

מבנים אלגבריים תרגול 5

21 באפריל 2021

1 משפט לגראנז'

תהי G חבורה סופית, ו- $H \leq G$ תת-חבורה. נסמן $|H| = m$, $|G| = n$: אז

$$m|n$$

מסקנות:

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

2. $\forall g \in G : g^n = e$ כי נסמן $o(g) = k$, אז יש a טבעי כך ש- $n = ka$ ולכן $.g^n = (g^k)^a = e^a = e$

תרגילים:

1. תהי G חבורה סופית. תהיינה $H_1, H_2 \leq G$ תתי-חבורות. נסמן $|H_1| = n$, $|H_2| = m$. נתון: $gcd(n, m) = 1$. (כאשר gcd זהו המחלק המשותף המקסימלי) הוכיחו:

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

פתרון: בתרגיל בית ראינו שחיתוך של תתי-חבורות זה תת-חבורה. לכן כאן נקבל:

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

נסמן $|H_1 \cap H_2| = k$. לכן לפי לגראנז' נקבל

$$k|n \wedge k|m$$

לפי הגדרת gcd אם $k|n, m$ אז $k|gcd(n, m) = 1$ ולכן $k = 1$. איבר היחידה נמצא בכל תת-חבורה ובפרט בחיתוך, ולכן החיתוך הוא:

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

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

3. תהי G חבורה מסדר 4 (כלומר, עם ארבעה איברים). הוכיחו: G אבליה. פתרון: לפי המסקנה הראשונה של לגארנו, סדרי איברי החבורה יכולים להיות: 1, 2, 4. סדר 1 שמור לאיבר היחידה בלבד. אם יש איבר מסדר 4, אז הוא יוצר את החבורה כי ראיתם משפט: $o(g) = |\langle g \rangle|$, ולכן החבורה G היא ציקלית (כלומר, יש $g \in G$ כך ש- $G = \langle g \rangle = \{g^a : a \in \mathbb{Z}\}$, לכן אבליה. אחרת, נקבל שהסדר של כל איבר (למעט היחידה שסדרו 1) הוא 2, ובסה"כ: $\forall g \in G : g^2 = e$. לפי תרגיל קודם G אבליה.

2 משפטי אוילר ופרמה

לכל n טבעי נסמן:

$$\mathbb{Z}_n^\times = \{1 \leq a \leq n : \gcd(a, n) = 1\}$$

פונקציית אוילר מוגדרת ע"י:

$$\phi(n) = |\mathbb{Z}_n^\times|$$

פונקציית אוילר במילים: כמה מספרים הקטנים או שווים ל- n זרים לו. וראיתם ש- $(\mathbb{Z}_n^\times, \cdot)$ היא חבורה קומוטטיבית. דוגמאות:

1. $\mathbb{Z}_7^\times = \{1, 2, 3, 4, 5, 6\}$ (באופן כללי, עבור p ראשוני נקבל $\mathbb{Z}_p^\times = \{1, \dots, p-1\}$, ובנוסף אם p ראשוני אז \mathbb{Z}_p^\times ציקלית). למשל כאן 3 יוצר.

2. $\mathbb{Z}_{10}^\times = \{1, 3, 7, 9\}$. נבדוק את הסדרים שלהם, ונראה האם החבורה ציקלית או לא:

$$3^2 = 9 \not\equiv 1 \pmod{10}$$

אם הסדר לא 2 אז חייב להיות 4:

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

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

3. תעברו על \mathbb{Z}_8^\times ותראו שהיא לא ציקלית.

משפט אוילר: לכל n ולכל $1 \leq a \leq n$ הזר ל- n מתקיים:

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

משפט פרמה: לכל ראשוני p ולכן $a < p$ מתקיים:

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

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

תרגילים:

1. חשבו את $13^{613} \pmod{103}$

פתרון: 103 ראשוני, ולכן נקבל מפרמה:

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

ולכן:

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

2.

(א) מהן 2 הספרות האחרונות של 7^{5762} ?

פתרון: אנחנו רוצים לחשב בעצם $7^{5762} \pmod{100}$. לכן צריך לדעת מהו

$\phi(100)$? זר ל-100 הוא מספר עם ספרות אחדות 1,3,7,9, ולכן יש 4 בכל עשרת

ובסה"כ: $\phi(100) = 40$. לכן:

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

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

(ב) מה נעשה עבור $7^{5781} \pmod{100}$?

פתרון: שיטה קודמת לא עוזרת:

$$7^{5781} = (7^{40})^{144} \cdot 7^{21}$$

אנחנו בעצם מתבוננים בחבורה \mathbb{Z}_{100}^\times שיש בה כאמור $\phi(100) = 40$ איברים.

נחשב את הסדר של 7:

$$7^2 = 49 \neq 1$$

כיון שצריך להתקיים $o(7)|40$ נוכל לעבור לבדוק האם הסדר הוא 4.

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

לכן הסדר הוא 4, ולכן נקבל:

$$7^{21} = 7 \cdot (7^4)^5 \equiv 7 \pmod{100}$$

ולכן 2 הספרות האחרונות הן 07.