

## פתרון תרגיל בית 8 מבוא לחוגים ומודולים 88-212 סמסטר ב' תשפ"א

**שאלה 1.** קבעו האם הפולינומים הבאים הם אי פריקים בחוג הנתון, ואם הם פריקים מצאו את פירוק שלהם לגורמים אי פריקים.

1. בחוג  $\mathbb{F}_2[x]$   $x^2 + x + 1$ .

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

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

4. בחוג  $\mathbb{Q}[x, y]$   $x^2 + y^2 - 1$ . העשרה:  $x^n + y^m - 1$  לכל  $n, m \in \mathbb{N}$ .

פתרו. לפי פתרון בתרגיל בית 8 תשע"ה.

א. אי פריק. פולינום מדרגה 2 ללא שורשים.

ב. הפירוק הוא  $x \cdot x \cdot (x^4 - 4x^2 + 6)$ . הגורם האחרון אי פריק בעזרת קריטריון אייזנשטיין עם  $p = 2$ .

ג. בעזרת המיון של ראשוניים ב- $\mathbb{Z}[i]$ , אנחנו יודעים כי ישנו פירוק  $71 = (4+i)(4-i)$ . כעת ניתן להשתמש בקריטריון אייזנשטיין עם  $p = 4+i$ . צריך להוכיח כי  $4+i$  ראשוני וגם שהוא לא מחלק את  $2i$ , למשל לפי חישוב נורמות.

ד. שתי דרכים: בדרך הראשונה, לפולינום  $y^2 + (x^2 - 1)$  אין שורשים מעל  $\mathbb{Q}[x]$ , כי  $x^2 - 1 = (x-1)(x+1)$ . אנחנו בתחום פריקות יחידה, ולכן אין פירוק אחר ל- $x^2 - 1$  שבו הוא ריבוע.

בדרך השנייה, אפשר להשתמש בקריטריון אייזנשטיין עם  $p = x - 1$ , שהוא ראשוני כי  $\mathbb{Q}[x]/\langle x - 1 \rangle \cong \mathbb{Q}$  תחום שלמות. לגבי ההעשרה, כדי להעזר בקריטריון אייזנשטיין עם  $x - 1$  נשים לב כי  $(x - 1) \nmid (x^{n-1} + \dots + x + 1)$ . אבל  $(x - 1) \mid (x^{n-1} + \dots + x + 1)$  כי 1 הוא שורש של  $x - 1$  ולא של  $x^{n-1} + \dots + x + 1$ .

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

א.  $\mathbb{Q}$

ב.  $\mathbb{Q}[\sqrt{2}]$

ג.  $\mathbb{R}$

ד.  $\mathbb{Z}/5\mathbb{Z}$

פתרו. עוד לפני שחושבים, אפשר לשים לב שכל המונומים הם ממעלה זוגית, ולפרק

$$f(x) = (x^2 - 2)(x^2 - 3)$$

א. הפירוק שכתבנו למעלה הוא הפירוק המלא מעל  $\mathbb{Q}$ . שני הגורמים הם אי-פריקים כי הם ממעלה 2 ואין להם שורשים ב- $\mathbb{Q}$ .

ב. פה הגורם הראשון פריק, ומקבלים

$$f(x) = (x + \sqrt{2})(x - \sqrt{2})(x^2 - 3)$$

הגורם השני אי-פריק כי הוא ממעלה 2 ואין לו שורשים ב- $\mathbb{Q}[\sqrt{2}]$ .

ג. אפשר לפרק את  $f(x)$  למכפלה של גורמים לינאריים:

$$f(x) = (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$$

ד. מספיק לבדוק לאילו מן הגורמים שמצאנו אין שורש ב- $\mathbb{Z}/5\mathbb{Z}$ , כי שניהם ממעלה 2. נחשב את  $x^2$  לכל  $x \in \mathbb{Z}/5\mathbb{Z}$ , ונקבל

$$(1 + 5\mathbb{Z})^2 = (4 + 5\mathbb{Z})^2 = 1 + 5\mathbb{Z}, \quad (2 + 5\mathbb{Z})^2 = (3 + 5\mathbb{Z})^2 = 4 + 5\mathbb{Z}$$

לכן לשניהם אין שורש, כלומר שניהם אי-פריקים.

**שאלה 3.** יהי  $p$  מספר ראשוני. הראו שהפולינום  $f(x) = \frac{x^p - 1}{x - 1}$  הוא אי פריק מעל  $\mathbb{Q}$ . רמז: הסתכלו על  $f(x + 1)$ .

פתרון. נלך לפי הרמז:

$$f(x + 1) = \frac{(x + 1)^p - 1}{x + 1 - 1} = \frac{\sum_{i=0}^p \binom{p}{i} x^i - 1}{x} = \frac{\sum_{i=1}^p \binom{p}{i} x^i}{x} = \sum_{i=1}^p \binom{p}{i} x^{i-1}$$

נראה שהפולינום מקיים את קריטריון אייזנשטיין ביחס לראשוני  $p$ . קל לבדוק שזהו פולינום מתוקן; כל מקדם לא מוביל (כלומר  $0 < i < p$ ) הוא  $\binom{p}{i}$  שמתחלק ב- $p$ , כי  $p$  ראשוני (אז  $p$  מופיע במונה של  $\binom{p}{i}$  אבל לא במכנה); והמקדם החופשי הוא  $\binom{p}{1} = p$  לא מתחלק ב- $p^2$ . לכן  $f(x + 1)$  אי-פריק מעל  $\mathbb{Z}$ , ומכאן שגם  $f(x)$  אי-פריק מעל  $\mathbb{Z}$ , כלומר מעל  $\mathbb{Q}$ .

**שאלה 4.** נתבונן בפולינום  $f(x) = x^2 + 4$  מעל  $\mathbb{Z}$ . הראו ש- $f(ax + b)$  לא מקיים את קריטריון אייזנשטיין לכל  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , למרות ש- $f(x)$  אי פריק.

פתרון. נציב:

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

כדי ש- $f(ax + b)$  יקיים את קריטריון אייזנשטיין ביחס לראשוני  $p$  כלשהו, צריך:

$$p \nmid a^2, \quad p \mid 2ab, b^2 + 4, \quad p^2 \nmid (b^2 + 4)$$

מהחלק הראשון נקבל  $a \nmid p$ , ולכן  $p \mid 2ab$  גורר  $p \mid 2b$ . יש שתי אפשרויות:

- $p \mid 2$ , כלומר  $p = 2$ . אם  $b$  זוגי,  $4 \mid b^2$  ולכן  $4 \mid (b^2 + 4)$  בסתירה. אם  $b$  אי-זוגי, אז  $2 \nmid (b^2 + 4)$  בסתירה.

- $p \nmid 2$ , כלומר  $p \neq 2$ . לכן  $p \mid b$ . אבל אז  $p \mid b^2, b^2 + 4$ , לכן  $p \mid 4$  בסתירה.

זה מראה ש- $f(ax + b)$  לעולם אינו מקיים את קריטריון אייזנשטיין. לעומת זאת, הוא אי-פריק כי אין לו שורשים ב- $\mathbb{Q}$ .

**שאלה 5.** יהי  $R$  תחום פריקות יחידה, ויהי  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$  ש- $a_0 \neq 0$ .

א. הוכיחו כי  $f$  הוא אי פריק ב- $R[x]$  אם ורק אם הוא אי פריק ב- $R[x, x^{-1}]$ .

ב. נתבונן בפולינום  $\tilde{f}(x) = a_0x^n + \dots + a_{n-1}x + a_n$  שבו הפכנו את סדר המקדמים של  $f$ . הוכיחו בעזרת הסעיף הקודם שאם  $\tilde{f}$  מקיים את קריטריון אייזנשטיין, אז  $f$  אי פריק.

פתרון. א. נניח  $f = gh$  פריק ב- $R[x]$ . נשים לב שהמקדם החופשי של  $g$  ו- $h$  חייב להיות שונה מ-0, כי המקדם החופשי של  $f$  שונה מ-0. לכן  $g$  ו- $h$  לא יהיו הפיכים ב- $R[x, x^{-1}]$  (אפשר לוודא ישירות). זה מראה שהפירוק  $f = gh$  נשאר פירוק אמיתי של  $f$  ב- $R[x, x^{-1}]$ , כנדרש.

כעת נניח ש- $f = gh$  פירוק של  $f$  ב- $R[x, x^{-1}]$ . אפשר לכתוב  $g = a_mx^m + \dots$  ו- $h = b_kx^k + \dots + b_\ell x^\ell$  עבור  $h = b_kx^k + \dots + b_\ell x^\ell$  ו- $a_m, b_k \neq 0$  ו- $m < n, k < \ell, m, n, k, \ell \in \mathbb{Z}$ . אבל הוא צריך להיות שווה ל- $a_0$ , לכן  $m = -k$ . אם  $k \leq 0$ , אז  $m \geq 0$  ונקבל  $f = (x^{-m}g)(x^mh)$  פירוק של  $f$  ב- $R[x]$ , כשאף גורם לא הפיך כי הם לא קבועים.

ב. צריך לתקן את השאלה: הוכיחו שאם  $\tilde{f}$  פרימיטיבי ומקיים את קריטריון אייזנשטיין, אז  $f$  אי-פריק. מהנתון,  $\tilde{f}$  הוא אי פריק. נשים לב כי

$$\tilde{f}(x) = a_0x^n + \dots + a_n = x^n \cdot f(x^{-1})$$

אם  $\tilde{f}$  אי פריק ב- $R[x]$ , מהסעיף הקודם הוא אי-פריק ב- $R[x, x^{-1}]$ ; לכן  $f(x^{-1})$  הוא אי-פריק ב- $R[x, x^{-1}]$ ; לכן  $f$  הוא אי-פריק ב- $R[x, x^{-1}]$ ; ולכן  $f$  אי-פריק ב- $R[x]$ .

**שאלה 6** (רשות). הוכיחו שלכל  $n \in \mathbb{N}$  הפולינום

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

הוא אי פריק בחוג  $\mathbb{Z}[x]$ .

פתרון. לפי פתרון בתרגיל בית 8 תשע"ה.

נשים לב כי  $p_n(x)$  הוא מתוקן, ולכן פרימיטיבי. נניח בשלילה כי  $p_n(x) = f(x)g(x)$  עבור פולינומים  $f(x), g(x) \in \mathbb{Z}[x]$  מדרגה שקטנה ממש  $n$ - $\deg p_n(x)$ . לכל  $1 \leq i \leq n$  מתקיים  $p_n(i) = f(i)g(i) = -1$  מפני שהפולינומים מעל  $\mathbb{Z}$ , והצבנו ערכים שלמים, אז בהכרח  $\{f(i), g(i)\} = \{-1, 1\}$ . בפרט  $f(i), g(i)$  הם עם סימנים הפוכים. נתבונן בפולינום  $h(x) = f(x) + g(x)$ , שעבורו כל  $1 \leq i \leq n$  הוא שורש כי  $h(i) = \pm 1 \mp 1 = 0$  (נעזרים בכך שהסימנים הפוכים). הדרגה של  $h(x)$  קטנה ממש  $n$ , כי הדרגות של  $f(x), g(x)$  קטנות ממש  $n$ . לכן קיבלנו ש- $h(x) \equiv 0$ . כלומר  $h(x) = -g(x)$ . נציב בחזרה ונקבל  $p_n(x) = -f(x)^2$ . בפרט  $p_n(x)$  תמיד לא חיובי, אבל לפי הגדרת  $p_n(x)$  אפשר לראות שעבור  $x$  מספיק גדול הפולינום הוא חיובי. זו סתירה, ולכן הפולינום  $p_n(x)$  אי פריק. הערה: אפשר להחליף את  $1, \dots, n$  בכל קבוצה  $\{a_1, \dots, a_n\}$  של שלמים שונים כלשהם.

**שאלה 7** (רשות). נתבונן באידאל  $I = \langle 21, 9 + 3\sqrt{-5}, -2 + 4\sqrt{-5} \rangle \triangleleft \mathbb{Z}[\sqrt{-5}]$

א. הוכיחו כי  $I$  אידאל ראשי.

ב. הוכיחו כי  $I$  לא מקסימלי. רמז: אפשר להראות כי הוא אפילו לא ראשוני.

פתרון.

א. נייעזר בפונקציית הנורמה הכפלית

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a + b\sqrt{-5}) = a^2 + 5b^2$$

שהיא הצמצום של  $N(z) = |z|^2$  ל- $\mathbb{Z}[\sqrt{-5}]$ . אם  $I = \langle x \rangle$ , אז  $21, 9 \mid x$ ,  
 $3\sqrt{-5}, -2 + 4\sqrt{-5}$  וכיוון ש- $N$  כפולית נקבל בפרט

$$N(x) \mid N(21) = 441, N(9 + 3\sqrt{-5}) = 9^2 + 5 \cdot 9 = 126, N(-2 + 4\sqrt{-5}) = 4 + 5 \cdot 4^2 = 84$$

לכן  $N(x) \mid \gcd\{441, 126, 84\} = 21$ . נחפש איבר מנורמה 21:

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 21 \implies (a, b) \in \{(\pm 4, \pm 1), (\pm 1, \pm 2)\}$$

עכשיו כשאנחנו יודעים לאן לכוון, ננסה למצוא איזה איבר מביניהם מחלק את כל היוצרים של  $I$ . מספיק לבדוק את האיברים  $4 \pm \sqrt{-5}, 1 \pm 2\sqrt{-5}$ . כולם מחלקים את 21, כי הוא הנורמה שלהם. נבדוק את היוצר השני:

$$\frac{9 + 3\sqrt{-5}}{4 + \sqrt{-5}} = \frac{9 + 3\sqrt{-5}}{4 + \sqrt{-5}} \cdot \frac{4 - \sqrt{-5}}{4 - \sqrt{-5}} = \frac{36 - 9\sqrt{-5} + 12\sqrt{-5} + 15}{21} = \frac{17}{7} + \frac{1}{7}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$$

$$\frac{9 + 3\sqrt{-5}}{4 - \sqrt{-5}} = \frac{9 + 3\sqrt{-5}}{4 - \sqrt{-5}} \cdot \frac{4 + \sqrt{-5}}{4 + \sqrt{-5}} = \frac{36 + 9\sqrt{-5} + 12\sqrt{-5} - 15}{21} = 1 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$$

$$\frac{9 + 3\sqrt{-5}}{1 + 2\sqrt{-5}} = \frac{9 + 3\sqrt{-5}}{1 + 2\sqrt{-5}} \cdot \frac{1 - 2\sqrt{-5}}{1 - 2\sqrt{-5}} = \frac{9 - 18\sqrt{-5} + 3\sqrt{-5} + 30}{21} = \frac{13}{7} - \frac{5}{7}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$$

$$\frac{9 + 3\sqrt{-5}}{1 - 2\sqrt{-5}} = \frac{9 + 3\sqrt{-5}}{1 - 2\sqrt{-5}} \cdot \frac{1 + 2\sqrt{-5}}{1 + 2\sqrt{-5}} = \frac{9 + 18\sqrt{-5} + 3\sqrt{-5} - 30}{21} = -1 + \sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$$

פסלנו שתי אפשרויות. נבדוק מי מחלק גם את היוצר השלישי:

$$\frac{-2 + 4\sqrt{-5}}{4 - \sqrt{-5}} = \frac{-2 + 4\sqrt{-5}}{4 - \sqrt{-5}} \cdot \frac{4 + \sqrt{-5}}{4 + \sqrt{-5}} = \frac{-8 - 2\sqrt{-5} + 16\sqrt{-5} - 20}{21} = -\frac{4}{3} + \frac{2}{3}\sqrt{-5} \notin \mathbb{Z}[\sqrt{-5}]$$

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

לכן  $\langle 1 - 2\sqrt{-5} \rangle \subseteq I$ . נרצה להראות את הכיוון ההפוך. אכן,

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

זה מראה ש- $I$  ראשי.

ב. כדי להראות ש- $I$  לא מקסימלי, אפשר לשים לב ש- $3 \cdot 7 = 21 \in I$ , אבל  $3, 7 \notin I$ .  
 (אחרת  $N(3) = 9 \mid N(1 - 2\sqrt{-5}) = 21$  או  $21 \mid N(7) = 49$ ). לכן הוא אפילו לא ראשוני.

**שאלה 8** (העשרה). א. יהי  $f(x) \in \mathbb{Z}[x]$  פולינום פריק ופרימיטיבי, ויהי  $p$  מספר ראשוני. נתבונן בהטלה  $\bar{f}(x) \in \mathbb{Z}/p\mathbb{Z}[x]$  מודולו  $p$  של  $f(x)$ . הוכיחו שאם  $\deg \bar{f} = \deg f$ , אז  $\bar{f}(x)$  פריק מעל  $\mathbb{Z}/p\mathbb{Z}$ .

ב. הסיקו מהסעיף הקודם שהפולינום  $x^4 + 88212x^2 + x + 1$  הוא אי פריק מעל  $\mathbb{Z}$ .

ג. יהי פולינום  $g(x) \in \mathbb{Z}[x]$  מדרגה לפחות 2. הוכיחו שקיים מספר ראשוני  $p$  כך ש- $\bar{g}(x)$  הוא פריק מעל  $\mathbb{Z}/p\mathbb{Z}$  (אפשר להוכיח שישנם אינסוף ראשוניים כאלו).

פתרון.

א. נניח  $f = g \cdot h$  עבור פולינומים  $g, h$  מדרגות נמוכות מ- $\deg f$ . ההטלה של המקדמים מודולו  $p$  היא הומומורפיזם של חוגים  $\mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x]$ , ולכן  $\bar{f} = \bar{g} \cdot \bar{h}$  ומודולו  $p$ . למעשה אנחנו משתמשים באחת מהגרסאות של הלמה של גאוס:  $c(f) = c(g) \cdot c(h)$ , ולכן  $g, h$  הם גם פרימיטיביים, וכך גם אחרי הטלה מודולו  $p$ . בלי הגבלת הכלליות אפשר להניח  $\deg \bar{g} \leq \deg \bar{h}$ . אם  $\bar{g} \equiv 0$ , אזי כל המקדמים של  $g$  מתחלקים ב- $p$ , וזו תהיה סתירה לכך ש- $f$  פרימיטיבי (כי אז  $p$  מחלק את כל

המקדמים שלו). אם  $\deg \bar{g} = 0$ , אזי  $g \in \mathbb{Z}$ , וזו שוב תהיה סתירה לכך ש- $f$  פרימיטיבי (או ש- $g = \pm 1$  וזו סתירה לכך שהפירוק  $f = g \cdot h$  אמיתי). אזי  $\deg \bar{g} > 0$ , ולכן מדובר בפירוק אמיתי מעל  $\mathbb{Z}/p\mathbb{Z}$ . יש טעות בהוכחה הנ"ל! נתבונן בפולינום  $(px+1)^2$  שהוא פרימיטיבי, ומודולו  $p$  הוא 1. לכן אי-פריק. מסקנה מיידית: פולינום מתוקן ופריק הוא פריק גם מודולו כל ראשוני.

ב. מודולו 2 נקבל  $x^2 + x + 1 \equiv 400x^{400} + x^4 + x + 1 \pmod{2}$  שראינו שהוא אי פריק מעל  $\mathbb{Z}/2\mathbb{Z}$ , כי אין לו שורשים בשדה.

ג. נמצא  $a \in \mathbb{Z}$  כך ש- $g(a) = n \neq \pm 1$ . הבינו למה אפשר לעשות זאת (כי הדרגה חיובית). אם  $n = 0$ , סיימנו כי נוכל לבחור כל ראשוני שאינו מחלק את  $g(x)$ . אחרת, אפשר למצוא  $n$  שיש לו מחלק ראשוני  $p$  שאינו מחלק את  $g(x)$  (כי  $g(x)$  יכול לקבל את אותו הערך רק מספר סופי של פעמים. זה נראה שזה לא פותר אם הרדיקל של  $g(a)$  חסום, אבל זה לא יתכן כי אז  $g(x)$  יגדל לפחות כמו  $2^x$ ), ואז מודולו  $p$  נקבל  $g(a) \equiv 0$ , ולכן פריק. אם פולינום  $f(x)$  מקבל אינסוף ערכים שהם מספרים ראשוניים, אז הוא אי פריק. הרי אם  $f(x) = g(x)h(x)$  הוא פירוק לדרגות חיוביות, אז  $g(x)$  או  $h(x)$  מקבלים את הערך  $\pm 1$  אינסוף פעמים. זו סתירה כי פולינום מדרגה חיובית לא מקבל את אותו ערך אינסוף פעמים.

בהצלחה!