

אלגברה מופשטת 3 – פתרון תרגיל 1

1. בדקו האם הפולינומים הבאים אי-פריקים ב  $\mathbb{Q}[x]$

א.  $3x^2 - 7x - 5 \equiv x^2 + x + 1 \pmod{2}$

לפולינום מימין אין שורשים ב  $\mathbb{F}_2$ , ולכן הוא אי-פריק, לכן גם  $3x^2 - 7x - 5$  אי-פריק. ניתן גם לראות שלדיסקרימיננטה  $b^2 - 4ac = 49 - 60 = -11$  אין שורשים רציונליים.

ב.  $6x^3 - 3x - 18 = 3(2x^3 - x - 6)$

וברור ששקול לבדוק אי-פריקות של  $2x^3 - x - 6$ .

נראה שאין שורשים ב  $\mathbb{Q}$ : אם  $\frac{r}{s}$  שורש של  $2x^3 - x - 6$  (כאשר  $r, s$  זרים) אזי  $r \mid 6$  וגם

$s \mid 2$ . לכן האפשרויות הן:  $\pm 1, \pm 2, \pm 3, \pm 6, \pm \frac{1}{2}$ . כעת ניתן לבדוק ולראות שאלה אינם שורשים של הפולינום.

ג.  $x^3 - 7x + 1 \equiv x^3 + x + 1 \pmod{2}$  לפולינום מימין אין שורשים ב  $\mathbb{F}_2$ , ולכן הוא אי-פריק, לכן גם

הפולינום המקורי אי-פריק מעל  $\mathbb{Q}$ .

ד.  $x^3 - 9x - 9 \equiv x^3 + x + 1 \pmod{2}$  כמו ג.

ה.  $f(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$ ,  $f(x+1) = x^4 + 8x^3 + 24x^2 + 30x + 14$ . כעת לפי איזנשטיין הוא אי-פריק, כי 2 מקיים את תנאי המשפט.

2. יהי  $F$  שדה. הראו שאם  $a_n x^n + \dots + a_1 x + a_0$  אי-פריק ב  $F[x]$  אז

$$a_n + a_{n-1}x + \dots + a_1 x^{n-1} + a_0 x^n \text{ אי פריק ב } F[x]$$

פתרון: נשים לב שייתכן ש  $a_0 = 0$  ואז הדרגה יורדת כשאנחנו עוברים מהפולינום הראשון לשני,

אבל מקרה זה בלתי אפשרי כאשר  $f$  אי-פריק, כי אם  $a_0 = 0$  אז  $x \mid f$ .

$$\text{נסמן } f(x) = a_n x^n + \dots + a_1 x + a_0 \quad g(x) = a_n + a_{n-1}x + \dots + a_1 x^{n-1} + a_0 x^n$$

ניתן להניח תחילה ש  $\deg f = \deg g$ , כי אחרת  $a_0 = 0$  ואז  $f$  פריק ואין מה להוכיח. בנוסף גם

ניתן להניח  $a_n \neq 0$ , אחרת היינו מתחילים מלכתחילה עם  $n$  קטן יותר.

נניח ש  $g$  פריק, ונוכיח ש  $f$  פריק.

מתקיים  $g(x) = u(x)v(x)$  כאשר  $v(x) = c_0 + c_1 x + \dots + c_{n-k} x^{n-k}$ ,  $u(x) = b_0 + b_1 x + \dots + b_k x^k$ ,

$$1 \leq k \leq n-1$$

אם כך בהכרח מתקיים  $b_0c_0 = a_n, b_0c_1 + b_1c_0 = a_{n-1}, \dots$  או בצורה כללית  $a_t = \sum_{i+j=n-t} b_i c_j$ .

נגדיר כעת  $\tilde{u}(x) = b_0x^k + \dots + b_k, \tilde{v}(x) = c_0x^{n-k} + \dots + c_{n-k}$  נעיר כאן שבהכרח  $b_0 \neq 0, c_0 \neq 0$

$$\tilde{u}(x)\tilde{v}(x) = \sum_{t=0}^n \left( \sum_{i+j=t} b_{k-i} c_{n-k-j} \right) x^t = \sum_{t=0}^n \left( \sum_{i+j=n-t} b_i c_j \right) x^t = \sum_{t=0}^n a_t x^t$$

כי אחרת  $a_n = 0$ . כעת  $\tilde{u}(x)\tilde{v}(x) = \sum_{t=0}^n a_t x^t$ , כלומר  $f$  פריק כנדרש.

3. יהי  $c \in F$  איבר בשדה. הראו ש  $p(x) \in F[x]$  אי-פריק אם ורק אם  $p(x+c) \in F[x]$  אי-פריק.

פתרון: אם  $p(x) = g(x)h(x)$  פירוק אמיתי, אזי  $p(x+c) = g(x+c)h(x+c)$ , כעת נשאר להראות שהפירוק עדיין אמיתי. אם  $g(x+c)$  הפיך אזי הוא קבוע שונה מאפס, אבל אז גם  $g(x)$  קבוע, סתירה (ניתן להוכיח באינדוקציה על דרגת הפולינום ש  $g(x)$  ו  $g(x+c)$  הם בעלי אותה דרגה).

בכיוון השני, אם  $p(x+c) = g(x)h(x)$

פירוק אמיתי אזי  $p(x) = g(x-c)h(x-c)$  הוא פירוק אמיתי, וסיימנו.

דרך שניה: נגדיר  $\varphi_c : F[x] \rightarrow F[x]$  הומומורפיזם חוגים ע"י  $\varphi_c(f) = g$  כאשר

$$g(x) = f(x+c)$$

בנוסף האיזומורפיזם שומר על דרגות הפולינומים, ולכן כפוליות ההומומורפיזם נותנת לנו פריקות אם ורק אם פריקות.

4. מצאו את ה gcd של  $f(x) = x^3 - 2x^2 + 1, g(x) = x^2 - x - 3$  מעל  $\mathbb{Q}[x]$  והציגו אותו כצירוף

לינארי של  $f(x), g(x)$ . נשתמש באלגוריתם החלוקה של אוקלידס:

$$\begin{aligned} x^3 - 2x^2 + 1 &= (x^2 - x - 3) \cdot (x - 1) + (2x - 2) \\ x^2 - x - 3 &= (2x - 2) \cdot \frac{1}{2}x + -3 \\ 2x - 2 &= -3 \cdot \left(-\frac{2}{3}x + \frac{2}{3}\right) + 0 \end{aligned}$$

המחלק המשותף המקסימלי הוא הפולינום המתוקן שיוצר את האידיאל שנוצר מהשארית הראשונה שאינה 0, כלומר  $\langle -3 \rangle = \langle 1 \rangle$ , ולכן הפולינומים זרים.

5. הראו שלכל  $f(x) \in \mathbb{F}_p[x]$  מתקיים  $(f(x))^p = f(x^p)$  (רמז: משפט פרמה  $(a^p \equiv a \pmod{p})$ ).

נראה באינדוקציה על הדרגה של  $f$ . נסמן  $n = \deg f$ . אם  $n = 0$  אזי  $f(x) = a \in \mathbb{F}_p$  ואז לפי

$$\text{משפט פרמה } f(x) = a \implies f(x)^p = a^p = f(x^p)$$

אזי  $f(x) = a_n x^n + \dots + a_1 x + a_0$   $f(x^p) = a_n x^{pn} + \dots + a_1 x^p + a_0$  ניתן להשתמש במשפט פרמה

עבור כל אחד מהמקדמים ולקבל

$$f(x^p) = a_n^p x^{pn} + \dots + a_1^p x^p + a_0^p = (a_n x^n)^p + \dots + (a_1 x)^p + a_0^p$$

מצד שני,  $f(x)^p = (a_n x^n + g(x))^p = \sum_{i=0}^p \binom{p}{i} (a_n x^n)^i g(x)^{p-i}$ , כאשר

$g(x) = a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ . כיוון ש  $1 \leq i \leq p-1$ ,  $p \mid \binom{p}{i}$ , נקבל שכל הגורמים מתאפסים

פרט לראשון ולאחרון, ולכן  $f(x)^p = (a_n x^n)^p + g(x)^p = (a_n x^n)^p + g(x^p)$  כאשר השיויון האחרון

הוא לפי הנחת האינדוקציה. כעת ניתן לראות (כמו עבור  $f$ ) שמתקיים

$$g(x^p) = (a_{n-1} x^{n-1})^p + \dots + (a_1 x)^p + a_0^p.$$

שאלת בונוס: הראו שהפולינום  $f(x) = x^n + 5x^{n-1} + 3$  אי-פריק ב  $\mathbb{Q}[x]$  לכל  $n > 1$ .

פתרון: תחילה ניתן לבדוק בדרך הרגילה (ראה 1.ב) שאין ל  $f$  שורשים מעל  $\mathbb{Q}$ .

אם מבצעים רדוקציה מודולו 3 של הפולינום, אז נקבל  $x^n + 2x^{n-1} = x^{n-1}(x+2)$ . אם הפולינום  $f(x)$  מתפרק

אזי  $f(x) = g(x)h(x)$  וכאשר נבצע רדוקציה מודולו 3 נקבל  $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$  כאשר סימון הגג מסמן פולינום

לאחר רדוקציה מודולו 3. ניתן לדאוג לכך שהפולינומים  $g, h$  מתוקנים, ושדרגותיהם זהות לאלה של  $\bar{g}, \bar{h}$ . נקבל

שבהכרח (אולי עם החלפת זהות  $(g, h)$ )  $\bar{g}(x) = x^k, \bar{h}(x) = x^{n-k}(x+2)$  עבור  $1 \leq k \leq n-2$  לא לינארי

אחרת יש לנו שורש, ולכן גם  $\bar{h}$  אינו לינארי). אם כך כל המקדמים של  $g$  פרט למקדם של  $x^k$  מתחלקים ב 3.

אם כך בהכרח המקדם החופשי של  $h(x)$  הוא  $\pm 1$  והמקדם החפשי של  $g(x)$  הוא  $\pm 3$  (כי המקדם החפשי של

מכפלת פולינומים הוא המכפלה של המקדמים החפשיים). אבל אם כך המקדם החפשי של  $\bar{h}$  שונה מאפס, וזאת

סתירה.