

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 $n, m \in \mathbb{N}$.

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. $\mathbb{Z}/5\mathbb{Z}$

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 $f(x + 1)$.

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

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

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

ב. נניח $a_0 \neq 0$, ונתבונן בפולינום $\tilde{f}(x) = a_0 x^n + \dots + a_{n-1} x + a_n$ שבו הפכנו את סדר המקדמים של f . הוכיחו בעזרת הסעיף הקודם שאם \tilde{f} מקיים את קריטריון איזונשטיין, אז f אי פריק.

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

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

הוא אי פריק בחוג $\mathbb{Z}[x]$.

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.

שאלה 8 (העשרה). א. יהי $f(x) \in \mathbb{Z}[x]$ פולינום פריק, 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).

בהצלחה!