

# Okruhy polynomů

Ondřej Klíma

Okruhy polynomů – p.1/31

## Polynomy

Př:  $f = 4x^5 - x^3 + 7x^2 + 1$

Co je to polynom?

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

kde  $n \in \mathbb{N}$  ("stupeň") a  $a_n, a_{n-1}, \dots, a_1, a_0 \in \mathbb{R}$  (koeficienty).

Definice?

Oblíbený způsob: formální součet. Uděláme jinak.

Reprezentace?

Konečná posloupnost koeficientů. Př:  $f = (4, 0, -1, 7, 0, 1)$ .

Technické potíže — např. sčítání.

Standardní trik: nekonečná posloupnost s konečným počtem nenulových čísel.  $(1, 0, 7, -1, 0, 4, 0, 0, 0, \dots)$

Okruhy polynomů – p.2/31

Nechť  $(R, +, \cdot)$  je okruh. **Polynom nad okruhem  $R$**  definujeme jako nekonečnou posloupnost  $f = (f_0, f_1, f_2, \dots)$ , kde  $f_i \in R$  pro  $i \in \mathbb{N}_0$ , takovou, že množina  $\{i \in \mathbb{N}_0 \mid f_i \neq 0\}$  je konečná.

Ekvivalentní vyjádření poslední podmínky je:  
 $(\exists n \in \mathbb{N})(\forall i > n)(f_i = 0)$

Prvky  $f_0, f_1, \dots$  nazýváme **koeficienty** polynomu  $f$ .

Množinu všech polynomů nad okruhem  $R$  označujeme symbolem  $R[x]$ .

## Příklady

- $4x^5 - x^3 + 7x^2 + 1$  (1, 0, 7, -1, 0, 4, 0, 0, \dots)
- $4x^5 + x^3 + \frac{8}{3}x^2 - \frac{1}{2}$  (-\frac{1}{2}, 0, \frac{8}{3}, 1, 0, 4, 0, 0, \dots)
- $4x^4 - \sqrt{3}x^3 + \pi x^2 + 1$  (1, 0, \pi, -\sqrt{3}, 4, 0, 0, \dots)
- $2x^4 - (1 + i)x^3 + \pi x^2 + i$  (i, 0, \pi, -1 - i, 4, 0, 0, \dots)

Jednoduché pozorování:  $R \subseteq S \implies R[x] \subseteq S[x]$ .

Co "polynomy"

- $x^2 + ix^2 + 3x + i$
- $x^4 + x^3 + 4x^3 + x^2 + 5x^2 - 3x^2 + x + 9x + 1$  ?

- polynomy nad  $\mathbb{Z}_n \dots$
- polynomy nad maticemi

$$\begin{pmatrix} 5 & 2 \\ 0 & 3 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 0 \\ 0 & 6 \end{pmatrix} x + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\left( \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 5 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \dots \right)$$

- $R$  triviální okruh  $\implies$  existuje jediný polynom

## ”Divoký” příklad

$A = \{a, b, c\}$ . Okruh  $(\mathcal{P}(A), \div, \cap)$ ;  
 $\emptyset$  neutrální prvek vzhledem k  $\div$ , tj. 0;  
 $A$  neutrální prvek vzhledem k  $\cap$ .

Polynom  $f = (\{a\}, \emptyset, \{c\}, \{a, b, c\}, \emptyset, \emptyset, \dots)$ ;

$$f = \dots + \emptyset x^4 + \{a, b, c\} x^3 + \{c\} x^2 + \emptyset x + \{a\};$$

$$f = \{a, b, c\} \cap x^3 \div \{c\} \cap x^2 \div \{a\}.$$

Co dál s polynomy?

Cíl je definovat operaci ”sčítání” polynomů.

Tato operace musí v naší interpretaci odpovídat ”skutečnému” sčítání.

Stejně tak pro násobení, tj. např.  $x^2 = x \cdot x$ .

Bud'  $f = (f_0, f_1, \dots)$  a  $g = (g_0, g_1, \dots)$  polynomy nad  $R$ .

Očekáváme

$$\begin{aligned} & (\dots f_n x^n + \dots + f_1 x + f_0) + (\dots g_n x^n + \dots + g_1 x + g_0) \\ & = \dots (f_n + g_n) x^n + \dots + (f_1 + g_1) x + (f_0 + g_0) \end{aligned}$$

Pro  $f$  a  $g$  polynomy nad  $R$  definujeme polynom  $f + g$  vztahem  $(f + g)_k = f_k + g_k$  pro  $k \in \mathbb{N}_0$ .

## Definice součinu polynomů

Bud'  $f = (f_0, f_1, \dots)$  a  $g = (g_0, g_1, \dots)$  polynomy nad  $R$ .

Očekáváme

$$\begin{aligned} & (\dots f_n x^n + \dots + f_1 x + f_0) \cdot (\dots g_n x^n + \dots + g_1 x + g_0) \\ & = \dots (f_2 g_0 + f_1 g_1 + f_0 g_2) x^2 + (f_1 g_0 + f_0 g_1) x + f_0 g_0 \end{aligned}$$

$$(f \cdot g)_k = \sum_{i=0}^k f_i \cdot g_{k-i} \quad (*)$$

Pro  $f$  a  $g$  polynomy nad  $R$  definujeme polynom  $f \cdot g$  vztahem  $(*)$  pro  $k \in \mathbb{N}_0$ .

**Věta.**

Bud'  $(R, +, \cdot)$  okruh. Pokud na množině  $R[x]$  definujeme operace + a · vztahy

i)  $(f + g)_k = f_k + g_k$  pro  $k \in \mathbb{N}_0$ ,

ii)  $(f \cdot g)_k = \sum_{i=0}^k f_i \cdot g_{k-i}$  pro  $k \in \mathbb{N}_0$ ,

pak  $(R[x], +, \cdot)$  je okruh.

Je-li  $(R, +, \cdot)$  komutativní okruh, pak  $(R[x], +, \cdot)$  je také komutativní okruh.

$(R[x], +, \cdot)$  se nazývá **okruh polynomů nad okruhem**  $(R, +, \cdot)$ .

## Konstantní polynomy

Neutrální prvek vzhledem k + je polynom  $(0, 0, 0, 0, \dots)$ ; tzv. **nulový polynom**.

Neutrální prvek vzhledem k · je polynom  $(1, 0, 0, 0, \dots)$ .

Polynomy tvaru  $(a, 0, 0, 0, \dots)$ , kde  $a \in R$ , se nazývají **konstantní polynomy**.

Zobrazení  $k : R \rightarrow R[x]$  dané vztahem  $k(a) = (a, 0, 0, 0, \dots)$ , pro  $a \in R$  je prostý homomorfismus okruhů.

Konstantní polynomy můžeme tedy ztotožnit s prvky okruhu  $R$  a chápat  $R$  jako podokruh okruhu  $R[x]$ .

**Stupeň** nenulového polynomu  $f$  je největší číslo  $n \in \mathbb{N}_0$  takové, že  $f_n \neq 0$ . (Označujeme  $\text{st}(f)$ .)

Koeficient  $f_n$  se nazývá **vedoucí koeficient** polynomu  $f$ .

Lineární, kvadratické, kubické polynomy.

Polynom  $x = (0, 1, 0, 0, 0, \dots)$

Označme polynom  $(0, 1, 0, 0, 0, \dots) \in R[x]$  symbolem  $x$ . Pak

●  $x^2 = x \cdot x = (0, 1, 0, 0, \dots) \cdot (0, 1, 0, 0, \dots) = (0, 0, 1, 0, 0, \dots)$

●  $x^3 = (0, 0, 0, 1, 0, 0, 0, \dots)$

●  $a \cdot x^2 = (a, 0, \dots) \cdot (0, 0, 1, 0, \dots) = (0, 0, a, 0, 0, \dots)$

## Vyjádření polynomu pomocí $x$

**Věta.**

Bud'  $(R, +, \cdot)$  okruh a  $f \in R[x]$  polynom stupně  $n$ . Pak platí

$$f = f_n \cdot x^n + f_{n-1} \cdot x^{n-1} + \dots + f_1 \cdot x + f_0,$$

kde koeficienty  $f_0, f_1, \dots, f_{n-1}, f_n$  chápeme jako konstantní polynomy v  $R[x]$  a operace  $+, \cdot$  jsou operacemi okruhu  $(R[x], +, \cdot)$ .

Cíl je splněn: polynom  $f = (f_0, f_1, \dots, f_{n-1}, f_n, 0, 0, \dots)$  můžeme zapisovat ve tvaru

$$f = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0.$$

- Polynom — nekonečná posloupnost prvků  $f_i \in R$  (skoro všechny = 0)
- Na množině všech polynomů se definují operace  $+$  a  $\cdot$ .
- Ukáže se, že  $(R[x], +, \cdot)$  je okruh.
- Při označení  $a = (a, 0, 0, \dots)$ ,  $x = (0, 1, 0, 0, \dots)$  lze pak každý polynom  $(f_0, f_1, \dots, f_n, 0, 0, \dots)$  psát ve tvaru

$$f = f_n \cdot x^n + f_{n-1} \cdot x^{n-1} + \dots + f_1 \cdot x + f_0.$$

- Pozn. V předchozím jsou  $+$  a  $\cdot$  korektně definované operace na množině všech polynomů  $R[x]$ .
- Co dál? Rozklad polynomů na "prvočinitele".

Okruhy polynomů – p.13/31

## Rozklad na prvočinitele v $\mathbb{Z}$

$$m = \pm 1 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k,$$

kde  $p_i$  prvočísla; jednoznačnost.

Důkaz — hlavní body

- $m$  není prvočíslo, pak  $m$  rozložíme na součin "menších"
- proces rozkládání se zastaví
- jednoznačnost  $p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l$   
 $q_l \mid p_1 p_2 \dots p_k \implies q_l = p_i$  pro vhodné  $i$ 
  - lemma:  $q \mid a \cdot b, (q, a) = 1 \implies q \mid b$
  - Bezoutova rovnost
  - Euklidův algoritmus
  - dělení se zbytkem

Okruhy polynomů – p.14/31

Postup:

- definice dělení (v libovolném komutativním okruhu)  
 $a \mid b \iff (\exists c) b = c \cdot a$
- "porovnávání" prvků
- dělení se zbytkem
- Euklidův algoritmus (Bezoutova rovnost)
- ireducibilní prvky (nerozložitelné)

Pozn: dělitelnost v tělesech  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

Prvky se navzájem dělí  $a, b \in \mathbb{Q}, a, b \neq 0 \implies$

$$b = (ba^{-1}) \cdot a, \quad a = (ab^{-1}) \cdot b \quad \text{tzn.} \quad a \mid b, \quad b \mid a.$$

## Dělení a invertibilní prvky okruhu

Nechť  $e$  je invertibilní prvek komutativního okruhu a  $b = e \cdot a$ , pak

$$a = e^{-1} \cdot (ea) = e^{-1} \cdot b, \quad \text{tj.} \quad a \mid b, \quad b \mid a.$$

Příklad v  $\mathbb{Q}[x]$ :

$$f = 2x^3 + x^2 + x + \frac{1}{2}$$

$$f = (x^2 + \frac{1}{2}) \cdot (2x + 1) = (2x^2 + 1) \cdot (x + \frac{1}{2})$$

$$f = 2 \cdot (x^2 + \frac{1}{2}) \cdot (x + \frac{1}{2})$$

Budeme chtít vědet jak vypadají invertibilní prvky v  $R[x]$ .

Nenulový polynom se nazývá **normovaný**, je-li jeho vedoucí koeficient 1.



Jak porovnávat polynomy při rozkládání? Příklad:

$$x^3 + 1 = (x + 1) \cdot (x^2 - x + 1);$$

polynomy  $(x + 1)$  a  $(x^2 - x + 1)$  mají menší stupeň.

## Věta.

Bud'  $(R, +, \cdot)$  okruh. Pak pro libovolné dva polynomy  $f, g$  z  $R[x]$  platí

$$\text{st}(f + g) \leq \max\{\text{st}(f), \text{st}(g)\} \quad \text{a} \quad \text{st}(f \cdot g) \leq \text{st}(f) + \text{st}(g).$$

Je-li navíc  $(R, +, \cdot)$  obor integrity, pak ve druhé nerovnosti platí vždy rovnost.

## Definice stupně — doplnění

Příklad: polynomy nad  $\mathbb{Z}_4$ :

$$2x \cdot 2x = 0$$

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

Pro nulový polynom  $0 = (0, 0, 0, \dots)$  klademe jeho stupeň rovný  $-\infty$ . Přičemž:

$$-\infty < n$$

$$(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$$

pro všechna  $n \in \mathbb{N}_0$ .

$$\text{st}(f \cdot g) \leq \text{st}(f) + \text{st}(g)$$

$(R, +, \cdot)$  obor integrity a  $f, g \in R[x]$  pak,

$$\text{st}(f \cdot g) = \text{st}(f) + \text{st}(g)$$

Důsledky:

- $(R[x], +, \cdot)$  je obor integrity,
- invertibilní prvky v  $R[x]$  jsou právě konstantní polynomy, které odpovídají invertibilním prvkům okruhu  $R$ ,
- $R[x]$  není nikdy těleso.

## Dělení se zbytkem v $R[x]$

Pro jednoduchost —  $(R, +, \cdot)$  těleso.  
(Skripta — zobecnění pro obory integrity.)

**Věta.**

Nechť  $(R, +, \cdot)$  je těleso a  $f, g \in R[x]$  jsou dva polynomy takové, že  $g \neq 0$ . Pak existují polynomy  $q, r \in R[x]$  takové, že platí

$$f = g \cdot q + r, \quad \text{st}(r) < \text{st}(g).$$

Přitom tyto polynomy  $q, r$  jsou určeny jednoznačně.

$q$  se nazývá **podíl** a  $r$  **zbytek**.

Důkaz: má dvě části: existenci a jednoznačnost sami — skripta; zde — pouze ideje.

- Pro dané  $f, g \in R[x]$  chceme  $q, r \in R[x]$  tak, aby  $f = g \cdot q + r$ ,  $\text{st}(r) < \text{st}(g)$ .
  - $\text{st}(f) < \text{st}(g) \implies f = g \cdot 0 + f$
  - $\text{st}(f) \geq \text{st}(g)$  indukci vzhledem k  $\text{st}(f)$

**Př:**  $f = 3x^4 + 2x^3 - x^2 + 1$ ,  $g = 2x^2 + 2x - 3$  pak  $q = \frac{3}{2}x^2$

$$3x^4 + 2x^3 - x^2 + 1 = (2x^2 + 2x - 3) \cdot \frac{3}{2}x^2 + ?$$

$$= 3x^4 + 3x^3 - \frac{9}{2}x^2 + ?$$

$$= 3x^4 + 3x^3 - \frac{9}{2}x^2 + (-x^3 + \frac{7}{2}x^2 + 1)$$

Polynom  $(-x^3 + \frac{7}{2} + 1)$  má menší stupeň než  $f$ .

$$-x^3 + \frac{7}{2}x^2 + 1 = (2x^2 + 2x - 3) \cdot \frac{-1}{2}x + (\frac{9}{2}x^2 - \frac{3}{2}x + 1)$$

$$\frac{9}{2}x^2 - \frac{3}{2}x + 1 = (2x^2 + 2x - 3) \cdot \frac{9}{4} + (-6x + \frac{31}{4})$$

**Celkem**  $f = (2x^2 + 2x - 3) \cdot (\frac{3}{2}x^2 - \frac{1}{2}x + \frac{9}{4}) + (-6x + \frac{31}{4})$

## Jednoznačnost při dělení

- $g \cdot q + r = g \cdot q' + r'$
- $g \cdot (q - q') = r' - r$ , kde  $\text{st}(r' - r) < \text{st}(g) \in \mathbb{N}_0$
- $\text{st}(g) + \text{st}(q - q') = \text{st}(r' - r)$
- Odtud**  $\text{st}(q - q') = \text{st}(r' - r) = -\infty$
- $r' - r = 0$ , tj.  $r = r'$
- $q - q' = 0$ , tj.  $q = q'$

Polynom  $h \in R[x]$  se nazývá **společný dělitel** polynomů  $f, g \in R[x]$ , jestliže  $h \mid f$  a také  $h \mid g$ .

Polynom  $d \in R[x]$  se nazývá **největší společný dělitel**  $f, g \in R[x]$ , jestliže je společný dělitel  $f$  a  $g$  a všechny ostatní společné dělitele jej dělí.

Tj.  $d \mid f, d \mid g$  a  $(\forall h \in R[x])(h \mid f \wedge h \mid g \implies h \mid d)$ .

Polynomy nad  $\mathbb{Z}_4$ :

●  $f = 2x = 2 \cdot (x + 2), \quad g = x^2 + 2x = x \cdot (x + 2)$ .

Vidíme, že  $x$  i  $x + 2$  jsou společné dělitele  $f, g$ .

Neexistuje největší společný dělitel  $f$  a  $g$ .

## Existence n.s.d v $R[x]$

**Věta.**

Nechť  $(R, +, \cdot)$  je těleso a  $f, g \in R[x]$  polynomy z nichž alespoň jeden je nenulový. Pak

- existuje největší společný dělitel  $f$  a  $g$ ;
- je-li  $d$  největší společný dělitel  $f, g$ , pak každý největší společný dělitel je tvaru  $a \cdot d$ , kde  $a$  je konstantní nenulový polynom;
- existuje jediný normovaný největší společný dělitel polynomů  $f$  a  $g$ .

Značíme  $(f, g)$ , případně  $\text{nsd}(f, g)$ .

Klademe  $(0, 0) = 0$  (není normovaný).

Dále  $(f, 0) = f_n^{-1} \cdot f$ , pro  $f$  nenulový polynom stupně  $n$ .

Existence — Euklidův algoritmus:

$$f = g \cdot q_0 + r_0, \quad \text{st}(r_0) < \text{st}(g),$$

$$g = r_0 \cdot q_1 + r_1, \quad \text{st}(r_1) < \text{st}(r_0),$$

$$r_0 = r_1 \cdot q_2 + r_2, \quad \text{st}(r_2) < \text{st}(r_1),$$

...

$$r_{n-2} = r_{n-1} \cdot q_n + r_n, \quad \text{st}(r_n) < \text{st}(r_{n-1}),$$

$$r_{n-1} = r_n \cdot q_{n+1}.$$

Kde  $r_n$  je n.s.d — nemusí být normovaný.

Bezoutova rovnost — stejně jako v  $\mathbb{Z}$ :

$$\begin{aligned} r_n &= r_{n-2} + r_{n-1} \cdot (-q_n) = r_{n-2} + (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot (-q_n) = \\ &= r_{n-3} \cdot (-q_n) + r_{n-2} \cdot (1 + q_{n-1} \cdot q_n) = \dots = f \cdot ? + g \cdot ? \end{aligned}$$

## Poznámky k popisu všech n.s.d

Pokud  $d, h$  dva největší dělitelé  $f, g$ , pak se navzájem dělí.

Tj. existují  $a, b \in R[x]$ , tak, že  $d = a \cdot h, h = b \cdot d$ .

Celkem  $d = a \cdot b \cdot d$ .

Odtud (po diskusi zda něco není nulový polynom)

krácením ( $R[x]$  je obor integrity) dostaneme

$$1 = a \cdot b.$$

Oba dva důkazy — skripta.

Tamtéž Bezoutova rovnost a její důsledek

$$f \mid g \cdot h, (f, g) = 1 \implies f \mid h.$$

Polynom  $f \in R[x]$  je **ireducibilní nad**  $R$ , jestliže  $f$  je nekonstantní a nelze rozložit na součin dvou nekonstantních polynomů.

- Každý lineární polynom (nad oborem integrity) je ireducibilní.
- Polynom  $2x + 2$  není ireducibilní nad  $\mathbb{Z}_4$ ;  
 $2x + 2 = (2x + 2)(2x + 1)$ .
- Polynom  $x^3 - 2$  je ireducibilní nad  $\mathbb{Q}$ , ale není ireducibilní nad  $\mathbb{R}$  a  $\mathbb{C}$ ;  
 $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$  — příště.

## Jednoznačný rozklad v $R[x]$

### Věta.

Bud'  $(R, +, \cdot)$  těleso. Pak pro každý nenulový polynom  $f \in R[x]$  existují normované polynomy  $p_1, p_2, \dots, p_k \in R[x]$  ireducibilní nad  $R$  a konstantní polynom  $a \in R[x]$  tak, že

$$f = a \cdot p_1 \cdot p_2 \cdot \dots \cdot p_k.$$

Tento rozklad polynomu  $f$  je jediný až na pořadí činitelů.

Hovoříme o **okruhu s jednoznačným rozkladem**.

Okruh Gaussových celých čísel  $G$  je okruh s jednoznačným rozkladem.

$$G = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Porovnávání — pomocí normy:

$$N(a + bi) = (a + bi) \cdot (a - bi) = a^2 + b^2 \in \mathbb{N}_0.$$

Platí  $N(x \cdot y) = N(x) \cdot N(y)$ .

Odtud plyne, že pro invertibilní prvek  $x$  musí platit

$N(x) = 1$ , tj. invertibilní prvky jsou  $1, -1, i, -i$ .

Lze dělit se zbytkem (není jednoznačně určen).

Př:  $5 + 5i = 3 \cdot (2 + i) + (-1 + 2i) = 3 \cdot (1 + 2i) + (2 - i),$

kde pro zbytky platí  $N(-1 + 2i) = N(2 - i) = 5 < 9 = N(3)$ .

Euklidův algoritmus, Bezout, jednoznačný rozklad.

Př:  $5 = (1 + 2i)(1 - 2i)$ .  $N(x)$  prvočíslo  $\implies x$  invertibilní.

## Negativní "divoký" příklad

Okruh  $\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$  není okruh s jednoznačným rozkladem.

Norma tentokrát  $N(a + bi\sqrt{5}) = a^2 + 5b^2$ , invertibilní prvky  $\pm 1$ .

Př:  $9 = 3 \cdot 3 = (2 + 1 \cdot i\sqrt{5}) \cdot (2 - 1 \cdot i\sqrt{5}),$

kde  $3, 2 + i\sqrt{5}$  i  $2 - i\sqrt{5}$  ireducibilní, neboť

$N(3) = N(2 \pm i\sqrt{5}) = 9$  a neexistuje prvek s normou 3.

Taktéž neexistuje  $(9, 3 \cdot (2 + i\sqrt{5}))$ , protože mezi společné dělitele patří  $3$  i  $2 + i\sqrt{5}$ .

Co se bude požadovat:

- vlastnosti  $(R[x], +, \cdot)$ ,
- rozkládání polynomů — příště,
- hlavní věty (tučné),
- základní pojmy — stupeň, ved. koef., ireduc. pol., ...
- prakticky Euklides, Bezout — nad tělesy.

Co se nebude požadovat :

”divoké” příklady, tj. rozklady mimo  $R[x]$ .