

תרגיל מספר 11 מבנים אלגבריים

21 בינואר 2016

1. מצאו $(3x + 2)^{-1}$ (כלומר את ההופכי של $3x + 2$)
בשדה $\mathbb{F}_{11^2} = \mathbb{Z}_{11}[x]/\langle x^2 + x + 4 \rangle$
פתרון: נחשב $\gcd(3x + 2, x^2 + x + 4)$:

$$(3x + 2)(4x + 5) = 12x^2 + 8x + 15x + 10 = x^2 + x + 10$$

ולכן

$$x^2 + x + 4 = (3x + 2)(4x + 5) + 5$$

$$3x + 2 = (5)(5x + 7) + 0$$

ולכן

$$5 = x^2 + x + 4 - (3x + 2)(4x + 5)$$

נכפיל ב $5^{-1} = 9$ ונקבל

$$1 = 9(x^2 + x + 4) + 2((3x + 2)(4x + 5))$$

מודולו $x^2 + x + 4$ נקבל

$$1 \equiv (3x + 2) \cdot 2(4x + 5)$$

ולכן

$$(3x + 2)^{-1} = 2(4x + 5) = 8x + 10$$

2. נסתכל במשוואה $X^2 + 1 = 0$. למשוואה זאת אין פתרון מעל \mathbb{Z}_3 (כלומר, לכל $a \in \mathbb{Z}_3$ מתקיים כי $a^2 + 1 \neq 0$). מצאו שדה \mathbb{F} כך ש

$$\mathbb{Z}_3 \subseteq \mathbb{F} \quad (\text{א})$$

(ב) קיים $a \in \mathbb{F}$ כך ש $a^2 + 1 = 0$ (כלומר יש פתרון למשוואה מעל \mathbb{F})
פתרון: כיוון שהפולינום $x^2 + 1$ הוא אי פריק מעל \mathbb{Z}_3 נוכל להגדיר את השדה

$$\mathbb{F}_9 = \mathbb{Z}_3[x]/\langle x^2 + 1 \rangle$$

ומתקיים כי $\mathbb{Z}_3 \subseteq \mathbb{F}_9$ ובנוסף, $x \in \mathbb{F}_9$ מקיים $x^2 + 1 = 0$ כלומר פתרון למשוואה.

3. יהא $\mathbb{F}_{16} = \mathbb{Z}_2[x] / \langle x^4 + x^3 + 1 \rangle$ שדה. נסתכל על החבורה הכפלית $G = \mathbb{F}_{16} \setminus \{0\}$. הוכח כי $x \in G$ (הפולינום x) הוא יוצר של G . (רמז: לא צריך לחשב את כל החזקות של x אם נעזרים במשפט לגרנג)
פתרון: בחבורה הכפלית יש $16 - 1 = 15$ איברים. ולכן הסדר של כל איבר בחבורה הוא אחד מ $\{1, 3, 5, 15\}$.
 כעת:

- רק איבר היחידה הוא מסדר 1.
 - $x^3 \neq 1$ ולכן הסדר של x אינו 3
 - $x^5 = x^4 x = (x^3 + 1)x = x^4 + x = x^3 + 1 + x \neq 1$ ולכן הסדר של x אינו 5
 - מסקנה: הסדר של x הוא 15 ולכן הוא יוצר של החבורה G (כי זה הגודל שלה)
4. יהי $\mathbb{F} = \mathbb{F}_{2^n}$ שדה סופי עם מאפיין 2 כלומר $1 + 1 = 0$. הוכיחו כי כל איבר בו הוא ריבוע כלומר $\forall x \in \mathbb{F} \exists y \in \mathbb{F} : x = y^2$.
 הדרכה: נגדיר העתקה $\phi : \mathbb{F} \rightarrow \mathbb{F}$ ע"י $\phi(x) = x^2$ הראו שהעתקה זו היא חח"ע והסיקו כי ϕ על ולכן הטענה מתקיימת.
פתרון: נראה חח"ע: נניח $\phi(a) = \phi(b)$ אזי $a^2 = b^2$ כעת,
 אם $a = 0$ נקבל ש $b^2 = 0$ שזה גורר כי $b = 0$ (אחרת b הפיך, נכפול בהופכי משני הצדדים ונקבל כי $b = 0$)
 אם $b = 0$ נקבל באופן דומה ש $a = 0$
 אחרת, $a, b \neq 0$ אזי $a, b \in \mathbb{F}^\times$ החבורה הכפלית של השדה (חבורה עם $2^n - 1$ איברים) ולכן

$$a^{2^n - 1} = 1 = b^{2^n - 1}$$

מה שגורר כי

$$a^{2^n} = a, b^{2^n} = b$$

כעת נתון ש $a^2 = b^2$. נעלה בחזקת 2^{n-1} ונקבל

$$a = (a^2)^{2^{n-1}} = (b^2)^{2^{n-1}} = b$$

שזה מסיים את ההוכחה כי ϕ חח"ע.

כעת פונקציה מקבוצה סופית לעצמה היא חח"ע אמ"מ היא על ולכן ϕ על. בפרט לכל איבר יש מקור. יהא $x \in \mathbb{F}$ אזי יש לו מקור כלומר קיים $y \in \mathbb{F}$ כך ש $y^2 = \phi(y) = x$

5. יהא $\mathbb{F} = \mathbb{F}_p$ שדה עם p^n איברים. הוכיחו כי

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}^\times} (x - \alpha)$$

כאשר השיוון הוא שיוון פולינומים.
 הסיקו את משפט וילסון: יהא p מספר ראשוני אי זוגי אזי

$$(p - 1)! \equiv -1 \pmod{p}$$

פתרון: כיוון שכל איבר $\alpha \in \mathbb{F}^\times$ מתקיים כי $\alpha^{p^n-1} = 1$ (משפט לגרנז' עבור החבורה הכפלית (\mathbb{F}^\times) נקבל כי כל איבר $\alpha \in \mathbb{F}^\times$ הוא שורש של הפולינום $x^{p^n-1} - 1$. כיוון שלפולינום זה יכול להיות לכל היותר $p^n - 1$ שורשים (כמעלת הפולינום) בעצם מצאנו את כולם ולכן השיוון מתקיים.
 כעת נציב $x = 0$ ונקבל כי

$$-1 = \prod_{\alpha \in \mathbb{F}^\times} -\alpha = (-1)^{|\mathbb{F}^\times|} \prod_{\alpha \in \mathbb{F}^\times} \alpha$$

במקרה הפרטי של השדה \mathbb{Z}_p (כאשר p ראשוני אי זוגי) נקבל כי

$$-1 = (-1)^{p-1} \prod_{i=1}^{p-1} i = (p-1)!$$

שיוון זה מתקיים בשדה שלנו שזה שקול ל

$$(p-1)! \equiv -1 \pmod{p}$$