

תרגיל מספר 10 מבנים אלגבריים

1. יהיו $a(x), b(x) \in \mathbb{F}[x]$ שני פולינומים. נחלק את $a(x)$ ב $b(x)$ ע"י אלגוריתם לחילוק פולינומים ונקבל $q(x), r(x)$ כך ש

$$a(x) = q(x)b(x) + r(x)$$

הוכיחו כי $\gcd(a(x), b(x)) = \gcd(b(x), r(x))$
פתרון :

טענה: לכל $y(x)$ מתקיים כי:

$$y(x)|a(x), b(x) \text{ אמ"מ } y(x)|b(x), r(x)$$

בכיוון אחד: נתון $y(x)|a(x), b(x)$ ולכן $y(x)|a(x) - q(x)b(x) = r(x)$ ולכן $y(x)|b(x), r(x)$.

בכיוון השני: נתון $y(x)|b(x), r(x)$ ולכן $y(x)|q(x)b(x) + r(x) = a(x)$ ולכן $y(x)|a(x), b(x)$.
 בפרט $\gcd(a(x), b(x)), \gcd(b(x), r(x))$ מחלקים אחד את השני. בפרט קיימים $\alpha(x), \beta(x)$ כך ש

$$\gcd(a(x), b(x)) = \alpha(x) \cdot \gcd(b(x), r(x))$$

$$\gcd(b(x), r(x)) = \beta(x) \cdot \gcd(a(x), b(x))$$

ביחד נקבל כי

$$\gcd(a(x), b(x)) = \alpha(x) \cdot \gcd(b(x), r(x)) = \alpha(x) \cdot \beta(x) \cdot \gcd(a(x), b(x))$$

ולכן $\alpha(x) \cdot \beta(x) = 1$ בפרט $\alpha(x), \beta(x)$ פולינומים קבועים, כלומר $\alpha(x) = c_1\beta(x) = c_2$ עבור $c_1, c_2 \in \mathbb{F}$ קבועים.
 לכן

$$\gcd(a(x), b(x)) = c_1 \cdot \gcd(b(x), r(x))$$

כיוון ששני הפולינומים מתוקנים (לפי הגדרה) נקבל כי $c_1 = 1$ ולכן $\gcd(a(x), b(x)) = \gcd(b(x), r(x))$

2. יהיו $a(x), b(x), c(x) \in \mathbb{F}[x]$ שלושה פולינומים הוכיחו כי אם $\gcd(a(x), c(x)) = \gcd(b(x), c(x)) = 1$ אזי

$$\gcd(a(x)b(x), c(x)) = 1$$

פתרון : לפי משפט קיימים פולינומים $t_1(x), s_1(x), t_2(x), s_2(x)$ כך ש

$$t_1(x)a(x) + s_1(x)c(x) = 1$$

$$t_2(x)b(x) + s_2(x)c(x) = 1$$

נכפיל ונקבל כי

$$[t_1(x)a(x) + s_1(x)c(x)][t_2(x)b(x) + s_2(x)c(x)] = 1$$

אחרי פתיחת סוגריים נקבל

$$t(x)a(x)b(x) + s(x)c(x) = 1$$

[כאשר $t(x) = t_1(x)t_2(x)$, $s(x) = t_1(x)a(x)s_2(x) + s_1(x)t_2(x)b(x) + s_1(x)c(x)s_2(x)$]

טענה: $\gcd(a(x)b(x), c(x)) = 1$. ברור כי 1 מחלק את $c(x), a(x)b(x)$. נניח $d(x)|c(x), a(x)b(x)$ אזי $d(x)$ מחלק גם את הצירוף $t(x)a(x)b(x) + s(x)c(x) = 1$ ולכן $d(x)|1$ ולכן $d(x) \in \mathbb{F}$ בפרט

$$\deg(d) = 0 \leq \deg(1)$$

וסיימנו.

3. תרגיל: הוכיחו כי אם $p(x) \in \mathbb{F}[x]$ פולינום (מדרגה גדולה ממש מאפס) אי פריק אזי הוא ראשוני. [היעזרו בתרגיל הקודם]

פתרון: נתון $p(x)$ אי פריק. צ"ל p ראשוני.

קעת יהיו a, b פולינומים כך ש $p|ab$ נוכיח כי $p|a$ או $p|b$. נסמן $d = \gcd(a, p)$.

אזי בפרט $d|p$ ולכן קיים q כך ש $p = dq$ כיוון ש p אי פריק חייב להיות כי הדרגה של d או q שווה ל p ושל הפולינום השני היא 0.

אם $\deg(d) = \deg(p)$ אז $\deg(q) = 0$ ולכן $q \in \mathbb{F}$ פולינום קבוע ואז $p(x) = d(x)q$. כיוון ש $q \neq 0$ נקבל כי $d(x) = p(x) \cdot q^{-1}$ ובפרט $d(x) = p(x) \wedge d(x)|a(x)$ ולכן $p(x)|a(x)$ וסיימנו.

אחרת $\deg(d(x)) = 0$ ואז $d(x) = 1$.

באותו אופן נסמן $d'(x) = \gcd(b(x), p(x))$. ואז אם $\deg(d'(x)) = \deg(p(x))$ אז $p(x)|b(x)$ וסיימנו.

אחרת $d'(x) = 1$ ואז $\gcd(a, p) = \gcd(b, p) = 1$ ולפי תרגיל קודם $\gcd(ab, p) = 1$ אבל $p|ab$ ולכן $\deg(p) \leq \deg(1) = 0$ כלומר p פולינום קבוע כלומר מדרגה 0. סתירה.

4.

(א) נגדיר: $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ מצא $d = \gcd(a, b)$ ומצאו $p, q \in \mathbb{R}[x]$ כך ש $ap + qb = d$ **פתרון:** נחשב

$$a(x) = b(x) \cdot (2x - 4) + 9$$

$$b(x) = (9) \left(\frac{1}{9}x + \frac{2}{9} \right) + 0$$

ולכן

$$9 = a(x) - b(x) \cdot (2x - 4)$$

ומכאן ש

$$1 = \frac{1}{9}a(x) - \frac{2x-4}{9}b(x)$$

לכן $\gcd(a, b) = 1$ מכאשר $p(x) = \frac{1}{9}$, $q(x) = -\frac{2x-4}{9}$

(ב) נגדיר: $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x$, $b(x) = x^3 + x^2 \in \mathbb{R}[x]$ ומוצא $d = \gcd(a, b)$

$p, q \in \mathbb{R}[x]$ כך ש $ap + qb = d$

פתרון : נחשב

$$\begin{aligned} a(x) &= b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5) + (-3x^2 + x) \\ b(x) &= (-3x^2 + x) \left(-\frac{x}{3} - \frac{4}{9} \right) + \left(\frac{4}{9}x \right) \\ (-3x^2 + x) &= \left(\frac{4}{9}x \right) \cdot \left(-\frac{27}{4}x + \frac{9}{4} \right) + 0 \end{aligned}$$

ולכן

$$\begin{aligned} \frac{4}{9}x &= b(x) - (-3x^2 + x) \left(-\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) - [a(x) - b(x) \cdot (7x^4 - x^3 + 6x^2 - 2x + 5)] \left(-\frac{x}{3} - \frac{4}{9} \right) \\ &= b(x) \left[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left(-\frac{x}{3} - \frac{4}{9} \right) \right] + a(x) \left(\frac{x}{3} + \frac{4}{9} \right) \end{aligned}$$

ומכאן ש

$$x = b(x) \frac{[1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left(-\frac{x}{3} - \frac{4}{9} \right)]}{4/9} + a(x) \frac{\left(\frac{x}{3} + \frac{4}{9} \right)}{4/9}$$

ולכן (אם ניקח פולינום מתוקן) $\gcd(a, b) = x$ והוא צירוף לינארי המבוקש עם $p(x) = \frac{9}{4} \left(\frac{x}{3} + \frac{4}{9} \right)$, $q(x) = \frac{9}{4} [1 + (7x^4 - x^3 + 6x^2 - 2x + 5) \left(-\frac{x}{3} - \frac{4}{9} \right)]$

.5

(א) יהא $f(x) \in \mathbb{F}[x]$ פולינום עם $2 \leq \deg(f) \leq 3$. הוכיחו כי ראשוני אמ"מ ל $f(x)$ אין שורש (שורש של $f(x)$ הוא $a \in \mathbb{F}$ המקיים $f(a) = 0$)

פתרון :

(\Rightarrow) נתון ל $f(x)$ אין שורש. צ"ל $f(x)$ ראשוני. נניח בשלילה כי $f(x)$ אינו ראשוני אזי $f(x)$ פריק ולכן קיימים $a(x), b(x)$ כך ש

$$f(x) = a(x)b(x)$$

ובנוסף $3 \leq \deg(f(x)) < \deg(a(x)), \deg(b(x)) \in \{1, 2\}$ ולכן $\deg(a(x)) = 2$ אם $\deg(a(x)) = 2$ אזי $\deg(b(x)) = 1$ כי $\deg(f(x)) = \deg(a(x)b(x)) = \deg(a(x)) + \deg(b(x))$. בכל מקרה, או $a(x)$ או $b(x)$ פולינום מדרגה 1 כלומר מהצורה

$$x - \alpha$$

עבור $\alpha \in \mathbb{F}$ ולכן)

$$f(\alpha) = a(\alpha)b(\alpha) = 0$$

ולכן α הוא שורש של $f(x)$. סתירה.

(\Leftarrow) נתון $f(x)$ ראשוני. צ"ל ל $f(x)$ אין שורש. נניח בשלילה כי קיים ל $f(x)$ שורש שנסמנו ב a אז נבצע חילוק פולינומים ונקבל כי קיים $q(x), r(x)$ כך ש

$$f(x) = (x - a)q(x) + r(x)$$

ו $\deg(r(x)) < \deg(x - a) = 1$ או $r = 0$. כלומר, בכל מקרה $c \in \mathbb{F}$ $r(x) = c$. אם נציב a במשוואה נקבל

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

ומכאן ש $r(a) = 0$ ומכאן ש $r(x) = 0$ ומכאן ש $f(x) = (x - a)q(x)$ כלומר $f(x)$ פריק (כי $1 \leq \deg(q)$) ולכן לא ראשוני

(ב) הראו שיש בדיוק פולינום אי-פריק אחד ממעלה שניים ב $\mathbb{Z}_2[x]$.

פתרון : פולינום מדרגה לכל היותר 2 הוא מהצורה $p(x) = ax^2 + bx + c$ כאשר $a, b, c \in \mathbb{Z}_2$. אם הפולינום הוא אי פריק בפרט אין לו שורשים ולכן $p(0) \neq 0$ שזה גורר כי $c \neq 0$ וגם $p(1) \neq 0$ מה שגורר כי $a + b + c \neq 0$. כיוון שמדובר ב \mathbb{Z}_2 אזי שונה מאפס אומר שווה ל-1 ולכן

$$\begin{aligned} c &= 1 \\ a + b + c &= 1 \end{aligned}$$

וביחד

$$\begin{aligned} c &= 1 \\ a &= b \end{aligned}$$

כיוון שרוצים דרגה בדיוק 2 אזי $a \neq 0$ ולכן $a = 1$ ובס"ה נקבל כי $p(x) = x^2 + x + 1$ הוא אכן לא פריק כי אם הוא היה פריק היה לו שורש (לפי תרגיל קודם) אבל $p(1) \neq 0$ וגם $p(0) \neq 0$ ואלו השורשים היחידים האפשריים בשדה שלנו.

(ג) העזרו בסעיף א כדי לקבוע האם $x^5 + x^4 + 1 \in \mathbb{Z}_2[x]$ פריק.

פתרון : אם $p(x) = x^5 + x^4 + 1$ היה פריק אזי $p(x) = a(x)b(x)$ כאשר המעלה של $a(x)$ היא 0 או 1 או 2 או 3 או 4 או 5. נעבור על האפשרויות

מעלה 0 לא יכול לפי הגדרת פריקות של $p(x)$

מעלה 1 אומר של $p(x)$ יש שורש אבל $1 \neq p(0) = p(1)$

מעלה 2 אומר ש $a(x) = x^2 + x + 1$ לפי סעיף קודם כלומר $x^2 + x + 1$ מחלק את $p(x)$. נבדוק ונמצא שאכן

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

(ד) העזרו בסעיף א כדי לקבוע האם $x^5 + x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$ פריק.

פתרון : אם $p(x) = x^5 + x^4 + x^3 + x^2 + 1$ היה פריק אזי $p(x) = a(x)b(x)$ כאשר המעלה של $a(x)$ היא 0 או 1 או 2 או 3 או 4 או 5. נעבור על האפשרויות

מעלה 0 לא יכול לפי הגדרת פריקות של $p(x)$

מעלה 1 אומר של $p(x)$ יש שורש אבל $1 \neq p(0) = p(1)$

מעלה 2 אומר ש $a(x) = x^2 + x + 1$ לפי סעיף קודם כלומר $x^2 + x + 1$ מחלק את $p(x)$. נבדוק, מחילוק פולינומים נקבל כי

$$p(x) = a(x)(x^3 + 1) + (-x)$$

בפרט $a(x)$ לא מחלק את $p(x)$.
מעלה 3/4/5 אומר שהמעלה של $b(x)$ היא $2/1/0$ וכמו המקרה של $a(x)$ זה לא אפשרי.