

תרגול 14 שדות סופיים

28 ביוני 2021

תזכורת: חוג מנה $R = \mathbb{F}[x]/\langle f \rangle = \{g + \langle f \rangle \mid g \in \mathbb{F}[x]\}$ במקום לרשום איבר בצורה $g + \langle f \rangle$ רושמים פשוט $[g]$. חיבור:

$$[g] + [h] = [g + h]$$

כפל:

$$[g][h] = [gh]$$

איבר האפס הוא $[0]$, איבר היחידה הוא $[1]$.
תרגילים:

1. סוג של תזכורת, להבנת ההמשך. יהי \mathbb{F} שדה, ויהי $f, g \in \mathbb{F}[x]$. רוצים למצוא $a, b \in \mathbb{F}[x]$ כך ש- $gcd(f, g) = af + bg$.
פתרון: האלגוריתם אומר לעשות חילוק עם שארית

$$(1) : f = q_1g + r_1$$

, ואז $gcd(f, g) = gcd(g, r_1)$, ושוב לפי האלגוריתם מחלקים

$$(2) : g = q_2r_1 + r_2$$

ונניח כעת ש- $r_2 \in \mathbb{F}$ קבוע. ראינו שבמקרה זה $gcd(f, g) = gcd(g, r_1) = 1$. כדי למצוא את הצירוף הלינארי נשים לב שממשוואה (2) מקבלים:

$$r_2 = g - q_2r_1$$

כעת, נשים לב שממשוואה (1) מקבלים:

$$r_1 = f - q_1g$$

נציב זאת במה שקיבלנו לעיל:

$$r_2 = g - q_2r_1 = g - q_2(f - q_1g) = (-q_2)f + (1 + q_1q_2)g$$

כעת, $r_2 \in \mathbb{F}$ ולכן יש $r_2^{-1} \in \mathbb{F}$, ולכן:

$$1 = r_2^{-1} r_2 = \underbrace{r_2^{-1}(-q_2)}_{=a} \cdot f + \underbrace{r_2^{-1}(1 + q_1 q_2)}_{=b} \cdot g$$

2. נסמן $\mathbb{F} = \mathbb{Z}_5[x]/\langle p(x)=x^3+x+1 \rangle$.

(א) הוכיחו: שדה \mathbb{F} שדה. כמה איברים יש בו?

(ב) מצאו את ההופכי של $[x^2 + x + 1]$ בשדה זה.

פתרון: א. באופן כללי, $\mathbb{G}[x]/\langle f \rangle$ הוא שדה (כאשר \mathbb{G} שדה) אם f אי-פריק. אצלנו, מכיון ש- $\deg(x^3 + x + 1) = 3$ אז מספיק להראות שאין לו שורש, כדי להוכיח שהוא אי-פריק. נראה שאין לו שורש:

$$p(0) = 1 \neq 0$$

$$p(1) = 3 \neq 0$$

$$p(2) = 11 \equiv 1 \pmod{5} \neq 0$$

$$p(3) = 31 \neq 0$$

$$p(4) = 69 \neq 0$$

בסה"כ אין לו שורש בשדה \mathbb{Z}_5 , ולכן $p(x)$ אי-פריק, ו- \mathbb{F} שדה. כדי למצוא את מספר האיברים, נזכר במה שנאמר בהרצאה: מספר האיברים בשדה $\mathbb{Z}_q[x]/\langle f \rangle$ עבור f, q ראשוניים הוא: $q^{\deg(f)}$. לכן אצלנו נקבל:

$$|\mathbb{F}| = 5^3$$

רעיון ההוכחה: מראים שלכל פולינום h עם $\deg(h) \geq \deg(p)$ קיים פולינום g עם $\deg(g) < \deg(p)$ כך ש- $[g] = [h]$. כלומר, האיברים הם מהצורה $ax^2 + bx + c$, וכאלה יש 5^3 .

ב. כדי למצוא את ההופכי של $[x^2 + x + 1]$ נשים לב, שמכיון ש- p אי-פריק זאת אומרת ש- $\gcd(p(x), x^2 + x + 1) = 1$ כי אם בשלילה יש להם מחלק שאיננו קבוע, אז הוא מלמד על פריקות p בסתירה. לכן, לפי האלגוריתם נוכל למצוא $a, b \in \mathbb{Z}_5[x]$ כך ש-:

$$1 = a \cdot p + b(x^2 + x + 1)$$

ואז נקבל:

$$[1] = [a] \cdot \underbrace{[p]}_{=[0]} + [b] \cdot [x^2 + x + 1] = [b] \cdot [x^2 + x + 1]$$

הסבר:

$$[p] = p + \langle p \rangle$$

כעת, מכיון ש- $-p \in \langle p \rangle$, ולכן $0 = p + (-p) \in p + \langle p \rangle$, ולכן $[0] = [p]$. נמצא את b :
לכן $[b] = [x^2 + x + 1]^{-1}$.

$$\begin{array}{r|l} q_1(x) = x + 4 & \\ \hline x^3 + x + 1 & x^2 + x + 1 \\ x^3 + x^2 + x & \\ \downarrow & \\ 4x^2 + 1 & \\ 4x^2 + 4x + 4 & \\ \downarrow & \\ r_1(x) = x + 2 & \end{array}$$

כעת צריך להמשיך:

$$\begin{array}{r|l} q_2(x) = x + 4 & \\ \hline x^2 + x + 1 & x + 2 \\ x^2 + 2x & \\ \downarrow & \\ 4x + 1 & \\ 4x + 3 & \\ \downarrow & \\ r_2(x) = 3 & \end{array}$$

כעת, נעשה את הקילוף אחורה:

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

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

כעת, מהשלב הראשון ידוע:

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

ולכן:

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

נציב במשוואה שקיבלנו לעיל:

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

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

או בסימונים לפי מה שהראנו על הלוח (וכתוב כעת בפתרון שאלה 1):

$$r_2 = 3 = (1 + q_1 q_2)(x^2 + x + 1) + (-q_2)(x^3 + x + 1)$$

כעת נכפיל בהופכי של 3, ונקבל:

$$1 \equiv 2 \cdot 3 = \underbrace{2(1 + q_1 q_2)}_{=b}(x^2 + x + 1) + \underbrace{-2q_2}_a(x^3 + x + 1)$$

ובסה"כ:

$$[x^2 + x + 1]^{-1} = [b] = \underbrace{[2(1 + (x + 4)^2)]}_{x^2 + 3x + 2} \equiv [2x^2 + x + 4]$$