5. Obory integrity a dělitelnost (okruhy polynomů, pravidla dělitelnosti, Gaussovy a Eukleidovy okruhy)

Okruhy polynomů

Upralgfin-esf.pdf (str. 39)

budeme definovat **okruh polynomů** neurčité x nad R jako podokruh $(R[x],+,0,-,\cdot,1)$ okruhu R[[x]] (Okruh R[[x]] se nazývá okruh formálních mocninných řad neurčité x nad R) takový, že $R[x] := \{a_0 + a_1x + ... + a_nx^n \mid n \in \mathbb{N}_0, a_i \in R\}$.

Prvky množiny R[x] se nazývají polynomy a zapisují se jako f(x), p(x), … Každý polynom $p(x) \in R[x]$ má tvar $p(x) = \sum^n_{k=0} a_kx^k$, kde $n \in \mathbb{N}_0$. Buď dále $q(x) = \sum^m_{k=0} b_kx^k$, $m \leq n$.
Kdy platí p(x) = q(x)? Zřejmě platí $q(x) = \sum^n_{k=0} b_kx^k$, přičemž $b_k = 0$ pro $m < k \leq n$. Máme tedy $p(x) = q(x) \Leftrightarrow a_k = b_k$ pro k = 0, ..., n.

S polynomy se počítá podle zákonů komutativního okruhu R[x] s jednotkovým prvkem.
Je-li $p(x) = \sum^n_{k=0} a_kx^k$, kde $a_n \neq 0$, pak se n nazývá **stupeň** polynomu p(x)
(píšeme n = grad p(x)).

Je-li $p(x) = \sum^n_{k=0} a_kx^k \in R[x]$, pak se prvky a_k nazývají **koeficienty** polynomu p(x). $0 \in R[x]$ je **nulový polynom**, $a \in R \subseteq R[x]$ se nazývá **konstantní** polynom. Platí-li grad p(x) = n a $a_n = 1$, pak se p(x) nazývá **normovaný** polynom. Polynomy tvaru ax + b, kde $a \neq 0$, se nazývají **lineární** polynomy.

Mocninné řady a polynomy n neurčitých $x_1, \ldots, x_n$

Indukcí se definuje:

$$R[[x_1]] := R[[x]],\ R[[x_1, \ldots, x_n]] := (R[[x_1, \ldots, x_{n-1}]])[[x_n]],\ n > 1$$

a podobně:

$$R[x_1] := R[x],\ R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n],\ n > 1.$$

Potom platí (důkaz úplnou indukcí podle *n*):

$$R[x_1, \ldots, x_n] = \{ \sum_{0 \leq i_1, \ldots, i_n \leq m} a_{i_1 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid m \in \mathbb{N}_0,\ a_{i_1 \ldots i_n} \in R \}.$$

Např. prvek z $R[x_1, x_2]$ má obecný tvar: $p(x_1, x_2) = a_{00} + a_{10}x_1 + a_{01}x_2 + a_{20}x^2_1 + a_{11}x_1x_2 + a_{02}x^2_2 + \ldots + a_{jk}x^j_1x^k_2$.

Polynomy a funkce

Princip dosazování. Buď $(R,+,0,-,\cdot,1)$ komutativní okruh s jednotkovým prvkem a $p(x) = a_nx^n + \cdots + a_1x + a_0 \in R[x]$. Pro $a \in R$ je potom $p(a) := a_na^n + \cdots + a_1a + a_0$ opět prvkem z R, který se nazývá **hodnota polynomu** v *a*. Funkce

$$\begin{cases} R \to R \\ a \mapsto p(a) \end{cases}$$

se nazývá polynomiální funkce **indukovaná polynomem** p(x) a často se také označuje p.

Buď $p(x) \in R[x]$ (R komutativní okruh s jednotkovým prvkem). Potom se $a \in R$ nazývá **kořen**

polynomu $p(x) :\Leftrightarrow p(a) = 0$. Polynom $p(x)$ se nazývá **dělitelný** polynomem $q(x) \in R[x]$ (formálně: $q(x)|p(x)) :\Leftrightarrow p(x) = q(x)r(x)$, kde $r(x) \in R[x]$.

Je-li *a* kořen polynomu $p(x)$, pak je $p(x)$ dělitelný linearním polynomem $x - a$ (a opačně).

Buď $p(x) \in R[x] \setminus \{0\}$ a nechť $a \in R$ je kořenem $p(x)$. Potom největší číslo $k \in N$ takové, že $(x - a)^k|p(x)$, se nazývá násobnost kořene a. ($k \leq n$)

Nechť $a_1, \ldots, a_r$ jsou po dvou různé kořeny polynomu $p(x) \in R[x]$ s násobnostmi $k_1, \ldots, k_r$. Potom platí:

$$(x - a_1)^{k_1} \ldots (x - a_r)^{k_r} |p(x).$$

Důsledek: Nechť $a_1, \ldots, a_r$ jsou po dvou různé kořeny polynomu $p(x) \in R[x]$ s násobnostmi $k_1, \ldots, k_r$. Potom platí: $k_1 + \ldots + k_r \leq \text{grad } p(x)$.

Polynom nemusí mít žádné kořeny.

Pole K se nazývá **algebraicky uzavřené**, jestliže každý polynom $p(x) \in K[x]\backslash K$ má aspoň jeden kořen.

(Gaussova základní věta algebry) Množina $\mathbb{C}$ je algebraicky uzavřená.

Vypočet kořenů polynomů nad poli

1. grad $p(x) = 1$: trivialni.
2. grad $p(x) = 2$: $p(x) = ax^2 + bx + c$ ($a \neq 0$) ma kořeny $(-b \pm \sqrt{(b^2-4ac)})/2a$ (”2” resp. ”4” zde označuje $1 + 1$ resp. $1 + 1 + 1 + 1$; vyjádřeni kořenů musí existovat a musí být $1 + 1 \neq 0$).
3. grad $p(x) = 3, 4$: Cardanovy vzorce (Cardano Tartaglia).
4. grad $p(x) > 4$: zde už neexistují obecné ”vzorce” (vyžadující pouze základní početní postupy a odmocňování).

Interpolace pomocí polynomů

Buď K pole a $f : K \to K$ funkce.
Zadáno: $b_i = f(a_i)$ pro po dvou různá $a_i \in K$, $1 \leq i \leq n$ (např.: výsledek řady měření).
Hledá se: $p(x) \in K[x]$, kde $p(a_i) = b_i = f(a_i)$, $1 \leq i \leq n$, a $\text{grad } p(x) < n$. (Existuje nejvýše jeden takový polynom $p(x)$: z $p(a_i) = q(a_i)$, $1 \leq i \leq n$, kde grad $p(x)$, grad $q(x) < n$
totiž plyne $p = q$.)

Lagrangeovy interpolačni vzorce:

Buď:

$$q_i(x) := \prod_{\substack{1 \leq j \leq n, \\ j \neq i}} (x - a_j) = (x - a_1) \cdots (x - a_{i-1})(x - a_{i+1}) \cdots (x - a_n).$$

Potom platí:

$$q_i(a_k) = \begin{cases} 0 & \text{pro } i \neq k, \\ \prod_{1 \leq j \leq n,\, j \neq i} (a_k - a_j) \neq 0 & \text{pro } i = k. \end{cases}$$

pro:

$$p(x) := \sum_{i=1}^{n} b_i \frac{q_i(x)}{q_i(a_i)}$$

platí potom $p(a_j) = b_j$, $1 \leq j \leq n$.

Důsledek: Je-li K konečné pole (např. $K = \mathbb{Z}_p$, p prvočíslo), $f : K \to K$, potom existuje polynom $p(x) \in K[x]$ takový, že $f(a) = p(a)$ pro všechna $a \in K$.

Newtonovy interpolační vzorce

Obor integrity

Upralgfin-esf.pdf (str. 45)

Komutativní okruh s jednotkovým prvkem (R,+, 0,–, ·, 1) se nazývá **obor integrity** :⇔

1. $R \setminus \{0\} \neq \emptyset$ (tj. $0 \neq 1$),
2. $\forall x, y \in R : x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$ (tj. neexistují dělitelé nuly).

Jednoduchá pravidla dělitelnosti

Buď (I,+, 0,–, ·, 1) obor integrity. Jsou-li *a*, *b* ∈ I, potom říkáme, že prvek *a* je **dělitelný** prvkem *b* a *b* se nazývá **dělitel** prvku *a* (*b* „dělí“ *a*, formálně: $b|a$) :⇔$\exists c \in I : a = bc$.

Elementární pravidla dělitelnosti:

1. $\forall a \in I : a|0$,
2. $\forall a \in I : 1|a$,
3. $\forall a \in I : a|a$,
4. $\forall a, b, c \in I : a|b \wedge b|c \Rightarrow a|c$,
5. $\forall a, b, c \in I : a|b \Rightarrow a|bc$,
6. $\forall a, b, c \in I : a|b \wedge a|c \Rightarrow a|b + c$,
7. $\forall a, b, c \in I, c \neq 0 : a|b \Leftrightarrow ac|bc$,
8. $\forall a, b, c, d \in I : a|b \wedge c|d \Rightarrow ac|bd$,
9. $\forall a, b \in I, n \in \mathbb{N} : a|b \Rightarrow a^n|b^n$.

Buď (I,+, 0,–, ·, 1) obor integrity. Dělitel prvku 1 se nazývá jednotka oboru integrity I. Buď E(I) množina všech jednotek I. Prvky a, b ∈ I se nazývají **asociované**.

(formálně: $a \sim b) :\Leftrightarrow \exists e \in E(I) : a = be$

Příklady:

1. $I = \mathbb{Z}$: $E(I) = \{\pm 1\}$, tedy $a \sim b \Leftrightarrow a = \pm b$.
2. I = K (K pole): $E(I) = K \setminus \{0\}$, tedy $a \sim b \Leftrightarrow a, b \neq 0 \vee a = b = 0$.
3. I = K[x] (K pole): $E(I) = K \setminus \{0\}$ (jelikož grad p(x)q(x) = grad p(x) + grad q(x)), platí $p(x) \sim q(x) \Leftrightarrow \exists a \in K \setminus \{0\} : p(x) = aq(x)$.

- e ∈ I je jednotka oboru integrity I ⇔ $\exists f \in I : ef = 1$.
- (E(I), ·) je abelovska grupa, ktera se nazyva **grupa jednotek** oboru integrity I.
- ~ je relace kongruence na (I, ·).
- $\forall a, b \in I : a \sim b \Leftrightarrow a|b \wedge b|a$.

Příklad: Třídy ekvivalence vzhledem k $\sim$:

1. $I = \mathbb{Z}$: $\{0\}, \{\pm 1\}, \{\pm 2\}, \ldots, \{\pm n\}, \ldots, n \in \mathbb{N}$.
2. $I = K$: $\{0\}, K \setminus \{0\}$.
3. $I = K[x]$: $\{0\}, \{ap(x) \mid a \in K \setminus \{0\}, p(x)$ normovaný$\}$.

Buď $(I,+,0,-,\cdot,1)$ obor integrity, $a \in I$.
Triviální dělitelé prvku a: jsou všechna $e \in E(I)$ a všechna b taková, že $b \sim a$.
Vlastní dělitel prvku a: všechna b taková, že $b|a$, $b \notin E(I)$ a $b \not\sim a$.

Prvek $a \in I \setminus E(I)$, $a \neq 0$, se nazývá **ireducibilní** prvek $:\Leftrightarrow$ a má pouze triviální dělitele.

Přiklady:

1. $I = \mathbb{Z}$: $a \in I$ je ireducibilní prvek $\Leftrightarrow a = \pm p$, p prvočíslo.
2. $I = K[x]$ (K Pole): Ireducibilní prvky se nazývají ireducibilní polynomy. Např. Lineární polynom $ax + b$, $a \neq 0$ je vždy ireducibilní prvek. V algebraicky uzavřeném poli je každý ireducibilní polynom take lineární.
3. $I = \mathbb{R}[x]$: ireducibilní prvky jsou zde všechny lineárni polynomy a polynomy ax^2+bx+c, kde $a \neq 0$ a $b^2 - 4ac < 0$. (Ze základní věty algebry plyne, že žádné jiné neexistují.)
4. $I = K[x]$, K konečné pole: ke každému $n \in N$ existuje polynom $p(x) \in K[x]$ takový, že grad $p(x) = n$ a $p(x)$ je ireducibilní prvek.

$p \in I \setminus E(I)$, $p \neq 0$, se nazývá **prvočinitel** $:\Leftrightarrow p|ab \Rightarrow p|a \vee p|b$.

Gaussovy okruhy

Obor integrity I se nazýva Gaussův okruh $:\Leftrightarrow$ Ke každému prvku $a \in I \setminus E(I)$, $a \neq 0$, existují prvočinitelé $p_1, \ldots, p_r$ tak, že platí že $a = p_1 \ldots p_r$.

Jednoznačnost rozkladu na prvočinitele: Buď I Gaussův okruh, $a \in I \setminus E(I)$, $a \neq 0$, $a = p^{(1)}_1 \ldots p^{(1)}_{r1} = p^{(2)}_1 \ldots p^{(2)}_{r2}$, kde $p^{(1)}_i$, $p^{(2)}_j$ jsou prvočinitele. Potom je $r_1 = r_2 =: r$ a existuje permutace π množiny $\{1, \ldots, r\}$ takova, že $p^{(1)}_i \sim p^{(2)}_{\pi(i)}$, $i = 1, \ldots, r$.

Příklad: $\mathbb{Z}$ a $K[x]$ (K pole) jsou Gaussovy okruhy

Buď I obor integrity, $a_1, \ldots, a_n \in I$.

1. $d \in I$ se nazývá největší společný dělitel (NSD) prvků $a_1, \ldots, a_n \in I :\Leftrightarrow$ (i) $d|a_i$, $i = 1, \ldots, n$ a (ii) $\forall t \in I : t|a_i$, $i = 1, \ldots, n \Rightarrow t|d$.
2. $v \in I$ se nazývá nejmenší společný násobek (NSN) prvků $a_1, \ldots, a_n \in I :\Leftrightarrow$ (i) $a_i|v$, $i = 1, \ldots, n$ a (ii) $\forall w \in I : a_i|w$, $i = 1, \ldots, n \Rightarrow v|w$.

V Gaussově okruhu I je každý ireducibilní prvek prvočinitelem.

Uvažujme faktorovou množinu $I/\sim = \{[a]_\sim \mid a \in I\}$ a nechť z každe třidy rozkladu $[a]_\sim = \{b \in I \mid b \sim a\}$ je vybran pevny prvek $n([a]_\sim)$ (to je možne dle tzv. axiomu vyběru, ktery užívame), tj.

$$n : \begin{cases} I/\sim \longrightarrow I \\ [a]_\sim \mapsto n([a]_\sim) \in [a]_\sim. \end{cases}$$

Prvky množiny n(I/ ∼) se nazývají **normované prvky** (vzhledem k n).
Každá třída $[a]_\sim$, kde a je prvočinitel, se skládá pouze z prvočinitelů. Prvky $n([a]_\sim)$, kde a je prvočinitel, se nazývají **normovaní prvočinitelé**.

Přiklad:
1. $I = \mathbb{Z}$, $n([a]_\sim) = n(\{\pm a\}) = |a|$.
2. $I = K[x]$, $n(\{0\}) = 0$, $n([p(x)]_\sim) = q(x)$, přičemž $p(x) = a_n x^n + \dots + a_1 x + a_0$, $a_n \neq 0$, $q(x) = (1/a_n)p(x)$.

Buď I Gaussův okruh, $a_1, \dots, a_n \in I$, $a_i \neq 0$, $a_i = e_i p_1^{e_{1i}} \dots p_r^{e_{ri}}$, $e_i \in E(I)$, p_j navzájem různí normovaní prvočinitelé, $e_{ji} \in \mathbb{N}_0$. Potom platí:

a
$$\mathrm{NSD}(a_1, \dots, a_n) = p_1^{\min_{1\le i\le n}(e_{1i})} \dots p_r^{\min_{1\le i\le n}(e_{ri})}$$
$$\mathrm{NSN}(a_1, \dots, a_n) = p_1^{\max_{1\le i\le n}(e_{1i})} \dots p_r^{\max_{1\le i\le n}(e_{ri})}.$$

Jsou-li některá $a_i = 0$, potom je $\mathrm{NSD}(a_1, \dots, a_n) = \mathrm{NSD}(a_i \mid a_i \neq 0)$; jsou-li všechna $a_i = 0$, potom je $\mathrm{NSD}(a_1, \dots, a_n) = 0$. Jsou-li některá $a_i = 0$, pak je $\mathrm{NSN}(a_1, \dots, a_n) = 0$.

Eukleidovy okruhy
Obor integrity I se nazývá **Eukleidův okruh** :⇔ existuje zobrazeni $H : I \setminus \{0\} \to \mathbb{N}_0$ (eukleidovské ohodnocení) s následující vlastností: pro všechna $a \in I \setminus \{0\}$, $b \in I$ existují $q, r \in I$ tak, že $b = aq + r$, kde $r = 0 \vee H(r) < H(a)$ (dělení se zbytkem).

Příklad:
1. $\mathbb{Z}$ je Eukleidův okruh, kde $H(a) := |a|$.
2. Každé pole je Eukleidův okruh ($q = a^{-1}b$, $r = 0$).

Každý Eukleidův okruh je Gaussův okruh.

Eukleidův algoritmus pro výpočet NSD v Eukleidových okruzích:
Buď I Eukleidův okruh a a, b ∈ I. Pro a = b = 0 je NSD(a, b) = 0. Nechť bez újmy na obecnosti $a \neq 0$.

Po
$$\begin{array}{rcl}
 & \text{Pak} & \exists q_1, r_1 \in I : b = aq_1 + r_1,\ r_1 = 0 \vee H(r_1) < H(a), \\
\text{pro } r_1 \neq 0 & \Rightarrow & \exists q_2, r_2 \in I : a = r_1 q_2 + r_2,\ r_2 = 0 \vee H(r_2) < H(r_1), \\
\text{pro } r_2 \neq 0 & \Rightarrow & \exists q_3, r_3 \in I : r_1 = r_2 q_3 + r_3,\ r_3 = 0 \vee H(r_3) < H(r_2), \\
 & \vdots & \\
\text{obecně:} & & \\
\text{pro } r_i \neq 0 & \Rightarrow & \exists q_{i+1}, r_{i+1} \in I : r_{i-1} = r_i q_{i+1} + r_{i+1},\ r_{i+1} = 0 \vee H(r_{i+1}) < H(r_i). \\
 & & (\text{Přitom je třeba dosadit } a = r_0 \text{ a } b = r_{-1}.)
\end{array}$$
konečném počtu kroků (vzhledem k tomu, že $H(a) = H(r_0) > H(r_1) > H(r_2) > \dots$) obdržíme k takové, že $r_k = 0$ a $r_{k-1} \neq 0$. $r_{k-1} = \mathrm{NSD}(a, b)$.