

תזכורת

R חוג קומוטטיבי עם יחידה
 R תחום אוקלידי(חלוקה עם שארית) $R \Leftarrow$ תחום ראשי(כל האידיאלים מהצורה $\langle a \rangle$
כאשר $a \in R$) $R \Leftarrow$ תחום פריקות יחידה(כל איבר מתפרק בצורה יחידה עד כדי מכפלה
בהפיך לגורמים אי פריקים) $R \Leftarrow$ תחום שלמות(אין מחלקי אפס).

הגדרה

$a \in R$ אי פריק אם $a = bc$ או c הפיכים לכל $b, c \in R$.

טענות

רוצים לבדוק מתי $p(x) \in \mathbb{F}[x]$ (כאשר \mathbb{F} שדה) הוא פריק?

1. יהי $p(x) \in \mathbb{F}[x]$, $\deg(p(x)) \leq 3$. אזי $p(x)$ אי-פריק אם ורק אם אין ל- $p(x)$ שורש ב- \mathbb{F} .

2. $p(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$. אם $\frac{r}{s} = t \in \mathbb{Q}$ הוא שורש של $p(x)$ (כאשר r, s שלמים זרים) אזי $s \mid a_n, r \mid a_0$.

3. $p(x) \in \mathbb{F}[x]$ אי-פריק אם ורק אם $p(ax + b)$ אי-פריק לכל $a \in \mathbb{F}^*, b \in \mathbb{F}$.

משפט גאוס

יהי U תחום פריקות יחידה, $\mathbb{F} = \text{Frac}(U) = \left\{ \frac{a}{b} \mid a, b \in U, b \neq 0 \right\}$ (שדה השברים של U).
 $p(x) \in U[x]$ לא ניתן לפירוק למכפלת פולינומים לא קבועים שדרגתם קטנה מ- $\deg(x)$
 $\Leftrightarrow p(x)$ אי-פריק ב- $\mathbb{F}[x]$.

דוגמה

$2(x-1) = 2x-2 \in \mathbb{Z}[x]$ אי פריק
 $2x-2 \in \mathbb{Q}[x]$ אי-פריק

תרגיל

$$f(x) = 8x^3 - 6x - 1$$

האם f אי-פריק ב- $\mathbb{Q}[x]$?

פתרון

לפי טענה 1, מספיק לבדוק אם יש לו שורש ב- \mathbb{Q} . לפי טענה 2, אם $\frac{r}{s}$ הוא שורש של f , אז $s = 1, 2, 4, 8 \leftarrow s$ ו- $r = \pm 1 \leftarrow r$.
בודקים את כל האפשרויות...

קריטריון אינשטיין

$$p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

אם קיים ראשוני p כך ש:

א. $p \nmid a_n$

ב. $p \mid a_0, \dots, a_{n-1}$

ג. $p^2 \nmid a_0$

אזי הפולינום אי-פריק ב- $\mathbb{Q}[x]$.

תרגיל

בדקו שהפולינום הבא אי-פריק: $p \in \mathbb{Z}$ ראשוני

$$g(x) = x^{p-1} + x^{p-2} + \dots + x + 1$$

פתרון

הפולינום הק-דיקלוטומי:

$$g(x) = \frac{x^p - 1}{x - 1}$$

$$h(x) = (x - 1)g(x) = x^p - 1$$

נחליף את x ב- $x + 1$:

$$x \cdot g(x + 1) = h(x + 1) = (x + 1)^p - 1 = \sum_{k=1}^p \binom{p}{k} x^k + 1 - 1 = \sum_{k=1}^p \binom{p}{k} x^k$$

מחלקים ב x ומקבלים:

$$g(x+1) = x^{p-1} + \dots + \binom{p}{k} x^{k-1} + \dots + p$$

יודעים ש $\binom{p}{k} \mid p$ כאשר $1 \leq k \leq p-1$, וכמוכן $p \nmid p^2$, לכן לפי אייזנשטיין $g(x+1)$ אי פריק $\Leftrightarrow g(x)$ אי-פריק.

טענה

יהי R תחום, יהי \mathbb{F} שדה, ויהי $\sigma : R \rightarrow \mathbb{F}$ הומומורפיזם של חוגים. ניתן להגדיר הומומורפיזם $\sigma^* : R[x] \rightarrow \mathbb{F}[x]$ ע"י

$$\sigma^*(a_n x^n + \dots + a_0) = \sigma(a_n) x^n + \dots + \sigma(a_0)$$

משפט(שיטת הרדוקציה)

R תחום, \mathbb{F} שדה, $\sigma : R \rightarrow \mathbb{F}$ הומומורפיזם, $p(x) \in R[x]$. נגדיר $g(x) = \sigma^*(p(x))$. אם $\deg(g(x)) = \deg(p(x))$ וגם $g(x)$ אי-פריק ב $\mathbb{F}[x]$ אזי $p(x)$ לא ניתן להצגה כמכפלת פולינומים לא קבועים מדרגה קטנה מ $p(x)$.

הוכחה

$$f(x) = g(x) h(x)$$

↓

$$\sigma^*(f) = \sigma^*(g) \sigma^*(h)$$

תרגיל

הראו ש $f(x) = 8x^3 - 6x - 1 \in \mathbb{Z}[x]$ הוא אי-פריק בעזרת שיטת הרדוקציה.

פתרון

נבחר $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}_p$, σ הוא מודולו p .

נעבור על p ים קטנים עד שנמצא אחד שמקיים את תנאי המשפט.

$$\sigma^*(f(x)) = 1, \quad \deg(1) < \deg(f) \quad p = 2$$

$$g(x) = \sigma^*(f(x)) = 2x^3 + 2 + 2(x^3 + 1) \quad p = 3$$

$$\sigma^*(f) = 3x^3 - x - 1 \quad p = 5$$

מצויים $0, \dots, 4$ ובודקים שאין שורשים מוד 5 $\Leftrightarrow \sigma^*(f)$ אי-פריק, ואז לפי המשפט f פריק.