

# תרגול השלמה – חוגי פולינומים מעל תחומי שלמות

## אי פריקות של פולינומים

**משפט 1.** יהי  $F$  שדה, ויהי  $f(x) \in F[x]$  פולינום ממעלה  $n \geq 1$ . אז ל- $f$  יש לכל היותר  $n$  שורשים שונים ב- $F$ .

**הערה 2.** המשפט לעיל אינו נכון כאשר  $F$  אינו שדה. למשל לפולינום  $x^2 + x$  יש ארבעה פתרונות בחוג  $\mathbb{Z}/6\mathbb{Z}$ , ולפולינום  $x^2$  יש אינסוף שורשים בחוג  $M_2(\mathbb{R})$ .

**משפט 3.** יהי  $R$  חוג חילופי, ויהיו  $c \in R$  ו- $f(x) \in R[x]$ . אז  $f(c) = 0$  אם ורק אם  $(x - c) | f(x)$  ב- $R[x]$ .

**משפט 4.** יהי  $F$  שדה, ויהי  $f(x) \in F[x]$  פולינום ממעלה 2 או 3. אז  $f(x)$  אי פריק אם ורק אם אין לו שורשים ב- $F$ .

**דוגמה 5.** הפולינום  $x^3 + x^2 + 2$  אי פריק ב- $\mathbb{F}_3[x]$  כי אין לו שורשים בשדה  $\mathbb{F}_3$ .

**הערה 6.** המשפט לעיל אינו נכון לפולינומים ממעלות גבוהות יותר. למשל הפולינום  $(x^2 + 1)^2$  פריק ב- $\mathbb{R}[x]$ , אבל אין לו שורשים ב- $\mathbb{R}$ .

**תרגיל 7.** יהי פולינום

$$f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

ונניח שישנו שבר מצומצם  $\frac{c}{d} \in \mathbb{Q}$  שהוא שורש של  $f$ . הוכיחו ש- $d | a_n$  ו- $c | a_0$ .

פתרון. נציב את השורש  $\frac{c}{d}$  ונכפיל ב- $d^n$ :

$$f\left(\frac{c}{d}\right) = a_n \left(\frac{c}{d}\right)^n + \dots + a_1 \left(\frac{c}{d}\right) + a_0$$

$$0 = a_n c^n + \dots + a_1 c d^{n-1} + a_0 d^n$$

$$-a_0 d^n = a_n c^n + \dots + a_1 c d^{n-1} = c (a_n c^{n-1} + \dots + a_1 d^{n-1})$$

ולכן  $c | a_0 d^n$ . הנחנו שהשבר  $\frac{c}{d}$  הוא מצומצם, כלומר  $(c, d) = 1$ . לכן  $c | a_0$ , כדרוש. באופן דומה מוכיחים  $d | a_n$ . נעיר שהתרגיל תקף עבור כל תחום פריקות יחידה  $R$  במקום  $\mathbb{Z}$ , ושדה השברים של  $R$  במקום  $\mathbb{Q}$ .

**תרגיל 8.** יהי  $p$  מספר ראשוני. הראו שלכל  $n > 1$  טבעי המספר  $\sqrt[n]{p}$  הוא אי רציונלי.

פתרו. נתבונן בפולינום  $f(x) = x^n - p$ . ברור כי  $\sqrt[n]{p}$  הוא שורש של  $f$ . אם  $\frac{c}{d} \in \mathbb{Q}$  שורש של  $f$ , אז  $c \in \{\pm 1, \pm p\}$  ו- $d \in \{\pm 1\}$  לפי תרגיל 7. אבל לכל  $n > 1$  מתקיים

$$f\left(\frac{c}{d}\right) = (\pm p)^n - p \neq 0$$

ולכן אין שורש רציונלי ל- $f$ .

לשאר התרגול נניח כי  $R$  הוא תחום פריקות יחידה, ו- $F$  הוא שדה השברים שלו, אלא אם נאמר אחרת.

האינטואיציה הראשונית היא לחשוב שבשדה השברים יותר דברים מתפרקים, בדומה לכך ש- $x^2 + 1$  אי פריק מעל  $\mathbb{R}$  אבל פריק מעל  $\mathbb{C}$ . מסתבר שזה לא ממש כך:

**דוגמה 9.** הפולינום  $2x + 2$  פריק מעל  $\mathbb{Z}$ :  $2x + 2 = 2(x + 1)$  וזה פירוק אמיתי. אבל מעל  $\mathbb{Q}$  הפירוק הזה לא אמיתי (כי 2 הפיך) והפולינום אי פריק. אבל הפירוק הזה מעל  $\mathbb{Z}$ , הוא לא באמת "הוגן" ולכן אנחנו קוראים לפירוק של פולינום כשאחד הגורמים הוא סקלר **פירוק לא אמיתי**. פירוק אמיתי של פולינומים הוא פירוק לפולינומים מדרגות נמוכות יותר.

Content

**הגדרה 10.** יהי  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$  פולינום. **התכולה** של  $f$  היא המחלק המשותף המירבי של המקדמים  $a_0, a_1, \dots, a_n$  ומסמנים אותה ב- $c(f)$ .

Primitive

**הגדרה 11.** פולינום  $f \in R[x]$  יקרא **פרימיטיבי** אם מקדמיו זרים, כלומר  $c(f) = 1$ .

**דוגמה 12.** כל פולינום מתוקן הוא פרימיטיבי. הפולינום  $6x^2 + 10x + 15 \in \mathbb{Z}[x]$  גם הוא פרימיטיבי, למרות שכל זוג מקדמים שלו אינו זר.

Eisenstein's criterion

**משפט 13** (קריטריון אייזנשטיין). יהי  $R$  תחום פריקות יחידה, ויהי  $P \triangleleft R$  אידיאל ראשוני. יהי  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$  פולינום המקיים

$$\bullet a_i \in P \text{ לכל } i \neq n$$

$$\bullet a_n \notin P$$

$$\bullet a_0 \notin P^2$$

אז  $f$  אי פריק ב- $F[x]$  (אין לו פירוק אמיתי מעל  $R$ ). אם  $f$  פרימיטיבי ב- $R$ , אז  $f$  אי פריק ב- $R[x]$ .

במקרה הפרטי שבו  $P = \langle p \rangle$  עבור איבר ראשוני  $p$  התנאים לעיל שקולים לכך ש- $p$  לא מחלק את  $a_n$ , מחלק את  $a_i$  עבור  $i \neq n$  ו- $p^2$  לא מחלק את  $a_0$ .

הוכחה. נניח בשלילה כי  $f = g \cdot h$  פירוק אמיתי. נסמן

$$g(x) = c_k x^k + \dots + c_1 x + c_0, \quad h(x) = b_{n-k} x^{n-k} + \dots + b_1 x + b_0$$

עבור  $0 < k < n$ . יהי  $b_i$  המקדם עם אינדקס מינימלי ב- $h$  שלא שייך ל- $P$  ויהי  $c_j$  המקדם עם אינדקס מינימלי ב- $g$  שלא שייך ל- $P$ . נתבונן בפירוק הפולינומים מעל תחום השלמות  $R/P$ , ונקבל  $b_i c_j \equiv a_{i+j} \pmod{P}$ . מפני ש- $P$  ראשוני, אז  $b_i c_j \notin P$ , ולכן  $a_{i+j} \notin P$ . זה יתכן רק כאשר  $i+j = n$ , ולכן  $i = n-k$  ו- $j = k$ . בפרט,  $b_0, c_0 \in P$ , ולכן  $a_0 = b_0 c_0 \in P^2$ . שזו סתירה. לכן אין פירוק אמיתי.  $\square$

**דוגמה 14.** הפולינום  $f(x) = 22x^5 + 27x + 15$  הוא אי פריק מעל  $\mathbb{Z}$  כי הוא מקיים את קריטריון אייזנשטיין עבור  $p = 3$ . כלומר 3 לא מחלק את 22, מחלק את 27 ואת 15, אבל  $3^2$  לא מחלק את 15.

**דוגמה 15.** הפולינום  $f(x) = x^6 - 30x + 15$  הוא אי פריק מעל  $\mathbb{Z}[i]$  כי הוא מקיים את קריטריון אייזנשטיין עבור  $P = \langle 3 \rangle$ , וראיתם בתרגיל בית כי 3 ראשוני ב- $\mathbb{Z}[i]$ .

**תרגיל 16.** הוכיחו כי הפולינום  $f(x, y) = y^2 + x^2 y + 2y + x^4 + 5x^2 + 6$  הוא אי פריק ב- $\mathbb{Z}[x, y]$ .

פתרו. נסמן  $S = \mathbb{Z}[x]$ , ונחשוב על  $f(x, y)$  כאיבר בחוג  $S[y] = \mathbb{Z}[x, y]$ . כלומר

$$f(x, y) = y^2 + (x^2 + 2)y + (x^2 + 2)(x^2 + 3)$$

נזכר ש- $S$  הוא תחום פריקות יחידה, ונשים לב שהאיבר  $p(x) = x^2 + 2$  הוא ראשוני ב- $S$  (למשל לפי קריטריון אייזנשטיין עבור 2). כעת ניתן להשתמש בקריטריון אייזנשטיין לגבי האידיאל  $\langle p \rangle$  ב- $S[y]$  כדי להוכיח ש- $f$  אי פריק.

**תרגיל 17.** הוכיחו האם  $f(x) = x^2 - 3$  אי פריק ב- $\mathbb{Z}[\sqrt{-2}][x]$ .

פתרו. בחוג  $S = \mathbb{Z}[\sqrt{-2}]$  אי אפשר להשתמש בקריטריון אייזנשטיין עם  $P = \langle 3 \rangle$  כי  $1 + \sqrt{-2} \in S$  אבל  $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ , כלומר 3 פריק, ולכן אינו ראשוני.  $N(1 + \sqrt{-2}) = 1^2 + 2 \cdot 1^2 = 3$ , מפני שהנורמה שלו היא ראשונית, כלומר בנוסף,  $S$  אוקלידי, ובתחום אוקלידי מתקיים שכל איבר אי פריק הוא ראשוני. כלומר ניתן להשתמש בקריטריון אייזנשטיין עם  $P = \langle 1 + \sqrt{-2} \rangle$ , ולהוכיח ש- $f$  אי פריק ב- $\mathbb{Z}[\sqrt{-2}][x]$ .

**הערה 18.** קריטריון אייזנשטיין נותן תנאי מספיק, אך לא הכרחי לאי פריקות של פולינומים. לדוגמה  $x^2 + 4$  או  $x^2 + 1$  אי פריקים מעל  $\mathbb{Q}$ , למרות שאינם מקיימים את הקריטריון. לעומת זאת  $x^4 + 4$  פריק ב- $\mathbb{Q}$ , שכן

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

**טענה 19.** יהיו  $a, b \in F$ , ונניח  $a \neq 0$ . אז  $f(x) \in F[x]$  אי פריק אם ורק אם  $f(ax+b)$  אי פריק.

**דוגמה 20.** כדי להוכיח ש- $f(x) = 8x^3 + 6x^2 + 1$  אי פריק מעל  $\mathbb{Q}$  נציב  $x \mapsto x + 1$  ונקבל

$$f(x+1) = 8x^3 + 30x^2 + 36x + 15$$

שמקיים את קריטריון אייזנשטיין עבור  $p = 3$ . לכן  $f(x+1)$  אי פריק, ולכן  $f(x)$  אי פריק מעל  $\mathbb{Q}$ .

**דוגמה 21.** כדי להוכיח ש- $f(x) = x^4 + 4x^3 + 6x^2 + 2x + 1$  אי פריק מעל  $\mathbb{Q}$  נציב  $x \mapsto x - 1$  ונקבל

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

שמקיים את קריטריון אייזנשטיין עבור  $p = 2$ . לכן  $f(x-1)$  אי פריק, ולכן  $f(x)$  אי פריק מעל  $\mathbb{Q}$ .

**תרגיל 22.** הוכיחו כי  $x^n - y \in F[[y]][x]$  הוא אי פריק.

פתרון. נרצה להשתמש בקריטריון אייזנשטיין עבור  $y \in F[[y]]$ . לשם כך נראה כי  $y$  ראשוני שם.

תחילה נוכיח שהוא אי פריק. נניח שיש פירוק  $y = \alpha(y) \cdot \beta(y) = (\sum a_n y^n) (\sum b_m y^m)$  נשווה מקדמים ונקבל

$$a_0 b_0 = 0, \quad a_0 b_1 + a_1 b_0 = 1$$

בלי הגבלת הכלליות קיבלנו  $b_0 = 0$ , ואז מהמשוואה השנייה נקבל  $a_0 b_1 = 1$ . לכן  $a_0 \neq 0$ , ולכן  $\alpha(y)$  הפיך ב- $F[[y]]$ . כלומר  $y$  הוא אי פריק. הוכחנו ש- $F[[y]]$  הוא אוקלידי ולכן  $y$  גם ראשוני. כל מה שנשאר הוא לשים לב ש- $x^n - y$  מקיים את קריטריון אייזנשטיין עבור  $P = \langle y \rangle$  ולכן הוא אי פריק.

**משפט 23** (אחת הגרסאות של הלמה של גאוס). יהי  $f(x) \in R[x]$  פרימיטיבי. אז  $f(x)$  אי פריק מעל  $R$  אם ורק אם  $f$  אי פריק מעל  $F$ .

**מסקנה 24.** תחת אותם תנאים, נניח  $g(x) \in R[x]$ . אז  $g|f$  ב- $R[x]$  אם ורק אם  $g|f$  ב- $F[x]$ .

כלומר בעיות פירוק וחלוקה של פולינומים מעל  $\mathbb{Q}$  "שקולות" לבעיות פירוק וחלוקה של פולינומים מעל  $\mathbb{Z}$ .

**תרגיל 25.** הוכיחו כי החוג הבא הוא שדה:

$$T = \mathbb{Q}[i](x)[y] / \langle y^9 - x^5 + 10 \rangle$$

פתרון. נסמן  $F = \mathbb{Q}[i](x)$  שהוא שדה. זהו חוג השברים של  $R = \mathbb{Z}[i][x]$  (ודאו שאתם יודעים למה). נשים לב ש- $F[y]$  הוא תחום אוקלידי, ולכן כדי להוכיח ש- $T$  הוא שדה, מספיק להראות שהפולינום  $f(y) = y^9 + (-x^5 + 10)$  במשתנה  $y$  הוא אי פריק ב- $F[y]$ . הרי כל אי פריק הוא ראשוני בתחום ראשי, ואידאל ראשוני הוא מקסימלי שם. לפי הלמה של גאוס, מספיק להראות ש- $f(y)$  אי פריק ב- $R[y]$ , כי  $f(y)$  פרימיטיבי. נראה שהוא אי פריק בעזרת קריטריון אייזנשטיין. נרצה להראות ש- $-x^5 + 10$  הוא ראשוני ב- $R$ . מפני ש- $R$  תחום פריקות יחידה, מספיק להוכיח שהוא אי פריק. אז שוב נשתמש בקריטריון אייזנשטיין עם  $1 + i$  שידוע לנו שהוא ראשוני ב- $\mathbb{Z}[i]$  (וששאר הדרישות מתקיימות). שימו לב ש-2 ו-5 אינם ראשוניים ב- $\mathbb{Z}[i]$ , ולכן לא יכולנו להשתמש בהם.

קיבלנו ש- $-x^5 + 10$  אי פריק ב- $R$ , לכן ראשוני שם, לכן  $f(y)$  אי פריק ב- $R[y]$ , לכן אי פריק ב- $F[y]$ , לכן  $\langle f(y) \rangle$  מקסימלי ב- $F[y]$ , ולכן  $T$  שדה. שימו לב שהשימוש בלמה של גאוס היה קריטי, כי אחרת לא יכולנו להשתמש בקריטריון אייזנשטיין.

**תרגיל 26.** יהי  $f(x, y, z) = x^2 + y^2 + z^2 \in F[x, y, z]$ . נניח  $\text{char } F \neq 2$ . הוכיחו כי  $f$  אי פריק.

פתרון. נעיר שאם  $\text{char } F = 2$ , אז  $f$  פריק מפני ש- $f(x, y, z) = (x + y + z)^2$ . נסמן  $S = F[y, z]$ , ואז  $F[x, y, z] = S[x]$ . מעל  $S$  הפולינום  $f$  הוא פולינום מתוקן ממעלה 2 עם מקדם חופשי  $y^2 + z^2$ . נרצה להראות שקיים  $p \in S$  ראשוני כך ש- $p$  מחלק את  $y^2 + z^2$ , אבל  $p^2$  לא מחלק אותו.

החוג  $S$  הוא תחום פריקות יחידה, ולכן כל איבר מתפרק למכפלת ראשוניים. יהי  $p \in S$  איבר ראשוני עם חזקה לא טריוויאלית של  $z$  המחלק את  $y^2 + z^2$ . נסמן  $T = F[y]$ , וב- $k$  את שדה השברים שלו (כלומר  $k = F(y)$ ). נשים לב כי  $S = T[z]$ . מכיוון ש- $y^2 + z^2$  פולינום מתוקן ב- $T[z]$ , אז לכל פולינום  $g(z) \in T[z]$ , לפי המסקנה  $g|f$  ב- $T[z]$  אם ורק אם  $g|f$  ב- $k[z]$ .

נניח בשלילה כי  $p^2$  מחלק את  $y^2 + z^2$  ב- $k[z]$ . אז  $y^2 + z^2 = p^2 \cdot h(z)$  ואז  $\frac{\partial(y^2+z^2)}{\partial z} = 2z$ . לכן כל צירוף לינארי (עם מקדמים מ- $k[z]$ ) של  $y^2 + z^2$  ו- $\frac{\partial(y^2+z^2)}{\partial z}$  מתחלקת ב- $p$ . אבל

$$\frac{1}{y^2}(y^2 + z^2) - \frac{z}{2y^2} \cdot \frac{\partial(y^2 + z^2)}{\partial z} = 1$$

(כאן אנחנו משתמשים בכך שהמאפיין שונה מ-2), וזו סתירה. כלומר  $p^2$  לא מחלק את  $y^2 + z^2$  ב- $k[z]$ , ולכן הוא לא מחלק את  $y^2 + z^2$  ב- $T[z]$ . כלומר קיים ראשוני  $p \in S$  המחלק את  $y^2 + z^2$ , אבל  $p^2$  לא מחלק אותו. לכן מתקיים קריטריון אייזנשטיין, ולכן  $f$  אי פריק ב- $F[x, y, z] = S[x]$ .