

תרגיל מספר 9 מבנים אלגבריים

22 בינואר 2017

1. יהא $f(x) \in \mathbb{F}[x]$ פולינום n . יהיו g_1, g_2 שני פולינומים מדרגה קטנה מ n . נתבונן במחלקות שקילות שלהם $[g_1], [g_2] \in \mathbb{F}[x]/\langle f \rangle$ הוכיחו כי

$$[g_1] = [g_2] \iff g_1 = g_2$$

פתרון :

(\Leftarrow) ברור.

(\Rightarrow) נתון $[g_1] = [g_2]$ אזי g_1 מתייחס ל g_2 כלומר $g_1 - g_2 \in \langle f \rangle$. ומכאן כי

$$\exists g \in \mathbb{F}[x] : g_1 - g_2 = fg$$

נרצה להראות כי $g = 0$. נניח בשלילה כי $g \neq 0$ אזי $\deg(fg) = \deg(f) + \deg(g) \geq \deg(f) + 1 > n$ מצד שני $\deg(g_1 - g_2) \leq \max\{\deg(g_1), \deg(g_2)\} < n$. סתירה.

2.

(א) יהא $f(x) \in \mathbb{F}[x]$ ויהיה $\mathbb{F}[x]/\langle f \rangle$ חוג המנה ביחס לאידיאל $\langle f \rangle$. הוכיחו כי $\mathbb{F}[x]/\langle f \rangle$ שדה אמ"מ f ראשוני

פתרון : (\Rightarrow) נתון f ראשוני. צ"ל $R = \mathbb{F}[x]/\langle f \rangle$ שדה. הוכחה:

• נראה כי $\mathbb{F}[x]/\langle f \rangle$ חבורה חילופית ביחס לחיבור.

- סגירות: לכל $[y_1], [y_2] \in R$ מתקיים כי $[y_1] + [y_2] = [y_1 + y_2] \in R$
- קיבוציות: לכל $[y_1], [y_2], [y_3] \in R$ מתקיים כי $([y_1] + [y_2]) + [y_3] = [y_1 + y_2] + [y_3] = [y_1 + (y_2 + y_3)]$
- $[y_1] + ([y_2] + [y_3]) = [y_1 + (y_2 + y_3)] = [y_1 + (y_2 + y_3)]$ ואילו $[y_1 + y_2][y_3] = [y_1 + y_2 + y_3]$
מתקיים קיבוציות

- נטרלי: $[0] \in R$ נטרלי כי לכל $[y] \in R$ מתקיים $[y] + [0] = [y + 0] = [y]$

- הופכי: לכל $[y] \in R$ מתקיים כי $[y] + [-y] = [0]$ ולכן $[-y]$ הוא הופכי של $[y]$.

- חילופיות נובע מחילופיות של הפולינומים.

• נראה כי $\mathbb{F}[x]/\langle f \rangle$ בלי $[0]$ הוא חבורה כפלית חילופית

- סגירות: לכל $[y_1], [y_2] \in R$ מתקיים כי $[y_1][y_2] = [y_1 y_2] \in R$
- קיבוציות: לכל $[y_1], [y_2], [y_3] \in R$ מתקיים כי $([y_1][y_2])[y_3] = [y_1 y_2] y_3 = [y_1 (y_2 y_3)]$ ואילו $[y_1 y_2][y_3] = [y_1 y_2 y_3]$
- $[y_1]([y_2][y_3]) = [y_1 y_2 y_3] = [y_1 (y_2 y_3)]$ ואילו $[y_1 y_2][y_3] = [y_1 y_2 y_3]$
ושני אלו שווים כי בפולינומים מתקיים קיבוציות

- נטרלי: $[1] \in R$ נטרלי כי לכל $[y] \in R$ מתקיים $[y][1] = [y \cdot 1] = [y]$
 - הופכי: יהא $[y] \in R$ $[0] \neq [y]$ טענה: $\gcd(f, y) = 1$ הוכחה: אחרת $\gcd(f, y) = d$ עם מעלה גדולה מ-0. ואז $d|f$ שזה גורר כי קיים $dt = f$ אבל f ראשוני ולכן אי פריק ולכן $\deg(d) = \deg(f)$ או $\deg(d) = 0$ כיוון ש $\deg(d) > 0$ נקבל כי $\deg(d) = \deg(f)$ כיוון ש d מחלק את f נקבל כי $f(x) = c \cdot d(x)$ כאשר $c \in \mathbb{F}$ לכן $f|d$ גם כן ($d(x) = c^{-1}f(x)$ אבל $d|y$ ולכן $f|y$ מה שאומר כי $[y] = [0]$ סתירה. מסקנה $\gcd(f, y) = 1$ ולכן קיימים t, s כך ש $ft + ys = 1$ מה שאומר כי $1 - ys = ft \in \langle f \rangle$ ולכן $[1] = [ys] = [y][s]$ ולכן $[y]^{-1} = [s]$.
 • פילוג: לכל $[y_1], [y_2], [y_3] \in R$ מתקיים כי

$$([y_1] + [y_2])[y_3] = [y_1 + y_2][y_3] = [(y_1 + y_2)y_3] = [y_1y_3 + y_2y_3] = [y_1y_3] + [y_2y_3] = [y_1][y_3] + [y_2][y_3]$$

(\Leftarrow) נתון $R = \mathbb{F}[x]/\langle f \rangle$ שדה. צ"ל f ראשוני. יהיו a, b פולינומים כך ש $f|ab$ ונראה כי f מחלק אחד מהם. אכן: $f|ab$ ולכן $[ab] = [0]$ ב R כלומר $[a][b] = [0]$. כיוון שבשדה אין מחלקי אפס מוכרח להיות כי $[a] = [0]$ או $[b] = [0]$ במקרה הראשון נקבל כי $f|a$ ובמקרה השני נקבל כי $f|b$ וסיימנו.

(ב) יהא p מספר טבעי ראשוני ונגדיר $\mathbb{F} = \mathbb{Z}_p$. הוכיחו כי אם $f(x) \in \mathbb{F}[x]$ ראשוני מדרגה n אזי השדה $\mathbb{F}[x]/\langle f \rangle$ בעל p^n איברים.
פתרון: טענה: כל $y(x) \in \mathbb{F}[x]$ שקול לפולינום מדרגה קטנה מ n הוכחה: נבצע חילוק פולינום

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

עם $\deg(r(x)) < \deg(f(x))$ או $r(x) = 0$
 כיוון ש $r(x)$ שקול ל $y(x)$ כי

$$y(x) - r(x) = q(x)f(x) \in \langle f \rangle$$

נקבל ש

$$\mathbb{F}[x]/\langle f \rangle = \{ [y(x)]_{\equiv_f} : \deg(y(x)) < n \}$$

באופן מפורש

$$\mathbb{F}[x]/\langle f \rangle = \{ [a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_{\equiv_f} \mid \forall i : a_i \in \mathbb{F} \}$$

בנוסף לכל $(a_0, \dots, a_{n-1}) \neq (b_0, \dots, b_{n-1}) \in \mathbb{F}^n$ מתקיים כי

$$[a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_{\equiv_f} \neq [b_0 + b_1x + \dots + b_{n-1}x^{n-1}]_{\equiv_f}$$

לפי תרגיל קודם. ולכן מספר האיברים ב

$$\mathbb{F}[x]/\langle f \rangle = \{ [a_0 + a_1x + \dots + a_{n-1}x^{n-1}]_{\equiv_f} \mid \forall i : a_i \in \mathbb{F} \}$$

שווה למספר האיברים ב

$$\mathbb{F}^n = \left\{ \left(\begin{array}{c} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{array} \right) : a_0, \dots, a_{n-1} \in \mathbb{F} = \mathbb{Z}_p \right\}$$

שבקבוצה זאת p^n איברים.

3. עבור הפולינומים $a(x) = 1 + 2x^2, b(x) = 2 + x \in \mathbb{R}[x]$ ראינו ב.ש.ב. הקודמים כי $1 = \gcd(a, b)$ ומתקיים

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

מצאו פולינום $f(x)$ המקיים

$$f(x) \equiv_{a(x)} x$$

$$f(x) \equiv_{b(x)} 5$$

[השתמשו ברעיון דומה למשפט השאריות הסיני]

פתרון :

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

לכן

$$\frac{1}{9}a(x) \equiv_{b(x)} 1, \quad -\frac{1}{9}a(x) \equiv_{a(x)} 0$$

$$-\frac{2x-4}{9}b(x) \equiv_{b(x)} 0, \quad -\frac{2x-4}{9}b(x) \equiv_{a(x)} 1$$

ומכאן שנגדיר

$$f(x) = x \cdot \left[\frac{1}{9}a(x) \right] + 5 \cdot \left[-\frac{2x-4}{9}b(x) \right]$$

יקיים

$$f(x) \equiv_{a(x)} 5 \cdot \left[-\frac{2x-4}{9}b(x) \right] \equiv_{a(x)} 5 \cdot 1 = 5$$

ובנוסף

$$f(x) \equiv_{b(x)} x \cdot \left[\frac{1}{9}a(x) \right] \equiv_{b(x)} x \cdot 1 = x$$

כנדרש.

.4

(א) יהא $f(x) \in \mathbb{F}[x]$ פולינום עם $\deg(f) \leq 3$. 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 $\deg(a(x)), \deg(b(x)) < \deg(f(x)) \leq 3$ ולכן $\deg(a(x)) \in \{1, 2\}$ 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 $r(x) = 0$. כלומר, בכל מקרה $r(x) = c \in \mathbb{F}$ 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 ולכן לא ראשוני

.5

(א) 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 $p(0) \neq 0$ ו $c \neq 0$ 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

$$c = 1$$

$$a + b + c = 1$$

וביחד

$$c = 1$$

$$a = b$$

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 (כי אם $p(x) = a(x)b(x)$ אזי a, b פולינומים מדרגה 1 ואז אם $a(x) = x - \text{const}$ נקבל כי $p(\text{const}) = a(\text{const})b(\text{const}) = 0 \cdot \text{const} = 0$ אבל $p(1) \neq 0$ וגם $p(0) \neq 0$ ואלו השורשים היחידים האפשריים בשדה שלנו.

(ב) 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 $p(1) = p(0) = 1 \neq 0$ 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

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

(ג) 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 $p(1) = p(0) = 1 \neq 0$ 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.