

תרגיל מספר 10 מבנים אלגבריים

שיעורי בית 10

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

(א) יהא \mathbb{F} שדה. יהיו $a, b \in \mathbb{F}$ שונים מאפס. הוכיחו כי $ab \neq 0$
פתרון: נניח בשלילה כי $ab = 0$ אזי אם נכפיל ב a^{-1} (קיים כי a שונה מאפס) נקבל כי

$$b = a^{-1}0 = 0$$

סתירה.

(ב) יהא \mathbb{F} שדה סופי עם p^t איברים עבור p ראשוני ו t טבעי. נגדיר $K = \{1, 1+1, 1+1+1, \dots\} = \{1n : n \in \mathbb{N}\}$ (כלומר $2 = 1+1, 3 = 1+1+1, \dots$)
וכו' הוכיחו כי K שדה עם מספר p איברים.
פתרון: כיוון שהשדה סופי קיימים $n < m \in \mathbb{N}$ שונים כך ש $1n = 1m$
(אחרת כולם שונים ויש ∞ איברים ב K ולכן גם ב \mathbb{F} . סתירה). לכן

$$(1m - 1n) = 0$$

נגדיר $p' = \min \{k \in \mathbb{N} : 1k = 0\}$ טענה ראשוני. הוכחה: אחרת קיימים $1a \cdot 1b = 1ab = 1p' = 0$ אבל $1a, 1b \neq 0$ ואז $p' = ab < a, b < p'$
סתירה לסעיף הקודם. לכן

$$K = \{1, 2, \dots, p' - 1, 0\}$$

כאשר והכפל והחיבור ב K מתנהגים כמו כפל וחיבור מודולו p' ולכן ההוכחה ש $\mathbb{Z}_{p'}$ שדה תעבוד גם עבור K .

כעת \mathbb{F} הוא מרחב וקטורי מעל K ולכן קיים לו בסיס $B = \{v_1, \dots, v_n\}$. כל $x \in \mathbb{F}$ הוא צירוף לינארי יחיד $x = \sum_{i=1}^n \alpha_i v_i$ עבור $\alpha_1, \dots, \alpha_n \in K$ ולכן מספר האיברים ב \mathbb{F} הוא

$$|\mathbb{F}| = \left| \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} : a_1, \dots, a_n \in K \right\} \right| = p'^n$$

לפי הנתון $p'^n = p^t$ כיוון ש p', p ראשוניים נקבל כי $p' = p$ ו $n = t$

(ג) יהא \mathbb{F} שדה סופי ויהא $K = \{1, 1 + 1, 1 + 1 + 1, \dots\}$ מסעיף קודם בעל p איברים כאשר p ראשוני. הוכיחו כי מספר האיברים ב \mathbb{F} הוא p^n עבור n טבעי. הדרכה: חישובו על \mathbb{F} כמרחב וקטורי מעל K
פתרון: נסמן $K = \{1, 1 + 1, 1 + 1 + 1, \dots\}$ כמו מסעיף קודם אזי קיים p ראשוני כך שב K יש p איברים.
 כעת \mathbb{F} הוא מרחב וקטורי מעל K ולכן קיים לו בסיס $B = \{v_1, \dots, v_n\}$. כל $x \in \mathbb{F}$ הוא צירוף לינארי יחיד $x = \sum_{i=1}^n \alpha_i v_i$ עבור $\alpha_1, \dots, \alpha_n \in K$ ולכן מספר האיברים ב \mathbb{F} הוא

$$|\mathbb{F}| = \left| \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} : a_1, \dots, a_n \in K \right\} \right| = p^n$$

3. יהא \mathbb{F} שדה סופי עם p^n איברים עבור p ראשוני ו n טבעי ויהא $K = \{1, 1 + 1, 1 + 1 + 1, \dots\}$ מסעיף קודם. יהא $p(x) = x^{p^n} - x \in K[x]$ ויהא $f(x) \in K[x]$ אי פריק מתוקן שמחלק את $p(x)$.

(א) הוכיחו כי קיים $a \in \mathbb{F}$ המקיים כי $f(a) = 0$.

פתרון:

לפי נתון קיים $q(x)$ כך ש $p(x) = f(x)q(x)$. ראינו בתירגול כי השורשים של $p(x)$ אלו בדיוק איברי השדה \mathbb{F} ולכן קיים $a \in \mathbb{F}$ המקיים כי $f(a) = 0$.

(ב) נסמן ב $q(x) \in K[x]$ את הפולינום המתוקן עם הדרגה המינימאלית המקיים $q(a) = 0$ וששונה מפולינום האפס. הוכיחו כי $f(x) = q(x)$.

פתרון:

נחלק את $f(x)$ ב $q(x)$ ונקבל

$$f(x) = t(x)q(x) + r(x)$$

עבור $\deg(r(x)) < \deg(q(x))$. נציב a ונקבל

$$r(a) = f(a) - t(a)q(a) = 0$$

כיוון ש $q(x)$ עם דרגה מינימאלית שונה מאפס מתוקן המקיים $q(a) = 0$ נקבל ש $r(x) = 0$ ואז

$$f(x) = t(x)q(x)$$

כיוון ש $f(x)$ אי פריק אזי הדרגה של $q(x)$ היא 0 או $\deg(f)$.

כיוון ש $\deg(q) \neq 0$ (כי אז הוא פולינום קבוע ואז $q(a) \neq 0$ נקבל כי $\deg(f) = \deg(q)$ כיוון ששניהם מתוקנים נקבל כי $t(x) = 1$ ולכן $f(x) = q(x)$)

(ג) הוכיחו כי $K[a] = \{q(a) : q(x) \in K[x]\}$ הוא תת שדה של \mathbb{F}

פתרון: נראה כי $K[a]$ חבורה חילופית ביחס לחיבור.

• סגירות: יהיו $q_1(x), q_2(x) \in K[x]$ ויהיו $q_1(a), q_2(a) \in K[a]$ אזי $q_1(x) + q_2(x) \in K[x]$ ומתקיים כי $q_1(a) + q_2(a) = (q_1 + q_2)(a) \in K[a]$

- קיבוציות: נובע מקיבוציות ב \mathbb{F}

- נטרלי: עבור פולינום האפס $0(x) \in K[x]$ נקבל כי $0(a) = 0 \in K[a]$ ולכן איבר האפס שייך ל $K[a]$

- נגדי: יהיה $q(x) \in K[x]$ ויהא $q(a) \in K[a]$ אזי $-q(x) \in K[x]$ ו $-q(a) \in K[a]$ ומתקיים כי $q(a) + (-q(a)) = 0$ ולכן ל $q(a)$ יש נגדי ב $K[a]$

- חילופיות נובע מחילופיות ב \mathbb{F} .

• נראה כי $K[a]$ בלי $0(a) = 0$ הוא חבורה כפליית חילופית

- סגירות: יהיו $q_1(x), q_2(x) \in K[x]$ ויהיו $q_1(a), q_2(a) \in K[a]$ אזי $q_1(x)q_2(x) \in K[x]$ ו $0 \neq q_1(x)q_2(x) \in K[x]$ שדה ולכן אין מחלקי אפס ב $K[x]$ ומתקיים כי $0 \neq q_1(a)q_2(a) = (q_1q_2)(a) \in K[a]$

- קיבוציות: נובע מקיבוציות ב \mathbb{F}

- נטרלי: הפולינום $1(x) \in K[x]$ מקיים כי $1(a) = 1 \in K[a]$ שהוא הנטרלי ב \mathbb{F} ובפרט ב $K[a]$

- הופכי: יהיה $q(x) \in K[x]$ ויהא $q(a) \in K[a]$ נמצא לו הופכי. כיוון ש $\gcd(f(x), q(x)) = 1$ קיימים $s(x), t(x) \in K[x]$ כך ש

$$s(x)f(x) + q(x)t(x) = 1$$

ולכן

$$s(a)f(a) + q(a)t(a) = 1$$

כיוון ש $f(a) = 0$ נקבל כי $q(a)t(a) = 1$ ולכן $t(a) \in K[a]$ ההופכי של $q(a)$

• פילוג: נובע מחילופיות ב \mathbb{F} .

(ד) הוכיחו כי מספר האיברים ב $K[a]$ שווה ל $p^{\deg(f)}$

פתרון:

נסמן $X = \{q(x) \in K[x] : \deg(q(x)) < \deg(f(x))\}$ נראה כי

$$K[a] = \{q(a) : q(x) \in K[x]\} = \{q(a) : q(x) \in X\}$$

הכיוון (\supseteq) הוא טריאלי.

(\subseteq) יהא $q(x) \in K[x]$ ויהא $q(a) \in K[a]$. נחלק את $q(x)$ ב $f(x)$ ונקבל

$$q(x) = t(x)f(x) + r(x)$$

עבור $r(x) \in X$ נציב a ונקבל

$$q(a) = t(a)f(a) + r(a) = r(a)$$

כי $f(a) = 0$ ולכן $q(a) = r(a)$.

כעת נראה כי לכל $q_1(x) \neq q_2(x) \in X$ מתקיים כי $q_1(a) \neq q_2(a)$.
 נניח בשלילה כי $q_1(a) = q_2(a)$ ואז $q_1(x) - q_2(x) = 0$ נגדיר $q(x) = q_1(x) - q_2(x)$ אזי $q(a) = 0$. ובנוסף, $\deg q(x) < \deg(f)$ ולכן לפי סעיף קודם $q(x) = 0$ ולכן $q_1(x) = q_2(x)$ ולכן $q_1(a) = q_2(a)$
 לסיכום קיבלנו כי

$$|K[a]| = |\{q(a) : q(x) \in X\}| = \left| \left\{ \sum_{i=0}^{\deg(f)-1} \alpha_i a^i : \forall i : \alpha_i \in K \right\} \right| = |K|^{\deg(f)} = p^{\deg(f)}$$

(ה) הסיקו/הוכיחו כי הדרגה של p מחלקת את n .

פתרון :

הוכחנו בתירגול כי הגודל של כל תת שדה של שדה עם p^n הוא p^t עבור $t|n$.
 ולכן הגודל של $K[a]$ כמתת שדה של \mathbb{F} הוא p^t עבור $t|n$. מסעיף קודם נקבל כי

$$p^t = p^{\deg(f)}$$

$$\deg(f) = t|n \text{ ולכן}$$

4. 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 $\phi : \mathbb{F} \rightarrow \mathbb{F}$ 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 $\mathbb{F} = \mathbb{F}_{p^n}$ 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 $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$. 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

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