

# Drsná matematika IV – 3. přednáška

## Okruhy polynomů a tělesa

Jan Slovák

Masarykova univerzita  
Fakulta informatiky

5. 3. 2009

# Obsah přednášky

- 1 Literatura
- 2 Okruhy
- 3 Polynomy
- 4 Dělitelnost a nerozložitelnost
- 5 Polynomy více proměnných
- 6 Podílová tělesa

## Kde je dobré číst?

- vlastní poznámky, texty současného přednášejícího, GOOGLE, atd.
- Riley, K.F., Hobson, M.P., Bence, S.J. Mathematical Methods for Physics and Engineering, second edition, Cambridge University Press, Cambridge 2004, ISBN 0 521 89067 5, xxiii + 1232 pp.
- Zvára, Štěpán: Pravděpodobnost a matematická statistika ISBN 80-86732-71-7, 4.. vydán, 232 str., Matfyzpres, Praha.

S grupami se setkáváme nejčastěji jako s množinami transformací. U skalárů i vektorů ale vystupovalo hned více obdobných struktur zároveň.

Jako standardní příklady mějme na mysli **skaláry** (tj. celá čísla  $\mathbb{Z}$ , racionální čísla  $\mathbb{Q}$ , komplexní čísla  $\mathbb{C}$ ) a **množiny polynomů nad takovými skaláry**  $\mathbb{K}$ .

### Definition

Komutativní grupa  $(M, +)$  s neutrálním prvkem  $0 \in M$ , spolu s další operací  $\cdot$  splňující

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ , pro všechny  $a, b, c \in M$ ;
- $a \cdot b = b \cdot a$ , pro všechny  $a, b \in M$ ;
- existuje prvek  $1$  takový, že pro všechny  $a \in M$  platí  $1 \cdot a = a$ ;
- $a \cdot (b + c) = a \cdot b + a \cdot c$ , pro všechny  $a, b, c \in M$ ;

se nazývá **komutativní okruh**.

Jestliže v okruhu  $\mathbb{K}$  platí  $c \cdot d = 0$  právě, když alespoň jeden z prvků  $c$  a  $d$  je nulový, pak nazýváme okruh  $\mathbb{K}$  **oborem integrity**.

Poslední vlastnosti v našem výčtu axiomů okruhu se říká **distributivita**.

Pokud neplatí vlastnost komutativity operace  $\cdot$ , hovoříme o (nekomutativním okruhu). V dalším se ovšem omezíme pouze na okruhy komutativní.

Operaci  $+$  budeme říkat **sčítání** a operaci  $\cdot$  **násobení**. Navíc budeme vždy předpokládat existenci **jedničky** 1 pro operaci násobení, neutrálnímu prvku pro sčítání říkáme **nula**.

Obecně říkáme, že  $a \in \mathbb{K}$  **dělí**  $c \in \mathbb{K}$ , jestliže existuje  $b$  tak, že  $a \cdot b = c$ . Skutečnost že  $c \in \mathbb{K}$  je dělitelné  $a \in \mathbb{K}$  zapisujeme  $a|c$ .  
Dodatečnou vlastností oboru integrity oproti obecnému okruhu je neexistence netriviálních dělitelů nuly. Okamžitě odtud také vyplývá jednoznačnost dělitelů:

je-li  $b = a \cdot c$  a  $b \neq 0$ , pak  $c$  je jednoznačně dáno volbou  $a, b$ . Pro  $b = ac = ac'$  totiž platí  $0 = a \cdot (c - c')$  a  $a \neq 0$ , proto  $c = c'$ .

Dělitelé jedničky, tj. invertibilní prvky v  $\mathbb{K}$ , se nazývají **jednotky**.

Jednotky v komutativním okruhu vždy tvoří komutativní grupu.

Netriviální (komutativní) okruh, ve kterém jsou všechny nenulové prvky invertibilní, se nazývá (komutativní) **těleso**.

Komutativní těleso se také nazývá **pole**.

Typickým příkladem komutativních okruhů, tj. polí, jsou číselné obory  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ . Dále pak všechny okruhy zbytkových tříd  $\mathbb{Z}_p$  s prvočíselným  $p$ .

Dobrým příkladem nekomutativního okruhu s jedničkou je množina  $\text{Mat}_k(\mathbb{K})$  všech čtvercových matic nad okruhem  $\mathbb{K}$  s  $k$  řádky a sloupci. Jak jsme viděli dávno, není to ani obor integrity. Jako příklad nekomutativního tělesa uveďme těleso kvaternionů  $\mathbb{H}$ .

V každém komutativním okruhu  $\mathbb{K}$  s jedničkou platí následující vztahy (které nám jistě připadají samozřejmé u skalárů)

- 1  $0 \cdot c = c \cdot 0 = 0$  pro všechny  $c \in \mathbb{K}$ ,
- 2  $-c = (-1) \cdot c = c \cdot (-1)$  pro všechny  $c \in \mathbb{K}$ ,
- 3  $-(c \cdot d) = (-c) \cdot d = c \cdot (-d)$  pro všechny  $c, d \in \mathbb{K}$ ,
- 4  $a \cdot (b - c) = a \cdot b - a \cdot c$ ,
- 5 celý okruh  $\mathbb{K}$  je triviální množinou  $\{0\} = \{1\}$  právě, když  $0 = 1$ .



Polynomem rozumíme jakýkoliv konečný výraz, který lze poskládat ze známých konstantních prvků  $\mathbb{K}$  a jedné neznámé proměnné pomocí operací sčítání a násobení:

### Definition

Nechť  $\mathbb{K}$  je jakýkoliv komutativní okruh skalárů s jedničkou. Polynomem nad  $\mathbb{K}$  rozumíme konečný výraz

$$f(x) = \sum_{i=0}^k a_i x^i$$

kde  $a_i \in \mathbb{K}$ ,  $i = 0, 1, \dots, k$ , jsou tzv. **koeficienty polynomu**. Je-li  $a_k \neq 0$ , říkáme, že  $f(x)$  má **stupeň**  $k$ , píšeme  $\deg f = k$ . Nulový polynom nemá stupeň, polynomy stupně nula jsou právě nenulové prvky v  $\mathbb{K}$ , kterým říkáme konstantní polynomy.

Polynomy  $f(x)$  a  $g(x)$  jsou stejné, jestliže mají stejné nenulové koeficienty. Množinu všech polynomů nad okruhem  $\mathbb{K}$  budeme značit  $\mathbb{K}[x]$ .

Každý polynom zadává zobrazení  $f : \mathbb{K} \rightarrow \mathbb{K}$ , jehož hodnota vznikne dosazením hodnoty  $c$  za nezávislou proměnnou  $x$ , tj.

$$f(c) = a_0 + a_1c + \cdots + a_kc^k.$$

Všimněme si, že konstantní polynomy odpovídají právě konstantním zobrazením.

**Kořen polynomu**  $f(x)$  je takový prvek  $c \in \mathbb{K}$ , pro který je  $f(c) = 0 \in \mathbb{K}$ .

Obecně mohou různé polynomy definovat různá zobrazení. Např. polynom  $x^2 + x \in \mathbb{Z}_2[x]$  zadává identicky nulové zobrazení.

Obecněji, pro každý konečný okruh  $\mathbb{K} = \{a_0, a_1, \dots, a_k\}$  zadává polynom  $f(x) = (x - a_0)(x - a_1) \dots (x - a_k)$  identicky nulové zobrazení. Zároveň ale platí tvrzení, které dokážeme zanedlouho:

### Theorem

*Jestliže je  $\mathbb{K}$  nekonečný okruh, pak dva polynomy  $f(x)$  a  $g(x)$  nad  $\mathbb{K}$  jsou stejné právě, když jsou stejná příslušná zobrazení  $f$  a  $g$ .*

Dva polynomy  $f(x) = \sum_i a_i x^i$  a  $g(x) = \sum_i b_i x^i$  umíme přirozeně také sčítat i násobit:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_k + b_k)x^k$$

$$(f \cdot g)(x) = (a_0 b_0) + \cdots + (a_0 b_\ell + \cdots + a_\ell b_0)x^\ell + \dots$$

kde uvažujeme nulové koeficienty všude, kde v původním výrazu pro polynomy nenulové koeficienty nejsou a u sčítání nechť je  $k$  maximální ze stupňů  $f$  a  $g$ .

Tato definice vskutku odpovídá příslušným operacím sčítání a násobení hodnot zobrazení  $f, g : \mathbb{K} \rightarrow \mathbb{K}$ , díky vlastnostem „skalárů“ v původním okruhu  $\mathbb{K}$ .

Přímo z definice vyplývá, že množina polynomů  $\mathbb{K}[x]$  nad komutativním okruhem s jedničkou je opět komutativním okruhem s jedničkou, přičemž jedničkou v  $\mathbb{K}[x]$  je opět jednička 1 v okruhu  $\mathbb{K}$  vnímaná jako polynom stupně nula.

### Lemma

*Okruh polynomů nad oborem integrity je opět obor integrity.*

### Důkaz.

Máme ukázat, že v  $\mathbb{K}[x]$  mohou být netriviální dělitelé nuly pouze, jetliže jsou už v  $\mathbb{K}$ . To je ale zřejmé z výrazu pro násobení polynomů. Jsou-li  $f(x)$  a  $g(x)$  polynomy stupně  $k$  a  $\ell$  jako výše, pak koeficient u  $x^{k+\ell}$  v součinu  $f(x) \cdot g(x)$  je součin  $a_k \cdot b_\ell$  a ten musí být nenulový, pokud nejsou dělitelé nuly v  $\mathbb{K}$ . □

Směřujeme nyní ke zobecnění rozkladů polynomů nad číselnými obory a k tomu nejprve potřebujeme ujasnit, co je dělitelnost v základním okruhu  $\mathbb{K}$  samotném. Uvažujme proto nějaký pevně zvolený obor integrity  $\mathbb{K}$ , třeba celá čísla  $\mathbb{Z}$  nebo okruh  $\mathbb{Z}_p$  s prvočíselným  $p$ .

- je-li  $a|b$  a zároveň  $b|c$  pak také  $a|c$ ;
- $a|b$  a zároveň  $a|c$  pak také  $a|(\alpha b + \beta c)$  pro všechny  $\alpha, \beta \in \mathbb{K}$ ;
- $a|0$  pro všechny  $a \in \mathbb{K}$  (je totiž  $a \cdot 0 = 0$ );
- každý prvek  $a \in \mathbb{K}$  je dělitelný všemi jednotkami  $e \in \mathbb{K}$  a jejich násobky  $a \cdot e$  (jak přímo plyne z existence  $e^{-1}$ )

Řekneme, že prvek  $a \in \mathbb{K}$  je **nerozložitelný**, jestliže je dělitelný pouze jednotkami  $e \in \mathbb{K}$  a jejich násobky  $a \cdot e$ .

Řekneme, že okruh  $\mathbb{K}$  je **obor integrity s jednoznačným rozkladem**, jestliže platí:

- pro každý nenulový prvek  $a \in \mathbb{K}$  existují nerozložitelné  $a_1, \dots, a_r \in \mathbb{K}$  takové, že  $a = a_1 \cdot a_2 \dots a_r$
- jsou-li prvky  $a_1, \dots, a_r$  a  $b_1, \dots, b_s$  nerozložitelné, nejsou mezi nimi žádné jednotky a  $a = a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$ , pak je  $r = s$  a ve vhodném přeuspořádání platí  $a_j = e_j b_j$  pro vhodné jednotky  $e_j$ .

## Example

- 1  $\mathbb{Z}$  je obor integrity s jednoznačným rozkladem.
- 2 Každé pole (komutativní těleso) je obor integrity s jednoznačným rozkladem (a každý nenulový prvek je jednotka).
- 3 Necht'  $\mathbb{K}$  má prvky tvaru  $a_0 + \sum_{i=1}^k a_i \left( \sqrt[2^{n_i}]{x^{m_i}} \right)$  kde  $a_0, \dots, a_k \in \mathbb{Z}$ ,  $m_i, n \in \mathbb{Z}_{>0}$ . Pak jednotky jsou pouze prvky  $\pm 1$ , všechny prvky s  $a_0 = 0$  jsou rozložitelné, ale např. výraz  $x$  nelze vyjádřit jako součin nerozložitelných. (Nerozložitelných je zde příliš málo.)

Základním nástrojem pro diskusi dělitelnosti, společných dělitelů apod. v okruhu celých čísel  $\mathbb{Z}$  je procedura dělení se zbytkem a Euklidův algoritmus pro hledání největších společných dělitelů. Tyto postupy nyní zobecníme.

### Lemma (Algoritmus pro dělení se zbytkem)

*Nechť  $\mathbb{K}$  je komutativní okruh bez dělitelů nuly a  $f, g \in \mathbb{K}[x]$  polynomy,  $g \neq 0$ . Pak existuje  $a \in \mathbb{K}$ ,  $a \neq 0$ , a polynomy  $q$  a  $r$  splňující  $af = qg + r$ , kde  $r = 0$  nebo  $\deg r < \deg g$ . Je-li navíc  $\mathbb{K}$  pole, nebo je aspoň vedoucí koeficient polynomu  $g$  roven jedné, potom lze volit  $a = 1$  a polynomy  $q$  a  $r$  jsou v tomto případě určeny jednoznačně.*



Proceduru dělení se zbytkem můžeme okamžitě využít k diskusi kořenů polynomů.

Uvažme polynom  $f(x) \in \mathbb{K}[x]$ ,  $\deg f > 0$ , a dělme jej polynomem  $x - b$ ,  $b \in \mathbb{K}$ .

Protože je vedoucí koeficient jednička, algoritmus pro dělení dává jednoznačný výsledek. Dostáváme tedy jednoznačně zadané polynomy  $q$  a  $r$  splňující  $f = q(x - b) + r$ , kde  $r = 0$  nebo  $\deg r = 0$ , tj.  $r \in \mathbb{R}$ . Tzn., že hodnota polynomu  $f$  v  $b \in \mathbb{K}$  je rovna právě  $f(b) = r$ .

Proto je prvek  $b \in \mathbb{K}$  kořen polynomu  $f$  právě, když  $(x - b) \mid f$ .

Protože po vydělení polynomem stupně jedna vždy klesne stupeň výsledku alespoň o jedničku, dokázali jsme následující tvrzení:

### Corollary

*Každý polynom  $f \in \mathbb{K}[x]$  má nejvýše  $\deg f$  kořenů.*

Dva polynomy nad nekonečným komutativním okruhem, které zadávají stejné zobrazení  $\mathbb{K} \rightarrow \mathbb{K}$ , mají rozdíl, jehož kořenem je každý prvek v  $\mathbb{K}$ . Protože rozdíl polynomů má jen konečný stupeň, pokud není nulový, dokázali jsme tak již dříve uvedené tvrzení:

### Theorem

*Jestliže je  $\mathbb{K}$  nekonečný okruh, pak dva polynomy  $f(x)$  a  $g(x)$  nad  $\mathbb{K}$  jsou stejné právě, když jsou stejná příslušná zobrazení  $f$  a  $g$ .*

Polynom  $h$  je **největší společný dělitel** dvou polynomů  $f$  a  $g \in \mathbb{K}[x]$  jestliže:

- $h|f$  a zároveň  $h|g$
- jestliže  $k|f$  a zároveň  $k|g$  pak také  $k|h$ .

### Theorem (Bezoutova rovnost)

*Nechť  $\mathbb{K}$  je pole a necht'  $f, g \in \mathbb{K}[x]$ . Pak existuje největší společný dělitel  $h$  polynomů  $f$  a  $g$ . Polynom  $h$  je určený jednoznačně, až na násobek nenulovým skalárem. Přitom existují polynomy  $A, B \in \mathbb{K}[x]$  takové, že  $h = Af + Bg$ .*

Důkaz následujícího tvrzení je poměrně technický a nebudeme jej prezentovat v detailech (i když jsme si vše potřebné pro něj již v podstatě připravili).

### Theorem

*Je-li  $\mathbb{K}$  obor integrity s jednoznačným rozkladem, pak také okruh polynomů  $\mathbb{K}[x]$  je obor integrity s jednoznačným rozkladem.*

Důsledkem této věty je skutečnost, že každý polynom nad komutativním okruhem s jednoznačným rozkladem můžeme rozložit tak, jak to známe s polynomy s reálnými nebo komplexními koeficienty. Pokud má polynom tolik kořenů, včetně násobnosti, jako je jeho stupeň  $\deg f = k$ , je odpovídající rozklad tvaru

$$f(x) = (x - a_1) \cdot (x - a_2) \dots (x - a_k).$$

Zatímco reálné polynomy mohou být i úplně bez kořenů, každý komplexní polynom naopak takovýto rozklad připouští. To je obsahem tzv. základní věty algebry:

### Theorem (Základní věta algebry)

*Pole  $\mathbb{C}$  je algebraicky uzavřené, tj. každý polynom stupně alespoň 1 má kořen.*

Okruhy polynomů v proměnných  $x_1, \dots, x_r$  definujeme induktivně vztahem

$$\mathbb{K}[x_1, \dots, x_r] := \mathbb{K}[x_1, \dots, x_{r-1}][x_r].$$

Např.  $\mathbb{K}[x, y] = \mathbb{K}[x][y]$ , tzn. že uvažujeme polynomy v proměnné  $y$  nad okruhem  $\mathbb{K}[x]$ . Snadno se ověří, že polynomy v proměnných  $x_1, \dots, x_r$  lze chápat jako výrazy vzniklé z písmen  $x_1, \dots, x_n$  a prvků okruhu  $\mathbb{K}$  konečným počtem (formálního) sčítání a násobení v komutativním okruhu.

Například prvky v  $\mathbb{K}[x, y]$  jsou tvaru

$$\begin{aligned} f &= a_n(x)y^n + a_{n-1}(x)y^{n-1} + \dots + a_0(x) \\ &= (a_{mn}x^m + \dots + a_{0n})y^n + \dots + (b_{p0}x^p + \dots + b_{00}) \\ &= c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2 + \dots \end{aligned}$$

Jako důsledek naší definice a předchozích výsledků pro polynomy nad obecnými komutativními okruhy dostáváme:

### Corollary

- 1 *Jestliže v okruhu  $\mathbb{K}$  nejsou dělitelé nuly, pak také v okruhu polynomů  $\mathbb{K}[x_1, \dots, x_r]$  nejsou dělitelé nuly.*
- 2 *Je-li  $\mathbb{K}$  obor integrity s jednoznačným rozkladem, pak také okruh polynomů  $\mathbb{K}[x_1, \dots, x_r]$  je obor integrity s jednoznačným rozkladem.*

Nechť  $\mathbb{K}$  je komutativní okruh (s jedničkou) bez dělitelů nuly. Jeho **podílové těleso** definujeme jako třídy ekvivalence dvojic  $(a, b) \in \mathbb{K} \times \mathbb{K}$ ,  $b \neq 0$ , které zapisujeme  $\frac{a}{b}$ , a ekvivalence je dána

$$\frac{a}{b} = \frac{a'}{b'} \Leftrightarrow ab' = a'b.$$

Sčítání a násobení definujeme prostřednictvím reprezentantů tříd

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \frac{c}{d} = \frac{ac}{bd}$$

Snadno se ověří korektnost této definice a všechny axiomy komutativního tělesa. Zejména je  $\frac{0}{1}$  neutrální prvek vzhledem ke sčítání,  $\frac{1}{1}$  je neutrální prvek vzhledem k násobení a pro  $a \neq 0$ ,  $b \neq 0$  je  $\frac{a}{b} \frac{b}{a} = \frac{1}{1}$ .



Podílové těleso okruhu  $\mathbb{K}[x_1, \dots, x_r]$  nazýváme **těleso racionálních funkcí** a značíme je  $\mathbb{K}(x_1, \dots, x_r)$ .

Všechny algebraické operace s polynomy v softwarových systémech jako je Maple nebo Mathematica jsou prováděny ve skutečnosti nad podílovými tělesy, tj. v tělesech racionálních funkcí, zpravidla s použitím  $\mathbb{K} = \mathbb{Q}$ .