, H_2$$

ולכן לפי לגראנז': הגודל של החיתוך מחלק את  $m, k$ . כלומר, נסמן

$$|H_1 \cap H_2| = a$$

אז:

$$a|m, a|k$$

לפי הגדרת  $\gcd(m, k)$  כל מספר שמחלק את  $m, k$  מחלק גם את  $\gcd(m, k)$ . ולכן אצלנו, כיון ש-  $a|m, a|k$  נקבל

$$a|\gcd(m, k) = 1$$

ולכן נקבל

$$a = 1$$

איבר היחידה נמצא בכל תת-חבורה, ולכן הוא היחיד שנמצא בחיתוך. מש"ל.

2. תהי  $G$  חבורה. הוכיחו: אם  $\forall g \in G : g^2 = e$  אז  $G$  חילופית (אבלית). פתרון: ש"ב.

3. תהי  $G$  חבורה עם ארבעה איברים. הוכיחו:  $G$  אבלית. פתרון: לפי המסקנה הראשונה ממשפט לגראנז' נקבל שסדרי איברי החבורה יכולים להיות: 1, 2, 4. סדר 1 שמור רק לאיבר היחידה. אם יש איבר מסדר 4 אז הוא יוצר את החבורה ולכן  $G$  ציקלית ולכן אבלית. אחרת, נקבל שכל האיברים שאינם היחידה הינם מסדר 2, ולכן בטה"כ מתקיים:

$$\forall g \in G : g^2 = e$$

ולכן לפי תרגיל קודם נקבל ש- $G$  אבלית. דוגמא לחבורה אבלית לא ציקלית עם 4 איברים:

$$\mathbb{Z}_2 \times \mathbb{Z}_2$$

## 2 משפטי אוילר ופרמה

יהי  $n \in \mathbb{N}$  ונסמן:

$$U_n = \{1 \leq a \leq n-1 : \gcd(a, n) = 1\}$$

. פונקציית אוילר היא:

$$\phi(n) = |U_n|$$

אנחנו נקרא לחבורה  $(U_n, \cdot_n)$  חבורת אוילר. דוגמאות:

1.  $U_7 = \{1, 2, 3, 4, 5, 6\}$  באופן כללי, לכל ראשוני  $p$

$$U_p = \{1, \dots, p-1\}$$

(ועבור ראשוני  $z$  גם חבורה ציקלית). כאן למשל  $3$  יוצר.

2.  $U_8 = \{1, 3, 5, 7\}$ . נבדוק האם ציקלית: מקבלים שכל האיברים מסדר  $2$  ולכן לא ציקלית.

3.  $U_{10} = \{1, 3, 7, 9\}$ . נבדוק סדרים:

$$3^2 = 9$$

$$3^3 = 27 \equiv 7 \pmod{10}$$

$$3^4 = 81 \equiv 1 \pmod{10}$$

ולכן  $o(3) = 4$  והוא יוצר את החבורה ולכן היא ציקלית.

משפט אוילר: לכל  $n$  ולכל  $a$  שזר ל- $n$  מתקיים:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

רעיון ההוכחה: נתבונן בחבורת אוילר  $U_n$ . כיון ש- $\gcd(a, n) = 1$  נקבל  $a \in U_n$ , לפי מסקנה 2 של לגראנז' כיון ש- $\phi(n) = |U_n|$  אז

$$a^{\phi(n)} = e \equiv 1 \pmod{n}$$

משפט פרמה: לכל ראשוני  $p$ ,  $1 \leq a \leq p-1$  מתקיים:

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^p \equiv a \pmod{p}$$

תרגילים:

1. חשבו את  $13^{613} \pmod{103}$ .  
 פתרון: אכן 103 הוא ראשוני (כדי לבדוק אם מספר הוא ראשוני מספיק לבדוק עד  $\sqrt{n}$ ). ולכן לפי פרמה:

$$13^{102} \equiv 1 \pmod{103}$$

ולכן:

$$13^{613} = 13 \cdot \underbrace{(13^{102})^6}_{\equiv 1 \pmod{103}} \equiv 13 \pmod{103}$$

2. כידוע מתרגלים אוהבים לתת שאלות עם השנה.

(א) לעיתים שנה מתקבעת ולא מתקדמת. מהן 2 הספרות האחרונות של  $7^{5762}$ .  
 שאלה זו משנה ה'תשס"ב.  
 פתרון: אנחנו בעצם רוצים לחשב  $7^{5762} \pmod{100}$ . נחשב את  $\phi(100)$ . מי זר למאה? נחשב מי לא זר למאה: הזוגיים וכפולות של 5 שאינם זוגיים. יש 49 זוגיים בין 1 ל-99, ובנוסף יש עוד עשרה מתחלקים ב-5 שאינם זוגיים. בסה"כ:

$$\phi(100) = 99 - 49 - 10 = 40$$

ולכן:

$$7^{40} \equiv 1 \pmod{100}$$

ולכן:

$$7^{5762} = (7^{40})^{144} \cdot 7^2 \equiv 49 \pmod{100}$$

(ב) מתרגל החליט לעדכן את השאלה לשנה הנוכחית ולחשב את  $7^{5781} \pmod{100}$ .  
 לא היה לו כח אז הוא שם בש"ב. עזרו לו לפתור:  
 פתרון: מה שעשינו עד כה לא בדיוק עוזר כי נצטרך לחשב

$$(7^{40})^{144} \cdot 7^{21} \pmod{100}$$

אלא שכאן ניסוי וטעייה או תעייה - כל אחד מה שקורה לו. נחשב את הסדר של 7 בחבורת אוילר ונשתמש בזה:

$$7^2 = 49 \not\equiv 1$$

$$7^3 = 343 \not\equiv 1 \pmod{100}$$

(האמת היא שאת זה לא צריך לחשב כי הסדר לא יכול להיות 3, הרי הוא צריך לחלק את גודל החבורה).

$$7^4 = 2401 \equiv 1 \pmod{100}$$

ולכן:

$$(7^{40})^{144} \cdot 7^{21} \equiv 1 \cdot (7^4)^5 \cdot 7 \equiv 7 \pmod{100}$$