להלן $\mathbb{F} = q(R)$ - שדה השברים מעל R

קריטריון אייזנשטיין

יהי $f \in R[x]$ פולינום על R תחום שלמות כלשהו. רוצים להוכיח שf אי פריק מעל R.

הגדרה: פירוק מעל R נקרא "לא אמיתי" אם אחד הגורמים הוא סקלר.

הערה: אם $f \in R[x]$ פריק מעל R, אז:

- או שיש לו פירוק אמיתי - ואז הוא פריק גם מעל $\mathbb{F}$
- או שאין לו פירוק אמיתי - ואז הוא אי־פריק מעל $\mathbb{F}$

קריטריון אייזנשטיין

יהי $M \lhd R$ אידאל מקסימלי. נניח ש$f = a_n x^n + \cdots + a_0 \in R[x]$ כך ש

$$a_{n-1}, a_{n-2}, \ldots a_1, a_0 \in M$$

$$a_n \notin M$$

$$a_0 \notin M^2$$

אזי אין לf פירוק אמיתי מעל R.

הוכחה

נניח שיש פירוק אמיתי

$$f = gh$$

$$g = \cdots + b_0 \qquad h = \cdots + c_0$$

נתבונן בפירוק מודולו M, כלומר בחוג

$$\mathrm{R[x]}/\mathrm{M \cdot R[x]} = \mathrm{R[x]}/\mathrm{M[x]} \cong \left(\underbrace{\mathrm{R}/\mathrm{M}}_{\text{field}}\right)[x]$$

בחוג המנה $\overline{f} = a_n x^n = \overline{g} \cdot \overline{h}$ הפירוקים היחידים של x^n מעל השדה R/M הם $\begin{matrix}\overline{g} \sim x^i \\ \overline{h} \sim x^{n-i}\end{matrix}$, כלומר

$$g = b_i x^i + \cdots + b_0 \Rightarrow b_0 \in M$$

$$h = c_{n-1} x^{i-i} + \cdots + c_0 \in M$$

ולכן $a_0 = b_0 \cdot c_0 \in M^2$ - סתירה!

מקרה פרטי

$R=\mathbb{Z}$. נניח שp ראשוני, $f=a_nx^n+\cdots+a_0$ ומתקיים

$$p|a_{n-1},\dots a_0$$

$$p\nmid a_n$$

$$p^2\nmid a_0$$

אז לf אין פירוק אמיתי מעל $\mathbb{Z}$.

דוגמאות

$f\left(x\right)=x^5-7x^2+70x-14$ - לפי קריטריון אייזנשטיין עם $p=7$, f אי פריק מעל $\mathbb{Z}$.

הערה

הקריטריון לא מדד ל$f\left(x\right)=x^5-7x^2+70-49$, או ל$f\left(x\right)=-7x^5-7x^2+10x^2-14$.

דוגמה

p ראשוני

$$x^p-1=\left(x-1\right)\left(x^{p-1}+x^{p-2}+\cdots+1\right)$$

נסמן $f\left(x\right)=\dfrac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+1$, ואז

$$f\left(x+1\right)=\frac{\left(x+1\right)^p-1}{\left(x+1\right)-1}=\sum_{i=0}^{p}\binom{p}{i}x^{i-1}=x^{p-1}+\binom{p}{p-1}x^{p-2}+\binom{p}{p-2}x^{p-3}+\cdots+\binom{p}{1}x^0$$

למשל עבור $p=5$,

$$f\left(x+1\right)=x^4+5x^3+10x^2+10x+5$$

ידוע ש$p|\binom{p}{k}=\dfrac{p!}{k!\left(p-k\right)!}$ לכל $0<k<p$.
p מחלק את כל המקדמים פרט לראשון.
המקדם הראשון = 1.
המקדם החופשי = p ולא מתחלק בp^2
$\Leftarrow$הפולינום $f\left(x+1\right)$ אי פריק
$\Leftarrow$ הפולינום $f\left(x\right)$ אי פריק

תרגיל

$$p = \cos\frac{2\pi}{9} + i\sin\frac{2\pi}{9}$$

מאפס את הפולינום $\left(x^3-1\right)\left(x^6+x^2+1\right) = x^9-1$
העזרו בקריטריון אייזנשטיין כדי להוכיח שx^6+x^3+1 אי פריק.

מסקנה

$$\dim_{\mathbb{Q}} \mathbb{Q}\left[p_9\right] = 6$$

הערה

יהיו $\mathbb{F}$ שדה ו$f \in \mathbb{F}m[x]$.

$$\mathbb{F}[x]/\langle f\rangle = \{g + \langle f\rangle | g \in \mathbb{F}\left[x\right]\} = \left\{ r + \langle f\rangle \middle| \begin{array}{c} r \in \mathbb{F}\left[x\right] \\ \deg\left(r\right) < n \end{array} \right\}$$

מתי $r + \langle f\rangle = 0 + \langle f\rangle$? זה קורה אם ורק אם $f|r$. אבל אם $\deg r < \deg f$, זה יכול לקרות רק אם $r = 0$.
כלומר כל האיברים כאן שונים זה מזה, כי

$$r_1 + \langle f\rangle = r_2 + \langle f\rangle \Rightarrow f|\left(r_1 - r_2\right) \Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$$

מסקנה

$$\mathbb{F}\left[x\right] = \mathrm{span}_{\mathbb{F}}\left\{1, x, \ldots x^{n-1}\right\}$$

זה בסיס!

הוכחנו ש

$$\dim_{\mathbb{F}}\left(\mathbb{F}[x]/\langle f\rangle\right) = \deg f$$

מסקנה

אם $\mathbb{F} \subseteq K$ שדות, $a \in K$,

$$K \supseteq \mathbb{F}[a] = \mathrm{Im}\Phi_a \cong {}^{\mathbb{F}[x]}/_{\ker \Phi_a} = {}^{\mathbb{F}[x]}/_{\langle g_a \rangle}$$

אז

$$\dim_{\mathbb{F}} \mathbb{F}[a] = \deg g_a$$

דוגמה

$\dim_{\mathbb{Q}} \mathbb{Q}\left[\sqrt[3]{2}\right] = 3$ כי $x^3 - 2$ הוא הפולינום המינימלי של $\sqrt[3]{2}$.

הוכחה

$x^3 - 2$ אי פריק מעל $\mathbb{Z}$ לפי קריטריון אייזנשטיין$(p = 2)$

דוגמה

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

$$(3x + (1 + 2\xi))\left(x + \frac{3 - 2\xi}{3}\right) = 3x^2 + 4x + 3$$

- אי פריק מעל $\mathbb{R}$ ומעל $\mathbb{Z}$.
- פריק מעל $\mathbb{Q}\left[\sqrt{-5}\right] = \mathbb{Q}[\xi]$
- אי פריק מעל $\mathbb{Z}[\xi]$

הלמה של גאוס

מעכשיו ננית שR תחום פריקות יחידה.

הגדרה

$$f = a_n x^n + \cdots + a_0 \in R[x]$$

התכולה של f = $c(f)$ = מכפלת הגורמים הראשוניים המשותפים של כל המקדמים.

דוגמאות

- $c\left(3x^2+9x+12\right)=3$ מעל $\mathbb{Z}$
- $c\left(a^2x^5+a^2bx^3+12a^4b^5\right)=a^2$ מעל $\mathbb{Q}\left[a,b\right]$

הגדרה

f נקרא פרימיטיבי אם $c\left(f\right)=1$. שימו לב שלכל פולינום f,

$$\hat{f}=\frac{1}{c\left(f\right)}f\left(x\right)\in R\left[x\right]$$

$\hat{f}$ תמיד פרימיטיבי.

הערה

נניח ש$f\in R\left[x\right]$, $a\in R$, אזי

$$c\left(a\cdot f\right)=a\cdot c\left(f\right)$$

הלמה של גאוס(גירסה I)

המכפלה של פולינומים פרימיטיביים היא פרימיטיבית.

הוכחה

נניח שf,g פרימיטיביים, ונניח $p|c\left(fg\right)$ עבור ראשוני p.

$$f\cdot g\equiv 0\pmod{p}$$

$$\Downarrow$$

$$f\cdot g=0\in\left({}^{\mathrm{R}}\!/_{\mathrm{pR}}\right)\left[x\right]$$

מכיוון ש${}^{\mathrm{R}}\!/_{\mathrm{pR}}$ תחום שלמות, גם $\left({}^{\mathrm{R}}\!/_{\mathrm{pR}}\right)\left[x\right]$ תחום שלמות, ולכן $f\equiv 0$ או $g\equiv 0$ - בסתירה לפרימיטיביות של f וg.

מסקנה - הלמה של גאוס (גירסה II)

$$c\left(f\cdot g\right)=c\left(f\right)\cdot c\left(g\right)$$

הוכחה

$$f = c(f)\cdot\hat{f} \qquad g = c(g)\cdot\hat{g}$$

$$c(fg) = c\left(c(f)\cdot\hat{f}\cdot c(g)\cdot\hat{g}\right) = c(f)\cdot c(g)\cdot \underbrace{c\left(\hat{f}\hat{g}\right)}_{=1} = c(f)\cdot c(g)$$

הלמה של גאוס(גירסה III)

יהי $f\in R[x]$ פרימיטיבי ואי פריק מעל R, אזי f אי פריק מעל $\mathbb{F}$.

הוכחה

נניח שf מתפרק מעל $\mathbb{F}$. אז יש פולינומים $g,h\in R[x]$ וסקלר $a\in R$ כך ש$f=\frac{1}{a}\cdot g\cdot h$.

הערה: כל פולינום מעל $\mathbb{F}$ אפשר לכתוב בצורה יחידה(עד כדי חברות)

$$\frac{a}{b}\cdot f$$

כאשר $a,b\in R$ זרים, $f\in R[x]$ פרימיטיבי.ו

$\Leftarrow b\cdot f = a\cdot gh \Leftarrow$

$$b = b\cdot c(f) = c(bf) = c(a\cdot gh) = a\cdot c(gh) = a$$

$\Leftarrow f = gh$ פירוק מעל R.

הערה

יהיו $f,g\in R[x]$
$f|g$ מעל $R \Leftrightarrow c(f)\,|\,c(g)$ וכן $\hat{f}|\hat{g}$

הוכחה

$$f = c(f)\cdot\hat{f} \qquad g = c(g)\cdot\hat{g}$$

$\Rightarrow$ טריוויאלי

$\Leftarrow$ נניח ש$f|g$, כלומר $g=f\cdot h, h\in R[x]$, אז $c(f)\,|\,c(g) \Leftarrow c(g)=c(f)\cdot c(h)$, ו

$$\hat{g} = \frac{1}{c(g)}\cdot g = \widehat{fh} = \frac{1}{c(fh)}\cdot fh = \left(\frac{1}{c(f)}\cdot f\right)\cdot\left(\frac{1}{c(h)}\cdot h\right) = \hat{f}\cdot\hat{h}$$

$\Leftarrow \hat{f}|\hat{h}$

משפט(הלמה של גאוס, IV)

יהי R תחום פריקות יחידה. אזי $R[x]$ תחום פריקות יחידה.

מסקנה

$\begin{matrix}\mathbb{Z}[x_1,\dots x_n]\\ \mathbb{F}[x_1,\dots x_n]\end{matrix}$ כולם תחומי פריקות יחידה.

הוכחת המשפט

תחום פריקות יחידה = אטומי +כל אי פריק ראשוני.
יהי f פולינום מעל R. הוא פולינום של $\mathbb{F}$ ולכן יש לו פירוק לגורמים אי פריקים מעל $\mathbb{F}$:

$$f = g_1 \cdots g_n$$

כאשר $g_i \in \mathbb{F}[x]$ אי פריקים. כל g_i אפשר לכתוב כמכפלה

$$g_i = \frac{a_i}{b_i} \cdot h_i$$

$h_i \in R[x]$ פרימיטיבי, a_i, b_i זרים.

$$f = \frac{a}{b} \cdot h_1 \cdots h_n$$

$$\Downarrow$$

$$bf = a \cdot h_1 \cdots h_n$$

$$f = \underbrace{\square}_{\text{scalar}} \cdot h_1 \cdots h_n$$

כאשר $h_1, \dots h_n$ פרימיטיבים + אי פריקים מעל $\mathbb{F}$ $\Leftarrow$ אי פריק מעל R.
נשאר להוכיח שכל אי פריק בחוג $R[x]$ הוא ראשוני.
יהי f פולינום אי פריק בחוג $R[x]$(בפרט f פרימיטיבי). נניח $f|gh$ מעל R.
מכיוון שf אי פריק מעל $\mathbb{F}$, f ראשוני שם, לכן $f|g$ או $f|h$ מעל $\mathbb{F}$.
לכן לפי הטענה הקודמת, $f|g$ או $f|h$ מעל R.