Polynómy

13. mája 2024

Korene polynómov

Definícia

Nech F je pole a F' je jeho nadpole. Prvok $c \in F'$ nazývame *koreňom* polynómu $f(x) \in F[x] \subset F'[x]$, ak $f(c) = 0$ (t.j. po dosadení c do polynómu F dostaneme 0).

Príklad

Číslo i je koreňom polynómu $x^2 + 1$, lebo $i^2 + 1 = 0$.

Korene polynómov

Lema

Ak $f(x) \in F[x]$, kde F je pole, a $c \in F$, tak zvyšok polynómu $f(x)$ po delení polynómom $x - c$ je rovný $f(c)$, t.j. existuje polynóm $g(x) \in F[x]$ taký, že

$$f(x) = (x - c)g(x) + f(c). \tag{1}$$

Lema

Nech F je pole a F' je jeho nadpole. Nech $f(x) \in F[x]$. Potom $c \in F'$ je koreňom $f(x)$ práve vtedy, keď $x - c \mid f(x)$ v $F'[x]$, t.j. existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x - c)$.

Dosadzovací homomorfizmus

Definícia

Nech R je komutatívny okruh s jednotkou. *Polynomickou funkciou* nad R budeme rozumieť ľubovoľnú funkciu $f\colon R \to R$ určenú predpisom

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

pre nejaké $n \in \mathbb{N}$ a $a_1 \dots a_n \in R$.

Okruh polynomických funkcií: $(F\langle x\rangle, +, \cdot)$
polynóm: $p = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$
funkcia: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$

$$\varphi\colon F[x] \to F\langle x\rangle$$

Počet koreňov

Tvrdenie

Nech F je pole a $f(x) = a_n x^n + \cdots + a_1 x + a_0$ a $a_n \neq 0$. Potom $f(x)$ má najviac n koreňov. (Stručne: Pre nenulové polynómy je počet koreňov menší alebo rovný jeho stupňu.)

Dôkaz – matematickou indukciou.

$$f(x) = (x = c)^k g(x)$$

Polynomické funkcie

Tvrdenie

Ak F je nekonečné pole tak polynomická funkcia $f\colon F \to F$

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

sa rovná nulovej funkcii práve vtedy, keď $a_0 = a_1 = \cdots = a_n = 0$, t.j. vtedy, keď sú všetky koeficienty nulové.

$$F[x] \cong F\langle x \rangle$$

Dosadzovací homomorfizmus

Ak $b \in R$, dá sa b dosadiť do polynómu
$f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in R[x]$.

$$f_b \colon R[x] \to R$$
$$f_b \colon f \mapsto a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0$$

Násobné korene

Definícia

Nech F' je nadpole poľa F, $f(x) \in F[x]$ a c je koreň $f(x)$. Hovoríme, že *násobnosť* koreňa c je k (alebo tiež, že c je k-násobný koreň $f(x)$), ak $(x-c)^k \mid f(x)$ (t.j. ak existuje polynóm $g(x) \in F'[x]$ taký, že $f(x) = g(x)(x-c)^k$) a súčasne $(x-c)^{k+1} \nmid f(x)$.
Pre $k = 1$ voláme k-násobný koreň *jednoduchý koreň* polynómu $f(x)$, ak $k > 1$ tak hovoríme o násobnom koreni.

Príklad

Čísla ± 1 sú dvojnásobné korene polynómu $x^4 - 2x^2 + 1$, lebo $x^4 - 2x^2 + 1 = (x^2-1)^2 = (x-1)^2(x+1)^2$

Hornerova schéma

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

$$\begin{array}{c|ccccc|}
 & 1 & -3 & 0 & 2 & -1 \\
2 & & 2 & -2 & -4 & -4 \\
\hline
 & 1 & -1 & -2 & -2 & \boxed{-5}
\end{array}$$

$$x^4 - 3x^3 + 2x - 1 = (x^3 - x^2 - 2x - 2)(x - 2) - 5$$

Hornerova schéma

$$
\begin{array}{c|cccc}
 & a_n & a_{n-1} & a_{n-2} & \dots \\
c & & a_n c & (a_n c + a_{n-1})c & \dots \\
\hline
 & a_n & a_n c + a_{n-1} & a_n c^2 + a_{n-1} c + a_{n-2} & \dots
\end{array}
$$

$$
\begin{array}{cc|}
\dots & a_0 \\
\dots & (a_n c^{n-1} + a_{n-1} c^{n-2} + \dots + a_1)c \\
\hline
\dots & a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0 = f(c)
\end{array}
$$

Racionálne korene polynómu s celočíselnými koeficientami

Tvrdenie

Ak $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *je polynóm s celočíselnými koeficientami a racionálne číslo* $c = \frac{p}{q}$ *je koreň* $f(x)$ *(pričom* $\gcd(p,q) = 1$*, t.j. racionálne číslo c je zapísané v základnom tvare), tak*

$$p \mid a_0 \qquad a \qquad q \mid a_n.$$

Racionálne korene polynómu s celočíselnými koeficientami

$$f(c) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0 = 0$$

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

$$-a_n p^n = (a_{n-1} p^{n-1} + \cdots + a_1 p q^{n-2} + a_0 q^{n-1}) q$$

$$q \mid a_n p^n \wedge \gcd(p, q) \sim 1 \Rightarrow q \mid a_n$$

Podobne dostaneme

$$-a_0 q^n = (a_n p^{n-1} + a_{n-1} p^{n-2} q + \cdots + a_1 q^{n-1}) p,$$

čiže $p \mid a_0 q^n$, a teda (na základe nesúdeliteľnosti) $p \mid a_0$.

Racionálne korene polynómu s celočíselnými koeficientami

$f(x) = 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6$
$p \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$
$q \in \{1, 2, 3, 4, 6, 8, 12, 24\}$ $\frac{p}{q} \in \{\pm 1, \pm \frac{1}{2}, \pm \frac{1}{3}, \dots\}$

	24	10	-1	-19	-5	6
$\frac{1}{2}$		12	11	5	-7	-6
	24	22	10	-14	-12	$\boxed{0}$
$\frac{1}{2}$		12	17	$\frac{27}{2}$		
	24	34	27	$-\frac{1}{2}$	$\neq 0$	

Racionálne korene polynómu s celočíselnými koeficientami

$$\begin{aligned} f(x) &= 24x^5 + 10x^4 - x^3 - 19x^2 - 5x + 6 \\ &= 24(x - \frac{1}{2})(x + \frac{2}{3})(x - \frac{3}{4})(x^2 + x + 1) \end{aligned}$$

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

Algebraicky uzavreté polia

Definícia

Pole F sa nazýva *algebraicky uzavreté*, ak každý polynóm $f(x) \in F[x]$ stupňa aspoň jedna má v poli F aspoň jeden koreň.

Tvrdenie

Ak F je algebraicky uzavreté pole, tak každý polynóm $f(x)$ je v $F[x]$ rozložiteľný na koreňové činitele.

Algebraicky uzavreté polia

Bez dôkazu spomeňme:

Veta (Základná veta algebry)

Pole komplexných čísel $\mathbb{C}$ je algebraicky uzavreté.

Veta (Steinitz)

Pre každé pole F existuje algebraicky uzavreté nadpole F'.

Korene polynómov v $\mathbb{C}$

Tvrdenie

Ak $f(x) \in \mathbb{R}[x]$ je polynóm s reálnymi koeficientami a $z = a + bi \in \mathbb{C}$ je koreň polynómu $f(x)$, tak aj komplexne združené číslo $\overline{z} = a - bi$ je koreňom polynómu $f(x)$. Pritom násobnosť koreňa $\overline{z}$ je rovnaká ako násobnosť z.

$$\begin{aligned}\overline{f(z)} &= \overline{a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0} \\ &= a_n (\overline{z})^n + a_{n-1} (\overline{z})^{n-1} + \cdots + a_0 \\ &= f(\overline{z})\end{aligned}$$

Dôsledok

Každý polynóm $f(x) \in \mathbb{R}[x]$ nepárneho stupňa má aspoň 1 reálny koreň.

Ireducibilné polynómy

Definícia

Polynóm $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ sa nazýva *normovaný* (alebo tiež *monický*,) ak $a_n = 1$ (vedúci koeficient sa rovná 1).

Definícia

Ak R je obor integrity, tak ireducibilné prvky okruhu $R[x]$ nazývame *ireducibilné polynómy* v $R[x]$.

Ireducibilné polynómy

Tvrdenie

Ak F je pole a $f(x) \in F[x]$ je polynóm stupňa 2 alebo 3, tak polynóm $f(x)$ je ireduciblný v F práve vtedy, keď $f(x)$ nemá koreň v F.

Ireducibilné polynómy

- V $\mathbb{C}[x]$ sú ireducibilné polynómy práve polynómy stupňa 1.
- V $\mathbb{R}[x]$ majú ireducibilné polynómy stupeň 1 alebo 2.

Ireducibilné polynómy

$$f(x) = x^4 + 1$$

Ireducibilný nad $\mathbb{Q}$, nie je ireducibilný nad $\mathbb{R}$, $\mathbb{C}$

$$\begin{aligned} x^4 + 1 &= (x^4 + 2x^2 + 1) - 2x^2 \\ &= (x^2 + 1)^2 - (\sqrt{2}x)^2 \\ &= (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \end{aligned}$$

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

Formálna derivácia

Definícia

Formálna derivácia polynómu $f(x) = \sum_{k=0}^{n} a_k x^k$ je polynóm $Df(x) = \sum_{k=1}^{n} k \times a_k x^{k-1}$.

Tvrdenie

Nech F je pole. Pre ľubovoľné $c \in F$, $f(x), g(x) \in F[x]$ platí

$$D(f(x) + g(x)) = Df(x) + Dg(x)$$
$$D(cf(x)) = cDf(x)$$
$$D(f(x)g(x)) = Df(x).g(x) + f(x).Dg(x)$$

Derivácia a násobné korene

Tvrdenie

Nech F je pole, $F' \supseteq F$ je jeho nadpole. Nech $f(x) \in F[x]$ je polynóm nad poľom F. Ak v nadpoli F' existuje násobný koreň polynómu $f(x)$, tak polynómy $f(x)$ a $Df(x)$ sú súdeliteľné, t.j.

$$\mathrm{st}(\gcd(f(x), D(f(x)))) \geq 1.$$

Nech $f(x) = g(x)(x-c)^k$, kde $k > 1$. Potom

$$\begin{aligned} Df(x) = Dg(x)(x-c)^k + k \times g(x)(x-c)^{k-1} = \\ = (x-c)^{k-1}(Dg(x)(x-c) + k \times g(x)) \end{aligned}$$

Taylorov rozvoj

Tvrdenie

Nech F je pole, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in F[x]$. Potom existujú jednoznačne určené $b_0, b_1, \ldots, b_n \in F$ také, že

$$f(x) = b_n(x-c)^n + \cdots + b_1(x-c) + b_0. \tag{2}$$

Tvrdenie

Ak F je pole charakteristiky ∞, tak koeficienty $b_0, \ldots, b_n$ z predošlého tvrdenia možno vyjadriť ako

$$b_n = \frac{D^{(n)} f(c)}{n!},$$

kde znak $D^{(n)}$ znamená, že polynóm $f(x)$ zderivujeme n-krát.