

**שאלה 1:**

קבעו האם הפולינומים הבאים הם אי פריקים בחוג הנתון, ואם הם פריקים מצאו את פירוק שלהם לגורמים אי פריקים.

1.

$$x^2 + x + 1 \in F_2[x]$$

נוכל לבדוק את כל האפשרויות לפולינומים ולראות שהוא אינו פריק. פירוק לפולינום מסדר שני וסקלר הוא לא נחשב כי סקלר הפיך, לכן נשאר רק לבדוק מכפלות של פולינומים מסדר 1:

$$x \cdot x = x^2$$

$$x \cdot (x + 1) = x^2 + x$$

$$(x + 1) \cdot (x + 1) = x^2 + 2x + 1 = x^2 + 1$$

כלומר אין 2 פולינומים שמכפלתם הפולינום הנ"ל ולכן הוא אינו פריק.

2.

$$x^6 - 4x^4 + 6x^2 \in \mathbb{Z}[x]$$

ניתן להוציא גורם משותף:

$$x \cdot x \cdot (x^4 - 4x^2 + 6)$$

נראה כי פולינום שנשאר אינו פריק לפי קריטריון אייזשטיין:  
נבחר את:

$$P = \langle 2 \rangle$$

ידוע כי 2 הוא מספר ראשוני ב- $\mathbb{Z}$ .  
ועבורו מתקיים:

$$a_4 = 1 \notin P$$

$$a_2 = -4 \in P$$

$$a_0 = 6 \in P$$

$$a_0 = 6 \notin P^2 = \langle 4 \rangle$$

וכן זה פולינום פרימיטיבי כי  $a_4 = 1$ . כל הדרישות מתקיימות ולכן זה פולינום אי-פריק.

לכן בסהכ הפירוק הוא:

$$x^6 - 4x^4 + 6x^2 = x \cdot x \cdot (x^4 - 4x^2 + 6)$$

3.

$$2ix^5 + 71 \in \mathbb{Z}[i][x]$$

נפעיל על פולינום זה את קריטריון אייזשטיין:  
נבחר את:

$$P = \langle 71 \rangle$$

צריך להוכיח ש- $P$  הוא ראשוני. נוכיח זאת בכך שנראה שהוא לא פריק ובגלל ש- $\mathbb{Z}[i]$  הוא תחום ראשי זה שקול.

ברור כי 71 הוא אינו תוצאה של אף קומבינציה מהצורה  $(a + bi)(a - bi) = a^2 + b^2$  מפני שהנורמה של כל איבר במכפלה גדולה מ-1 וגם הם מחלקים 71 שהוא מספר ראשוני(הפירוק מהצורה הזו הוא הפירוק היחיד כי חייבים לקבל מספר ממשי).

$$a_5 = 2i \notin P$$

$$a_0 = 71 \in P$$

$$a_0 = 71 \notin P^2 = \langle 71^2 \rangle$$

ולכן הפולינום אינו פריק.

4.

$x^n + y^m - 1 \in \mathbb{Q}[x, y]$   
 נסתכל על הפולינום כפולינום (במשתנה  $y$ ) מעל החוג הפולינומיים (במשתנה  $x$ )  
 ולכן:

$$a_m = 1$$

$$a_0 = x^n - 1$$

נבחר את:

$$P = \langle x - 1 \rangle$$

הוא ראשוני ומתקיים:

$$a_m = 1 \notin P$$

$$a_0 = x^n - 1 = (x - 1) \cdot f(x) \in P$$

זה נכון כי  $x = 1$  הוא תמיד פתרון למשוואה:  $x^n = 1$ . נשים לב כי זה הוא שורש למשוואה מסדר ראשון ולכן גם מתקיים:

$$a_0 = x^n - 1 \notin P^2 = \langle (x - 1)^2 \rangle$$

ולכן פולינום זה מקיים את קריטריון אייזנשטיין ועבור כל  $n, m$  הוא אי-פריק.

## שאלה 2:

יהי  $f(x) = x^4 - 5x^2 + 6$ . פרקו את  $f(x)$  לגורמים ראשוניים מעל החוגים הבאים:

א.  $\mathbb{Q}$

נראה כי ניתן לפרק את הפולינום לצורה הבאה:

$$x^4 - 5x^2 + 6 = (x^2 - 2)(x^2 - 3)$$

נראה כי כל אחד מהם הוא אי-פריק לפי טענה מהתרגול:  
 הפולינום מסדר 2-3 הוא אי פריק מעל שדה אם אין לו שורשים בשדה.  
 אנחנו יודעים את השורשים של המשוואה הזאת והם:

$$x = \pm\sqrt{2}, \pm\sqrt{3}$$

אשר אינם נמצאים בשדה.

ב.  $\mathbb{Q}[\sqrt{2}]$

נראה כי ניתן לפרק את הפולינום לצורה הבאה:

$$x^4 - 5x^2 + 6 = (x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$$

נראה שכל פולינומים אלו הם אי-פריקים. שתיים המשמאל הם מסדר 1 ולכן אי-פריקים. הימני הוא אי-פריק מאותה טענה כמו בסעיף הקודם.

ג.  $\mathbb{R}$

אנחנו יודעים לפרק את הפולינום בצורה יחידה עם פולינומים מסדר 1:

$$x^4 - 5x^2 + 6 = (x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

ד.  $\mathbb{Z}/5\mathbb{Z}$

נראה כי ניתן לפרק את הפולינום באופן הבא:

$$x^4 + 5x^2 + 6 = x^4 + 1 = x^4 - 4 = (x^2 + 2)(x^2 - 2)$$

ונראה כי לא ניתן לפרק את הפולינום זה יותר כי צריך להתקיים:

$$x^2 + 2 = (x + a)(x - a) = x^2 + a^2 = \begin{cases} x^2 + 1 \\ x^2 + 4 \\ x^2 + 9 = x^2 + 4 \\ x^2 + 16 = x^2 + 1 \end{cases} \neq x^2 + 2$$

וכנל עבור  $x^2 - 2 = x^2 + 3$  שגם אותו לא נוכל ליצור.

### שאלה 3:

נתון  $f(x) = \frac{x^p - 1}{x - 1}$ . צ"ל שהוא אי-פריק מעל  $\mathbb{Q}[x]$ .

הפולינום הוא אי-פריק אם"ם ההזזה שלו אי-פריקה. נזיז את הפולינום הזה ב-1:

$$f(x + 1) = \frac{(x + 1)^p - 1}{x + 1 - 1} = [newton\ binom] = \frac{\sum_{k=0}^p \binom{p}{k} x^k - 1}{x} = \frac{\sum_{k=1}^p \binom{p}{k} x^k}{x} = \sum_{k=1}^p \binom{p}{k} x^{k-1}$$

נוכיח כי הוא אי-פריק לפי קריטריון אייזנשטיין עם:

$$P = \langle p \rangle$$

מתקיים:

$$\forall i \neq n, \exists b \in \mathbb{N}: a_i = \frac{p!}{i!(p-i)!} \in P$$

$$a_n = 1 \notin P$$

$$a_0 = p \notin P^2 = \langle p^2 \rangle$$

לכן לפי אייזנשטיין הפולינום הזה הוא אי פריק. בגלל שהפולינום ההזזה הוא אי-פריק גם  $f(x) = \frac{x^p - 1}{x - 1}$  הוא אי-פריק.

### שאלה 4:

נתון הפולינום:  $f(x) = x^2 + 4 \in \mathbb{Z}[x]$ . ידוע כי הוא אי-פריק, נראה ש:

$$\forall a, b \in \mathbb{Z} (a \neq 0): f(ax + b)$$

אינו מקיים את קריטריון אייזנשטיין.

הפולינום שלנו הוא:

$$f(ax + b) = a^2x^2 + 2abx + b^2 + 4$$

נניח בשלילה כי הוא מקיים את קריטריון אייזנשטיין ויהיה  $P$  ראשוני מתאים לקריטריון. ידוע ש- $\mathbb{Z}$  הוא ראשי ולכן נסמן את האיבר היוצר ב- $P = \langle p \rangle$ .

מהתנאים אנחנו יודעים כי מתקיים:

$$\begin{cases} p|b^2 + 4 \\ p^2 \nmid b^2 + 4 \\ p|2ab \\ p \nmid a^2 \end{cases}$$

מהתנאי השלישי וכי  $p$  הוא ראשוני, נקבל כי:

$$p|a \vee p|b \vee p|2$$

נבדוק על מקרה בנפרד ונגיע לסתירות:

נניח כי  $p|2$ :

חייב להתקיים:  $p = 2$ , לכן מתקיים:

$$\begin{cases} 2|b^2 + 4 \\ 4 \nmid b^2 + 4 \end{cases} \Leftrightarrow \begin{cases} 2|b^2 \\ 4 \nmid b^2 \end{cases}$$

בסתירה! אם 2 מחלק את  $b^2$  כך ש- $b$  מספר שלם, חייב להתקיים:  $4|b^2$ .

נניח כי  $p|a$ :

אבל ידוע כי:  $p \nmid a^2$ . בסתירה!

נניח כי  $p|b$ :

נקבל:

$$\begin{cases} p|b^2 + 4 \\ p|b \end{cases} \Rightarrow p|4 \Rightarrow p = 2 \vee p = 4$$

ראינו כי  $p = 2$  נותן סתירה וגם  $p = 4$  הוא לא ראשוני! בסתירה.

בכל מקרה קיבלנו סתירה ולכן קריטריון אייזנשטיין לא תקף עבור פולינום זה עם זאת שידוע שהוא אי-פריק.

## שאלה 5:

א.

$\Rightarrow$

נוכיח את הגרירה ההפוכה, שאם הפולינום פריק ב- $R[x]$  אז קיים לו פירוק גם ב- $R[x, x^{-1}]$ , שזה ברור כי ניתן לקחת את אותו פירוק. לכאורה סיימנו, אבל לא סיימנו מפני שנשאר להוכיח שהפירוק ב- $R[x, x^{-1}]$  הוא פירוק של שני איברים לא הפיכים, שזה לא נכון לפי הדוגמה הנגדית הפשוטה  $x(x+1)$  שהוא פריק ב- $R[x]$  אבל הוא אי פריק ב- $R[x, x^{-1}]$  מפני שהוא בעצם שקול ל- $x+1$  שהוא אי פריק. אם נדרוש ש  $a_0 \neq 0$  נקבל שהפתרון נכון מפני שכל האיברים ההפיכים ב- $R[x, x^{-1}]$  הם  $x^m$  וכאשר  $a_0 \neq 0$  אז  $x^m$  לא ישתתף בפירוק של הפולינום ב- $R[x]$ .

$\Leftarrow$

נוכיח את הגרירה ההפוכה, שאם הפולינום פריק ב- $R[x, x^{-1}]$  אז קיים לו פירוק גם ב- $R[x]$ .

אם הפולינום פריק ב- $R[x, x^{-1}]$  אז או יש לו פירוק לשני פולינומים לא הפיכים

$$f(x) = (b_{n_1}x^{n_1} + \dots + b_{m_1}x^{m_1})(c_{n_2}x^{n_2} + \dots + c_{m_2}x^{m_2})$$

כאשר  $n$  הוא המעלה המקסימלית ו- $m$  הוא המעלה המינימלית.

כאשר פותחים את הפירוק מקבלים שהאיבר עם המעלה המינימלית הוא  $b_{m_1}c_{m_2}x^{m_1+m_2}$ . הוא לא אפס מפני ש- $R$  הוא תחום שלמות. בנוסף המעלה שלו גדולה מאפס כי בפולינום המקורי אין איברים עם מעלות שליליות, ולכן קיבלנו:  $m_1 + m_2 \geq 0$ . אם  $m_1, m_2$  שניהם גדולים מאפס, סיימנו כי אז אפשר לקחת את הפירוק הזה בדיוק ל- $\mathbb{R}[x]$ . אם  $m_2$  בה"כ קטן מאפס אז  $m_1 \geq -m_2$ , ולכן אפשר להוציא מהפולינום הראשון  $x^{m_1}$  ולכפול אותו בפולינום השני וכך נקבל:

$$f(x) = (b_{n_1}x^{n_1-m_1} + \dots + b_{m_1}x^0)(c_{n_2}x^{n_2+m_1} + \dots + c_{m_2}x^{m_2+m_1})$$

אבל נשאר לבדוק מה קורה אם מלכך תחילה הפולינום ב- $R[x, x^{-1}]$  הוא הפיך, זה קורה אם

$$ax^m \quad m \in \mathbb{Z}, m \geq 0: \alpha \text{ הפיך, אם } m \neq 1 \text{ אז גם ב- } R[x] \text{ הוא הפיך. אם } m = 1 \text{ נקבל סתירה}$$

למשפט כי  $ax$  הוא הפיך ב- $R[x, x^{-1}]$  אך הוא אי-פריק ב- $R[x]$ . נשים לב שמספיק ש- $a_0 \neq 0$  בשביל שהמשפט יהיה נכון.

**ב.** ידוע שהפולינום  $\tilde{f}$  מקיים את קריטריון אייזנשטיין ולכן הוא אי-פריק. צ"ל ש- $f$  הוא אי-פריק. נניח בשלילה כי  $f$  הוא פריק, לכן קיים לו פירוק:

$$f(x) = a_n x^n + \dots + a_0 = (b_k x^k + \dots + b_0)(c_l x^l + \dots + c_0) \quad | \quad (k + l = n)$$

נתון כי  $a_0 \neq 0$  ולכן אם הוא פריק ב- $R[x]$  הוא פריק גם ב- $R[x, x^{-1}]$ . בחוג זה מתקיים:

$$f(x) = x^n(a_0 x^{-n} + \dots + a_n) \sim a_0 x^{-n} + \dots + a_n$$

$$f(x) = x^k(b_k x^{k-k} + \dots + b_0 x^{-k})x^l(c_l x^{l-l} + \dots + c_0 x^{-l}) \sim (b_k + \dots + b_0 x^{-k})(c_l + \dots + c_0 x^{-l})$$

ומכאן:

$$a_0 x^{-n} + \dots + a_n = (b_k + \dots + b_0 x^{-k})(c_l + \dots + c_0 x^{-l})$$

שזה איבר ב- $R[x^{-1}]$  וניקח איזומורפיזם:  $x \rightarrow x^{-1}$  בין  $R[x^{-1}]$  ל- $R[x]$  ונקבל ש:

$$\tilde{f}(x) = (b_0 x^k + \dots + b_k)(c_0 x^l + \dots + c_l)$$

קיבלנו פירוק עבור פולינום אי-פריק(האיברים לא הפיכים מפני ש- $b_k, c_l$  לא שווים ל-0), בסתירה.

## שאלה 6:

צ"ל כי  $\forall n \in \mathbb{N}$  הפולינום הבא הוא אי-פריק:

$$p_n(x) = (x-1)(x-2) \dots (x-n) - 1$$

פתרון:

נניח בשלילה כי הוא פריק והפירוק שלו הוא:

$$p_n(x) = f_n(x)g_n(x)$$

אנו יודעים כי זה הוא פירוק לא טריוויאלי כי המקדם המוביל הוא אחד ולכן חייב להתקיים:

$$\deg(p) > \deg(f_n), \deg(g_n)$$

נתבונן בפולינום:

$$h_n(x) = f_n(x) + g_n(x)$$

עבורו מתקיים:

$$\deg(h_n) = \max\{\deg(f_n), \deg(g_n)\}$$

נסתכל על ערך הפולינומים בנקודה:  $0 \leq k \leq n, k \in \mathbb{Z}$

$$p_n(k) = (k-1) \dots (k-k) \dots (k-n) - 1 = -1 = f_n(k) \cdot g_n(k)$$

ולכן מתקיים:

$$f_n(k) = 1, g_n(k) = -1 \text{ או } f_n(k) = -1, g_n(k) = 1$$

ובכל מקרה נקבל:

$$h_n(k) = 0$$

קיבלנו שהפולינום  $h_n$  מתאפס  $n$  פעמים ולכן מתקיים:

$$n = \deg(p_n) > \max\{\deg(f_n), \deg(g_n)\} = \deg(h_n) \geq n$$

בסתירה. לכן קיבלנו שהפולינום הוא אי-פריק.

## שאלה 7:

א. נתון האידיאל:

$$I = \langle 21, 9 + 3\sqrt{-5}, -2 + 4\sqrt{-5} \rangle \triangleleft \mathbb{Z}[\sqrt{-5}]$$

צ"ל הוא אידיאל ראשי.

הוכחה: נמצא לו איבר יחיד יוצר ולכן הוא ראשי, נקרא לו  $p$ .  
אנחנו יודעים שהנורמה (לא אוקלידית אך עדיין כפלית) של האיבר היוצר את שלושת האיברים האלו חייבת לחלק כל אחת מהם ולכן:

$$d(21) = 441, d(9 + 3\sqrt{-5}) = 126, d(-2 + 4\sqrt{-5}) = 84 \Rightarrow \gcd = 21$$

ולכן חייב להקיים:

$$d(p) | 21 \Rightarrow [21 \text{ is prime}] \Rightarrow d(p) = 21$$

נראה כי קיימים ארבע איברים עם נורמה מתאימה ונבדוק על כל אחד מהם:

$$d(1 \pm 2\sqrt{-5}, 4 \pm \sqrt{-5}) = 21$$

$4 - \sqrt{-5}$

$$\frac{-2 + 4\sqrt{-5}}{4 - \sqrt{-5}} = \frac{(-2 + 4\sqrt{-5})(4 + \sqrt{-5})}{21} = -\frac{4}{3} + \frac{2}{3}\sqrt{-5}$$

$$:4 + \sqrt{-5}$$

$$\frac{9 + 3\sqrt{-5}}{4 + \sqrt{-5}} = \frac{(9 + 3\sqrt{-5})(4 - \sqrt{-5})}{21} = \frac{13}{7} + \frac{1}{7}\sqrt{-5}$$

$$:1 + 2\sqrt{-5}$$

$$\frac{9 + 3\sqrt{-5}}{1 + 2\sqrt{-5}} = \frac{(9 + 3\sqrt{-5})(1 - 2\sqrt{-5})}{21} = \frac{5}{7} - \frac{5}{7}\sqrt{-5}$$

$$:1 - 2\sqrt{-5}$$

$$\frac{21}{1 - 2\sqrt{-5}} = 1 + 2\sqrt{-5} \Rightarrow (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 21$$

$$\frac{9 + 3\sqrt{-5}}{1 - 2\sqrt{-5}} = -1 + \sqrt{-5} \Rightarrow (-1 + \sqrt{-5})(1 - 2\sqrt{-5}) = 9 + 3\sqrt{-5}$$

$$\frac{-2 + 4\sqrt{-5}}{1 - 2\sqrt{-5}} = -2 \Rightarrow -2(1 - 2\sqrt{-5}) = -2 + 4\sqrt{-5}$$

אנחנו רואים שהמספר  $1 - 2\sqrt{-5}$  יוצר את האידיאל ונראה כי הוא שייך לאידיאל כי:

$$-1(21) + 2(9 + 3\sqrt{-5}) - 2(-2 + 4\sqrt{-5}) = 1 - 2\sqrt{-5}$$

מצאנו את האיבר היוצר את האידיאל ולכן האידיאל הזה הוא ראשי.

ב. נתבונן במנה המתקבלת. האיבר הכללי יהיה מהצורה:

$$\{a, a + \sqrt{-5} | a \in \mathbb{Z}\}$$

כי אם המקדם של שורש מינוס חמש יהיה לא אחד או אפס נוכל לעביר אותו לשקול במנה. נראה כי בחוג המנה הזה שורש מינוס חמש הפיך:

$$2 \cdot \sqrt{-5} = 2\sqrt{-5} \sim 1$$

צריך להוכיח שהאידיאל הוא לא מקסימלי, נראה כי המנה היא לא שדה ובכך סיימנו (כי  $\mathbb{Z}[\sqrt{-5}]$  הוא תחום שלמות).

נראה כי לא קיים הופכי ל-3:

$$3 \cdot (a + \sqrt{-5}) = 3a + 3\sqrt{-5} \sim 3a + 1 + \sqrt{-5}$$

קיבלנו כי תמיד יהיה  $\sqrt{-5}$  עם מקדם אי-זוגי ולכן לא התאפס. לכן, לא קיים איבר שהופכי ל-3 ולכן הוא לא שדה.

ולכן האידיאל לא מקסימלי.

שאלה 8:

קיימת בעיה בתרגיל כי הפולינום:

$$(px + 1)(px + 1) = p^2x^2 + 2px + 1 \sim 1$$

פריק ב-  $\mathbb{Z}[x]$  אך לא פריק ב-  $\mathbb{Z}/p\mathbb{Z}$  כי הוא הפיך.

בתקווה נתקן את התרגיל בהמשך.