

## אלגברה מופשטת 2 – תרגיל כיתה 9

מתרגלים: זר אפי כהן ואדם צ'פמן.

### תזכורת

חוג אוקלידי הוא תחום שלמות  $R$  עם פונקציה  $d: R \rightarrow \mathbb{N} \cup \{-\alpha\}$  כך ש  $d(0) < d(x)$  לכל  $x \in R$  וש:

$$1. d(a) \leq d(ba)$$

2. לכל  $b \neq 0$  ולכל  $a$  יש  $q, r \in R$  כך ש  $a = bq + r$  ו  $d(r) < d(b)$ .

למשל: עם הפונקציה  $d(x) = |x|$ .

### הערה

כל חוג אוקלידי הוא ראשי, ומכיוון שכל חוג ראשי הוא תחום פריקות יחידה, אז כל תחום אוקלידי הוא תחום פריקות יחידה.

$\mathbb{Z}[x]$  ו  $F[x, y]$  אינם חוגים אוקלידים מכיוון שהם אינם חוגים ראשיים למרות שהם כן תחומי פריקות יחידה.

### תרגיל

יהי  $R$  תחום אוקלידי. אז  $a \in R$  הפיך  $\Leftrightarrow d(a) = d(1)$ .

### פתרון

$\Leftarrow$  אם  $x$  הפיך אז קיים  $d(x) \leq d(x \cdot x^{-1}) = d(1)$ , ולכן  $d(x) = d(1)$ .

$\Rightarrow$  אם  $d(x) = d(1)$  אז נרשום  $1 = qx + r$  כש  $d(r) < d(x) = d(1)$  אך זה מתקיים רק כאשר  $r = 0$ , לכן  $1 = qx$  ו  $x$  הפיך.

### תרגיל

מה הם האיברים הראשוניים ב  $\mathbb{Z}[i]$ .

### פתרון

$\mathbb{Z}[i]$  אוקלידי ולכן ראשי, בחוג ראשי איבר ראשוני אם ורק אם הוא אי פריק.

נמצא את האיברים הראשוניים ע"י כמה טענות:

### טענה 1

אם  $2 < p \in \mathbb{Z}$  ראשוני, כך ש  $p \equiv 3 \pmod{4}$  אז  $p$  אי פריק ב  $\mathbb{Z}[i]$ .

### הוכחה

נניח ש  $p$  פריק ב  $\mathbb{Z}[i]$ , ז"א  $p = \alpha \cdot \beta$ ,  $N(\alpha) > 1$ ,  $N(\beta) > 1$ , לכן

$N(\alpha) = p \leftarrow p^2 = N(p) = N(\alpha)N(\beta)$ . אם  $\alpha = a + bi$  כך ש  $a, b \in \mathbb{Z}$  אז  $p = a^2 + b^2$  או

$$3 = p \equiv a^2 + b^2 \pmod{4} \text{ כעת}$$

$\mathbb{Z}_4^2 = \{x^2 : x \in \mathbb{Z}_4\} = \{0, 1\} \leftarrow \mathbb{Z}_4 = \{0, 1, 2, 3\}$  ו  $\{a^2 + b^2 : a, b \in \mathbb{Z}_4\} = \{0, 1, 2\}$  ולכן  $p$  לא

יכול להיות סכום של שני ריבועים וקיבלנו סתירה.

### טענה 2

אם  $\pi$  הוא אי פריק ב  $\mathbb{Z}[i]$  אז קיים מספר ראשוני  $p \in \mathbb{Z}$  כך ש  $\pi | p$ .

### הוכחה

$N(\pi) = \pi \cdot \bar{\pi} = n = p_1 \cdot \dots \cdot p_s$  כך ש  $p_i \in \mathbb{Z}$  ראשוניים, לכן  $\pi | p_i$  עבור איזשהו  $i$ .

נמצא את האי פריקים ב  $\mathbb{Z}[i]$  ע"י הפירוק של המספרים הראשוניים ב  $\mathbb{Z}$ .

### טענה 3

אם  $\alpha \in \mathbb{Z}[i]$  ו  $N(\alpha)$  מספר ראשוני, אז  $\alpha$  אי פריק.

### הוכחה

אם  $\alpha = m \cdot k$  אז  $N(\alpha) = N(m) \cdot N(k)$  ראשוני  $\leftarrow$  בה"כ  $\leftarrow N(m) = 1$  הפיך. (למשל  $1+i$  הוא אי פריק ב  $\mathbb{Z}[i]$  מכיוון ש  $N(1+i) = 2$  ו  $2$  מספר ראשוני.

### טענה 4

אם  $p = 1 \pmod{4}$  מספר ראשוני אז קיים  $x \in \mathbb{Z}$  כך ש  $x^2 \equiv -1 \pmod{p}$ .

### פתרון

נסתכל על החבורה  $U_p = \{1, 2, \dots, (p-1)\}$  עם פעולת הכפל  $\pmod{p}$  אם  $a^2 \equiv 1 \pmod{p}$  אז  $p | a^2 - 1$  ולכן  $p | a \pm 1$  והאיברים היחידים ב  $U_p$  מסדר 2 הם  $\pm 1$ . ב  $U_p$  מתקיים  $(p-1)! = 1 \cdot 2 \cdot \dots \cdot (p-1) = -1 \cdot 1 \cdot (2 \cdot 2^{-1}) \cdot (3 \cdot 3^{-1}) \cdot \dots = -1 \cdot 1 = -1 \pmod{p}$  (זהו משפט וילסון).

נסתכל על  $x = \left(\frac{p-1}{2}\right)!$  אזי

$$-1 \equiv (p-1)! \equiv 1 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \cdot \dots \cdot (p-1) \equiv x \cdot (-1)^{\frac{p-1}{2}} \cdot x = x^2 \cdot (-1)^{\frac{p-1}{2}} \equiv x^2$$

השוויון הראשון נובע ממה שהראינו קודם.

השוויון השני נובע  $\left(\frac{p-1}{2}\right) = \left(\frac{p+1}{2}\right)$   $-1 = p-1, -2 = p-2, \dots$   $x = 1 \cdot \dots \cdot \left(\frac{p-1}{2}\right)$

השוויון האחרון נובע  $p = 1 \pmod{4} \rightarrow 4 | p-1 \rightarrow 2 | \frac{p-1}{2}$

### טענה 5

אם  $p = 1 \pmod{4}$  מספר ראשוני אז קיים  $a+bi \in \mathbb{Z}[i]$  אי פריק כך ש  $a^2 + b^2 = p$  (ובנוסף גם  $a-bi$  הוא אי פריק).

### פתרון

מטענה 4 קיים  $a \in \mathbb{Z}$  כך ש  $a^2 \equiv -1 \pmod{p}$  ולכן  $p | a^2 + 1$  או  $p | (a+i)(a-i)$ . נניח בשלילה ש

$p$  אי פריק ב  $\mathbb{Z}[i]$ , ולכן ראשוני. ניתן להניח בה"כ ש  $p | (a+i)$   $\leftarrow p | (a-i)$   $\leftarrow p | (a+i)$

ולכן  $p | 2a$  ב  $\mathbb{Z}$ . לא מחלק את 2 כי  $p = 1 \pmod{4}$  מספר ראשוני ולכן

$p > 2$  ולכן  $p | a$   $\leftarrow p | a^2$  אך גם  $p | (a^2 + 1)$  מכיוון ש  $1 = a^2 + 1 - a^2$  נקבל ש  $p | 1$  סתירה. לכן  $p$

פריק ו  $p = \alpha \cdot \beta$ , כך ש  $1 < N(\beta), N(\alpha)$  ו"ז  $N(\alpha) \cdot N(\beta) = N(p) = p^2$  ולכן  $N(\alpha) = p$ .

נסמן  $\alpha = a+bi$ . מכיוון ש  $N(\alpha) = a^2 + b^2 = p$  מספר ראשוני אז מטענה 3 אי פריק.

### מסקנה

האיברים הראשוני ב  $\mathbb{Z}[i]$  (עד כדי חברות) הם:

1.  $1+i$

2. הראשוניים  $p=3 \pmod{4}$  ב  $\mathbb{Z}$ .

3. לכל  $p=1 \pmod{4}$ , זוג המספרים  $a \pm bi$  כש  $a^2 + b^2 = p$ .

### אי פריקות פולינומים

#### משפט

1. נניח ש  $F$  שדה ויהי  $f(x) \in F[x]$  פולינום ממעלה  $1 \leq n$  אז ל  $f$  יש לכל היותר  $n$  שורשים

שונים ב  $F$ .

2. יהי  $R$  חוג קומוטטיבי,  $c \in R$  ו  $f \in R[x]$ . אז  $f(c) = 0 \iff f(x) \mid (x-c)$  ב  $R[x]$ .

אם  $F$  אינו שדה אז סעיף 1 במשפט לא נכון, למשל למשוואה  $x^2 + x = 0$  יש 4 פתרונות ב  $\mathbb{Z}_6$ .

#### משפט

כאשר  $F$  שדה, יהי  $f(x) \in F[x]$  פולינום מדרגה 2 או 3 אז  $f(x)$  אי פריק אם ורק אם אין ל  $f(x)$

שורשים ב  $F$ .

המשפט לא נכון עבור פונקציה מדרגה גדולה מ 3, למשל  $f(x) = (x^2 + 1)^2$  פריק ב  $\mathbb{R}$  אבל אין לו

שורשים ב  $\mathbb{R}$ .

#### משפט

יהי  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . אם  $\frac{k}{l} \in \mathbb{Q}$  הוא שורש של  $f$  כאשר  $(k, l) = 1$  אז

$$k \mid a_0, l \mid a_n$$

#### הוכחה

$$f\left(\frac{k}{l}\right) = a_n \left(\frac{k}{l}\right)^n + \dots + a_1 \left(\frac{k}{l}\right) + a_0 = 0$$

ולכן  $a_n k^n + \dots + a_1 k l^{n-1} + a_0 l^n = 0$  ז"א

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

לכן  $k \mid a_0 l^n$ .  $(k, l) = 1$  ובאותו אופן מוכיחים ש  $l \mid a_n$ .

#### תרגיל

הראו שלכל  $p$  ראשוני,  $1 < n \in \mathbb{N}$ ,  $\sqrt[n]{p}$  אי רציונאלי.

#### פתרון

נתבונן ב  $f(x) = x^n - p$  כש  $\sqrt[n]{p}$  הוא שורש של  $f$ . אם  $\frac{k}{l} \in \mathbb{Q}$  שורש של  $f$ , אז

$$f\left(\frac{k}{l}\right) = (\pm p)^n - p \neq 0 \quad 1 < n \in \mathbb{N}$$

אבל לכל  $l \in \{\pm 1\}, k \in \{\pm 1, \pm p\}$  ולכן אין שורש רציונאלי ל  $f$ .

#### הגדרה

$f(x) \in R[x]$  הוא פולינום פרימיטיבי אם המחלק המשותף המקסימאלי של מקדמיו שווה ל 1.

#### הקריטריון של אייזנשטיין

יהי  $D$  תפ"י,  $F$  שדה השברים של  $D$ ,  $p \triangleleft D$  אידיאל ראשוני. יהי  $f(x) = a_n x^n + \dots + a_1 x + a_0$ ,  $1 \leq n$ , כך ש  $a_0 \notin p^2$ ,  $0 \leq i < n$ ,  $a_i \in p$ ,  $a_n \notin p$  ואם  $f$  פרימיטיבי ב  $D$  אז  $f$  אי פריק ב  $D[x]$ .

שימו לב: אם  $P = \langle p \rangle$  (איבר ראשוני) אז את תנאי הקריטריון ניתן לנסח כך -  $p$  לא מחלק את  $a_n$ ,  $p$  לא מחלק את  $a_i$  ו  $p^2$  לא מחלק את  $a_0$ .

### הוכחה

נניח בשלילה כי קיים  $f$  המקיים את הקריטריון הנ"ל שמתפרק באופן לא טריוויאלי  $f = g \cdot h$  כאשר  $\deg(g) = k, \deg(h) = m$  ( $m, k > 0, k + m = n$ ). נסמן  $f = a_n x^n + \dots + a_0$  ו  $h = b_m x^m + \dots + b_0$ . יהי  $g = c_k x^k + \dots + c_0$ . בהמקדם המינימלי ב  $h$  שלא נמצא ב  $P$ , ויהי  $c_j$  המקדם המינימלי ב  $g$  שלא נמצא ב  $P$ . אזי  $b_i c_j \equiv a_{i+j} \pmod{P}$ . אולם,  $b_i c_j$  לא נמצא ב  $P$  משום ש  $P$  ראשוני, ולכן  $a_{i+j}$  לא נמצא ב  $P$ , וזה קורה רק כאשר  $i + j = n$  (לפי הנתונים), ולכן  $i = m$  ו  $j = k$ . בפרט, זה אומר ש  $b_0, c_0 \in P$  ולכן  $a_0 = b_0 c_0 \in P^2$  בסתירה לנתונים.

### דוגמאות

1.  $f(x) = 22x^5 + 27x + 51$ ,  $f(x)$  הוא אי פריק מעל  $\mathbb{Z}$ , כי עבור  $p = 3$  מתקיים קריטריון אייזנשטיין (3 מחלק את 27, 51, 3 לא מחלק את 22 ו 9 לא מחלק את 51).  
 2. הראינו ש 3 הוא איבר ראשוני ב  $\mathbb{Z}[i]$ . לכן הפולינום  $x^6 - 30x + 15$  הוא אי פריק ב  $\mathbb{Z}[i]$  (עבור  $P = \langle 3 \rangle$ ).

3. האם  $f(x, y) = y^2 + (x^2 + 2)y + (x^2 + 2)(x^2 + 3)$  אי פריק ב  $\mathbb{Z}[x, y]$ ?  
 כן, נסתכל על  $\mathbb{Z}[x, y] = (\mathbb{Z}[x])[y]$ , ז"א  $D = \mathbb{Z}[x]$ . הפולינום  $p(x) = x^2 + 2$  הוא איבר ראשוני ב  $D$ . (כי  $D/P = \mathbb{Z}[x]/\langle x^2 + 2 \rangle \cong \mathbb{Z}[\sqrt{-2}]$  וזהו תחום שלמות.) ניתן עת להשתמש בקריטריון אייזנשטיין עם האידיאל  $\langle p \rangle$  עבור בדיקת האי פריקות של  $f$  ב  $D[y]$ .

4. האם  $x^2 - 3$  הוא אי פריק ב  $\mathbb{Z}[\sqrt{-2}][x]$ ? שימו לב שאי אפשר להשתמש בקריטריון של אייזנשטיין (ב  $D = \mathbb{Z}[\sqrt{-2}]$ ) עם  $p = 3$  כי  $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$ , ז"א 3 פריק ולכן אינו ראשוני. אבל  $1 + \sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$  הוא כן איבר ראשוני. מכיוון ש  $N(1 + \sqrt{-2}) = 1^2 + 2 \cdot 1^2 = 3$  ומכיוון שהנורמה הוא מספר ראשוני אזי  $1 + \sqrt{-2}$  הוא איבר אי פריק. מכיוון ש  $\mathbb{Z}[\sqrt{-2}]$  אוקלידי איבר אי פריק הוא ראשוני, לכן  $1 + \sqrt{-2}$  ראשוני. עתה נשתמש בקריטריון אייזנשטיין עם  $p = 1 + \sqrt{-2}$  ונקבל ש  $x^2 - 3$  אי פריק.

### הערה

קריטריון אייזנשטיין נותן תנאי מספיק ולא הכרחי, למשל הפולינום  $x^2 + 4$ ,  $x^2 + 1$  אי פריקים מעל  $\mathbb{Q}$  למרות שאינם מקיימים את הקריטריון. בנוסף  $x^4 + 4$  פריק ב  $\mathbb{Q}[x]$ , כי  $x^4 + 4 = (x^2 + 2x + 2)(x^2 - 2x + 2)$ .

### הערה

אם  $f(x)$  פריק מעל  $F[x]$  אז  $f(ax+b)$  פריק מעל  $F[x]$ .

### דוגמא

צ"ל ש  $g(x) = 8x^3 + 6x^2 + 1$  אי פריק מעל  $\mathbb{Q}$ . נציב  $x+1$  במקום  $x$  ונקבל ש  $g(x+1) = 8x^3 + 30x^2 + 36x + 15$  נפעיל את קריטריון אייזנשטיין עם  $p=3$  ונקבל ש  $g(x+1)$  אי פריק ולכן  $g(x)$  אי פריק.

### משפט

אם  $D$  תפ"י,  $F$  שדה השברים של  $D[x]$  ו  $f(x) \in D[x]$  פרימיטיבי אז  $f(x) \in D[x]$  אי פריק אם ורק אם  $f(x) \in F[x]$  אי פריק.

### מסקנה

עבור אותם התנאים, ועבור  $g(x) \in D[x]$ ,  $g|f$  ב  $D[x]$  אם ורק אם  $g|f$  ב  $F[x]$ .

### תרגיל

יהי  $f(x, y, z) = x^2 + y^2 + z^2$  פולינום ב  $k[x, y, z]$  ( $k$  שדה). נתון ש  $\text{char}(k) \neq 2$  צריך להוכיח ש  $f$  אי פריק ב  $k[x, y, z]$ .

### הערה

אם  $\text{char}(k) = 2$  אז  $f$  פריק מכיוון ש  $f(x, y, z) = (x + y + z)^2$ .

### פתרון

נסמן  $R = k[y, z]$ , ואז  $k[x, y, z] = R[x]$ . כלומר,  $f(x, y, z) = x^2 + y^2 + z^2$  הופך לפולינום מתוקן ממעלה 2 שהמקדם החופשי שלו הוא  $y^2 + z^2$ . ברצוננו להראות כי קיים איבר ראשוני  $p$  ב  $R$ , כך ש  $p$  מחלק את  $y^2 + z^2$  אך  $p^2$  לא מחלק אותו.  $R$  הוא תחום פריקות יחידה ולכן כל איבר בו מתפרק למכפלת ראשוניים. יהיה איזשהו פולינום ראשוני  $p$  (עם חזקה לא טריוויאלית של  $z$ ) ב  $R$  המחלק את  $y^2 + z^2$ . נסמן  $D = k[y]$ , ונסמן ב  $F$  את שדה השברים שלו, כלומר  $F = k(y)$ . כעת  $R = D[z]$ . מכיוון ש  $y^2 + z^2$  פולינום מתוקן ב  $D[z]$ , לכל פולינום  $g(z) \in D[z]$ ,  $g|f$  ב  $D[z]$  אם ורק אם  $g|f$  ב  $F[z]$ .

נניח בשלילה כי  $p^2$  מחלק את  $y^2 + z^2$  ב  $F[z]$ . אזי מתקיים  $y^2 + z^2 = p^2 \cdot h$ , ואז  $\frac{\partial(y^2 + z^2)}{\partial z} = 2z$ ,

ולכן כל קומבינציה ליניארית (עם מקדמים מ  $F[z]$ ) של  $y^2 + z^2$  ושל  $\frac{\partial(y^2 + z^2)}{\partial z}$  מתחלקת ב  $p$ . אולם,

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

ממאפיין שונה מ2 וזו סתירה.

משמע,  $p^2$  לא מחלק את  $y^2 + z^2$  ב  $F[z]$ , ולכן הוא גם לא מחלק את  $y^2 + z^2$  ב  $D[z]$ .

כלומר, קיים ראשוני  $p$  ב  $R$  המחלק את  $y^2 + z^2$  אך  $p^2$  לא מחלק אותו, ולכן מתקיים קריטריון

אייזנשטיין, ולכן  $f$  אי-פריק ב  $k[x, y, z] = R[x]$ .