ALGEBRA

Polynómy

doc. RNDr. Štefan Peško, CSc.

Katedra matematických metód, FRI ŽU

24. novembra 2015

Polynómy nad poľom

Nech $\mathbb{P}$ je pole s binárnymi operáciami $+$ a $\cdot$; $x \in \mathbb{P}$ a $n \in N$ prirodzené číslo. Označme $x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{\text{n-krát}}$. Nech $a_0, a_1, \ldots, a_n \in \mathbb{P}$ sú pevne zvolené prvky, $x \in \mathbb{P}$ je premenná, potom výraz

$$a_0 + (a_1 \cdot x) + (a_2 \cdot x^2) + \cdots + (a_n \cdot x^n)$$

nazveme polynómom nad poľom $\mathbb{P}$ a budeme značiť $p_n(x)$; prvky $a_0, a_1, \ldots, a_n$ nazveme koeficienty polynómu. Pre stručnosť zápisu budeme písať

$$p_n(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = a_0 + \sum_{i=1}^{n} a_i x^i.$$

Hovoríme, že polynóm

- $p_n(x)$ má stupeň n, ak $a_n \neq 0$,
- $p_0(x)$ je polynóm nultého stupňa, ak $p_0(x) = a_0, a_0 \neq 0$,
- $p(x) = 0$ je nulový polynóm.

Súčet, súčin a násobok polynómov

Nech $m \leq n$ a $p_n(x), q_m(x)$ sú polynómy nad poľom $\mathbb{P}$

$$p_n(x) = a_0 + \sum_{i=1}^{n} a_i x^i, \quad q_m(x) = b_0 + \sum_{i=1}^{m} b_i x^i.$$

Polynómy $p_n(x), q_m(x)$ sa rovnajú, $p_n(x) = q_m(x)$, ak $n = m$ a pre všetky $i \in \{0, 1, 2, \ldots, n\}$ platí $a_i = b_i$.

Súčtom a súčinom polynómov $p_n(x), q_m(x)$ sú polynómy $r_n(x) = p_n(x) + q_m(x)$ a $s_{n+m}(x) = p_n(x) \cdot q_m(x)$, kde $m \leq n$

$$r_n(x) = (a_0 + b_0) + \sum_{i=1}^{m} (a_i + b_i) x^i + \sum_{i=m+1}^{n} a_i x^i,$$

$$s_{n+m}(x) = c_0 + \sum_{k=1}^{n+m} c_k x^k, \quad c_k = \sum_{i+j=k} a_i b_j.$$

Násobok polynómu $p_n(x)$ prvkom $\alpha \in \mathbb{P}$ je polynóm $t_n(x) = \alpha \cdot p_n(x) = (\alpha \cdot a_0) + \sum_{i=1}^{n} (\alpha \cdot a_i) x^i$.

Poznámka

Každý polynóm $p_n(x)$ nad poľom $\mathbb{P}$ definuje zobrazenie $p_n : \mathbb{P} \to \mathbb{P}$.
Budeme rozlišovať medzi polynómom a zobrazením, ktoré definuje.

Príklad 5.1

Nech $p(x) = x^3 + x^2 + x + 1, q(x) = x + 1$ *sú dva rôzne polynómy nad poľom* $\mathbb{P}$. Uvažujme najskôr pole $\mathbb{P} = \mathbb{Q}$

$$\begin{aligned} r_3(x) &= p(x) + q(x) = x^3 + x^2 + 2x + 2, \\ s_4(x) &= p(x) \cdot q(x) = x^4 + 2x^3 + 2x^2 + 2x + 1, \\ t_3(x) &= 3 \cdot p(x) = 3x^3 + 3x^2 + 3x + 3. \end{aligned}$$

Zmeňme pole racioálnych čísel na pole zvyškových tried $\mathbb{P} = \mathbb{Z}_2$.
Aj teraz je $p(x)$ polynóm 3.stupňa a $q(x)$ je polynóm 1.stupňa a teda sú to rôzne polynómy, ale ako zobrazenia sú rovnaké $p(1) = 0 = q(1)$, $p(0) = 1 = q(0)$.

Preto definujeme polynóm ako výraz určený výpočtovou schémou a nie ako zobrazenie !

Vektorový priestor polynómov

Nech n je dané prirodzené číslo a $\mathcal{P}_n$ je množina všetkých polynómov stupňa nanajvýš n nad poľom $\mathbb{P}$ s operáciami súčtu polynómov a súčinu polynómu so skalárom. Množina $\mathcal{P}_n$ s príslušnými operáciami je vektorovým priestorom polynómov nad poľom $\mathbb{P}$.

Poznámka

Predpoklad obmedzenia stupňa polynómov na „nanajvýš n“ je významný. Uvažujme polynómy $p(x) = x + i, q(x) = -x + i$ prvého stupňa nad poľom $\mathbb{C}$. Potom ich súčet $p(x) + q(x) = 2i$ je polynóm nultého stupňa t.j. súčet polynómov prvého stupňa nepredstavuje binárnu operáciu na množine polynómov prvého stupňa.

Príklad 5.2

Uvažujme vektorový priestor polynómov nanajvýš 2. stupňa nad poľom reálnych čísel.

Bázou tohohto vektorového priestoru je $\mathcal{B}_0 = \{1, x, x^2\}$. Polynóm $p_2(x) = 4x^2 + 2x - 1$ má v tejto báze súradnice $p_2(x) = (-1, 2, 4)_{\mathcal{B}_0}$.

Uvažujme inú bázu $\mathcal{B}_1 = \{1, x, 1 + x^2\}$. Rovnica

$$t_1 + t_2 \cdot x + t_3 \cdot (1 + x^2) = 4x^2 + 2x - 1,$$

opäť vedie na sústavu troch rovníc o troch neznámych s riešením $(t_1, t_2, t_3) = (-5, 2, 4)$. Teda $p_2(x) = (-5, 2, 4)_{\mathcal{B}_1}$.

Riešenie môžeme overiť pomocou výpočtu matice prechodu $\mathbf{A}$ z bázy $\mathcal{B}_0$ do bázy $\mathcal{B}_1$ a vzťahu $(-5, 2, 4) = (-1, 2, 4)\mathbf{A}^{-1}$ tvrdenia *4.8*.

Základná veta algebry

Nech $p_n(x) = a_0 + \sum_{i=1}^{n} a_i x^i$ je polynóm nad poľom $\mathbb{P}$, $e \in \mathbb{P}$.

Hovoríme, že e je koreň polynómu $p_n(x)$ ak platí $p_n(e) = 0$.

Príklad 5.3

Polynóm $p_2(x) = x^2 + 1$ nemá nad poľom reálnych čísel $\mathbb{R}$ žiaden koreň, nad poľom zvyškových tried $\mathbb{Z}_2$ má jediný koreň $e = 1$ a nad poľom komplexných čísel $\mathbb{C}$ má dokonca dva rôzne korene $e_1 = i, e_2 = -i$.

Tvrdenie 5.1 (Základná veta algebry)

Polynóm $p_n(x)$ stupňa $n \geq 1$ má nad poľom komplexných čísel aspoň jeden koreň.

Tvrdenie 5.2

Nech $p_n(x)$ je polynóm n-tého stupňa nad poľom $\mathbb{P}$ a nech $c \in \mathbb{P}$ ľubovoľný prvok poľa. Potom

$$p_n(x) = p_n(c) + (x - c) \cdot q_{n-1}(x),$$

kde $q_{n-1}(x)$ je nejaký polynóm stupňa $n - 1$.

Dôkaz:
Nech $p_n(x) = a_0 + \sum_{i=1}^{n} a_i x^i$. Potom

$$p_n(x) - p_n(c) = a_0 + \sum_{i=1}^{n} a_i x^i - a_0 - \sum_{i=1}^{n} a_i c^i =$$

$$= (a_0 - a_0) + \sum_{i=1}^{n} a_i (x^i - c^i) = (x - c) \cdot$$

$$\cdot \underbrace{\left[a_1 + a_2(x + c) + \cdots + a_n \sum_{j=1}^{n} c^{j-1} x^{n-j} \right]}_{q_{n-1}(x)}.$$

Hornerova schéma

Ako získať koeficienty $q_{n-1}(x) = b_0 + \sum_{i=1}^{n-1} b_i x^i$? Po dosadení do $p_n(x) = p_n(c) + (x - c) \cdot q_{n-1}(x)$ dostaneme

$$a_0 + \sum_{i=1}^{n} a_i x^i = p_n(c) + (x - c) \cdot \left[b_0 + \sum_{i=1}^{n-1} b_i x^i \right],$$

po úprave máme na ľavej strane nulový polynóm

$$\underbrace{(a_0 - p_n(c) + cb_0)}_{0} + \sum_{i=1}^{n-1} \underbrace{(a_i - b_{i-1} + cb_i)}_{0} x^i + \underbrace{(a_n - b_{n-1})}_{0} x^n = 0.$$

Z rovnosti polynómov (pri označení $b_{-1} = p_n(c)$) máme rekurentné vzťahy

$$\begin{aligned} b_{n-1} &= a_n, \; b_{-1} = p_n(c), \\ b_{i-1} &= a_i + cb_i \quad i \in \{n-1, n-2, \ldots, 1, 0\}. \end{aligned}$$

Hornerova schéma

Rekurentné vzťahy sa zapisujú do tzv. Hornerovej schémy:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
c		cb_{n-1}	cb_{n-2}	$\cdots$	cb_1	cb_0
	b_{n-1}	b_{n-2}	b_{n-3}	$\cdots$	b_0	$\boxed{p_n(c)}$

Príklad 5.3 – pokračovanie

Polynóm $p_3(x) = x^3 - x^2 + x - 1$ nad poľom $\mathbb{R}$ vydelíme $x + 1$ pomocou Hornerovej schémy takto

	1	-1	1	-1
-1		-1	2	-3
	1	-2	3	$\boxed{-4}$

a máme opäť $p_3(x) = -4 + (x+1)\underbrace{(x^2 - 2x + 3)}_{q_2(x)}$.

Príklad 5.4

Polynóm $p_3(x) = x^3 + x^2 + x + 1$ nad poľom $\mathbb{Z}_2$ vydelíme $x + 1$ pomocou Hornerovej schémy takto

	1	1	1	1
1		1	0	1
	1	0	1	$\boxed{0}$

a máme $p_3(x) = 0 + (x + 1)\underbrace{(x^2 + 1)}_{q_2(x)}$.

Z toho vyplýva, že $c = 1$ je aj koreňom polynómu $p_3(x)$; $p_3(1) = 0$.

Tvrdenie 5.3

Nech c je koreňom polynómu $p_n(x)$ n-tého stupňa nad poľom $\mathbb{P}$. Potom existuje polynóm $q_{n-1}(x)$ stupňa $n-1$ taký, že

$$p_n(x) = (x - c) \cdot q_{n-1}(x).$$

Dôkaz: Zo vzťahu $p_n(c) = 0$ a z tvrdenia *5.2*. ■

Tvrdenie 5.4

Nech $p_n(x) = a_0 + \sum_{i=1}^{n} a_i x^i$ je polynóm n-tého stupňa nad poľom $\mathbb{P}$. Potom

$$p_n(x) = a_n \cdot (x - c_1) \cdot (x - c_2) \cdots (x - c_n),$$

ak $c_1, c_2, \ldots, c_n$ sú korene polynómu $p_n(x)$.

Dôkaz: Vyplýva z n - násobného použitia tvrdenia *5.3*. ■

Príklad 5.5

Polynóm $p_2(x) = 2x^2 + 1$ nad poľom $\mathbb{Z}_3$ má korene $c_1 = 1$ a $c_2 = 2$

$$2 \cdot (x-1) \cdot (x-2) = 2 \cdot (x^2 + 2) = 2x^2 + 1.$$

Príklad 5.6

Polynóm $p_3(x) = x^3 + 2x^2 + x + 2$ má nad poľom komplexných čísel korene $-2, i, -i \in C$. Overíme opakovanou Hornerovou schémou

	1	2	1	2
-2		-2	0	-2
	1	0	1	$\boxed{0}$
i		i	-1	
	1	i	$\boxed{0}$	
$-i$		$-i$		
	1	$\boxed{0}$		

Opakovaná Hornerova schéma

Táto schéma umožňuje vyjadriť polynóm $p_n(x)$ nad poľom $\mathbb{P}$ pomocou mocnín $(x-c)^k$ pre ľubovoľný prvok $c \in \mathbb{P}$:

$$\begin{aligned} p_n(x) &= p_n(c) + (x-c)q_{n-1}(x), \\ q_k(x) &= q_k(c) + (x-c)q_{k-1}(x), k \in \{n-1, n-2, \ldots, 2\} \end{aligned}$$

Spätným dosadzovaním dostaneme

$$p_n(x) = p_n(c) + \sum_{k=1}^{n} q_k(c)(x-c)^k \quad (\clubsuit)$$

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c		cb_{n-1}	$\cdots$	cb_1	cb_0
	b_{n-1}	b_{n-2}	$\cdots$	b_0	$\boxed{p_n(c)}$
c		cb'_{n-2}	$\cdots$	cb'_0	
	b'_{n-2}	b'_{n-3}	$\cdots$	$\boxed{q_1(c)}$	
$\vdots$					
	$\boxed{q_n(c)}$				

Príklad 5.7

Polynóm $p_4(x) = x^4 - 4x^3 + 3x^2 + 4x - 4$ vyjadríme pomocou mocnín $(x-2)^k, k \in \{0, 1, 2 \ldots, 4\}$

	1	-4	3	4	-4
2		2	-4	-2	4
	1	-2	-1	2	$\boxed{0}$
2		2	0	-2	
	1	0	-1	$\boxed{0}$	
2		2	4		
	1	2	$\boxed{3}$		
2		2			
	1	$\boxed{4}$			
2					
	$\boxed{1}$				

$c = 2$ je dvojnásobný koreň $p_4(x)$; $q_2(2) = 3, q_3(2) = 4, q_4(2) = 1$ a z (♣) máme $p_4(x) = 3(x-2)^2 + 4(x-2)^3 + (x-2)^4$.

Derivácia polynómu

Nech $p_n(x) = a_0 + \sum_{j=1}^{n} a_j x^j$ je polynóm n-tého stupňa nad poľom $\mathbb{P}$.

Deriváciou polynómu $p_n(x)$ nazveme polynóm

$$Dp_n(x) = a_1 + \sum_{j=2}^{n} j a_j x^{j-1}$$

a $D^k p_n(x)$ budeme označovať k-tu deriváciu polynómu $p_n(x)$

$$D^k p_n(x) = \begin{cases} p_n(x) & \text{ak } k = 0, \\ D(D^{k-1} p_n(x)) & \text{ak } k = 1, 2, \ldots \end{cases}$$

Taylorov rozvoj polynómu

Tvrdenie 5.5

Nech je $p_n(x) = a_0 + \sum_{j=1}^{n} a_j x^j$ *polynóm n-tého stupňa nad poľom* $\mathbb{P}$ *a nech* $c \in \mathbb{P}$. *Potom pre prvky* $q_k(c)$ *v Taylorovom rozvoji polynómu* $p_n(x)$ *v prvku* c

$$p_n(x) = p_n(c) + \sum_{k=1}^{n} q_k(c)(x-c)^k \quad (\clubsuit)$$

platí $q_k(c) = D^k p_n(c) \cdot (k!)^{-1}$ *pre* $k \in \{1, 2, \ldots, n\}$.

■

Poznámka

V matematickej analýze funkcie reálnej premennej je $\mathbb{P} = \mathbb{R}$ (resp. funkcie komplexnej premennej je $\mathbb{P} = \mathbb{C}$), a tak píšeme

$$q_k(c) = \frac{D^k p_n(c)}{k!}.$$

Príklad 5.7 - pokračovanie

Opakovanou Hornerovou schémou sme vyjadrili
$p_4(x) = x^4 - 4x^3 + 3x^2 + 4x - 4$ v tvare (♣)
$p_4(x) = 3(x-2)^2 + 4(x-2)^3 + (x-2)^4$.
Vypočítame $q_k(2)$ z Taylorovho rozvoja $p_4(x)$:

$$\begin{aligned} Dp_4(x) &= 4x^3 - 12x^2 + 6x + 4, \\ D^2p_4(x) &= 12x^2 - 24x + 6, \\ D^3p_4(x) &= 24x - 24, \\ D^4p_4(x) &= 24. \end{aligned}$$

Dostávame zhodné výsledky:

$$q_1(2) = \frac{Dp_4(2)}{1!} = \frac{0}{1} = 0, \quad q_2(2) = \frac{D^2p_4(2)}{2!} = \frac{6}{2} = 3,$$
$$q_3(2) = \frac{D^3p_4(2)}{3!} = \frac{24}{6} = 4, \quad q_4(2) = \frac{D^4p_4(2)}{4!} = \frac{24}{24} = 1.$$

Rozklad polynómu

Vzťah $p_n(x) = a_n \cdot (x - c_1) \cdot (x - c_2) \cdots (x - c_n)$ nazývame rozklad polynómu $p_n(x)$ na súčin koreňových činiteľov; polynómy prvého stupňa $x - c_i$ nazývame koreňovými činiteľmi.

Ak $p_n(x) = (x - c)^k \cdot q_{n-k}(x),\ q_{n-k}(c) \neq 0$, hovoríme, že c je k-násobným koreňom polynómu $p_n(x)$.

Príklad 5.8

Polynóm $p_3(x) = x^3 - ix^2 - x + i$ nad poľom $\mathbb{C}$ má dvojnásobný koreň $c_1 = i$ a jednoduchý koreň $c_2 = -i$. Jeho rozklad na súčin koreňových činiteľov je

$$p_3(x) = (x - i)^2 \cdot (x + i).$$

Tvrdenie 5.6

Nech $c_1, c_2, \ldots, c_r$ sú rôzne korene polynómu n-tého stupňa $p_n(x) = a_0 + \sum_{i=1}^{n} a_i x^i$ nad poľom komplexných čísel.

Nech c_i je k_i-násobný koreň $(i = 1, 2, \ldots, r)$ polynómu $p_n(x)$.

Potom $\sum_{i=1}^{r} k_i = n$ a platí:

$$p_n(x) = a_n \cdot (x - c_1)^{k_1} \cdot (x - c_2)^{k_2} \cdots (x - c_r)^{k_r}.$$

Dôkaz: Vyplýva z vety *5.4* aplikovanej nad poľom $\mathbb{C}$. ■

Tvrdenie 5.7

Polynóm n-tého stupňa nad poľom komplexných čísel $\mathbb{C}$ má v $\mathbb{C}$ práve n koreňov, ak tieto počítame aj s ich násobnosťami.

Dôkaz: Je dôsledkom tvrdenia *5.6*. ■

Tvrdenie 5.8

Nech je $p_n(x) = a_0 + a_1 x + \cdots + a_n x^n$ *polynóm s celočíselnými koeficientami. Ak je jeho koreňom racionálne číslo* $r = \frac{p}{q}$, *kde sú* p, q *nesúdeliteľné čísla, potom* p *delí* a_0 *a* q *delí* a_n.

Dôkaz: Ak je $\frac{p}{q}$ koreňom polynómu, potom $p_n\left(\frac{p}{q}\right) = 0$ a máme

$$\begin{aligned} 0 &= a_0 + \sum_{i=1}^{n} a_i \left(\frac{p}{q}\right)^i \\ 0 &= a_0 q^n + \sum_{i=1}^{n} a_i p^i q^{n-i} \\ a_0 q^n &= -p \sum_{i=1}^{n} a_i p^{i-1} q^{n-i} \quad (*) \\ a_n p^n &= -q \sum_{i=0}^{n-1} a_i p^i q^{n-i-1} \quad (**) \end{aligned}$$

p, q sú nesúdelitelné, $(*)$ deliteľné p; podobne $(**)$ deliteľné q. ■

Hľadanie racionálnych koreňov celočíselného polynómu

$$p_n(x) = a_0 + a_1 x + \cdots + a_n x^n.$$

- **Krok 1:** Vyhľadáme všetkých deliteľov $p_1, p_2, \ldots, p_r$ koeficienta a_0.
- **Krok 2:** Vyhľadáme všetkých deliteľov $q_1, q_2, \ldots, q_s$ koeficienta a_n.
- **Krok 3:** Overíme, či $p_n\left(\frac{p_i}{q_j}\right) = 0$, pre všetky dvojice (i, j), pre ktoré sú p_i, q_j nesúdeliteľné.

Príklad 5.9

Hľadáme všetky racionálne korene polynómu $p_4(x) = 6x^4 + 3x^3 - x^2 - 5x + 2$. Máme $a_4 = 6, a_0 = 2$.

- **Krok 1:** $p \in \{\pm 1, \pm 2\}$ delia $a_0 = 2$
- **Krok 2:** $q \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$ delia $a_4 = 6$
- **Krok 3:** Z možných podielov $\{\pm 1, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{1}{6}, \pm 2, \pm\frac{2}{3}\}$ je racionálny koreň polynómu $p_4(x)$ len jeden $c = \frac{1}{2}$.

Tvrdenie 5.9

Nech je $p_n(x) = a_0 + a_1x + \cdots + a_nx^n$ polynóm n-tého stupňa nad poľom komplexných čísel s reálnymi koeficientami. Ak je jeho koreňom komplexné číslo $c = \alpha + i\beta$, potom je jeho koreňom aj komplexne združené číslo $\overline{c} = \alpha - i\beta$.

Dôkaz: Nech $c = \alpha + i\beta$ je koreňom polynómu $p_n(x)$. Potom je $\overline{a}_i = a_i$. Po úpravách $p_n(c) = 0$ dostávame

$$\begin{aligned} a_0 + \sum_{i=1}^{n} a_i(\alpha + i\beta)^i &= 0, \\ \overline{a}_0 + \sum_{i=1}^{n} \overline{a_i(\alpha + i\beta)^i} &= \overline{0}, \\ a_0 + \sum_{i=1}^{n} a_i(\alpha - i\beta)^i &= 0. \end{aligned}$$

Z toho vyplýva, že aj $p_n(\overline{c}) = 0$. ■

Príklad 5.10

Korene c_1 a c_2 kvadratickej rovnice s reálnymi koeficientami $x^2 - 2x + 2 = 0$ sú v poli komplexných čísel komplexne združené

$$c_{1,2} = \frac{2 \pm \sqrt{4 - 4 \cdot 2}}{2} = 1 \pm i.$$

Ak ale upustíme od predpokladu reálnych koficientov napr. v kvadratickej rovnici $x^2 - 2ix - 1 = 0$, potom v poli komplexných čísel dostaneme dvojnásobný koreň $c = i$, platí

$$x^2 - 2ix - 1 = (x - i)^2.$$

Z toho vyplýva, že v tvrdení *5.9* je podstatný predpoklad o reálnych koeficientoch polynómu.

Ak sú $c = \alpha + i\beta$ a $\bar{c} = \alpha - i\beta$ pre $\beta \neq 0$ koreňami polynómu, potom

$$(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c\bar{c} = x^2 - 2\alpha x + (\alpha^2 + \beta^2)$$

má tvar kvadratického trojčlena s reálnymi koeficientami.

Príklad 5.10 – pokračovanie

Z komplexne združených koreňov polynómu $c_1 = 1 + i$ a $c_2 = 1 - i$ dostávame jeho tvar kvadratického trojčlena s reálnymi koeficientami

$$(x - 1 - i)(x - 1 + i) = x^2 - 2x + 2.$$

Tvrdenie 5.10

Nech je $p_n(x) = a_0 + a_1x + \cdots + a_nx^n$ *polynóm n-tého stupňa s reálnymi koeficientami. Nech* $c_1, c_2, \ldots, c_r$ *sú navzájom rôzne reálne korene s násobnosťami* $n_1, n_2, \ldots, n_r$ *a čísla* $\alpha_j + i\beta_j$ *navzájom rôzne komplexné korene také, že* $\beta_j > 0$ *pre* $j = 1, 2, \ldots, s$. *Potom aj čísla* $\alpha_j - i\beta_j$ *sú po rade* $m_1, m_2, \ldots, m_s$*-násobné korene polynómu* $p_n(x)$ *a platí*

$$p_n(x) = a_n \cdot \prod_{i=1}^{r}(x - c_i)^{n_i} \cdot \prod_{j=1}^{s}(x^2 + p_jx + q_j)^{m_j},$$

kde $p_j = -2\alpha_j, q_j = \alpha_j^2 + \beta_j^2$ *a platí*

$$n = \sum_{i=1}^{r} n_i + 2 \cdot \sum_{j=1}^{s} m_j.$$

Dôkaz: Priamo z tvrdení *5.6* a *5.9*. ■

Cvičenie 5.1

1. Nájdite taký polynóm najnižšieho stupňa s komplexnými (resp. reálnymi) koeficientami, ktorý má jednoduchý koreň $1 - 2i$ a dvojnásobný koreň 3.
2. Pomocou Hornerovej schémy vydeľte polynóm $p_5(x) = x^5 - 2x^4 + 6x^3 - 12x + 4$ polynómom $x - 2$.
3. Pre aké hodnoty parametra λ je $c = 2$ koreňom polynómu $p_4(x) = 2x^4 + x^3 + \lambda x^2 + 3$ v poli Z_5?
4. Nájdite korene polynómu $p_3(y) = 4y^3 + 14y^2 - 3y + 9$.
5. Nájdite Taylorov rozvoj polynómu $p_y(x) = x^4 + x^3 + 3x^2 + 4x + 1$ nad poľom $\mathbb{Z}_5$ v prvku 2.
6. Majme dve bázy polynómov nanajvýš 1. stupňa nad poľom reálnych čísel $\mathcal{A} = \{-5, 1 + x\}$ a $\mathcal{B} = \{1, x\}$. Nájdite maticu prechodu $\mathbf{A}$ od bázy $\mathcal{A}$ k báze $\mathcal{B}$.

Najväčší spoločný deliteľ polynómov

Nech $p(x), q(x)$ sú dva polynómy nad poľom $\mathbb{P}$. Hovoríme, že polynóm $q(x)$ delí polynóm $p(x)$ a značíme $q(x) \mid p(x)$, ak existuje taký polynóm $r(x)$ nad poľom $\mathbb{P}$, že platí

$$p(x) = q(x) \cdot r(x).$$

Polynóm $q(x)$ nazveme triviálnym deliteľom polynómu $p(x)$, ak stupeň $q(x)$ je 0 alebo $q(x) \mid p(x)$ aj $p(x) \mid q(x)$.

Ak polynóm $r(x)$ delí oba polynómy $p(x)$ aj $q(x)$ hovoríme, že je spoločným deliteľom polynómov $p(x)$ a $q(x)$.

Hovoríme, že polynóm $r(x)$ je najväčším spoločným deliteľom polynómov $p(x)$, $q(x)$ a značíme $r(x) = NSD\big(q(x), p(x)\big)$, ak je

- spoločným deliteľom polynómov $p(x)$, $q(x)$,
- deliteľný každým iným spoločným deliteľom polynómov $p(x)$ a $q(x)$.

Príklad 5.11

Uvažujme dva rôzne polynómy v poli reálnych čísel
$p(x) = (x-2)x(x-1)(x+1), q(x) = 2(x-3)(x-1)(x+1)$.
Potom $(x \pm 1) \mid p(x)$ aj $(x \pm 1) \mid q(x)$ a teda $(x \pm 1)$ je spoločným deliteľom $p(x)$ aj $q(x)$. Platí

$$r(x) = NSD\big(q(x), p(x)\big) = (x-1)(x+1).$$

V prípade, keď poznáme rozklady oboch polynómov $p(x), q(x)$, je hľadanie ich $NSD\big(q(x), p(x)\big)$ jednoduché. Ako ale postupovať v prípade, keď rozklady polynómov nepoznáme?

Delenie polynómov so zvyškom

Tvrdenie 5.11

Nech $m \leq n$ a nech sú $p_n(x)$ a $q_m(x) \neq 0$ plynómy n-tého a m-tého stupňa nad poľom $\mathbb{P}$. Potom existujú nad poľom $\mathbb{P}$ polynómy $s_{n-m}(x)$ a $r(x)$ s vlastnosťou

$$p_n(x) = q_m(x) \cdot s_{n-m}(x) + r(x),$$

pričom $s_{n-m}(x)$ je polynóm stupňa $n - m$ a $r(x)$ je polynóm stupňa menšieho m.

Dôkaz:
Stačí ukázať, že pre $i = 0, 1, \ldots, k-1$ je
$p_{n-i}(x) = p_{n-i-1}(x) + q_m(x) \cdot c_{n-i-m} \cdot x^{n-i-m}$, až kým stupeň $p_{n-k}(x)$ nie je menší než m, Potom $p_{n-k}(x) = r(x)$. ■

Reducibilný a ireducibilný polynóm

Hovoríme, že polynóm $p(x)$ najmenej prvého stupňa nad poľom $\mathbb{P}$ je reducibilný, ak existujú polynómy $q(x), r(x)$ oba najmenej prvého stupňa také, že

$$p(x) = q(x) \cdot r(x).$$

V opačnom prípade hovoríme, že $p(x)$ je ireducibilný polynóm.

Príklad 5.12

Polynóm $p_2(x) = x^2 + 1$ je ireducibilný nad poľom reálnych čísel $\mathbb{R}$, lebo sa nedá napísať ako súčin dvoch polynómov prvého stupňa t.j. súčin dvoch koreňových činiteľov. Nad poľom komplexných čísel $\mathbb{C}$ je však už reducibilný, pretože ho môžeme napísať v tvare

$$p_2(x) = (x - i)(x + i).$$

Tvrdenie 5.12

Polynóm $p(x)$ s reálnymi koeficientami je ireducibilný nad poľom reálnych čísel $\mathbb{R}$ práve vtedy, keď je 1. stupňa alebo je 2. stupňa a nemá reálne korene.

Príklad 5.13

Nad poľom $\mathbb{R}$ rozložíme polynómy $q(x) = x^3 - x^2 + x - 1$ a $p(x) = x^4 - 2x^2 + 1$ na súčin ireducibilných polynómov a nájdeme $NSD(q(x), p(x))$.

Z Hornerovej schémy vidíme, že $q(1) = 0$

	1	−1	1	−1
1		1	0	1
	1	0	1	0

a teda $q(x) = (x-1)(x^2+1)$, no polynóm x^2+1 je v $\mathbb{R}$ ireducibilný. Podobne $p(x) = (x^2-1)^2 = (x+1)^2(x-1)^2$. A tak máme

$$NSD(q(x), p(x)) = x - 1.$$

Rozklad rýdzo racionálnej funkcie na parciálne zlomky

V matematickej analýze sa stretávame s potrebou rozložiť rýdzo racionálnu funkciu reálnej premennej

$$f(x) = \frac{p_n(x)}{q_m(x)}, \ p_n(x) \nmid q_m(x), \ n < m$$

na súčet parciálnych zlomkov

$$\frac{d}{(x-c)^k} \text{ alebo } \frac{a_1 x + a_0}{(x^2 + b_1 x + b_0)^k},$$

kde $c, d, a_0.a_1, b_0, b_1 \in \mathbb{R}$, k je prirodzené číslo a $x^2 + b_1 x + b_0$ je ireducibilný polynóm nad poľom $\mathbb{R}$.

- **Krok 1:** Rozložíme polynóm $q_m(x)$ na súčin ireducibilných polynómov.
- **Krok 2:** Ku každému polynómu $(x-c)^k$ vytvoríme práve k zlomkov

$$\frac{d_1}{x-c}, \frac{d_2}{(x-c)^2}, \ldots, \frac{d_k}{(x-c)^k},$$

kde k je násobnosť koreňa c.

- **Krok 3:** Ku každému polynómu $(x^2+b_1x+b_0)^{k^*}$ vytvoríme práve k^* zlomkov

$$\frac{a_{11}x+a_{01}}{x^2+b_1x+b_0}, \frac{a_{12}x+a_{02}}{(x^2+b_1x+b_0)^2}, \ldots, \frac{a_{1k^*}x+a_{0k^*}}{(x^2+b_1x+b_0)^{k^*}},$$

kde k^* je násobnosť komplexne združených koreňov.

- **Krok 4:** Neznáme koeficienty vypočítame porovnaním koeficientov pri rovnakých mocninách, čo vedie na riešenie nehomogénneho systému lineárnych rovníc.

Príklad 5.14

Rozložme na parciálne zlomky funkciu $f(x) = \frac{x^2}{x^4-1}$ *reálnej premennej.*

Funkcia $f(x)$ je rýdzo racionálna, $p_2(x) = x^2, q_4(x) = x^4 - 1$.

- **Krok 1:** $q_4(x) = (x-1)(x+1)(x^2+1)$
- **Krok 2:** Pre korene $1, -1$ vytvoríme parciálne zlomky

$$\frac{d_1}{x-1}, \quad \frac{d_2}{x+1}.$$

- **Krok 3:** Pre komplexne združené korene $i, -i$ vytvoríme parciálny zlomok

$$\frac{a_1 x + a_0}{x^2+1}.$$

- **Krok 4:** Porovnáme koeficienty

$$\frac{x^2}{x^4-1} = \frac{d_1}{x-1} + \frac{d_2}{x+1} + \frac{a_1 x + a_0}{x^2+1}$$

$$\frac{x^2}{x^4-1} = \frac{d_1(x+1)(x^2+1) + d_2(x-1)(x^2+1) + (a_1x+a_0)(x^2-1)}{(x-1)(x+1)(x^2+1)}.$$

Pretože menovatele sa rovnajú, rovnajú sa aj čitatele a platí

$$x^2 = d_1(x+1)(x^2+1) + d_2(x-1)(x^2+1) + (a_1x+a_0)(x^2-1),$$

$$x^2 = x^3(d_1+d_2+a_1)+x^2(d_1-d_2+a_0)+x(d_1+d_2-a_1)+d_1-d_2-a_0.$$

Posledná rovnosť je ekvivalentná riešeniu sústavy lineárnych rovníc

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & -1 \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

ktorá má jediné riešenie $d_1 = \frac{1}{4}, d_2 = -\frac{1}{4}, a_1 = 0, a_0 = \frac{1}{2}$. A tak

$$\frac{x^2}{x^4-1} = \frac{1}{4(x-1)} - \frac{1}{4(x+1)} + \frac{1}{2(x^2+1)}.$$

Cvičenie 5.2

1. Určte hodnotu parametra α tak, aby bol $c = -1$ koreňom polynómu $p_6(x) = 2x^6 - \alpha x^4 - x^3 + \alpha x^2 + 3\alpha$.
2. Nájdite všetky korene polynómu $q_3(x) = 2x^3 - 7x^2 + 16x - 15$ nad poľom komplexných čísel ak poznáme jeden jeho koreň $1 - 2i$.
3. Aké podmienky musia spĺňať koeficient λ, μ aby pre polynómy nad poľom racionálnych čísel $p_3(x) = x^3 + \lambda x - 3$ a $q_2(x) = x^2 + \mu x + 2$ platil vzťah $q_2(x)|p_3(x)$.
4. Rozložte polynóm $p_5(x) = 7x^5 + 7x^4 + 35x^3 + 35x^2 + 28x + 28$ na súčin ireducibilných polynómov nad poľom reálnych čísel.
5. Rozložte na súčet parciálnych zlomkov funkciu

$$f(x) = \frac{7x^4 + 5x^3 + 2x^2 + 7x + 5}{(x^3 + 1)(x + 1)^2}.$$

Euklidov algoritmus

Nech $p(x), q(x)$ polynómy pričom stupeň $p(x)$ je väčší než stupeň $q(x)$ a $q(x) \nmid p(x)$. Potom

$$\begin{aligned}
p(x) &= q(x) \cdot s_0(x) + r_1(x), \\
q(x) &= r_1(x) \cdot s_1(x) + r_2(x), \\
r_1(x) &= r_2(x) \cdot s_2(x) + r_3(x), \\
&\vdots = \vdots \\
(i) \quad r_{k-2}(x) &= r_{k-1}(x) \cdot s_{k-1}(x) + r_k(x), \\
&\vdots = \vdots \\
(ii) \quad r_{m-2}(x) &= r_{m-1}(x) \cdot s_{m-1}(x) + r_m(x), \\
(iii) \quad r_{m-1}(x) &= r_m(x) \cdot s_m(x) + 0.
\end{aligned}$$

kde $s_{k-1}(x)$ je čiastočný podiel a $r_k(x)$ nenulový zvyšok v k-tom kroku. $NSD(q(x), p(x)) = r_m(x)$ lebo $r_m(x) \mid r_{m-1}(x)$, $r_m(x) \mid r_{m-2}(x), \ldots, r_m(x) \mid r_1(x)$, $r_m(x) \mid q(x)$, $r_m(x) \mid p(x)$.

Normovaný $NSD(q(x), p(x))$ je ten ich najväčší spoločný deliteľ, ktorého koeficient pri najvyššej mocnime x je 1. NSD(q(x),p(x)) získaný Euklidovým algoritmom nemusí byť normovaný.

Príklad 5.14 – pokračovanie

$q(x) = x^3 - x^2 + x - 1$ a $p(x) = x^4 - 2x^2 + 1$.

$$\begin{aligned} p(x) &= q(x) \cdot \underbrace{(x+1)}_{s_0(x)} + \underbrace{(-2x^2+2)}_{r_1(x)}, \\ q(x) &= r_1(x) \cdot \Big(\underbrace{-\frac{x}{2} + \frac{1}{2}}_{s_1(x)} \Big) + \underbrace{(2x-2)}_{r_2(x)}, \\ r_1(x) &= r_2(x) \cdot \underbrace{(-x-1)}_{s_2(x)} + 0. \end{aligned}$$

A tak máme $NSD(q(x), p(x)) = r_2(x) = 2(x-1)$, čo po normovaní dáva polynóm $x - 1$.

Metóda neurčitých koeficientov

Majme normované polynómy $p_n(x), q_m(x), m < n, q_m(x) \nmid p_n(x)$ s celočíselnými koeficientami nad poľom reálnych čísel a hľadajme $r(x) = NSD(p_n(x), q_m(x))$.

Polynóm $r(x)$ môže mať stupeň nanajvýš $m-1$ t.j. $r(x) = r_0 + \sum_{i=1}^{m-1} r_i x^i$. Predpokladajme naviac, že pre nejaké navzájom rôzne celé čísla α_i máme $p_n(\alpha_i) \geq 1, q_m(\alpha_i) \geq 1$, $i = 0, 1, \ldots, m-1$, ktoré sú kladnými celými číslami, a tak vieme vypočítať $\beta_i = NSD(p_n(\alpha_i), q_m(\alpha_i))$.

Neznáme koeficienty r_i sú tak riešením systému nelineárnych rovníc $r(\alpha_i) = \beta_i, i = 0, 1, \ldots, m-1$, ktoré vedú na riešenie nehomogénneho systému lineárnych rovníc

$$\begin{pmatrix} 1 & \alpha_0 & \alpha_0^2 & \ldots & \alpha_0^{m-1} \\ 1 & \alpha_1 & \alpha_1^2 & \ldots & \alpha_1^{m-1} \\ \vdots & \vdots & \vdots & \ldots & \vdots \\ 1 & \alpha_{m-1} & \alpha_{m-1}^2 & \ldots & \alpha_{m-1}^{m-1} \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ \vdots \\ r_{m-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{m-1} \end{pmatrix}.$$

Príklad 5.14 – pokračovanie

$p_4(x) = x^4 - 2x^2 + 1$ a $q_3(x) = x^3 - x^2 + x - 1$ sú normované polynómy s celočíselnými koeficentami nad poľom $\mathbb{R}$.

Najskôr treba nájsť také celé čísla $\alpha_0, \alpha_1, \alpha_2$, v ktorých nadobúdajú oba polynómy hodnoty kladných celých čísel. Zvoľme napríklad $\alpha_0 = 2, \alpha_1 = 3, \alpha_2 = 4$ a dostávame

i	α_i	$p_4(\alpha_i)$	$q_3(\alpha_i)$	β_i
0	2	9	5	1
1	3	64	30	2
2	4	225	51	3

Systém lineárnych rovníc zodpovedajúci $r(\alpha_i) = \beta_i, i = 0, 1, 2$

$$\begin{pmatrix} 1 & 2 & 4 \\ 1 & 3 & 9 \\ 1 & 4 & 16 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix},$$

má jediné riešenie $r(x) = (-1, 1, 0)_{\mathcal{B}_0} = x - 1$.

Bonusový príklad 5.1

1. (4b) Overte, že množina $\mathcal{R}_3$ polynómov nanavýš 3. stupňa nad poľom reálnych čísel vytvára vektorový priestor (3b) a nájdite jeho dve bázy (1b).
2. (3b) Pre aký parameter α polynómu $p_5(x) = x^5 - \alpha x^2 - i\alpha x + i$ nad poľom $\mathbb{C}$ je $c = -i$ jeho
   a) (1b) jednoduchý koreň,
   b) (2b) dvojnásobný koreň,
3. (8b) Vyjadrite polynóm $p(x) = x^4 + 3x^2 + \lambda x + 1$ v mocninách uvedeného lineárneho výrazu
   a) (2b) v poli $\mathbb{R}, x - 1$,
   b) (3b) v poli $\mathbb{C}, x - i$,
   c) (3b) v poli $\mathbb{Z}_5, x + 3$.
4. (4b) Najdite Taylorov rozvoj polynómu $p(x) = 3x^4 + (1 - 2i)x^2 - 1$ v prvku $c = 2$ (2b), $c = i$ (2b).
5. (4b) Rozložte funkciu $f(x) = \frac{x^2+2x+1}{(x+1)(x-2)(x^2+3)}$ na parciálne zlomky.

Bonusový príklad 5.2

Vytvorte program v Exceli (Calcu, Gnumericu):

1. (4b) Nájde všetky racionálne korene polynómu stupňa $n (2 \leq n \leq 10)$ s celočíselnými koeficientami.
2. (15b) Nájde $NSD(p_n(x), q_m(x))$ pre polynómy $p_n(x)$ a $q_m(x)$, kde $1 \leq m < n \leq 10$, nad poľom $\mathbb{Q}$ (4b), $\mathbb{Z}_3$ (5b), $\mathbb{C}$ (6b).
3. (10b) Pre zadaný polynóm $p_n(x) (3 \leq n \leq 5)$ nad poľom $\mathbb{Z}_{17}$
   a) (3b) nájde všetky korene polynómu $p_n(x)$,
   b) (2b) vypíše polynóm $p_n(x)$ v tvare súčinu koreňových činiteľov,
   c) (5b) nájde všetky ireducibiné polynómy deliace polynóm $p_n(x)$.
4. (10b) Pre dané celočíselné polynómy $p_{10}(x), q_8(x)$ a $r(x) = NSD(p_{10}(x), q_8(x))$, nájde také polynómy $u(x)$ a $v(x)$, že platí tzv. Bezoutova rovnosť:

$$r(x) = p(x) \cdot u(x) + q(x) \cdot v(x).$$

Pomoc: Spätným dosadzovaním v Euklidovom algoritme.