Дефиниција

Нека су $f(x), g(x) \in k[x]$, k поље.

Заједнички дјелитељ полинома $f(x), g(x)$ је сваки полином $c(x) \in k[x]$ такво да $c(x) \mid f(x)$ и $c(x) \mid g(x)$.

У случају да је бар један од полинома $f(x), g(x)$ ненулти, онда је $НЗД(f(x), g(x))$ заједнички дјелитељ највећег степена и водећег коефицијента 1.

Ако је $f(x) = g(x) = 0$, онда је $НЗД(f(x), g(x)) = 0$.

Теорема

Нека је k поље и $f(x), g(x) \in k[x]$, а $d(x) = НЗД(f(x), g(x))$. Онда постоје $s(x), t(x) \in k[x]$ такво да

$$d(x) = s(x) f(x) + t(x) g(x).$$

Последица

Нека је $f(x), g(x) \in k[x]$, k поље. Онда за сваки заједнички дјелитељ $c(x)$ полинома f и g вриједи $c(x) \mid d(x)$.

Дефиниција

Елемент p у домену R је <u>иредуцибилан</u> ако $p \neq 0$ и p није инвертибилан и ако за свако $p = u \cdot v$ у R вриједи да је u или v инвертибилан елемент.

<u>Примјер</u>

У скупу $\mathbb{Z}$, сваки прост број је иредуцибилан.

<u>Лема</u>

Ако је k поље, онда је полином $p(x) \in k[x]$ иредуцибилан ако и само ако је $\deg(p(x)) = n \geq 1$ и не постоји факторизација у $k[x]$ облика $p(x) = g(x)h(x)$, тако да су степени полинома $g(x)$ и $h(x)$ мањи од n.

<u>Доказ:</u>

$h(x) \in k[x]$ је инвертибилан ако и само ако $\deg(h(x)) = 0$.

Нека је $p(x) \in k[x]$ иредуцибилан,

$p(x) = g(x) \cdot h(x)$.

Јасно је да је $\deg(p(x)) \geq 1$.

С друге стране, због иредуцибилности $p(x)$, онда је $g(x)$ или $h(x)$ инвертибилан.

... $\deg(g(x))$ или $\deg(h(x))$

Што значи да је $\deg(g(x))$ или $\deg(h(x))$ $= \deg(p(x))$.

Супротан смјер: за вјежбу.

Иредуцибилност полинома зависи од прстена у ком посматрамо полином.
На примјер, $p(x) = x^2+1$ је иредуцибилан у $\mathbb{R}[x]$, али
$p(x) = (x+i)(x-i)$ у $\mathbb{C}[x]$.

Такође, ако посматрамо полином $p(x) = 2x+2$ у $\mathbb{Z}[x]$, закључујемо да $p(x)$ није иредуцибилан, јер

$$p(x) = 2\cdot(x+1)$$

а 2 ни $(x+1)$ нису инвертибилни.

Последица

Нека је k поље, а $f(x) \in k[x]$ квадратни или кубни полином. Онда је $f(x)$ иредуцибилан у $k[x]$ ако и само ако $f(x)$ нема нула (корјена) у k.

доказ: тривијално.

Примјер

Иредуцибилни полиноми малог степена у $\mathbb{Z}_2[x]$

степен 2: x^2+x+1

степен 3: x^3+x+1, x^3+x^2+1

степен 4: x^4+x^3+1, x^4+x+1, $x^4+x^3+x^2+x+1$

Иредуцибилни (монични) квадратни и кубни полиноми у $\mathbb{Z}_3[x]$

степен 2: x^2+1, x^2+x-1, x^2-x-1

степен 3: x^3-x+1, x^3+x^2-x+1, x^3-x^2+1, x^3-x^2+x+1

Лема

Нека је k поље, $p(x), f(x) \in k[x]$, а $d(x) = НЗД(p(x), f(x))$.

Ако је $p(x)$ моничан и иредуцибилан, онда

$$d(x) = \begin{cases} 1 & \text{ако } p(x) \nmid f(x) \\ p(x) & \text{ако } p(x) \mid f(x) \end{cases}$$

доказ:

тривијално.

Теорема (Еуклид)

Нека је k поље и $f(x), g(x) \in k[x]$

Нека је K поље и $f(x), g(x) \in K[x]$.

Ако је $p(x)$ иредуцибилан полином у $K[x]$, а $p(x) \mid f(x) \cdot g(x)$ онда $p(x) \mid f(x)$ или $p(x) \mid g(x)$.

Општије, ако $p(x) \mid f_1(x) \cdots f_n(x)$, онда $p(x) \mid f_i(x)$ за неко $i \in \{1, 2, \ldots, n\}$.

Скица доказа

Нека $p(x) \mid f(x) \cdot g(x)$ и $p(x) \nmid f(x)$.

Пошто је $p(x)$ иредуцибилан, онда $НЗД(p(x), f(x)) = 1$.

Слиједи

$$1 = s(x) \cdot p(x) + t(x) \cdot f(x)$$

за неке полиноме $s(x), t(x) \in K[x]$.

Одавде

$$g(x) = s(x) \cdot p(x) \cdot g(x) + t(x) \cdot \underbrace{f(x) \cdot g(x)}_{\text{дјељив са } p(x)}$$

Дакле, $p(x) \mid g(x)$.

Дефиниција

Два полинома $f(x), g(x) \in K[x]$, K је поље, су релативно проста ако је

$НЗД(f(x), g(x)) = 1$.

Последица

Нека су $f(x), g(x), h(x) \in k[x]$, k је поље, а $h(x)$ и $f(x)$ релативно прости.

Ако $h(x) \mid f(x)\cdot g(x)$ онда $h(x) \mid g(x)$.

доказ: вјежба.

Обновити Еуклидов алгоритам у прстену полинома $k[x]$, k је поље.

Последица

Нека је k потпоље поља K.

Ако су $f(x), g(x) \in k[x]$, онда

$$НЗД_{k[x]}(f(x), g(x)) = НЗД_{K[x]}(f(x), g(x)).$$

доказ

Посматрамо Еуклидов алгоритам дијељења у $K[x]$.

$$g(x) = Q[x]\cdot f(x) + R[x], \quad (*)$$

$Q[x]$ и $R[x] \in K[x]$, $R[x]=0$ или $\deg(R[x]) \le \deg(f(x))$.

Слично, Еуклидов алгоритам дијељења у $k[x]$

у $K[x]$ у је

$$g(x) = q(x)\cdot f(x) + r(x), \quad (**)$$

$q(x)$ и $r(x) \in k[x]$, $r(x)=0$ или $\deg(r(x)) \le \deg(f(x))$.

$k[x] \subseteq K[x]$.

Идентитет (**) је такође у $K[x]$.

Из чињенице да при датим условима имамо јединственост количника и остатка у Е. алгоритму, онда

$r(x) = R[x]$, $q(x) = Q[x]$

То значи да комплетан „Еуклидов низ" остаје у „најманем" прстену полинома над одређеним пољем, чиме је и резултат у њему.

Дакле, имамо да је НЗД$_{k[x]}(f(x), g(x))$ исто што и НЗД$_{K[x]}(f(x), g(x))$.

<u>пример</u>

НЗД$(x^3-x^2+x-1,\ x^4-1) = x^2+1$

без обзира да ли посматрамо полиноме x^3-x^2+x-1 и x^4-1 из $\mathbb{R}[x]$ или $\mathbb{C}[x]$.

Теорема

Ако је k поље, онда се сваки полином $f(x) \in k[x]$ степена ≥ 1 може представити као производ константе и моничних иредуцибилних полинома.

Посебно, ако је

$$f(x) = a \cdot \prod_{i=1}^{m} p_i(x), \quad f(x) = b \cdot \prod_{i=1}^{n} q_i[x],$$

гдје су a и b ненулте константе, а p_i и q_j монични иредуцибилни полиноми, онда $a=b$, $m=n$, те

$$q_i = p_{\pi(i)}, \text{ за } \pi \in S_n.$$

Примјер

Нека је $f(x) \in k[x]$, а r је коријен од $f(x)$ у k. Дакле, $f(r)=0$.

Онда $f(x) = (x-r)\,g(x)$, $g(x) \in k[x]$.

Дакле, $f(x)$ није иредуцибилан изузев ако $\deg(f) = 1$.

Теорема

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

$\subseteq \mathbb{Q}[x]$.

Сваки рационалан корijен r од $f(x)$ има форму $\frac{b}{c}$ гдје $b \mid a_0$ и $c \mid a_n$, подразумијевајући да је НЗД$(b,c)=1$.

<u>доказ:</u> вјежба.

<u>Дефиниција</u>

Комплексни број α називамо <u>алгебарски цијели</u> ако је α корijен <u>моничног</u> полинома $f(x) \in \mathbb{Z}[x]$.

<u>Посљедица</u>

Рационални број z који је и алгебарски цијели мора бити у $\mathbb{Z}$.

Другим ријечима, ако је $f(x) \in \mathbb{Z}[x]$ монични полином, онда сваки рационални корijен од $f(x)$ је цијели број који дијели слободни члан.

<u>Примјер</u>

Посматрајмо $f(x) = x^3 + 4x^2 - 2x - 1 \in \mathbb{Q}[x]$.

Ако $f(x)$ није иредуцибилан, онда мора

Ако f ...

имати нула у $\mathbb{Q}$.

Једини „кандидати" за нуле (коријене) су 1 или −1.

Пошто $f(1) \neq 0$, $f(-1) \neq 0$, онда закључујемо да је f иредуцибилан.

− <u>Хомоморфизми прстена</u> (обновити)

$$f: A \to R \text{ (хомоморфизам прстена)}$$

$\mathrm{Ker} f$, $\mathrm{Im} f$.

− идеал A прстена R

(1) $0 \in A$

(2) ако $a, b \in A \Rightarrow a+b \in A$

(3) ако $a \in A$, $r \in R \Rightarrow ra \in A$.

Тривијални идеали прстена R су $\{0\}$ и R.

Ако је идеал $I \neq R$, $I \neq \{0\}$, онда кажемо да је I <u>нетривијалан</u> или <u>прави</u> идеал.

<u>примјер</u>

... R прстен, a, $b_1, b_2, \dots, b_n \in R$

Ако је R прстен, ...

онда је

$$I = \left\{ \sum_{i=1}^{n} r_i b_i \mid r_i \in R \right\}$$

идеал у R. Пишемо $I = (b_1, b_2, \dots, b_n)$ и кажемо да је I генерисан са $b_1, b_2, \dots, b_n$.

Посебно, ако је $n = 1$, онда $I = (b) = \{ rb \mid r \in R \}$ кажемо да је I <u>главни</u> идеал.

Примјетимо да $R = (1)$, $\{0\} = (0)$.

У прстену $\mathbb{Z}$, скуп парних бројева је идеал генерисан елементом 2.

<u>Лема</u> Ако је $f : A \to R$ хомоморфизам прстена, онда је $\operatorname{Ker} f$ <u>идеал у</u> A, а $\operatorname{Im} f$ <u>потпрстен у</u> R.

Посебно, ако су A и R ненулти прстени, онда је $\operatorname{Ker} f$ прави идеал.

<u>Примјер</u>

(1) Ако идеал I садржи 1 онда $I = R$.

(1) [illegible]

(2) Једини идеали поља R су тривијални $\{0\}$ и R сам.

Лема

Хомоморфизам прстена $f: A \to R$ је инјекција ако и само ако $\mathrm{Ker} f = \{0\}$.

доказ: вјежба.

Посљедица

Ако је $f: K \to R$ хомоморфизам прстена, гдје је K поље, а $R \neq \{0\}$, онда $\mathrm{Ker} f = \{0\}$, односно f је инјекција.