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 čitatel 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

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

Není těžké nahlédnout, že jde o ekvivalenci: reflexivita je zřejmá, symetrie plyne z komutativity násobení a tranzitivitu získáme následujícím výpočtem: je-li $(a,b) \sim \sim (c,d) \sim (e,f)$, 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

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

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 $\mathbf{Q}$ množinu Q s operacemi $+, -, \cdot$ a konstantami 0,1.

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

Těleso $\mathbf{Q}$ 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 **R**.
- Jednotka: $\frac{a}{a} \cdot \frac{1}{1} = \frac{a\cdot 1}{a\cdot 1} = \frac{a}{a}$.
- Distributivita: $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} = \frac{abcf+abde}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf}$.
- $0 = \frac{0}{1} \neq 1 = \frac{1}{1}$, 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 **Q** je těleso. Zbývá dokázat, že prvky tvaru $\frac{a}{1}$ tvoří podobor $\mathbb{Q}$, což je snadné. □

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

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

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

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

nebo zkráceně

$$\sum_{i=0}^{n} a_ix^i,$$

kde $a_0, \ldots, a_n \in R$ a $a_n \neq 0$. Prvky $a_0, \ldots, a_n$ nazýváme *koeficienty* 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

$$\sum_{i=0}^{m} a_i x^i \;+\; \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{\max(m,n)} (a_i + b_i)x^i, \qquad -\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} (-a_i)x^i,$$

$$(\sum_{i=0}^{m} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) = \sum_{i=0}^{m+n} \big(\sum_{j+k=i} a_j b_k \big) x^i.$$

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 $a_0, a_1, \ldots \in R$; 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

$$\sum_{i=0}^{\infty} a_i x^i \;+\; \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i)x^i, \qquad -\sum_{i=0}^{\infty} a_i x^i = \sum (-a_i)x^i,$$

$$(\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{i=0}^{\infty} b_i x^i) = \sum_{i=0}^{\infty} \big(\sum_{j+k=i} a_j b_k \big) x^i.$$

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 $(\sum a_i x^i) \cdot (1 + 0 + 0 + \ldots)$ 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 $(\sum a_i x^i) \cdot ((\sum b_i x^i) \cdot (\sum c_i x^i)) = (\sum a_i x^i) \cdot ((\sum (\sum_{k+l=i} b_k c_l) x^i) = \sum (\sum_{j+k+l=i} a_j b_k c_l) x^i)$, 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 prověří 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

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

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. □

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

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

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 pomocí 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 **??** 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 $R \le S$ obory integrity. Polynom $f \in R[x]$ je formální výraz

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

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

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

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 $S \ge R$ můžeme uvažovat tzv. *polynomiální zobrazení* $S \to S$, 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 $\deg g \le \deg f$. (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 $f \bmod g = r$. Je vidět, že $g \mid f$ právě tehdy, když $f \bmod g = 0$.

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. Rekurzí 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. □

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 $x - a \mid f$. □

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. □

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 **??** 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 **??** 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 ± 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 $D : R[x] \to R[x]$ splňující následující podmínky pro všechny polynomy $f, g \in R[x]$:

(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

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n} \in R.$$

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

Lemma 2.6. *Buď $\mathbf{R}$ obor integrity, $f, g \in R[x]$ 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 **??** 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 předpokládejme, že charakteristika oboru* $\mathbf{R}$ *je buď* 0, *nebo je větší než* $\deg f$. *Pak jsou následující tvrzení ekvivalentní:*

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

Důkaz. (1) $\Rightarrow$ (2). Protože je a n-násobný kořen polynomu f, můžeme napsat

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

pro nějaký polynom g splňující $g(a) \neq 0$. Pomocí Leibnitzovy formule spočítáme k-tou derivaci polynomu f pro $k \leq n$:

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

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

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

Je-li $k = n$, pak

$$f^{(n)} = \binom{n}{n} \cdot n! \cdot g^{(0)} + \sum_{i=0}^{n-1} \binom{n}{i} \cdot n(n-1)\cdot\ldots\cdot(n-i+1)\cdot(x-a)^{n-i}\cdot g^{(n-i)}$$

a ze stejného důvodu

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

Kdyby $f^{(n)}(a) = 0$, měli bychom (z definice oboru integrity) buď $n! = 0$, nebo $g(a) = 0$. Přitom $g(a) \neq 0$ (viz začátek důkazu), takže $n! = n(n-1)\cdot\ldots\cdot 1 = 0$.

Opět, z definice oboru integrity, některý z prvků $1, \ldots, n$ by musel být roven nule. A to je ve sporu s předpokladem na charakteristiku oboru $\mathbf{R}$.

(2) $\Rightarrow$ (1) Protože $f^{(0)}(a) = f(a) = 0$, prvek a je kořen polynomu f. Musí to tedy být m-násobný kořen pro nějaké $m \geq 1$. Užitím výše dokázané implikace dostáváme, že $f^{(0)}(a) = \ldots = f^{(m-1)}(a) = 0$ a $f^{(m)}(a) \neq 0$, a tudíž $m = n$. □

Úloha. Spočtěte násobnost kořene 1 polynomu $f = x^4 + x^3 + x^2 + x + 1$ v $\mathbb{Z}_5[x]$.

Řešení. Nejprve si uvědomíme, že jsou splněny předpoklady Věty **??**, protože $\deg f = 4 < 5$, což je 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.) □

Je-li charakteristika oboru $\mathbf{R}$ příliš malá, Věta **??** neplatí: může se stát, že $f^{(n)}(a) = 0$. Podíváme-li se na závěr důkazu, zjistíme potenciální problém v tom, že může nastat $n! = 0$. Skutečně, uvažujeme-li například předchozí úlohu nad tělesem $\mathbb{Z}_2$, vyjde $f' = x^2 + 1$, a tedy $f'' = f''' = \ldots = 0$.

Z Věty **??** plyne jedno důležité kritérium existence vícenásobného kořene. Je-li a alespoň dvojnásobný kořen polynomu $f \in R[x]$ a charakteristika $\mathbf{R}$ je různá od 2, pak $x - a$ dělí polynomy f i f', tedy tyto dva jsou soudělné. Pokud je $\mathbf{R}$ těleso, můžeme spočítat Eukleidovým algoritmem největší společný dělitel polynomů f, f' (viz Sekce **??**), a pokud tento vyjde 1, polynom f určitě žádný dvojnásobný 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 $\mathbf{T}$ těleso. Mějme po dvou různé body $a_1, \ldots, a_n \in T$ a libovolné hodnoty $u_1, \ldots, u_n \in T$. Pak existuje právě jeden polynom $f \in T[x]$ stupně $< n$ splňující $f(a_i) = u_i$ pro všechna $i = 1, \ldots, n$.*

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

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

Zbývá dokázat jednoznačnost. Uvažujme dva polynomy f, g stupně $< n$ splňující $f(a_i) = g(a_i) = u_i$ pro všechna i a označme $h = f - g$. Pak $h(a_i) = 0$ pro všechna i, tedy podle Tvrzení **??** $(x - a_i) \mid h$ pro každé i. Indukcí podle n dokážeme, že $(x-a_1)\cdot\ldots\cdot(x-a_n) \mid h$. Pro $n = 1$ je tvrzení triviální. V indukčním kroku napišme $h = (x - a_n)\bar{h}$. Protože $0 = h(a_i) = (a_i - a_n)\bar{h}(a_i)$ pro všechna $i < n$, a protože $a_i \neq a_n$ pro všechna $i < n$, musí platit $\bar{h}(a_i) = 0$ pro všechna $i < n$. Z indukčního předpokladu plyne $(x - a_1) \cdot \ldots \cdot (x - a_{n-1}) \mid \bar{h}$ a ze vztahu $h = (x - a_n)\bar{h}$ plyne

dokazované tvrzení. Nyní si stačí uvědomit, že $\deg(x-a_1)\cdot\ldots\cdot(x-a_n) = n$, zatímco $\deg h < n$, takže musí být $h = 0$, což znamená $f = g$. □

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 $x - a_1, \ldots, x - a_n$. Řešení je určeno jedoznačně mezi polynomy omezeného stupně. Věta o interpolaci a čínská věta o zbytcích mají společné zobecnění, které je předmětem Sekce **??**.

Důsledek 2.9. *Buď* $\mathbf{T}$ *konečné těleso. Pak pro každou funkci* $f : T \to T$ *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 $a \in T$. □

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 $f : [u, v] \to \mathbb{R}$ 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

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

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 ν nazýváme *normou*. Základním pozorováním je fakt, že norma se chová hezky vzhledem k dělitelnosti.

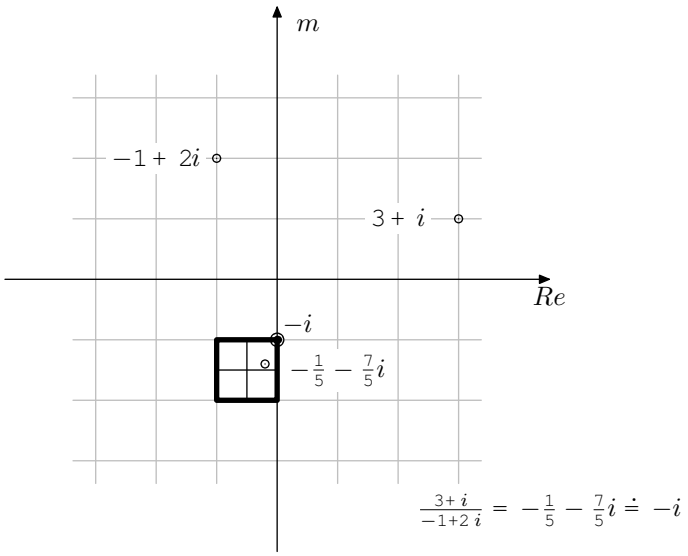
Tvrzení 3.1. *Pro každá* $u, v \in \mathbb{Z}[\sqrt{s}]$ *platí*

(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* $uw = 1$.

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 $\nu(u) = \nu(w) = 1$. □



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

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

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

□

Na rozdíl od situace v $\mathbb{Z}$ či pro polynomy (viz Tvrzení **??**), 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.