

## תרגיל מספר 12 מבנים אלגבריים

1.

(א) הוכיחו כי  $f(x) = x^2 + x + 4 \in \mathbb{Z}_{11}[x]$  ראשוני ולכן  $\mathbb{F} = \mathbb{Z}_{11}[x] / \langle x^2 + x + 4 \rangle$  שדה.

**פתרון:** בשיעורי בית קודמים ראינו כי פולינומים עד דרגה 3 הוא ראשוני אמ"מ אין לו שורש. נבדוק שאין ל  $f(x)$  שורש.

$$\begin{aligned}f(0) &= 4 \\f(1) &= 6 \\f(2) &= 10 \\f(3) &= 5 \\f(4) &= 2 \\f(5) &= 1 \\f(6) &= 2 \\f(7) &= 5 \\f(8) &= 10 \\f(9) &= 6 \\f(10) &= 4\end{aligned}$$

(ב) מצאו  $[3x + 2]^{-1}$  ב  $\mathbb{F}$  הנ"ל.

**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

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

מודלו  $x^2 + x + 4$  נקבל

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

ולכן

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

2. יהי  $\mathbb{F} = \mathbb{F}_{2^n}$  שדה סופי הוא מקיים כי  $1 + 1 = 0$ . הוכיחו כי כל איבר בו הוא ריבוע

כלומר  $\forall x \in \mathbb{F} \exists y \in \mathbb{F} : x = y^2$ .

הדרכה: נגדיר העתקה  $\phi : \mathbb{F} \rightarrow \mathbb{F} : \phi(x) = x^2$  ע"י  $\phi(x) = x^2$  הראו שהעתקה זו היא חח"ע והסיקו כי  $\phi$  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  $\phi$  חח"ע.

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

3. יהא  $\mathbb{F} = \mathbb{F}_{p^n}$  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 ו  $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$  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

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