

# OBORY POLYNOMŮ. KVADRATICKÁ ROZŠÍŘENÍ $\mathbb{Z}$ .

DAVID STANOVSKÝ

## 1. PODÍLOVÁ TĚLESA

**Cíl.** *Ukážeme abstraktní konstrukci tělesa zlomků.*

Tak jako lze obor celých čísel rozšířit do tělesa racionálních čísel, každý obor integrity  $\mathbf{R}$  lze rozšířit na tzv. *podílové těleso*, které lze zkonstruovat jako „těleso zlomků“, jejichž číselník i jmenovatel jsou prvky daného oboru. Podílová tělesa hrají v komutativní algebře důležitou roli, jak uvidíme například v Sekci ??, kde nám budou nástrojem k důkazu Gaussovy věty.

Konstrukce probíhá následujícím způsobem. Definujeme relaci  $\sim$  na množině  $R \times (R \setminus \{0\})$  předpisem

$$(a, b) \sim (c, d) \iff ad = bc.$$

Není těžké nahlédnout, že jde o ekvivalenci: reflexivita je zřejmá, symetrie plyne z komutativity násobení a tranzitivitu získáme následujícím výpočtem: je-li  $(a, b) \sim (c, d) \sim (e, f)$ , tedy  $ad = bc$  a  $cf = de$ . Pak ale  $adf = bcf = bde$ , a tedy  $af = be$ , protože  $d \neq 0$  (ke krácení potřebujeme předpoklad, že  $\mathbf{R}$  je obor integrity!).

Pro jednoduchost vyjadřování budeme značit blok  $[(a, b)]_{\sim}$  této ekvivalence jako zlomek  $\frac{a}{b}$ . Uvažujme množinu  $Q$  všech bloků této ekvivalence (tj. všech zlomků) a definujme na ní operace

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad -\frac{a}{b} = \frac{-a}{b}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad 0 = \frac{0}{1}, \quad 1 = \frac{1}{1}.$$

Je třeba dokázat, že tyto operace jsou dobře definované. Předně, aby jmenovatel součtu a součinu zůstal nenulový, potřebujeme předpoklad, že  $\mathbf{R}$  je obor integrity. A dále musíme dokázat, že pokud zvolíme jiné reprezentanty zlomků, výsledek operace zůstane stejný. Formálně, pokud  $\frac{a}{b} = \frac{a'}{b'}$  a  $\frac{c}{d} = \frac{c'}{d'}$ , potřebujeme dokázat, že  $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ , a podobně pro odčítání a násobení. Důkaz provedeme pro sčítání: chceme ověřit, že  $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ , tedy že  $(ad + bc)(b'd') = (a'd' + b'c')(bd)$ . Roznásobíme a využijeme faktu, že  $ab' = a'b$  a  $cd' = c'd$ . Označme  $Q$  množinu  $Q$  s operacemi  $+$ ,  $-$ ,  $\cdot$  a konstantami  $0, 1$ .

**Tvrzení 1.1.** *Bud'  $\mathbf{R}$  obor integrity a  $Q$  výsledek právě popsané konstrukce. Pak  $Q$  je těleso a obor  $\mathbf{R}$  je podoborem tělesa  $Q$ , pokud ztotožníme prvek  $a \in R$  s prvkem  $\frac{a}{1} \in Q$ .*

Těleso  $Q$  se nazývá *podílové těleso* oboru  $\mathbf{R}$ .

*Důkaz.* Ověříme postupně všechny axiomy:

- Asociativita sčítání:  $\frac{a}{b} + (\frac{c}{d} + \frac{e}{f}) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf} = \frac{adf+bcf+bde}{bdf} = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$ .

- Komutativita sčítání:  $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$ .
- Nula:  $\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b \cdot 1} = \frac{a}{b}$ .
- Odčítání:  $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{b^2} = \frac{0}{b^2} = 0$ .
- Asociativita a komutativita násobení plyne okamžitě z týchž vlastností oboru  $\mathbf{R}$ .
- Jednotka:  $\frac{a}{a} \cdot \frac{1}{1} = \frac{a \cdot 1}{a \cdot 1} = \frac{a}{a}$ .
- Distributivita:  $\frac{a}{b} \cdot \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{acf+ade}{bdf} = \frac{bcf+abde}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf}$ .
- $0 = \frac{0}{1} \neq 1 = \frac{1}{1}$ , protože  $0 \cdot 1 \neq 1 \cdot 1$ .

Navíc  $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$  pro každé  $\frac{a}{b} \neq 0$ , čili  $\mathbf{Q}$  je těleso. Zbývá dokázat, že prvky tvaru  $\frac{a}{1}$  tvoří podobor  $\mathbf{Q}$ , což je snadné.  $\square$

**Příklad.** Těleso racionálních čísel  $\mathbf{Q}$  je *definováno* jako podílové těleso oboru  $\mathbf{Z}$ .

**Příklad.** Je-li  $\mathbf{T}$  těleso, pak jeho podílové těleso je, při výše uvedeném ztotožnění  $a = \frac{a}{1}$ , rovno  $\mathbf{T}$ , protože  $\frac{a}{b} = \frac{ab^{-1}}{1}$  pro každé  $a, b \in T, b \neq 0$ .

**Příklad.** Podílové těleso oboru  $\mathbf{Z}[i]$  je, formálně vzato, těleso zlomků tvaru  $\frac{a+bi}{c+di}$ , kde  $a, b, c, d \in \mathbf{Z}$ . Pokud ztotožníme tento zlomek se číslem  $\frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$ , dostaneme těleso  $\mathbf{Q}[i]$ . (Formálně bychom řekli, že podílové těleso oboru  $\mathbf{Z}[i]$  je *izomorfní* s tělesem  $\mathbf{Q}[i]$ , viz Sekce ??).

## 2. POLYNOMY A FORMÁLNÍ MOCNINNÉ ŘADY

**Cíl.** Nejprve zformulujeme, co je to přesně polynom (a formální mocninná řada) a jak se definují základní operace, a poté se bude věnovat nejdůležitějším vlastnostem polynomů: dělení se zbytkem, souvislost kořenů s dělitelností, ukážeme, že za rozumných předpokladů má polynom stupně  $n$  nejvýše  $n$  kořenů, podíváme se, jak souvisí násobnost kořene daného polynomu s kořeny jeho derivací a na závěr zmíníme větu o interpolaci.

### 2.1. Definice a základní operace.

**Definice.** Polynomem proměnné  $x$  nad oborem integrity  $\mathbf{R}$  rozumíme formální výraz

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n,$$

nebo zkráceně

$$\sum_{i=0}^n a_i x^i,$$

kde  $a_0, \dots, a_n \in R$  a  $a_n \neq 0$ . Prvky  $a_0, \dots, a_n$  nazýváme *koefficienty* a symbol  $x$  *proměnná*. (Implicitně se rozumí se  $a_m = 0$  pro všechna  $m > n$ .) Číslo  $n$  nazýváme *stupeň polynomu*, značíme  $\deg f$ . Prvek  $a_n$  se nazývá *vedoucí koeficient* a  $a_0$  *absolutní člen*. Polynom se nazývá *monický*, pokud je vedoucí člen 1. Je třeba speciálně dodefinovat *nulový polynom*; pro něj položíme  $\deg 0 = -1$ .

Na množině všech polynomů definujeme operace předpisy

$$\begin{aligned} \sum_{i=0}^m a_i x^i + \sum_{i=0}^n b_i x^i &= \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i, & - \sum_{i=0}^m a_i x^i &= \sum_{i=0}^m (-a_i) x^i, \\ \left( \sum_{i=0}^m a_i x^i \right) \cdot \left( \sum_{i=0}^n b_i x^i \right) &= \sum_{i=0}^{m+n} \left( \sum_{j+k=i} a_j b_k \right) x^i. \end{aligned}$$

Jak si za chvíli dokážeme, dostaneme obor integrity; značíme jej  $\mathbf{R}[x]$ .

**Definice.** *Formální mocninnou řadou proměnné  $x$  nad oborem integrity  $\mathbf{R}$  rozumíme formální výraz*

$$\sum_{i=0}^{\infty} a_i x^i,$$

kde  $a_0, a_1, \dots \in R$ ; používáme obdobnou terminologii. Tedy polynom je mocninná řada, v níž je jen konečně mnoho nenulových koeficientů. Speciálně  $0 = \sum_{i=0}^{\infty} 0x^i$ . (Jde o *formální výrazy*, nikoliv o funkce nebo součty. Otázky typu konvergence nás nezajímají.)

Na množině všech formálních mocninných řad definujeme analogicky operace

$$\begin{aligned} \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i &= \sum_{i=0}^{\infty} (a_i + b_i) x^i, & - \sum_{i=0}^{\infty} a_i x^i &= \sum_{i=0}^{\infty} (-a_i) x^i, \\ \left( \sum_{i=0}^{\infty} a_i x^i \right) \cdot \left( \sum_{i=0}^{\infty} b_i x^i \right) &= \sum_{i=0}^{\infty} \left( \sum_{j+k=i} a_j b_k \right) x^i. \end{aligned}$$

Jak si nyní dokážeme, dostaneme obor integrity; značíme jej  $\mathbf{R}[[x]]$ . Polynomy zřejmě tvoří jeho podobor, protože součet i součin dvou polynomů je opět polynom.

**Tvrzení 2.1.** *Je-li  $\mathbf{R}$  obor integrity, pak  $\mathbf{R}[x]$  i  $\mathbf{R}[[x]]$  jsou také obory integrity.*

*Důkaz.* Důkaz stačí provést pro formální mocninné řady, protože polynomy jsou jejich speciálním případem (obecněji, podokruh oboru integrity je vždy oborem integrity).

Ověření rovností z definice komutativního okruhu je mechanická práce, ukážeme pouze hlavní myšlenky. Rovnosti pro sčítání jsou očividné, komutativita násobení také. Pro jednotku, součin  $(\sum a_i x^i) \cdot (1 + 0 + 0 + \dots)$  dává řadu  $\sum (\sum_{j+k=i} a_j b_k) x^i$ , kde všechny  $b_i$  kromě  $b_0$  jsou nulové, takže výsledkem je opět  $\sum a_i x^i$ . Asociativita je obtížnější: z jedné strany  $(\sum a_i x^i) \cdot ((\sum b_i x^i) \cdot (\sum c_i x^i)) = (\sum a_i x^i) \cdot ((\sum_{k+l=i} (\sum_{j+k+l=i} b_j c_l) x^i)) = \sum (\sum_{j+k+l=i} a_j b_k c_l) x^i$ , a je vidět, že stejně vyjde i analogický výpočet součinu  $((\sum a_i x^i) \cdot (\sum b_i x^i)) \cdot (\sum c_i x^i)$ . Distributivita se ověří podobně.

Zajímavější je důkaz, že pro  $f, g \neq 0$  je  $f \cdot g \neq 0$ . Buď  $f = \sum a_i x^i$  a  $g = \sum b_i x^i$  dva nenulové prvky  $\mathbf{R}[[x]]$  a označme  $m, n$  nejmenší indexy takové, že  $a_m, b_n \neq 0$ . Uvažujeme-li v součinu  $f \cdot g$  koeficient u  $x^{m+n}$ , dostáváme vyjádření

$$\sum_{j+k=m+n} a_j b_k = \underbrace{a_0 b_{m+n} + \dots + a_{m-1} b_{n+1}}_0 + \underbrace{a_m b_n}_{\neq 0} + \underbrace{a_{m+1} b_{n-1} + \dots + a_{m+n} b_0}_0.$$

Protože je  $\mathbf{R}$  obor integrity a  $a_m, b_n \neq 0$ , tak také  $a_m b_n \neq 0$  a tento koeficient je nenulový.  $\square$

Obory *polynomů a mocninných řad více proměnných* se definují induktivně, předpisy

$$\begin{aligned}\mathbf{R}[x_1, \dots, x_n] &= (\mathbf{R}[x_1, \dots, x_{n-1}])[x_n], \\ \mathbf{R}[[x_1, \dots, x_n]] &= (\mathbf{R}[[x_1, \dots, x_{n-1}]])[[x_n]].\end{aligned}$$

Polynom  $f$  z  $\mathbf{R}[x_1, \dots, x_n]$  je výraz tvaru  $f = \sum_{i=0}^{\infty} f_i x_n^i$ , kde  $f_i$  jsou polynomy z  $\mathbf{R}[x_1, \dots, x_{n-1}]$ . Za pomoci distributivity jej můžeme přepsat (právě jedním způsobem) do standardního tvaru

$$f = \sum_{k_1, \dots, k_n=0}^N a_{k_1, \dots, k_n} x_1^{k_1} \cdots x_n^{k_n}$$

s koeficienty  $a_{k_1, \dots, k_n} \in R$ . Podobně pro mocninné řady. Z Tvrzení 2.1 za pomoci indukce ihned plyne, že jde o obory integrity.

## 2.2. Hodnota polynomu v bodě.

Je třeba striktně rozlišovat mezi polynomem jako *formálním výrazem* a jeho *hodnotou po dosazení* nějakého prvku. Formálně, buď  $R \leq S$  obory integrity. Polynom  $f \in R[x]$  je formální výraz

$$f = a_0 + a_1 x + \dots + a_n x^n$$

(tento se bude zapisovat výhradně  $f$ , bez uvedení proměnné). Jeho hodnotou po dosazení prvku  $u \in S$  rozumíme prvek

$$f(u) = a_0 + a_1 u + \dots + a_n u^n \in S,$$

přičemž v uvedeném zápise provádíme všechny operace (mocnění, násobení i sčítání) v oboru  $\mathbf{S}$ . Např. pro  $\mathbf{R} = \mathbf{S} = \mathbb{Z}_p$  a  $f = x^p + 1$  platí  $f(0) = 1$ ,  $f(1) = 2$ ,  $f(2) = 3$  atd., viz malá Fermatova věta.

Pro daný polynom  $f \in R[x]$  a obor  $S \geq R$  můžeme uvažovat tzv. *polynomiální zobrazení*  $S \rightarrow S$ , které každému prvku  $u \in S$  přiřadí hodnotu  $f(u)$ . Různé polynomy mohou dávat stejná polynomiální zobrazení, např. výše uvedený polynom určuje na  $\mathbb{Z}_p$  stejné zobrazení jako polynom  $g = x + 1$ . (Jinak to pro konečné obory být ani nemůže, protože existuje nekonečně mnoho polynomů, ale pouze konečně mnoho zobrazení na konečné množině.)

Pojem hodnoty mocninné řady nemá v algebře smysl uvažovat. Bez další geometrické struktury není možné říci, co se rozumí nekonečným součtem, v řadě oborů (třeba konečných) se smysluplný pojem konvergence ani nedá vybudovat.

## 2.3. Dělení polynomů se zbytkem.

Buď  $f, g$  polynomy z  $\mathbf{R}[x]$ . Řekneme, že  $g$  *dělí*  $f$ , píšeme  $g \mid f$ , pokud existuje polynom  $h \in R[x]$  takový, že  $f = gh$ . Všimněte si, že pokud  $g \mid f$  a  $f \neq 0$ , pak  $\deg g \leq \deg f$ . (Každý polynom dělí nulový polynom, přitom stupeň nulového polynomu je  $-1$ .) Pokud  $g$  nedělí  $f$ , má smysl se ptát po zbytku po dělení.

**Tvrzení 2.2.** *Buď  $\mathbf{R}$  obor integrity,  $\mathbf{Q}$  jeho podílové těleso,  $f, g \in R[x]$ ,  $g \neq 0$ . Pak existuje právě jedna dvojice  $q, r \in Q[x]$  splňující  $f = gq + r$  a  $\deg r < \deg g$ . Navíc, je-li  $g$  monický, pak  $q, r \in R[x]$ .*

Díky jednoznačnosti můžeme definovat  $f \operatorname{div} g = q$  a  $f \operatorname{mod} g = r$ . Je vidět, že  $g \mid f$  právě tehdy, když  $f \operatorname{mod} g = 0$ .

*Důkaz.* Podíl a zbytek dvou polynomů se počítá podobně jako pro celá čísla. Algoritmus lze formulovat takto: inicializujeme  $q_0 = 0$ ,  $r_0 = f$ , a poté definujeme rekurzivně

$$q_{i+1} = q_i + \frac{l(r_i)}{l(g)} \cdot x^{\deg r_i - \deg g}, \quad r_{i+1} = r_i - \frac{l(r_i)}{l(g)} \cdot x^{\deg r_i - \deg g} \cdot g,$$

kde  $l(u)$  značí vedoucí koeficient polynomu  $u$ . Rekurzi pokračujeme do té doby, než bude  $\deg r_i$  menší než  $\deg g$ . To jistě někdy nastane, protože je vždy  $\deg r_{i+1} < \deg r_i$ . Přitom evidentně platí  $f = gq_i + r_i$  pro všechna  $i$ , a tedy poslední dvojice  $q_i, r_i$  je hledaným podílem a zbytkem.

Z algoritmu je vidět, že je-li  $g$  monický, žádné zlomky se neobjeví a výsledkem budou polynomy z  $\mathbf{R}[x]$

Jednoznačnost se dokáže podobně jako pro celá čísla. Kdyby  $f = gq_1 + r_1 = gq_2 + r_2$ , pak  $g(q_1 - q_2) = r_2 - r_1$ , tedy  $g \mid r_2 - r_1$ . Přitom  $\deg(r_2 - r_1) < \deg g$ , tedy  $r_2 - r_1 = 0$ , čili  $r_1 = r_2$ . Z toho ihned plyne  $q_1 - q_2 = 0$ , tj.  $q_1 = q_2$ , protože  $g \neq 0$  a jsme v oboru integrity.  $\square$

#### 2.4. Kořeny a dělitelnost.

Buď  $f$  polynom z  $\mathbf{R}[x]$  a  $a \in R$ . Řekneme, že  $a$  je *kořen*  $f$ , pokud  $f(a) = 0$ . Ukážeme si, jak existence kořene souvisí s děliteli daného polynomu.

**Tvrzení 2.3.** *Buď  $\mathbf{R}$  obor integrity,  $f \in R[x]$  a  $a \in R$ . Pak  $a$  je kořen polynomu  $f$  právě tehdy, když  $x - a \mid f$ .*

*Důkaz.* ( $\Leftarrow$ ) Předpokládejme, že  $x - a \mid f$ . Pak  $f = (x - a) \cdot g$  pro nějaké  $g \in R[x]$  a dosadíme-li do  $f$  prvek  $a$ , dostaneme

$$f(a) = (a - a) \cdot g(a) = 0 \cdot g(a) = 0.$$

( $\Rightarrow$ ) Buďte  $q, r$  podíl a zbytek při dělení polynomu  $f$  polynomem  $x - a$  (ty existují, neboť dělíme monickým polynomem). Tedy  $f = (x - a) \cdot q + r$  a  $r$  je konstantní polynom (zbytek musí mít menší stupeň než dělitel). Dosadíme-li prvek  $a$ , dostaneme

$$0 = f(a) = (a - a) \cdot q(a) + r(a) = 0 \cdot q(a) + r = r,$$

takže  $r = 0$  a  $x - a \mid f$ .  $\square$

**Věta 2.4.** *Buď  $\mathbf{R}$  obor integrity,  $0 \neq f \in R[x]$  a  $\deg f = n$ . Pak má polynom  $f$  nejvýše  $n$  kořenů.*

*Důkaz.* Budeme postupovat indukcí podle stupně polynomu  $f$ . Je-li  $\deg f = 0$ , tj.  $f$  je nenulový konstantní polynom, pak žádné kořeny nemá. Nyní předpokládejme, že tvrzení platí pro všechny polynomy stupně nejvýše  $n$ . Je-li  $\deg f = n + 1$ , pak jsou dvě možnosti. Buď polynom  $f$  nemá žádný kořen, v tom případě tvrzení platí. Nebo má polynom  $f$  nějaký kořen  $a$  a v tom případě jej lze podle předchozího lemmatu napsat jako  $f = (x - a) \cdot g$  pro nějaký polynom  $g$  stupně  $n$ . Je-li  $b$  nějaký jiný kořen, tj.  $f(b) = (b - a) \cdot g(b) = 0$ , pak, protože jde o obor integrity, musí být buď  $b = a$  nebo  $g(b) = 0$ . Protože má polynom  $g$  nejvýše  $n$  kořenů, má polynom  $f$  nejvýše  $n + 1$  kořenů.  $\square$

**Příklad.** Počet kořenů polynomu  $f$  samozřejmě může být menší než  $\deg f$ : např. polynom  $x^2 + 1$  nemá nad  $\mathbb{Z}$  žádný kořen a nad  $\mathbb{Z}_2$  má jeden.

**Poznámka.** Věta 2.4 neplatí, není-li  $\mathbf{R}$  oborem integrity, ale např. jen komutativním okruhem s jednotkou. Předpoklad jsme použili v poslední fázi důkazu, když z  $f(b) = (b - a) \cdot g(b) = 0$  plynulo  $b - a = 0$  nebo  $g(b) = 0$ . Uvažte např. polynom  $2x \in \mathbb{Z}_4[x]$  nebo  $x^2 + x \in \mathbb{Z}_6[x]$ . První z nich má kořeny 0, 2, druhý 0, 2, 3, 5.

**Poznámka.** Věta 2.4 neplatí, není-li  $\mathbf{R}$  oborem integrity, ale např. jen nekomutativním tělesem – celá teorie dělitelnosti funguje jinak. Příkladem je polynom  $x^4 - 1$  nad okruhem kvaternionů, jeho kořeny jsou  $\pm 1, \pm i, \pm j, \pm k$  (viz příklady v Sekci ??).

## 2.5. Derivace a vícenásobné kořeny.

Matematická analýza zavádí pojem *derivace* reálné funkce, tedy speciálně také polynomu nad reálnými čísly. V oboru reálných čísel má derivace jistý geometrický význam (tečna grafu) a tak se také definuje (pomocí limit). Pro polynomy se z této definice odvodí jistý vzorec, ve kterém figurují koeficienty původního polynomu. V diskrétních oborech se geometrická představa ztrácí (co je tečna grafu funkce na celých číslech?), ale přesto má smysl derivaci zavést, a to tak, že postulujeme základní vlastnosti, které derivace splňuje.

**Definice.** Definujeme *derivaci* v  $\mathbf{R}[x]$  jako zobrazení  $D : \mathbf{R}[x] \rightarrow \mathbf{R}[x]$  splňující následující podmínky pro všechny polynomy  $f, g \in \mathbf{R}[x]$ :

- (1)  $D(f + g) = D(f) + D(g)$ ;
- (2)  $D(fg) = gD(f) + fD(g)$ ;
- (3)  $D(x) = 1, D(c) = 0$  pro každý konstantní polynom  $c$ .

Derivaci polynomu zpravidla značíme zkráceně  $f' = D(f)$ . Dále definujeme induktivně derivace vyšších řádů jako

$$f^{(0)} = f \quad \text{a} \quad f^{(k+1)} = (f^{(k)})'.$$

Než ukážeme vzorec na výpočet derivace, musíme si ujasnit, co značí v obecném oboru  $\mathbf{R}$  přirozená čísla. Pod přirozeným číslem  $n$  budeme rozumět prvek

$$n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_n \in R.$$

*Charakteristikou* oboru  $\mathbf{R}$  pak rozumíme nejmenší  $n$  takové, že  $n \cdot 1 = 0$ , pokud takové  $n$  existuje, resp. 0 v opačném případě.

**Lemma 2.5.** *Na každém oboru integrity existuje právě jedna derivace a platí*

$$\left( \sum_{i=0}^n a_i x^i \right)' = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i.$$

*Důkaz.* Nejprve si všimněte, že z (2) plyne  $(cf)' = cf' + f'c = cf'$  pro každý polynom  $f$  a každý konstantní polynom  $c$ . Dále indukcí dokážeme, že  $(x^n)' = nx^{n-1}$ . Případ  $n = 1$  je pokryt vlastností (3) a dále, pomocí (2) a indukčního předpokladu,  $(x^n)' = x(x^{n-1})' + x^{n-1}x' = x(n-1)x^{n-2} + x^{n-1} = nx^{n-1}$ . Na závěr použijeme (1) a vidíme, že  $(\sum_{i=0}^n a_i x^i)' = \sum_{i=0}^n (a_i x^i)' = \sum_{i=0}^n a_i (x^i)' = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i$ .  $\square$

**Lemma 2.6.** *Bud'  $\mathbf{R}$  obor integrity,  $f, g \in \mathbf{R}[x]$  a  $n \in \mathbb{N}$ . Pak*

- (1)  $(f + g)^{(n)} = f^{(n)} + g^{(n)}$ ;
- (2)  $(f \cdot g)^{(n)} = \sum_{i=0}^n \binom{n}{i} \cdot f^{(i)} \cdot g^{(n-i)}$  [Leibnitzova formule];
- (3)  $(f^n)' = n \cdot f^{n-1} \cdot f'$ .

Důkaz je pouze technický výpočet a doporučujeme čtenáři jej provést samostatně. Níže je uveden stručný návod.

*Princip důkazu.* (1) Indukcí podle  $n$ . Pro  $n = 1$  viz definice. Indukční krok plyne z výpočtu  $(f + g)^{(n)} = ((f + g)^{(n-1)})' = (f^{(n-1)} + g^{(n-1)})' = (f^{(n-1)})' + (g^{(n-1)})' = f^{(n)} + g^{(n)}$ .

(2) Indukcí podle  $n$ . Pro  $n = 1$  viz definice. V indukčním kroku využijte známý vzorec  $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$ .

(3) se dokáže snadno indukcí podle  $n$  pomocí (2). □

Tvrzení 2.3 umožňuje definovat násobnost kořene daného polynomu.

**Definice.** Řekneme, že  $a \in R$  je  $n$ -násobný kořen polynomu  $f \in R[x]$ , pokud

$$(x - a)^n \mid f \quad \text{a} \quad (x - a)^{n+1} \nmid f.$$

Násobnost kořene daného polynomu úzce souvisí s kořeny derivací tohoto polynomu. Vztah popisuje následující věta. Její hlavní význam spočívá v tom, že umožňuje výpočetně podchytit pojem násobnosti kořene.

**Věta 2.7.** *Buď  $\mathbf{R}$  obor integrity,  $0 \neq f \in R[x]$ ,  $a \in R$  a  $n \in \mathbb{N}$ . Předpokládejme, že charakteristika oboru  $\mathbf{R}$  je buď 0, nebo  $\geq n$ . Pak jsou následující tvrzení ekvivalentní:*

- (1)  $a$  je alespoň  $n$ -násobný kořen polynomu  $f$ ;
- (2)  $f^{(0)}(a) = f^{(1)}(a) = \dots = f^{(n-1)}(a) = 0$ .

*Důkaz.* (1)  $\Rightarrow$  (2) Je-li  $a$  alespoň  $n$ -násobný kořen polynomu  $f$ , můžeme napsat

$$f = (x - a)^n \cdot g$$

pro nějaký polynom  $g \in R[x]$ . Pomocí Leibnitzovy formule spočítáme  $k$ -tou derivaci polynomu  $f$  pro  $k < n$ :

$$\begin{aligned} f^{(k)} &= \sum_{i=0}^k \binom{k}{i} \cdot ((x - a)^n)^{(i)} \cdot g^{(k-i)} \\ &= \sum_{i=0}^k \binom{k}{i} \cdot n(n-1) \cdot \dots \cdot (n-i+1) \cdot (x - a)^{n-i} \cdot g^{(k-i)}. \end{aligned}$$

Protože  $k < n$ , v každém členu součtu je člen  $x - a$  v nenulové mocnině, a tak dostáváme

$$f^{(k)}(a) = \sum_{i=0}^k 0 = 0.$$

(2)  $\Rightarrow$  (1) Protože  $f^{(0)}(a) = f(a) = 0$ , prvek  $a$  je kořenem polynomu  $f$ . Buď  $m$  jeho násobnost a pro spor předpokládejme, že  $m < n$ . Napišme

$$f = (x - a)^m \cdot g$$

pro nějaký polynom  $g \in R[x]$  splňující  $g(a) \neq 0$ . Pomocí Leibnitzovy formule spočítáme  $m$ -tou derivaci polynomu  $f$ :

$$\begin{aligned} f^{(m)} &= \sum_{i=0}^m \binom{m}{i} \cdot ((x - a)^m)^{(i)} \cdot g^{(m-i)} \\ &= \binom{m}{m} \cdot m! \cdot g^{(0)} + \sum_{i=0}^{m-1} \binom{m}{i} \cdot m(m-1) \cdot \dots \cdot (m-i+1) \cdot (x - a)^{m-i} \cdot g^{(m-i)} \end{aligned}$$

a po dosazení dostaneme

$$f^{(m)}(a) = 1 \cdot m! \cdot g(a) + \sum_{i=0}^{m-1} 0 = m! \cdot g(a).$$

Podle předpokladu  $f^{(m)}(a) = 0$ . Protože pracujeme v oboru integrity, musí platit  $m! = 0$  nebo  $g(a) = 0$ . Druhá možnost je ve sporu s volbou  $g$ , takže  $m! = m \cdot (m-1) \cdot \dots \cdot 1 = 0$ . Tedy některý z prvků  $1, \dots, m$  musí být roven nule, což je ve sporu s předpokladem na charakteristiku oboru  $\mathbf{R}$ .  $\square$

Z věty ihned plyne následující kritérium pro určení přesné násobnosti. Je-li charakteristika 0 nebo  $> n$ , pak  $a$  je (přesně)  $n$ -násobným kořenem polynomu  $f$  právě tehdy, když  $f^{(0)}(a) = f^{(1)}(a) = \dots = f^{(n-1)}(a) = 0$  a navíc  $f^{(n)}(a) \neq 0$ . Důvod je jednoduchý: kdyby  $f^{(n)}(a) = 0$ , šlo by o alespoň  $(n+1)$ -násobný kořen. Všimněte si však, že k tomuto argumentu potřebujeme charakteristiku ostře větší než  $n$ .

**Příklad.** Větu 2.7 lze použít k detekci vícenásobných kořenů i nad tělesem  $\mathbb{Z}_2$ , zatímco právě uvedené kritérium nikoliv: polynom  $f \in \mathbb{Z}_2[x]$  má vícenásobný (tj. alespoň 2-násobný) kořen  $a$  právě tehdy, když  $f(a) = f'(a) = 0$ . Pro přesně dvojnásobné kořeny však nemusí být pravda, že  $f''(a) \neq 0$ : např. pro  $f = x^3 + x = x(x+1)^2$  je 1 dvojnásobným kořenem, avšak  $f' = x^2 + 1$ ,  $f'' = 0$ , tedy  $f''(1) = 0$ .

**Úloha.** Spočítejte násobnost kořene 1 polynomu  $f = x^4 + x^3 + x^2 + x + 1$  nad tělesem  $\mathbb{Z}_5$ .

*Řešení.* Nejprve si uvědomíme, že můžeme použít Větu 2.7, protože  $f$  má stupeň 4, tedy 1 bude nejvýše 4-násobným kořenem, což je méně než charakteristika oboru  $\mathbb{Z}_5$ . Postupně spočteme  $f(1) = 0$ ;  $f' = 4x^3 + 3x^2 + 2x + 1$ , tedy  $f'(1) = 0$ ;  $f'' = 2x^2 + x + 2$ , tedy  $f''(1) = 0$ ;  $f''' = 4x + 1$ , tedy  $f'''(1) = 0$ ; a nakonec  $f'''' = 4$ . Čili 1 je 4-násobný kořen. (Roznásobením snadno ověříme, že  $(x-1)^4 = f$ , což nás mohlo, ale nemuselo napadnout hned na začátku.)  $\square$

Z Věty 2.7 plyne důležité kritérium existence vícenásobného kořene daného polynomu. Je-li  $\mathbf{R}$  obor integrity a  $f$  polynom nad  $\mathbf{R}$ , pak prvek  $a \in R$  je vícenásobným kořenem polynomu  $f$  právě tehdy, když  $f(a) = f'(a) = 0$ . Tedy, má-li  $f$  vícenásobný kořen, oba polynomy  $f, f'$  jsou dělitelné nějakým monočlenem  $x - a$ , a pokud existuje jejich největší společný dělitel, pak jej  $x - a$  dělí také. Tím dostáváme algoritmicky snadno ověřitelné kritérium: jsou-li  $f, f'$  nesoudělné, polynom  $f$  zaručeně žádný vícenásobný kořen nemá.

## 2.6. Věta o interpolaci.

S kořeny polynomů souvisí tzv. *interpolace*: předepíšeme-li hodnoty v  $n$  bodech, existuje právě jeden polynom stupně  $< n$ , který v těchto bodech nabývá daných hodnot.

**Věta 2.8** (o interpolaci). *Buď  $T$  těleso. Mějme po dvou různé body  $a_1, \dots, a_n \in T$  a libovolné hodnoty  $u_1, \dots, u_n \in T$ . Pak existuje právě jeden polynom  $f \in T[x]$  stupně  $< n$  splňující  $f(a_i) = u_i$  pro všechna  $i = 1, \dots, n$ .*

Není těžké nahlédnout, že řešením je polynom

$$f = \sum_{i=1}^n \left( u_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right),$$



říká se mu někdy *Lagrangeův interpolační polynom*.

*Důkaz.* Dosazením do uvedeného vzorce snadno zjistíme, že

$$f(a_k) = 0 + \dots + 0 + u_k \cdot \prod_{j \neq k} \frac{a_k - a_j}{a_k - a_j} + 0 + \dots + 0 = u_k.$$

Zbývá dokázat jednoznačnost. Uvažujme dva polynomy  $f, g$  stupně  $< n$  splňující  $f(a_i) = g(a_i) = u_i$  pro všechna  $i = 1, \dots, n$ . Polynom  $h = f - g$  je také stupně  $< n$ , avšak  $h(a_i) = f(a_i) - g(a_i) = 0$  pro všechna  $i$ , tedy  $h$  má aspoň  $n$  kořenů. To je spor s Větou 2.4.  $\square$

Důkaz věty o interpolaci nápadně připomíná důkaz čínské věty o zbytcích. Ve skutečnosti je velmi podobné i znění věty: podmínku  $f(a_i) = u_i$  lze napsat ekvivalentně jako  $f \equiv u_i \pmod{x - a_i}$ , takže vlastně řešíme soustavu kongruencí vzhledem k polynomům  $x - a_1, \dots, x - a_n$ . Řešení je určeno jednoznačně mezi polynomy omezeného stupně. Věta o interpolaci a čínská věta o zbytcích mají společné zobecnění, které je předmětem Sekce ??.

**Důsledek 2.9.** *Buď  $T$  konečné těleso. Pak pro každou funkci  $f : T \rightarrow T$  existuje právě jeden polynom  $g \in T[x]$  stupně  $< |T|$  takový, že  $f(a) = g(a)$  pro každé  $a \in T$ .*

*Důkaz.* Interpolujme v bodě  $a$  hodnotou  $f(a)$ , pro každé  $a \in T$ .  $\square$

Pro nekonečná tělesa samozřejmě nic takového platit nemůže, přesto polynomy hrají důležitou roli i v reálné analýze: např. *Weierstrassova věta* říká, že každou spojitou reálnou funkci na omezeném uzavřeném intervalu lze polynomem libovolně přesně aproximovat (tj. pro každou spojitou  $f : [u, v] \rightarrow \mathbb{R}$  a každé  $\varepsilon > 0$  existuje polynom  $g \in \mathbb{R}[x]$  takový, že  $|f(a) - g(a)| < \varepsilon$  pro každé  $a \in [u, v]$ ).

### 3. KVADRATICKÁ ROZŠÍŘENÍ CELÝCH ČÍSEL

**Cíl.** *Ukážeme si základní triky pro počítání v oborech  $\mathbb{Z}[\sqrt{s}]$ . Zvláštní pozornost bude věnována Gaussovým celým číslům.*

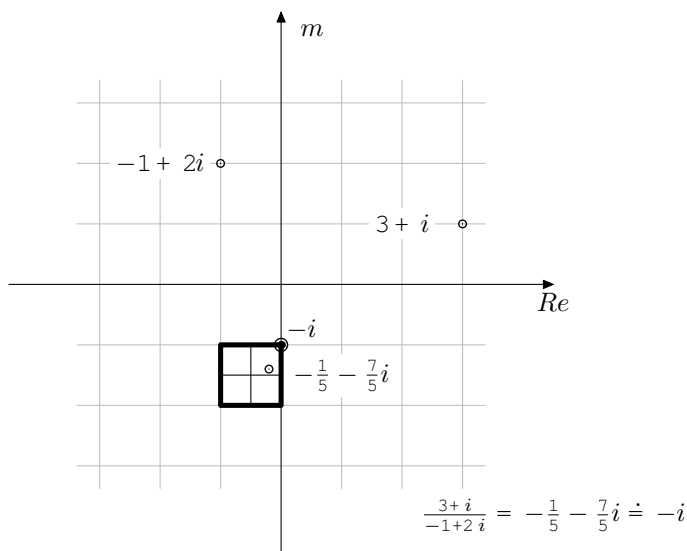
Mezi nejdůležitější rozšíření oboru celých čísel patří tzv. *kvadratická rozšíření*. Zde se soustředíme na obory  $\mathbb{Z}[\sqrt{s}]$ , pro obecnější teorii doporučujeme libovolnou knihu o algebraické teorii čísel. Buď  $s$  číslo, jež není dělitelné druhou mocninou žádného prvočísla, a definujme zobrazení

$$\nu : \mathbb{Z}[\sqrt{s}] \rightarrow \mathbb{N} \cup \{0\}, \quad a + b\sqrt{s} \mapsto |a^2 - sb^2|.$$

Je dobré mít na paměti, že pro  $s < 0$  je  $\nu(u) = |u|^2$ , čtverec obyčejné absolutní hodnoty komplexního čísla, díky čemuž se dá často aplikovat geometrický náhled na situaci. Zobrazení  $\nu$  nazýváme *normou*. Základním pozorováním je fakt, že norma se chová hezky vzhledem k dělitelnosti.

**Tvrzení 3.1.** *Pro každá  $u, v \in \mathbb{Z}[\sqrt{s}]$  platí*

- (1)  $\nu(u \cdot v) = \nu(u) \cdot \nu(v)$ ,
- (2)  $\nu(u) = 1 \Leftrightarrow u$  je invertibilní, tj. existuje  $w \in \mathbb{Z}[\sqrt{s}]$  takové, že  $uw = 1$ .

OBRÁZEK 1. Dělení se zbytkem v  $\mathbb{Z}[i]$ .

*Důkaz.* (1) Označme  $u = a + b\sqrt{s}$  a  $v = c + d\sqrt{s}$ . Pak

$$\begin{aligned} \nu(u \cdot v) &= \nu((ac + sbd) + (ad + bc)\sqrt{s}) \\ &= |a^2c^2 + 2sabcd + s^2b^2d^2 - s(a^2d^2 + 2abcd + b^2c^2)| \\ &= |a^2c^2 + s^2b^2d^2 - sa^2d^2 - sb^2c^2| \\ &= |a^2 - sb^2| \cdot |c^2 - sd^2| = \nu(u) \cdot \nu(v). \end{aligned}$$

(2) Pokud  $\nu(u) = \nu(a + b\sqrt{s}) = |a^2 - sb^2| = 1$ , pak  $a^2 - sb^2 = (a + b\sqrt{s})(a - b\sqrt{s}) = \pm 1$ , a tedy  $w = \pm(a - b\sqrt{s})$ . Opačná implikace plyne z (1): je-li  $uw = 1$ , pak  $1 = \nu(1) = \nu(uw) = \nu(u)\nu(w)$ , a tedy  $\nu(u) = \nu(w) = 1$ .  $\square$

Pro některé obory  $\mathbb{Z}[\sqrt{s}]$  umožňuje norma definovat *dělení se zbytkem*. Fakt, že zbytek by měl být „menší“ než dělitel, formalizujeme pomocí normy. Dělení se zbytkem funguje např. pro obory  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[i\sqrt{2}]$  nebo  $\mathbb{Z}[\sqrt{2}]$ , pro jiné podíl a zbytek v tomto smyslu neexistuje, např. pro  $\mathbb{Z}[i\sqrt{3}]$  nebo  $\mathbb{Z}[\sqrt{5}]$ . Důkaz provedeme pro Gaussova celá čísla.

**Tvrzení 3.2.** *Pro každá  $u, v \in \mathbb{Z}[i]$ ,  $v \neq 0$ , existují  $q, r \in \mathbb{Z}[i]$  splňující podmínky  $u = vq + r$  a  $\nu(r) < \nu(v)$ .*

*Důkaz.* Položme

$$z = \frac{u}{v} \in \mathbb{C}$$

(přesný podíl v  $\mathbb{C}$ ). Buď  $q$  nejbližší prvek  $\mathbb{Z}[i]$  k prvku  $z$  (tj. takový, pro který je  $|z - q|$  minimální); je-li takových více, zvolme libovolný z nich. Položme

$$r = u - vq.$$

Pak zřejmě  $vq + r = u$  a zbývá dokázat, že  $\nu(r) < \nu(v)$ . Jaká je vzdálenost  $q$  a  $z$ ? V nejhorším případě je  $z$  uprostřed čtverce s celočíselnými vrcholy, tedy určité

$|z - q| \leq \frac{\sqrt{2}}{2} < 1$ . Proto

$$\nu(r) = |r|^2 = |u - vq|^2 = |v|^2 \cdot \left| \frac{u}{v} - q \right|^2 = |v|^2 \cdot |z - q|^2 < |v|^2 = \nu(v).$$

□

Na rozdíl od situace v  $\mathbb{Z}$  či pro polynomy (viz Tvzení 2.2), podíl a zbytek  $q, r$  není určen jednoznačně: např.  $z = \frac{1}{2} + \frac{1}{2}i$  lze zaokrouhlit čtyřmi způsoby, každý z nich bude splňovat uvedené podmínky.

Pro obory  $\mathbb{Z}[i\sqrt{2}]$  či  $\mathbb{Z}[e^{2\pi i/3}]$  lze důkaz provést zcela analogicky, protože i zde platí  $\nu(u) = |u|^2$  a jediný rozdíl tak je v odhadu  $|z - q|$ . Pro  $\mathbb{Z}[i\sqrt{3}]$  už důkaz neprojde, protože střed obdélníka má vzdálenost od vrcholu rovnou 1. (Ve skutečnosti v tomto oboru není možné dělit se zbytkem žádným způsobem. Tato teorie je předmětem následujících dvou sekcí.) Pro obory  $\mathbb{Z}[\sqrt{s}]$  s kladným  $s$  schází geometrická představa, nicméně pro  $s = 2, 3$  funguje podobný algoritmus dělení, stačí zaokrouhlit koeficienty přesného podílu. Důkaz odhadu normy zbytku je však o něco komplikovanější.