

פתרון תרגיל בית 1 בשדות ותורת גלואה 88-311 סמסטר א' תשע"ט

שאלה 1. כהכנה לשבוע הבא, שחקו ב"אוקלידס: המשחק" (או בקישור הזה) והגיעו לפחות לשלב 6. הרבה יותר נוח להשתמש במחשב נייד או נייד מאשר בטלפון.

שאלה 2. בדקו האם הפולינומים הבאים אי פריקים:

א. $3x^2 - 7x - 5$ ב- $\mathbb{Q}[x]$ (גם בלי נוסחת השורשים).

פתרון. אפשר כמובן לחפש שורשים עם נוסחת שורשים. אבל אפשר להשתמש בשיטת הרדוקציה ל- $\mathbb{Z}/2\mathbb{Z}$ ולקבל את הפולינום

$$x^2 + x + 1$$

שהוא מאותה דרגה כמו הפולינום המקורי ובנוסף הוא אי פריק כי הצבה של 0, 1 לא מאפסת אותו.

ב. $x^3 - 7x + 2$ ב- $\mathbb{Q}[x]$.

פתרון. לפי "הטריק" של \mathbb{Q} , כל שורש מצומצם $\frac{q}{r}$ מקיים $2 \mid q$ ו- $1 \mid r$ ולכן האפשרויות היחידות לשורשים מעל \mathbb{Q} הן $\{\pm 1, \pm 2\}$. מציבים, ורואים שאף אחת מהאפשרויות אינה שורש, ולכן הפולינום אי פריק.

ג. $x^3 - 7x + 2$ ב- $\mathbb{Z}_5[x]$.

פתרון. ב- \mathbb{Z}_5 הפולינום הזה הוא בעצם $x^3 - 2x + 2$. מציבים כל אחת מהאפשרויות ורואים שאין שורשים ולכן הפולינום אי פריק.

ד. $x^3 - 6x - 9$ ב- $\mathbb{Q}[x]$.

פתרון. לפי הטריק של \mathbb{Q} , כל שורש $\frac{q}{r}$ חייב לקיים $9 \mid q$ ו- $1 \mid r$ ולכן האופציות היחידות לשורשים מעל \mathbb{Q} הם $\{\pm 1, \pm 3, \pm 9\}$. מציבים ורואים ש 3 הוא שורש ולכן הפולינום פריק.

ה. $x^4 + 4x^3 + 6x^2 + 2x + 1$ ב- $\mathbb{Q}[x]$.

פתרון. נשים לב (למשל לפי הכרות עם נוסחת הבינום) כי

$$(x + 1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1$$

ולכן

$$x^4 + 4x^3 + 6x^2 + 2x + 1 = (x + 1)^4 - 4x - 1 + 2x + 1 = (x + 1)^4 - 2(x + 1) + 2$$

הפולינום שלנו אי פריק אם ורק אם

$$x^4 - 2x + 2$$

אי פריק. אכן, $x^4 - 2x + 2$ אי פריק לפי קריטריון אייזנשטיין עבור $p = 2$.

שאלה 3. מצאו את הפירוק של הפולינום $x^4 - 2$ מעל השדות הבאים:

א. \mathbb{C}

פתרון. קל לראות ש-

$$x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)(x - \sqrt[4]{2})(x + \sqrt[4]{2})$$

ב. \mathbb{R}

פתרון. קל לראות ש-

$$x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x^2 + \sqrt{2})(x - \sqrt[4]{2})(x + \sqrt[4]{2})$$

ושהגורם $x^2 + \sqrt{2}$ אי פריק כי אין לו שורשים ממשיים.

ג. \mathbb{Q}

פתרון. הפולינום אי פריק לפי קריטריון אייזנשטיין עבור $p = 2$.

ד. \mathbb{Z}_3

פתרון. ננסה למצוא פירוק. ראשית, קל לוודא שאין לא שורשים ב- \mathbb{Z}_3 ולכן אם יש פירוק

$$x^4 - 2 = g(x)h(x)$$

בהכרח מתקיים ש- $\deg h(x) = \deg g(x) = 2$. נסמן

$$g(x) = a_2x^2 + a_1x + a_0$$

$$h(x) = b_2x^2 + b_1x + b_0$$

אפשר להניח בלי הגבלת כלליות ש- $b_2 = 1$ (אחרת נכפול את שני הפולינומים ב-2) ואז נקבל:

$$\begin{aligned} g(x)h(x) &= (a_2x^2 + a_1x + a_0)(x^2 + b_1x + b_0) = \\ &= a_2x^4 + (a_2b_1 + a_1)x^3 + (a_0 + b_0a_2 + a_1b_1)x^2 + (b_1a_0 + b_0a_1)x + a_0b_0 \end{aligned}$$

עכשיו נשווה מקדמים. מייד נסיק ש- $a_2 = 1$. מהשוואת המקדם של x^3 נקבל ש- $a_1 = -b_1$. שימו לב שזה מכריח כי

$$a_1b_1 = -b_1^2 \in \{0, 2\}$$

מהשוואת המקדם החופשי נקבל $a_0b_0 = 1$, וזה מכריח $a_0 = b_0 = 1$ או $a_0 = b_0 = 2$. אם $a_0 = b_0 = 1$ אז מהשוואת מקדם של x^2 נקבל

$$a_0 + b_0 + a_1b_1 = 2 + a_1b_1 \in \{1, 2\}$$

בסתירה לכך שצריך לקבל 0. ננסה את האופציה $a_0 = b_0 = 2$. במצב זה

$$a_0 + b_0 + a_1b_1 = 1 + a_1b_1 \in \{0, 1\}$$

אז צריך לקחת $a_1 = 2$ ו- $b_1 = -2$. נקבל פירוק אמיתי

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

כלומר הפולינום פריק.

שאלה 4. יהי $f(x) = a_n x^n + \dots + a_0$ פולינום עם מקדמים שלמים. נניח כי $a_n, f(0)$ ו- $f(1)$ הם אי זוגיים. הוכיחו כי ל- f אין שורשים ב- \mathbb{Q} . רמז: טענה מהתרגול. פתרו. נניח ש- $\frac{q}{r}$ הוא שורש רציונלי מצומצם. אז מתקיים

$$a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1} + a_0 r^n = 0$$

קעת נשים לב ש- q, r אי זוגיים כי $f(0) = a_0 = q \mid a_n - 1$. לכן עד כדי מודולו 2 נקבל

$$0 \equiv a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1} + a_0 r^n \equiv a_n + a_{n-1} + \dots + a_1 + a_0 \equiv f(1) \pmod{2}$$

אבל לפי הנתון $f(1) \equiv 1 \pmod{2}$, שזו סתירה.

שאלה 5. יהי $f(x) \in F[x]$ פולינום מדרגה $n \geq 1$.

א. הוכיחו כי $F[x]/\langle f(x) \rangle$ הוא מרחב וקטורי מעל F עם בסיס $\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$.

ב. הציגו את

$$x^4 - x^3 + x - 2 \in \mathbb{Q}[x]/\langle x^3 - x^2 - 1 \rangle$$

כצירוף לינארי של אברי הבסיס $\{\bar{1}, \bar{x}, \bar{x}^2\}$.

פתרו.

א. צריך להוכיח שהקבוצה הזו היא בת"ל ופורשת.

בת"ל: נניח כי $\alpha_0 \bar{1} + \alpha_1 \bar{x} + \dots + \alpha_{n-1} \bar{x}^{n-1} = \bar{0}$ עבור $\alpha_i \in F$. לכן

$$\alpha_0 + \alpha_1 x + \dots + \alpha_{n-1} x^{n-1} = 0$$

ולכן $\alpha_0 + \dots + \alpha_{n-1} x^{n-1} \in \langle f(x) \rangle$. זה קורה רק כאשר

$$f(x) \mid \alpha_0 + \dots + \alpha_{n-1} x^{n-1}$$

אבל זה לא ייתכן כי $\deg(f(x)) = n > n-1$. לכן בהכרח זהו פולינום האפס ($\alpha_i = 0$ לכל i), ולכן הקבוצה בת"ל.

פורשת: יהי $\bar{g} = g(x) + \langle f(x) \rangle \in F[x]/\langle f(x) \rangle$ עם נציג $g(x) \in F[x]$. נבצע חלוקה אוקלידית $g(x) = q(x)f(x) + r(x)$ כאשר $\deg r(x) < n$. לכן

$$\bar{g} = \bar{r} \pmod{f(x)}$$

והרי $\bar{r} \in \text{Span}\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$.

ב. נשתמש ביחס $\bar{0} = x^3 - x^2 - 1$. כלומר $x^3 = x^2 + 1$ ולכן

$$\overline{x^4 - x^3 + x - 2} = \overline{x(x^2 + 1) - (x^2 - 1) + x - 2} = \overline{x^3 - x^2 + 2x - 1} = \overline{2x}$$

שאלה 6 (חזרה לשיטת הרדוקציה למי ששכח). יהי $f(x) \in \mathbb{Z}[x]$ ויהי p מספר ראשוני. נסמן ב- $\mathbb{Z}/p\mathbb{Z}$ את הומומורפיזם ההטלה. אפשר להרחיב את φ לפונקציה

$$\psi: \mathbb{Z}[x] \rightarrow (\mathbb{Z}/p\mathbb{Z})[x]$$

שפשוט "עושה מודולו" לכל מקדם של הפולינום, והיא עדיין הומומורפיזם של חוגים. נניח ש- $\deg \psi(f(x)) = \deg f(x)$ וגם $\psi(f(x))$ אי פריק. הוכיחו כי $f(x)$ אי פריק. הדרכה: נניח בשלילה ש- $f(x) = g(x)h(x)$ הוא פירוק אמיתי (כלומר לאיברים לא הפיכים). שימו לב כי $\psi(f(x)) = \psi(g(x))\psi(h(x))$ ועכשיו משהו בדרגות הפולינומים לא מסתדר.

פתרון. היות ש- $g(x)$ ו- $h(x)$ לא הפיכים מתקיים

$$\deg g(x), \deg h(x) \geq 1$$

ולכן

$$\deg h(x) < \deg h(x) + \deg g(x) = \deg f(x)$$

אבל $\psi(f(x))$ אי פריק ולכן אחד מבין $\psi(g(x)), \psi(h(x))$ הוא הפיך. בלי הגבלת כלליות $\psi(g(x))$ הפיך ולכן $\deg \psi(g(x)) = 0$. כעת

$$\deg f(x) = \deg \psi(f(x)) = \deg \psi(g(x)) + \deg \psi(h(x)) = \deg \psi(h(x)) \leq \deg h(x)$$

אבל לפי החישוב שעשינו קודם $\deg h(x) < \deg f(x)$ בסתירה.

בהצלחה!