POLYNOMIÁLNÍ ALGEBRA

DAVID STANOVSKÝ

1. Polynomy nad gaussovskými obory

1.1. Gaussova věta.

Polynomy jedné proměnné nad tělesem tvoří eukleidovský obor, a podle Věty **??** jsou gaussovské. Polynomy více proměnných, nebo třeba polynomy nad $\mathbb{Z}$, eukleidovské nejsou. K důkazu jejich gaussovskosti potřebujeme jiný trik: dělitelnost polynomů nad oborem $\mathbf{R}$ lze do jisté míry převést na dělitelnost polynomů nad jeho podílovým tělesem $\mathbf{Q}$ a na dělitelnost v oboru $\mathbf{R}$ (viz Lemma 1.2 a Věta 1.3). Důsledkem bude, že z gaussovskosti $\mathbf{R}$ plyne gaussovskost $\mathbf{R}[x]$, čemuž se říká Gaussova věta (Věta 1.4).

Pro účely této sekce se nám budou hodit následující definice. Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom z $\mathbf{R}[x]$. Definujeme

$$\mathrm{c}(f) = \mathrm{NSD}(a_0, \ldots, a_n) \qquad \text{a} \qquad \mathrm{pp}(f) = \frac{1}{\mathrm{c}(f)} \cdot f.$$

Polynom se nazývá *primitivní*, pokud $\mathrm{c}(f) = 1$. Polynom $\mathrm{pp}(f)$ je očividně primitivní a nazývá se *primitivní částí* polynomu f.

Důkaz uvedených vět je založen na tvrzení známém jako Gaussovo lemma, které říká, že součin primitivních polynomů je primitivní.

Lemma 1.1 (Gaussovo lemma)**.** *Buď $\mathbf{R}$ gaussovský obor a f, g primitivní polynomy z $\mathbf{R}[x]$. Pak fg je primitivní polynom.*

Důkaz. Označme $f = \sum_{i=0}^{n} a_i x^i$ a $g = \sum_{i=0}^{m} b_i x^i$ a předpokládejme, že fg není primitivní polynom. Díky existenci ireducibilních rozkladů existuje ireducibilní prvek $p \in R$, který dělí všechny koeficienty součinu fg. Zvolme nejmenší j takové, že $p \nmid a_j$, a nejmenší k takové, že $p \nmid b_k$ (protože jsou polynomy f, g primitivní, p nemůže dělit všechny jejich koeficienty). Podívejme se na $(j+k)$-tý koeficient polynomu fg:

$$c_{j+k} = a_0 b_{j+k} + \ldots + a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \ldots + a_{j+k} b_0.$$

Protože $p \mid a_i$ pro všechna $i < j$, máme

$$p \mid a_0 b_{j+k} + \ldots + a_{j-1} b_{k+1}.$$

Protože $p \mid b_i$ pro všechna $i < k$, máme

$$p \mid a_{j+1} b_{k-1} + \ldots + a_{j+k} b_0.$$

Tedy p dělí všechny členy součtu vlevo i vpravo od $a_j b_k$. Tento člen naopak p dělitelný není, protože p je ireducibilní, tedy prvočinitel (Důsledek **??**), a přitom nedělí ani a_j, ani b_k. Čili $p \nmid c_{j+k}$, spor. □

Date: 7. ledna 2019.

Budoucí sekce III v nových skriptech.

Důsledkem je slibovaná souvislost dělitelnosti nad oborem a nad jeho podílovým tělesem.

Lemma 1.2. *Buď* $\mathbf{R}$ *gaussovský obor,* $\mathbf{Q}$ *jeho podílové těleso a* f, g *primitivní polynomy z* $\mathbf{R}[x]$*. Pak* $f \mid g$ *v* $\mathbf{R}[x]$ *právě tehdy, když* $f \mid g$ *v* $\mathbf{Q}[x]$*.*

Důkaz. $f \mid g$ v $\mathbf{R}[x]$ znamená, že existuje $h \in R[x]$ splňující $g = fh$. Podobně, $f \mid g$ v $\mathbf{Q}[x]$ znamená, že existuje $h \in Q[x]$ splňující $g = fh$. Čili implikace ($\Rightarrow$) je triviální a musíme dokázat tu opačnou. Mějme takový polynom $h \in Q[x]$ a zvolme $q \in Q$ tak, aby byl qh primitivní polynom z $\mathbf{R}[x]$ (stačí vzít $q = \frac{a}{b} \in Q$, kde a je NSN jmenovatelů všech koeficientů, a b je NSD čitatelů všech koeficientů polynomu h). Dostáváme $qg = f \cdot qh$. Na pravé straně je součin primitivních polynomů z $\mathbf{R}[x]$, takže podle Gaussova lemmatu je qg také primitivní polynom z $\mathbf{R}[x]$. Protože je g primitivní, jmenovatel q musí být invertibilní. Protože je qg primitivní, čitatel q musí být také invertibilní. Čili $1 \parallel q \in R$, a tedy $h \in R[x]$. □

Věta 1.3. *Buď* $\mathbf{R}$ *gaussovský obor,* $\mathbf{Q}$ *jeho podílové těleso a* f, g *polynomy z* $\mathbf{R}[x]$*. Pak*

(1) $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ *existuje a je roven součinu* $c \cdot h$*, kde* $c = \mathrm{NSD}_{\mathbf{R}}(\mathrm{c}(f), \mathrm{c}(g))$ *a* h *je primitivní polynom z* $\mathbf{R}[x]$ *splňující* $h = \mathrm{NSD}_{\mathbf{Q}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$*.*
(2) f *je ireducibilní v* $\mathbf{R}[x]$ *právě tehdy, když*
   - $\deg f = 0$ *a* f *je ireducibilní v* $\mathbf{R}$*; nebo*
   - $\deg f > 0$*,* f *je primitivní a ireducibilní v* $\mathbf{Q}[x]$*.*

Předně je třeba vyjasnit, proč je formulace bodu (1) tak složitá, proč nemůžeme rovnou psát vzorec ve tvaru

$$\mathrm{NSD}_{\mathbf{R}[x]}(f, g) = \mathrm{NSD}_{\mathbf{R}}(\mathrm{c}(f), \mathrm{c}(g)) \cdot \mathrm{NSD}_{\mathbf{Q}[x]}(\mathrm{pp}(f), \mathrm{pp}(g)).$$

Je to kvůli nejednoznačnosti operátoru NSD. Následující tvrzení jsou platná v $\mathbb{Q}[x]$: $\mathrm{NSD}_{\mathbb{Q}[x]}(x^2 + 2x + 1, x^2 - 1) = 2x + 2$, $\mathrm{NSD}_{\mathbb{Q}[x]}(x^2 + 2x + 1, x^2 - 1) = \frac{3}{4}x + \frac{3}{4}$. První odpověď nemůžeme v $\mathbb{Z}[x]$ použít, protože výsledek je dělitelný 2, ale ani jeden z polynomů 2 dělitelný není. Druhou odpověď nemůžeme použít, protože výsledek ani neleží v $\mathbb{Z}[x]$. Věta říká, že použít máme primitivní výsledek, tj. v našem případě $x+1$ nebo $-x-1$. Takový polynom jistě existuje: stačí vzít libovolný $h = \mathrm{NSD}_{\mathbb{Q}[x]}(f, g)$ a přenásobit jej vhodným zlomkem (viz důkaz Lemmatu 1.2).

Důkaz Věty 1.3. (1) Nejprve dokážeme, že pro primitivní polynomy f, g existuje $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ a je roven primitivnímu polynomu h z $\mathbf{R}[x]$ splňujícímu $h = \mathrm{NSD}_{\mathbf{Q}[x]}(f, g)$. Polynom h dělí f, g v $\mathbf{Q}[x]$ a je primitivní, tedy díky Lemmatu 1.2 dělí f, g i v $\mathbf{R}[x]$, takže je to společný dělitel. Kdykoliv máme jiný společný dělitel $d \mid f, g$ v $\mathbf{R}[x]$, pak je jistě primitivní, $d \mid f, g$ v $\mathbf{Q}[x]$, tedy $d \mid h$ v $\mathbf{Q}[x]$, a opět podle Lemmatu 1.2 $d \mid h$ v $\mathbf{R}[x]$.

Nyní odvodíme obecný vztah. Protože $c = \mathrm{NSD}_{\mathbf{R}}(\mathrm{c}(f), \mathrm{c}(g))$ dělí $\mathrm{c}(f)$ i $\mathrm{c}(g)$, a zároveň $h = \mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$ dělí $\mathrm{pp}(f)$ i $\mathrm{pp}(g)$, tak jejich součin ch dělí oba polynomy f, g, čili ch je společný dělitel. Dokážeme, že je to největší společný dělitel: pokud nějaký d dělí f i g, pak $\mathrm{c}(d)$ dělí $\mathrm{c}(f)$ i $\mathrm{c}(g)$, tedy $\mathrm{c}(d) \mid c$; analogicky $\mathrm{pp}(d) \mid h$ a dostáváme $d \mid ch$.

(2) Rozložme $f = c(f) \cdot pp(f)$. Je-li f ireducibilní, pak $c(f) \parallel 1$ nebo $pp(f) \parallel 1$. V druhém případě je f konstantní a musí být ireducibilní v $\mathbf{R}$. V prvním případě je f primitivní. Zbývá si uvědomit, že primitivní polynom je ireducibilní v $\mathbf{R}[x]$ právě tehdy, když v $\mathbf{Q}[x]$. Pokud by měl v $\mathbf{Q}[x]$ vlastního dělitele g, pak uvažujme

$q \in Q$ takové, že qg je primitivní polynom z $\mathbf{R}[x]$, a tento bude díky Lemmatu 1.2 vlastním dělitelem v $\mathbf{R}[x]$. □

Příklad. Uvažujme obor $\mathbb{Z}[x]$ a polynomy

$$f = 4x^2 + 8x + 4, \qquad g = -6x^2 + 6.$$

Pak $c = \mathrm{NSD}_{\mathbb{Z}}(4, -6) = 2$, $h = \mathrm{NSD}_{\mathbb{Q}[x]}(x^2 + 2x + 1, x^2 - 1) = x + 1$, a tedy $\mathrm{NSD}_{\mathbb{Z}[x]}(f, g) = 2 \cdot (x + 1)$.

Příklad. Z bodu (2) plyne, že primitivní polynom je ireducibilní v $\mathbf{R}[x]$ právě tehdy, když v $\mathbf{Q}[x]$, ale obecně to neplatí:

- polynom $2x - 2$ je ireducibilní v $\mathbb{Q}[x]$, ale není ireducibilní v $\mathbb{Z}[x]$, rozkládá se jako $2 \cdot (x - 1)$;
- polynom 2 není ireducibilní v $\mathbb{Q}[x]$, protože je invertibilní, ale je ireducibilní v $\mathbb{Z}[x]$.

Nyní můžeme přistoupit k důkazu samotné Gaussovy věty.

Věta 1.4 (Gaussova věta)**.** *Je-li* $\mathbf{R}$ *gaussovský obor, pak je* $\mathbf{R}[x]$ *také gaussovský obor.*

Důkaz. Použijeme charakterizaci z Věty **??**. Existenci NSD v $\mathbf{R}[x]$ jsme dokázali ve Větě 1.3. Buď $f_1, f_2, f_3, \ldots$ nekonečná posloupnost vlastních dělitelů v $\mathbf{R}[x]$. Pak $\deg f_1 \geq \deg f_2 \geq \deg f_3 \geq \cdots \geq 0$, a tedy existuje n takové, že $\deg f_n = \deg f_{n+1} = \ldots$ Označíme-li u_i absolutní člen polynomu f_i, pak $u_n, u_{n+1}, u_{n+2} \ldots$ tvoří nekonečnou posloupnost vlastních dělitelů v $\mathbf{R}$, spor. □

Z Gaussovy věty ihned plyne, že také obory více proměnných nad gaussovským oborem jsou gaussovské: použije se indukce podle počtu proměnných a vztah $\mathbf{R}[x_1, \ldots, x_n] = (\mathbf{R}[x_1, \ldots, x_{n-1}])[x_n]$.

1.2. **Racionální kořeny a Eisensteinovo kritérium.**

Připomeňte si důkaz Gaussova lemmatu (Lemma 1.1). Na podobném principu jsou založena dvě užitečná kritéria, jedno na existenci racionálních kořenů, druhé na ireducibilitu.

Tvrzení 1.5. *Buď* $\mathbf{R}$ *gaussovský obor a* $\mathbf{Q}$ *jeho podílové těleso. Má-li polynom* $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ *kořen* $\frac{r}{s} \in Q$ *(předpokládáme* r, s *nesoudělná), pak* $r \mid a_0$ *a* $s \mid a_n$*.*

Důkaz. Dosaďme prvek $\frac{r}{s}$ do f. Protože $\sum_{i=0}^{n} a_i (\frac{r}{s})^i = 0$, přenásobením prvkem s^n dostáváme

$$a_0 s^n + a_1 r s^{n-1} + a_2 r^2 s^{n-2} + \ldots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

Protože r dělí všechny členy $a_1 r s^{n-1}, \ldots, a_n r^n$ i pravou stranu, musí dělit i první člen $a_0 s^n$. Protože jsou r, s nesoudělné, musí r dělit a_0 (zde využíváme gaussovskost, konkrétně Důsledek **??**(2) aplikovaný na všechny ireducibilní prvky v rozkladu r). Analogicky, protože s dělí všechny členy $a_0 s^n, \ldots, a_{n-1} r^{n-1} s$, musí dělit i poslední člen $a_n r^n$, tedy $s \mid a_n$. □

Příklad. Najdeme všechny racionální kořeny polynomu $2x^5 - 3x^4 + 2x - 3$. Podle Tvrzení 1.5 jsou jedinými kandidáty čísla ± 1, ± 3, $\pm\frac{1}{2}$ a $\pm\frac{3}{2}$. Dosazením zjistíme, že vyhovuje pouze číslo $-\frac{3}{2}$.

Příklad. Racionálními kořeny polynomu $x^n - p$, p prvočíslo, mohou být pouze čísla $\pm 1, \pm p$ a ani jedno očividně nevyhovuje (pro $n \geq 2$). Důsledkem je, že všechny odmocniny prvočísel $\sqrt[n]{p}$ jsou iracionální.

Tvrzení 1.6 (Eisensteinovo kritérium)**.** *Buď* $\mathbf{R}$ *obor integrity a* $f = \sum_{i=0}^{n} a_i x^i$ *primitivní polynom z* $\mathbf{R}[x]$*. Pokud existuje prvočinitel* $p \in R$ *splňující* $p \mid a_0$*,* $p \mid a_1$*,* $\ldots$*,* $p \mid a_{n-1}$ *a* $p^2 \nmid a_0$*, pak je polynom* f *ireducibilní v* $\mathbf{R}[x]$*.*

Připomeňme, že podle Důsledku **??**(2) jsou v gaussovských oborech prvočinitelé totéž, co ireducibilní prvky.

Důkaz. Pro spor uvažujme rozklad $f = gh$, kde $g = \sum_{i=0}^{k} b_i x^i$ a $h = \sum_{i=0}^{l} c_i x^i$ jsou polynomy z $\mathbf{R}[x]$ stupně alespoň 1. Protože prvočinitel p dělí $a_0 = b_0 c_0$, platí $p \mid b_0$ nebo $p \mid c_0$, ale určitě ne oboje zároveň, protože $p^2 \nmid a_0$. Nechť je to bez újmy na obecnosti b_0. Podobně, protože $p \mid a_1 = b_0 c_1 + b_1 c_0$ a $p \nmid c_0$, musí $p \mid b_1$. Protože $p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ a $p \nmid c_0$, musí $p \mid b_2$. Postupně zjistíme, že p dělí všechny koeficienty b_i, tedy $p \mid g \mid f$, což je spor s primitivitou. □

Příklad. Z Eisensteinova kritéria plyne ireducibilita polynomů $x^n \pm a$ v oboru $\mathbb{Z}[x]$ pro každé a takové, že existuje prvočíslo p splňující $p \mid a$, $p^2 \nmid a$.

2. Počítání modulo polynom

2.1. Čínská věta o zbytcích a interpolace.

Čínská věta o zbytcích hovoří o tom, jak vypadají řešení soustav lineárních kongruencí. V sekci **??** jsme viděli její variantu pro obor celých čísel, nicméně tato věta platí daleko obecněji. V této sekci si ukážeme další speciální případ, pro polynomy. V sekci **??** pak uvidíme její obecnou formulaci pro libovolné okruhy.

Věta 2.1 (čínská věta o zbytcích pro polynomy)**.** *Buď* $\mathbf{T}$ *těleso. Buď* $m_1, \ldots, m_n \in T[x]$ *po dvou nesoudělné polynomy, označme* $d = \sum \deg m_i$*. Buď* $u_1, \ldots, u_n \in T[x]$ *libovolné polynomy. Pak existuje právě jeden polynom* $f \in T[x]$ *stupně* $< d$*, který řeší soustavu kongruencí*

$$f \equiv u_1 \pmod{m_1}, \quad \ldots, \quad f \equiv u_n \pmod{m_n}.$$

Důkaz. Nejprve dokážeme jednoznačnost. Předpokládejme, že soustava má dvě řešení f, g stupně $< d$, tj. pro každé i platí

$$f \equiv g \equiv u_i \pmod{m_i}.$$

Polynom $f - g$ je také stupně $< d$, je dělitelný každým m_i, a protože jsou polynomy m_i navzájem nesoudělné, dostáváme (díky gaussovskosti oboru $\mathbf{T}[x]$)

$$M = m_1 \cdot \ldots \cdot m_n \mid f - g.$$

Čili polynom stupně d dělí polynom stupně $< d$, což je možné pouze v tom případě, že $f - g = 0$, tj. $f = g$.

Nyní dokážeme, že nějaké řešení existuje, indukcí podle počtu rovnic. Nejprve uvažujme soustavu dvou kongruencí. Z kongruence $f \equiv u_2 \pmod{m_2}$ vyjádříme $f = g m_2 + u_2$ pro nějaký polynom $g \in T[x]$ a dosadíme do první kongruence

$$f = g m_2 + u_2 \equiv u_1 \pmod{m_1}.$$

Označme $\widetilde{m_2}$ inverz polynomu m_2 modulo m_1, tj. takový polynom, pro který platí $m_2 \widetilde{m_2} \equiv 1 \pmod{m_1}$. Ten najdeme pomocí Bézoutovy rovnosti: napíšeme

$1 = \mathrm{NSD}(m_1, m_2) = um_1 + vm_2$ a vidíme, že $vm_2 \equiv 1 \pmod{m_1}$. Přenásobením původní kongruence polynomem $\widetilde{m_2}$ dostáváme

$$g \equiv \widetilde{m_2}(u_1 - u_2) \pmod{m_1},$$

řešením tedy je každý polynom $g = hm_1 + \widetilde{m_2}(u_1 - u_2)$, pro libovolné $h \in T[x]$. Zpětným dosazením dostaneme obecné řešení

$$f = gm_2 + u_2 = hm_1m_2 + (\widetilde{m_2}(u_1 - u_2) \bmod m_1)m_2 + u_2$$

a volbou $h = 0$ řešení stupně $< d$.

Všimněte si, že původní dvojice kongruencí je ekvivalentní jedné kongruenci $f \equiv u \pmod{m_1m_2}$, pro jisté u. Soustavu n kongruencí tak můžeme řešit redukcí na soustavu $n - 1$ kongruencí. Podmínka nesoudělnosti je zachovaná: jsou-li oba polynomy m_1, m_2 nesoudělné se všemi m_i, pak je s nimi nesoudělný i polynom m_1m_2 (opět se využije gaussovskost). □

Důkaz existence je zároveň návodem, jak řešení najít. Analogický postup funguje i pro celočíselné kongruence, používali jsme jej v příkladech v sekci **??** (tehdy jsme existenci řešení dokázali nekonstruktivně, ale pro polynomy tento důkaz neprojde, rozmyslete si proč).

Úloha. Najděte polynom $f \in \mathbb{Q}[x]$ stupně < 4 splňující

$$f \equiv 1 \pmod{x^2 - 1} \quad \text{a} \quad f \equiv x + 1 \pmod{x^2 + 1}.$$

Řešení. Budeme sledovat postup z důkazu Věty 2.1. Z druhé kongruence vyjádříme $f = g \cdot (x^2 + 1) + x + 1$ a dosadíme do první kongruence: budeme hledat $g \in \mathbb{Q}[x]$ splňující $g \cdot (x^2 + 1) \equiv -x \pmod{x^2 - 1}$. Všimněte si, že $\widetilde{x^2 + 1} = \frac{1}{2}$ (protože $x^2 + 1 \equiv 2$), takže dostaneme vyjádření $g \equiv -\frac{1}{2}x \pmod{x^2 - 1}$, čili řešením je každý polynom $g = h \cdot (x^2 - 1) - \frac{1}{2}x$, $h \in \mathbb{Q}[x]$. Zpětným dosazením dostaneme obecné řešení

$$f = h \cdot (x^2 - 1)(x^2 + 1) - \frac{1}{2}x(x^2 + 1) + (x + 1),\ h \in \mathbb{Q}[x],$$

a hledaný polynom $f = -\frac{1}{2}x^3 + \frac{1}{2}x + 1$ dostaneme volbou $h = 0$. □

Speciálním případem čínské věty o zbytcích je *věta o interpolaci*: ta říká, že pokud předepíšeme hodnoty v n různých bodech, pak existuje právě jeden polynom stupně $< n$, který těchto hodnot v daných bodech nabývá.

Důsledek 2.2 (věta 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* $i = 1, \ldots, n$*.*

Důkaz. Připomeňme, že $f \equiv f(u) \pmod{x - u}$. Řešíme tedy soustavu kongruencí $f \equiv u_i \pmod{x - a_i}$. □

Na rozdíl od obecné věty o zbytcích není těžké nalézt vzorec, který určuje řešení interpolační úlohy: je jím tzv. *Lagrangeův interpolační polynom*

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

Dosazením do vzorce snadno zjistíme, že

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

Jednoznačnost pak plyne z věty o počtu kořenů vztažené na rozdíl $f - g$ dvou řešení.

Důsledek 2.3. *Buď* $\mathbf{T}$ *konečné těleso. Pak pro každé zobrazení* $\varphi : T \to T$ *existuje právě jeden polynom* $f \in T[x]$ *stupně* $< |T|$ *takový, že* $f(a) = \varphi(a)$ *pro každé* $a \in T$.

Důkaz. Interpolujme v bodě a hodnotou $\varphi(a)$ pro každé $a \in T$. □

Pro *nekonečná* tělesa nic takového platit nemůže, přesto polynomy hrají důležitou roli i v reálné analýze: každou spojitou reálnou funkci lze libovolně přesně aproximovat polynomiální funkcí, v různých smyslech. Například, lokální aproximaci (na okolí daného bodu) popisují Taylorovy polynomy, globální (na intervalu) třeba Weierstrassova věta, která říká, že pro každou spojitou reálnou funkci $f : [u, v] \to \mathbb{R}$ na omezeném uzavřeném intervalu a pro každé $\varepsilon > 0$ existuje polynom $g \in \mathbb{R}[x]$ takový, že $|f(a) - g(a)| < \varepsilon$ pro každé $a \in [u, v]$.

2.2. **Faktorokruh modulo polynom.**

Připomeňme konstrukci oborů $\mathbb{Z}_m$. Začali jsme s oborem celých čísel a uvažovali všechny možné zbytky po dělení m, tj. čísla $0, \ldots, m-1$, a na nich operace modulo m. Pokud bylo m prvočíslo, dostali jsme těleso. Podobný postup lze provést i s polynomy, dostaneme tzv. *faktorokruhy*. Aby se nepletla proměnná v polynomech s prvky faktorokruhu, obvykle se v konstrukci používá proměnná α.

Buď $\mathbf{T}$ těleso a zvolme polynom $m \in T[\alpha]$ stupně $n \geq 1$. *Faktorokruhem* $\mathbf{T}[\alpha]/(m)$ rozumíme množinu všech polynomů stupně $< n$ se standardními operacemi sčítání a odčítání a s operací násobení modulo m. Ve zkratce,

$$\mathbf{T}[\alpha]/(m) = (\{f \in T[\alpha] : \ \deg f < n\}, +, -, \odot, 0, 1),$$

kde $f \odot g = f \cdot g \bmod m$. Předně je potřeba dokázat, že to je skutečně komutativní okruh. Axiomy obsahující pouze sčítání a odčítání jsou zřejmé, protože tyto operace jsou totožné jako v $\mathbf{T}[x]$. Pro úvahy s násobením je třeba si připomenout, že $f \equiv g \pmod m \Leftrightarrow f \bmod m = g \bmod m$, a že $f \bmod m \equiv f \pmod m$. Tímto způsobem lze všechny identity přeložit do kongruencí, kde je platnost zřejmá. Například pro asocitivitu dokazujeme

$$(f \odot g) \odot h = f \odot (g \odot h),$$

tj.

$$(f \cdot g \bmod m) \cdot h \bmod m = f \cdot (g \cdot h \bmod m) \bmod m,$$

což je ekvivalentní kongruenci

$$(f \cdot g) \cdot h \equiv f \cdot (g \cdot h) \pmod m,$$

což je pravda pro všechny polynomy f, g, h. Podobně můžeme ověřit distributivitu.

Příklad. Uvažujme faktorokruh $\mathbb{R}[\alpha]/(\alpha^2 + 1)$. Jeho prvky jsou polynomy $a + b\alpha$, $a, b \in \mathbb{R}$. Sčítání probíhá po složkách, tj. $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$. Násobení vypadá takto:

$$\begin{aligned}(a + b\alpha) \odot (c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2 \bmod (\alpha^2 + 1) \\ &= (ac - bd) + (ad + bc)\alpha.\end{aligned}$$

Všimněte si, že jsme dostali stejné vzorce jako pro sčítání a násobení komplexních čísel. Při ztotožnění symbolů i a α bychom mohli psát, že $\mathbb{R}[\alpha]/(\alpha^2+1) = \mathbb{C}$. Vysvětlení je prosté: při počítání modulo α^2+1 vlastně zaměňujeme α^2 za -1, neboť $\alpha^2 \equiv -1 \pmod{\alpha^2+1}$. Čili pracujeme přesně s vlastností, která definuje komplexní jednotku.

Podobně lze nahlédnout, že faktorokruh $\mathbb{Q}[\alpha]/(\alpha^2+1)$ lze ztotožnit s tělesem $\mathbb{Q}(i)$.

Příklad. Pro konečná tělesa je situace zajímavější.

- Faktorokruh $\mathbb{Z}_2[\alpha]/(\alpha^2+1)$ má čtyři prvky, ale není to těleso, dokonce ani obor integrity, protože
$$(\alpha+1) \odot (\alpha+1) = \alpha^2+1 \bmod (\alpha^2+1) = 0.$$
- Faktorokruh $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ má devět prvků. Je to těleso, ale na první pohled to vidět není.

Kdy dostaneme těleso vysvětluje následující tvrzení.

Tvrzení 2.4. *Buď* $\mathbf{T}$ *těleso a* $m \in T[\alpha]$ *stupně* ≥ 1. *Následující tvrzení jsou ekvivalentní:*

(1) $\mathbf{T}[\alpha]/(m)$ *je těleso,*
(2) $\mathbf{T}[\alpha]/(m)$ *je obor integrity,*
(3) m *je ireducibilní prvek v* $\mathbf{T}[\alpha]$.

Důkaz. (1) $\Rightarrow$ (2) viz Tvrzení **??**.

(2) $\Rightarrow$ (3). Pro spor předpokládejme, že v $\mathbf{T}[\alpha]$ existuje rozklad $m = f \cdot g$, kde $\deg f, \deg g < \deg m$. Pak ale v $\mathbf{T}[\alpha]/(m)$ platí $f \odot g = m \bmod m = 0$, spor.

(3) $\Rightarrow$ (1). Uvažujme polynom $f \neq 0$ stupně menšího než $\deg m$. Protože je m ireducibilní, platí $1 = \mathrm{NSD}(f, m) = uf + vm$ pro nějaké polynomy $u, v \in T[\alpha]$. Označme $\tilde{u} = u \bmod m$. Pak v $\mathbf{T}[\alpha]/(m)$ platí $\tilde{u} \odot f = \tilde{u}f \bmod m \equiv uf \equiv 1 \pmod{m}$, čili $\tilde{u}$ je hledaný inverzní prvek k f. □

V dalším textu budeme místo symbolu $\odot$ psát standardní symbol násobení; z kontextu bude vždy jasné, že jde o násobení ve faktorokruhu, tedy modulo m (stejně se používá standardní symbol pro násobení v okruzích $\mathbb{Z}_m$).

2.3. Kořenová rozšíření těles.

Nyní si ukážeme jednu důležitou aplikaci konstrukce faktorokruhu: každé těleso lze rozšířit tak, aby v něm měl daný polynom kořen. Pro racionální polynomy to zní triviálně, každý racionální polynom má přece komplexní kořen, ale tento fakt je předmětem Základní věty algebry (Věta 5.1), kterou zatím nemáme dokázanou. Naopak, existence rozkladového nadtělesa je stěžejním krokem k jejímu důkazu. A pro konečná tělesa žádnou analogii použít nelze.

Tvrzení 2.5. *Buď* $\mathbf{T}$ *těleso a* $f \in T[x]$ *stupně* ≥ 1. *Pak existuje těleso* $\mathbf{S} \geq \mathbf{T}$, *kde má polynom* f *kořen.*

Důkaz. Buď m nějaký ireducibilní dělitel polynomu f, označme $m = \sum a_i x^i$. Stačí najít nadtěleso, kde má kořen polynom m, ten bude kořenem i pro f. Uvažujme faktorokruh $\mathbf{S} = \mathbf{T}[\alpha]/(m(\alpha))$. Podle Tvrzení 2.4 je $\mathbf{S}$ těleso. Vyhodnotíme-li v $\mathbf{S}$ polynom m na prvku α, dostaneme

$$m(\alpha) = \sum a_i(\alpha^i \bmod m(\alpha)) \equiv \sum a_i \alpha^i = m(\alpha) \equiv 0 \pmod{m(\alpha)},$$

čili prvek α je kořenem obou polynomů m, f v nadtělese $\mathbf{S}$. □

Příklad.

- Pro polynom $x^3 - 2$ nad tělesem $\mathbb{Q}$ dostaneme těleso $\mathbb{Q}[\alpha]/(\alpha^3 - 2)$, které lze pomocí úvah v předchozí podsekci ztotožnit s tělesem $\mathbb{Q}(\sqrt[3]{2})$.
- Pro polynom $x^3 - 2$ nad tělesem $\mathbb{Z}_7$ dostaneme těleso $\mathbb{Z}_7[\alpha]/(\alpha^3 - 2)$, což je těleso s 7^3 prvky, které jste ještě asi nepotkali.

Indukcí snadno dokážeme, že existuje také nadtěleso, kde má daný polynom všechny kořeny, tj. kde se rozkládá na součin lineárních činitelů (polynomů stupně 1).

Věta 2.6. *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně ≥ 1. Pak existuje těleso $\mathbf{S} \geq \mathbf{T}$, kde se polynom f rozkládá na součin polynomů stupně 1.*

Důkaz. Budeme postupovat indukcí podle stupně polynomu f. Je-li f stupně 1, $f = ax - b$, pak má kořen $a^{-1}b$ již v tělese $\mathbf{T}$. V opačném případě uvažujme nadtěleso $\mathbf{U} \geq \mathbf{T}$, kde má polynom f kořen u, a uvažujme polynom $g \in U[x]$ takový že $f = g \cdot (x - u)$. Protože $\deg g < \deg f$, podle indukčního předpokladu existuje nadtěleso $\mathbf{S} \geq \mathbf{U}$, kde se g rozkládá na součin polynomů stupně 1, čili se tam rozkládá i f. □

3. Konečná tělesa a jejich aplikace

3.1. Konečná tělesa a počítačová reprezentace dat.

Důležitou aplikací faktorokruhů je konstrukce konečných těles. Buď p prvočíslo a uvažujme ireducibilní polynom $m \in \mathbb{Z}_p[\alpha]$ stupně k. Faktorokruh $\mathbb{Z}_p[\alpha]/(m)$ je podle Tvrzení 2.4 tělesem, jeho prvky jsou polynomy stupně $< k$ nad $\mathbb{Z}_p$, čili toto těleso má právě p^k prvků. Například,

- čtyřprvkové těleso můžeme zkonstruovat jako $\mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$,
- osmiprvkové jako $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha + 1)$ nebo $\mathbb{Z}_2[\alpha]/(\alpha^3 + \alpha^2 + 1)$,
- devítiprvkové jako $\mathbb{Z}_3[\alpha]/(\alpha^2 + 1)$ nebo $\mathbb{Z}_3[\alpha]/(\alpha^2 \pm \alpha + 2)$.

Pozor, p^k-prvkové těleso je něco jiného než okruh $\mathbb{Z}_{p^k}$! V sekci **??** si dokážeme Věty **??** a **??**, které říkají, že

(1) pro každé p, k existuje ireducibilní polynom stupně k nad $\mathbb{Z}_p$,
(2) každé konečné těleso lze sestrojit jako faktorokruh $\mathbb{Z}_p[\alpha]/(m)$,
(3) na volbě m nezáleží, tj. různé volby m dají tělesa, která „vypadají stejně“ (formálně, jsou *izomorfní*, viz sekce **??**).

Důkaz těchto vět je složitější, než se teď může zdát. Existence a jednoznačnost konečných těles plyne z teorie rozkladových nadtěles (sekce **??**) a k reprezentaci pomocí faktorokruhu budeme navíc potřebovat teorii rozšíření konečného stupně (sekce **??**). Konečné těleso velikosti p^k se zpravidla značí $\mathbb{F}_{p^k}$ (někdy též $GF(p^k)$, jako *Galois field*).

Konečná tělesa, zejména ta velikosti 2^k, mají zásadní využití v informatice. Jejich pomocí lze reprezentovat počítačová data a provádět s nimi různé operace, anebo v nich datové operace analyzovat. Velký význam má Důsledek 2.3 a jeho zobecnění pro zobrazení více proměnných (viz cvičení v sekci 2.1), které říká, že každou operaci na datech lze interpretovat jako polynomiální zobrazení nad příslušným tělesem. Tento fakt je základem moderní kryptologie. Reprezentaci dat si nyní vysvětlíme.

Základním datovým objektem, se kterým pracují počítače, jsou tzv. *bitvektory*, tedy k-tice nul a jedniček, tzv. *bitů*. Délka k bývá mocnina dvojky, na starých počítačích byl standard $k = 8$ (osmicím se říká *bajty*), na moderních strojích je obvykle $k = 32$ nebo $k = 64$. Bitvektory délky k lze přirozeně reprezentovat pomocí konečného tělesa $\mathbb{F}_{2^k} = \mathbb{Z}_2[\alpha]/(m)$, kde m je ireducibilní stupně k: slovo $(a_0, \ldots, a_{k-1})$ se reprezentuje polynomem $\sum_{i=0}^{k-1} a_i \alpha^i$.

Standardní operace na bitvektorech jsou posouvání vlevo/vpravo a různé operace po jednotlivých bitech. Posouvání odpovídá násobení a dělení prvkem α. Logická spojka XOR po bitech odpovídá tělesovému sčítání, logická spojka AND po bitech odpovídá „skalárnímu součinu“, tj. násobení v $\mathbb{Z}_2$ po koeficientech. Konečná tělesa přinášejí navíc dvě zajímavé operace, které pracují se všemi bity najednou: tělesové násobení a invertování. Tyto operace míchají zajímavým způsobem jednotlivé bity, což nachází uplatnění v konstrukci šifer.

Příklad. V současnosti nejpoužívanější symetrická šifra AES (*Advanced Encryption Standard*) pracuje s bitvektory délky 32, které reprezentuje pomocí čtyř prvků tělesa

$$\mathbb{F}_{256} = \mathbb{Z}[\alpha]/(\alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1).$$

Text je reprezentován jako matice $4 \times N$ prvků tělesa $\mathbb{F}_{256}$, pro jisté N. Zjednodušeně řečeno, šifra několikrát za sebou opakuje čtyři fáze. V první se provádí pro každý prvek matice následující operace:

$$u \mapsto u^{-1} \cdot (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4) + (1 + \alpha + \alpha^5 + \alpha^8) \bmod (\alpha^8 + 1),$$

kde inverz se bere nad tělesem $\mathbb{F}_{256}$ a zbytek výpočtu probíhá v $\mathbb{Z}_2[\alpha]$. V druhé fázi se rotují řádky o jistý počet pozic, ve třetí se mixují sloupce interpretované jako polynomy stupně < 4nad $\mathbb{F}_{256}[x]$ pomocí operace

$$f \mapsto f \cdot (\alpha + x + x^2 + (\alpha + 1)x^3) \bmod (x^4 + 1).$$

Ve čtvrté fázi se pak přičítá klíč (po bitech). Smysl prvních tří fází je rozprostřít změnu provedenou přičítáním klíče do celé tabulky (míchání prvků, řádků, sloupců) tak, aby se co nejlépe ztratily slabiny opakování klíče (který bývá mnohonásobně kratší než zpráva). Detaily najdete například v učebnici [Ruo].

Jiný návrh kryptografického protokolu využívající konečná tělesa najdete v sekci 3.2. Další uplatnění konečných těles najdeme v kryptoanalýze (každou šifru lze interpretovat jako polynomiální zobrazení díky Důsledku 2.3), nebo také v konstrukci samoopravných kódů (příklad najdete v sekci 3.3). Zajímavé jsou také konečné geometrie (afinní a projektivní prostory nad konečnými tělesy), které jsou zdrojem velmi symetrických objektů, ale také zajímavých výpočetních problémů, jako je například počítání na eliptických křivkách, opět s aplikací v návrhu šifer. V sekci 3.4 si ukážeme konstrukci navzájem ortogonálních latinských čtverců pomocí afinních zobrazení.

3.2. **Sdílení tajemství.**

Motivační úloha je následující: armáda má tajný kód, který umožňuje odpálit jaderné rakety. Zřejmě není dobré, aby jeden šílenec mohl odpálit rakety o své vůli. Ani dva šílenci by neměli mít možnost odpálit rakety. Prezident nařídil, že k odpálení raket je potřeba souhlas aspoň tří šílenců z pětičlenného generálního štábu. Jak to zařídit?

Obecně hovoříme o (k,n)-*schématu sdílení tajemství*, pokud se n účastníků dělí o tajemství, k jehož odhalení je potřeba přítomnost alespoň k z nich (kterýchkoliv). V celém odstavci budeme uvažovat, že sdílíme tajemství z nějakého tělesa $\mathbf{T}$. V praxi se typicky sdílí nějaké heslo, tedy bitvektor délky m, k jehož reprezentaci se použije buď těleso s 2^m prvky, anebo m hodnot z tělesa $\mathbb{Z}_2$.

Pro případ $k = n$ lze použít jednoduché schéma založené na *maskování hodnot*. Vlastník tajemství vydá každému účastníku náhodný prvek $a_i \in T$ a zveřejní hodnotu $c = t + \sum a_i$. Pokud má dojít k odhalení, každý účastník sdělí své a_i a společně spočtou $t = c - \sum a_i$. Pokud se sejde účastníků méně, byť jen $n-1$, o hodnotě t nemohou říci vůbec nic: chybějící prvek může hodnotu součtu změnit na libovolnou jinou hodnotu, s pravděpodobností přesně $\frac{1}{|T|}$ (protože zobrazení $x \mapsto a + x$ je permutace). V praxi se používá těleso $\mathbb{Z}_2$: pravděpodobnost uhodnutí jednoho bitu je $\frac{1}{2}$, čili pro m-bitový klíč je pravděpodobnost $(\frac{1}{2})^m$.

Klasickým řešením obecného (k,n)-schématu je tzv. *Shamirův protokol*. Vlastník tajemství náhodně zvolí polynom $f \in T[x]$ stupně $< k$ takový, že $f(0) = t$ (tj. tajemství je absolutní člen f), vybere n po dvou různých prvků $0 \neq a_1, \ldots, a_n \in T$ (ta mohou být veřejná) a jednotlivým účastníkům rozdá hodnoty $f(a_1), \ldots, f(a_n)$. Pokud se sejde libovolných k účastníků, vezmou své hodnoty, provedou interpolaci ve svých bodech a spočtou (ten jediný) polynom stupně $< k$, který vyhovuje jejich podmínkám; tajemství je jeho absolutní člen. Naopak, pokud se jich sejde méně, byť jen $k-1$, o absolutním členu nezjistí nic: $k-1$ nenulovými body lze proložit polynom s libovolnou hodnotou v bodě 0, a navíc rozložení hodnot v 0 je rovnoměrné. V praxi se pro m-bitový klíč používá těleso s 2^m prvky (musí být $2^m > n$), které zajistí pravděpodobnost náhodného uhodnutí $\frac{1}{2^m}$.

Schéma lze snadno modifikovat pro sofistikovanější úlohy. Například, co kdyby prezident rozhodl, že rakety mohou odpálit buď aspoň tři z pěti šílených generálů, nebo on sám? Snadná pomoc: vyrobíme $(3,8)$-schéma, každému z generálů dáme po jednom dílu a prezidentu dáme tři. A tak podobně.

Cvičení. V dvoupatrovém úřadě v Kocourkově sídlí 20 úředníků, v každém patře 10, a ředitel. Úřad smí vydat rozhodnutí s kulatým razítkem, je-li přítomno aspoň 5 úředníků z 1. patra a 3 z 2. patra, nebo aspoň 2 z 1. patra, 8 z 2. patra a ředitel. Navrhněte schéma sdílení klíče k sejfu s kulatým razítkem. (Podobnost s Rektorátem Univerzity Karlovy je čistě náhodná.)

3.3. **Samoopravné kódy.**

TODO Hamming, Reed-Salomon

3.4. **Ortogonální latinské čtverce a návrh experimentů.**

TODO

4. Symetrické polynomy a Viètovy vztahy

Buď $\mathbf{R}$ libovolný komutativní okruh. Polynom $f \in R[x_1, \ldots, x_n]$ nazveme *symetrický*, pokud po libovolném přeuspořádání proměnných dostaneme ten samý polynom. Formálně, pokud

$$f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$$

pro libovolnou permutaci π na množině indexů $\{1, \ldots, n\}$.

Příklad. Polynomy $x^k + y^k + z^k$ a $x^k y^k z^k$ třech proměnných x, y, z jsou symetrické, pro libovolné k.

Příklad. Roznásobme součin $(y-x_1)(y-x_2)(y-x_3)$ a podívejme se na něj jako na polynom v proměnné y, jehož koeficienty jsou z $\mathbf{R}[x_1,x_2,x_3]$:

$$(y-x_1)(y-x_2)(y-x_3) = y^3-(x_1+x_2+x_3)y^2+(x_1x_2+x_1x_3+x_2x_3)y-(x_1x_2x_3).$$

Vidíme, že všechny koeficienty jsou symetrické polynomy vzhledem k proměnným x_1,x_2,x_3.

Předchozí příklad lze zobecnit na libovolný počet činitelů. Označme

$$\text{(V)}\quad (y-x_1)\cdot\ldots\cdot(y-x_n) = y^n - s_1y^{n-1} + s_2y^{n-2} - s_3y^{n-3} + \ldots + (-1)^n s_n.$$

Vzhledem k tomu, že v součinu nezáleží na pořadí, všechny koeficienty budou symetrické polynomy, přičemž je snadné dopočítat, že

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n = \sum_i x_i,\\
s_2 &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \sum_{i<j} x_ix_j,\\
&\ldots\\
s_k &= \sum_{i_1<\ldots<i_k} x_{i_1}\cdots x_{i_k},\\
&\ldots\\
s_n &= x_1x_2\cdots x_n.
\end{aligned}$$

Těmto polynomům se říká *elementární symetrické polynomy* v proměnných $x_1,\ldots,x_n$. Z rovnosti (V) pak plynou známé *Viètovy vztahy.*

Tvrzení 4.1 (Viètovy vztahy)**.** *Buď $\mathbf{T}$ těleso a $f=\sum a_ix^i$ polynom z $\mathbf{T}[x]$ stupně ≥ 1. Uvažujme jeho rozklad $f = a_n(x-u_1)\cdot\ldots\cdot(x-u_n)$ v nějakém nadtělese $\mathbf{S}\geq\mathbf{T}$. Pak*

$$\frac{a_{n-i}}{a_n} = (-1)^i\cdot s_i(u_1,\ldots,u_n).$$

Důkaz. Uvažujme polynom $g=a_n^{-1}f$. Do rovnosti (V) dosadíme za proměnné x_i prvky $u_i\in S$ a dostaneme

$$g=\sum_{i=0}^n \frac{a_i}{a_n}x^i = (x-u_1)\cdot\ldots\cdot(x-u_n) = x^n + \sum_{i=1}^n (-1)^i s_i(u_1,\ldots,u_n)x^{n-i}.$$

Porovnáním koeficientů dostaneme Viètovy vztahy. □

Díky Viètovým vztahům můžeme určit některé vlastnosti kořenů daného polynomu, aniž bychom znali jejich konkrétní hodnoty. Například víme, že jejich součet je $-\frac{a_{n-1}}{a_n}$ (dosaďte do s_1), jejich součin je $(-1)^n\frac{a_0}{a_n}$ (dosaďte do s_n).

Příklad. Všimněte si, že

$$x_1^2+\ldots+x_n^2 = s_1^2 - 2s_2$$

(ověřte roznásobením!). Z Viètových vztahů plyne, že součet čtverců všech kořenů daného polynomu $\sum a_ix^i$ je roven

$$u_1^2+\ldots+u_n^2 = s_1(u_1,\ldots,u_n)^2 - 2s_2(u_1,\ldots,u_n) = \left(\frac{a_{n-1}}{a_n}\right)^2 - 2\cdot\frac{a_{n-2}}{a_n}.$$

Všimněte si, že součet, rozdíl a součin symetrických polymů je symetrický polynom (čili symetrické polynomy tvoří podokruh okruhu všech polynomů). Speciálně, různé součty a součiny elementárních symetrických polynomů jsou symetrické. Je pravda i opačné trvrzení? V předchozím příkladě jsme viděli, že součet čtverců, což je symetrický polynom, lze takto vyjádřit. Důležitým poznatkem je, že tuto vlastnost má každý symetrický polynom.

Věta 4.2 (Základní věta o symetrických polynomech)**.** *Buď* $\mathbf{R}$ *obor integrity a* $f \in R[x_1, \ldots, x_n]$ *symetrický polynom. Pak existuje* právě jeden *polynom* $g \in R[z_1, \ldots, z_n]$ *takový, že* $f = g(s_1, \ldots, s_n)$.

Polynom g ve znění věty popisuje, jak získat f pomocí součtů a součinů elementárních polynomů. Například pro $f = x_1^2 + \ldots + x_n^2 = s_1^2 - 2s_2$ bude $g = z_1^2 - 2z_2$.

Ve zbytku sekce dokážeme Větu 4.2. Předvedeme si Gaussův důkaz obsahující algoritmus, který vyjádření daného symetrického polynomu najde. Nejprve si však musíme vysvětlit, jak uspořádat členy v polynomech více proměnných, abychom mohli pracovat s pojmem vedoucího členu.

Termem v proměnných $x_1, \ldots, x_m$ rozumíme výraz $x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, kde $k_1, \ldots, k_n \geq 0$. Definujeme relaci na termech:

$$x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} < x_1^{l_1} x_2^{l_2} \cdots x_n^{l_n},$$

pokud existuje $i \geq 0$ takové, že $k_1 = l_1$, …, $k_i = l_i$ a $k_{i+1} < l_{i+1}$. Definujeme $t \leq s$ právě tehdy, když $t < s$ nebo $t = s$. Jak si ukážeme, jde o uspořádání, tzv. *lexikografické uspořádání*, velmi podobné uspořádání slov ve slovníku. *Vedoucím členem* polynomu $f \in R[x_1, \ldots, x_n]$ se pak rozumí ten člen, který má lexikograficky největší term; značíme jej $\ell(f)$.

Příklad. Pro polynomy tří proměnných se zpravidla používají proměnné x, y, z, implicitně se rozumí v tomto pořadí.

- $\ell(x + y + z) = x$, neboť $x = x^1 y^0 z^0$ je větší než $y = x^0 y^1 z^0$, a to je větší než $z = x^0 y^0 z^1$.
- $\ell(100z^{10} + 2x^2 y - 5x^2 z^2) = 2x^2 y$, neboť $x^2 y > x^2 z^2 > z^{10}$ (koeficienty nerozhodují).

Lemma 4.3. *Relace* $\leq$ *má následující vlastnosti:*

(1) *je to lineární uspořádání,*
(2) *pro libovolné termy platí, že* $t_1 > t_2$ *a* $s_1 > s_2$ *implikuje* $t_1 s_1 > t_2 s_2$,
(3) *neexistuje nekonečný klesající řetězec termů* $t_1 > t_2 > t_3 > \ldots$

Důkaz lemmatu přenecháváme čtenáři jako snadné, byť poněkud pracné cvičení.

Lemma 4.4. *Buď* $\mathbf{R}$ *obor integrity a* $f, g \in R[x_1, \ldots, x_n]$. *Pak*

(1) $\ell(fg) = \ell(f)\ell(g)$,
(2) *je-li* f *symetrický a* $\ell(f) = a x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$, *pak* $k_1 \geq k_2 \geq \ldots \geq k_n$.

Důkaz. (1) Díky Lemmatu 4.3(2) platí, že součin termů vedoucích členů je větší než součin libovolných jiných termů. Protože jsme v oboru integrity, koeficient součinu nebude nulový.

(2) Kdyby $k_i < k_j$, mohli bychom prohodit proměnné x_i, x_j, ze symetrie bychom dostali ten samý polynom, ale člen s prohozenými proměnnými by byl větší. □

Lemma 4.5. *Buď* $k_1 \geq k_2 \geq \ldots \geq k_n$ *nezáporná čásla. Pak existuje* právě jedna n*-tice nezáporných čísel* $l_1, \ldots, l_n$ *taková, že* $\ell(s_1^{l_1} s_2^{l_2} \cdots s_n^{l_n}) = x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n}$.

Důkaz. Nejprve spočteme vedoucí člen $\ell(s_1^{l_1}s_2^{l_2}\cdots s_n^{l_n})$. Díky Lemmatu 4.4(1) je roven součinu

$$\begin{aligned}\ell(s_1)^{l_1}\ell(s_2)^{l_2}\cdots\ell(s_n)^{l_n} &= x_1^{l_1}\cdot(x_1x_2)^{l_2}\cdot(x_1x_2x_3)^{l_3}\cdot\ldots\cdot(x_1\cdots x_n)^{l_n}\\ &= x_1^{l_1+\ldots+l_n}x_2^{l_2+\ldots+l_n}\cdots x_{n-1}^{l_{n-1}+l_n}x_n^{l_n}.\end{aligned}$$

Máme dány exponenty $k_1,\ldots,k_n$, hledáme $l_1,\ldots,l_n$ splňující soustavu rovnic

$$k_1 = l_1+\ldots+l_n,\ k_2 = l_2+\ldots+l_n,\ \ldots,\ k_{n-1}=l_{n-1}+l_n,\ k_n = l_n.$$

Odečtením dvou po sobě jdoucích rovnic zjistíme, že existuje právě jedno řešení, a to

$$l_1 = k_1-k_2,\ l_2 = k_2-k_3,\ \ldots,\ l_{n-1}=k_{n-1}-k_n,\ l_n = k_n.$$

Tato řešení jsou nezáporná, protože $k_i \geq k_{i+1}$ pro všechna i. □

Nyní zformulujeme Gaussův algoritmus na výpočet vyjádření daného symetrického polynomu pomocí elementárních.

Gaussův algoritmus. Buď $\mathbf{R}$ obor intergrity.

- `VSTUP:` $f \in R[x_1,\ldots,x_n]$ symetrický
- `VÝSTUP:` $g \in R[z_1,\ldots,z_n]$ takový, že $f = g(s_1,\ldots,s_n)$
- $f_1 = f$, $g_1 = 0$
- pro $i = 2,3,\ldots$ prováděj následující:
  najdi $l_1,\ldots,l_n$ takové, že $\ell(f_i) = c\cdot\ell(s_1^{l_1}\cdots s_n^{l_n})$ pro nějaké $c\in R$
  $f_{i+1} = f_i - c\cdot s_1^{l_1}\cdots s_n^{l_n}$
  $g_{i+1} = g_i + c\cdot z_1^{l_1}\cdots z_n^{l_n}$
  pokud je $f_{i+1}\in R$ (konstantní polynom), odpověz $g_{i+1}+f_{i+1}$

Nyní dokážeme správnost algoritmu. Všimněte si, že pro všechna i platí

- f_i je symetrický polynom,
- $g_i \in R[z_1,\ldots,z_n]$,
- $f_i + g_i(s_1,\ldots,s_n) = f$.

(Pro $i=1$ to platí triviálně a dále postupujeme indukcí.) Z těchto tří pozorování plyne správnost odpovědi i fakt, že taková $l_1,\ldots,l_n$ vždy najdeme (Lemmata 4.4(2) a 4.5, resp. algoritmus výpočtu skrytý v důkazu). Na závěr zbývá zpozorovat, že se termy vedoucích členů polynomů $f_1, f_2, \ldots$ zmenšují, čili podle Lemmatu 4.3(3) se algoritmus musí zastavit.

Příklad. Mějme na vstupu polynom $f = x_1^3+\ldots+x_n^3$.

- $f_1 = x_1^3+\ldots+x_n^3$, $g_1 = 0$.
- Vidíme, že $\ell(f_1) = x_1^3 = \ell(s_1^3)$, čili
$$f_2 = f_1 - s_1^3 = -3\sum_{i\neq j}x_i^2x_j - 6\sum_{i<j<k}x_ix_jx_k,\quad g_2 = g_1+z_1^3 = z_1^3.$$
- Vidíme, že $\ell(f_2) = -3x_1^2x_2 = -3\ell(s_1s_2)$, čili:
$$f_3 = f_2-(-3)s_1s_2 = 3\sum_{i<j<k}x_ix_jx_k,\quad g_3 = g_2+(-3)z_1z_2 = z_1^3-3z_1z_2.$$
- Vidíme, že $\ell(f_3) = 3x_1x_2x_3 = 3\ell(s_3)$, čili
$$f_4 = f_3-3s_3 = 0,\quad g_4 = g_3+3z_3 = z_1^3-3z_1z_2+3z_3.$$

Odpovědí je polynom g_4, čili $f = g_4(s_1,\ldots,s_n) = s_1^3-3s_1s_2+3s_3$.

Důkaz Věty 4.2. Existence byla prokázána Gaussovým algoritmem. Jednoznačnost dokážeme sporem. Uvažujme dvě vyjádření $f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$, $g_1 \neq g_2$, a označme $g = g_1 - g_2 = \sum a_i t_i$, kde t_i jsou jednotlivé termy. Tyto termy jsou různé, a tedy díky jednoznačnosti v Lemmatu 4.5 mají polynomy $t_i(s_1, \ldots, s_n)$ různé vedoucí členy. Uvažujte ten lexikograficky největší z nich. Tím, že je striktně větší než všechny ostatní členy, se v součtu $\sum a_i t_i(s_1, \ldots, s_n)$ nemůže pokrátit, a tedy $g(s_1, \ldots, s_n) \neq 0$, spor. □

Základní věta o symetrických polynomech má zajímavý důsledek, který použijeme v důkazu Základní věty algebry. Uvažujme celočíslený polynom a jeho komplexní kořeny. To mohou být komplexní čísla, která nelze nijak pěkně vyjádřit. Přesto, pokud je dosadíme do symetrického polynomu, vyjde racionální číslo (dokonce celé, pokud byl tento polynom monický).

Důsledek 4.6. *Buď* $\mathbf{T}$ *těleso a* f *polynom z* $\mathbf{T}[x]$ *stupně* $n \geq 1$. *Buď* $u_1, \ldots, u_n$ *jeho kořeny (včetně násobnosti) v nějakém nadtělese. Pak pro každý symetrický polynom* $s \in T[x_1, \ldots, x_n]$ *platí* $s(u_1, \ldots, u_n) \in T$.

Důkaz. Označme $f = \sum a_i x^i$. Díky Viètovým vztahům platí $s_i(u_1, \ldots, u_n) = (-1)^i \frac{a_{n-i}}{a_n} \in T$. Díky Větě 4.2 existuje polynom $g \in T[z_1, \ldots, z_n]$ splňující $s = g(s_1, \ldots, s_n)$, čili $s(u_1, \ldots, u_n)$ je rovno hodnotě polynomu g na n-tici prvků z T, což je opět prvek T. □

5. Základní věta algebry

Cílem této sekce je dokázat, že každý komplexní polynom má komplexní kořen. Tomuto faktu se říká Základní věta algebry, i když název je poněkud zastaralý a odpovídá době svého vzniku, tedy přelomu 18. a 19. století, kdy se algebra zabývala především řešením polynomiálních rovnic. Trochu zavádějící je i samotný odkaz na algebru: důkaz nutně musí využít nějaké analytické metody, neboť se principiálně týká vlastností reálných funkcí, resp. jejich komplexních rozšíření.

Věta 5.1 (Základní věta algebry)**.** *Každý komplexní polynom stupně* ≥ 1 *má nějaký komplexní kořen.*

Důkazů základní věty algebry existuje celá řada, ať už čistě analytické (pomocí komplexní analýzy), geometrické, či algebraické, snažící se minimalizovat potřebné množství vlastností reálných čísel. Ukážeme si Gaussův důkaz z roku 1816, který patří do poslední rodiny, je poměrně jednoduchý a pěkně odděluje analytické a algebraické principy potřebné k důkazu. Z algebry jsou stěžejním nástrojem

- existence rozkladových nadtěles (Věta 2.6),
- teorie symetrických polynomů (klíčový krok důkazu je založen na úvaze podobné Důsledku 4.6).

Z reálné analýzy pak využijeme

- spojitost polynomiálních funkcí,
- větu o středním bodě,

které implikují, že reálné polynomy lichého stupně mají aspoň jeden reálný kořen. Začneme užitečným pozorováním, že problém lze zredukovat na reálné polynomy. K důkazu stačí pár elementárních výpočtů s komplexně sdruženými čísly.

Lemma 5.2. *Předpokládejme, že každý reálný polynom stupně ≥ 1 má nějaký komplexní kořen. Pak má každý komplexní polynom stupně ≥ 1 nějaký komplexní kořen.*

Důkaz. Buď $f \in \mathbb{C}[x]$ stupně ≥ 1. Označme $g = f \cdot \bar{f}$, kde $\bar{f}$ značí komplexně sdružený polynom, tj. pro $f = \sum a_i x^i$ definujeme $\bar{f} = \sum \bar{a}_i x^i$. Všimněte si, že $g \in \mathbb{R}[x]$: součin má tvar

$$f \cdot \bar{f} = \sum a_i x^i \cdot \sum \bar{a}_i x^i = \sum_k \left(\sum_{i+j=k} a_i \bar{a}_j \right) x^k.$$

Všechny koeficienty jsou reálné, protože pro $i = j$ máme $a_i \bar{a}_i \in \mathbb{R}$, a pro $i \neq j$ máme $a_i \bar{a}_j + a_j \bar{a}_i \in \mathbb{R}$ (všimněte si, že $r\bar{s} + \bar{r}s \in \mathbb{R}$ pro každé $r, s \in \mathbb{C}$). Čili podle předpokladu má polynom g komplexní kořen u. Čili $f(u) = 0$ nebo $\overline{\bar{f}(u)} = 0$. V prvním případě jsme hotovi a v druhém případě si všimneme, že $0 = \overline{\bar{f}(u)} = f(\bar{u})$, a tedy f má kořen u nebo $\bar{u}$. □

Lemma 5.3. *Komplexní polynom stupně 2 má komplexní kořen.*

Důkaz. Kořeny polynomu ax^2+bx+c lze spočítat vzorcem $u = \frac{-b \pm \sqrt{b^2-4ac}}{-2a}$ (důkaz najdete v sekci **??**), výsledkem je komplexní číslo. Poněkud skrytý je fakt, že v komplexních číslech lze odmocňovat, protože $\sqrt{re^{ia}} = \sqrt{r}e^{ia/2}$, kde využíváme faktu, že kladná reálná čísla lze odmocňovat, což je důsledek spojitosti funkce $x \mapsto x^2$ a věty o středním bodě. □

Lemma 5.4. *Reálný polynom lichého stupně má reálný kořen.*

Důkaz. Reálný polynom f určuje spojitou reálnou funkci. Má-li lichý stupeň, pak v závislosti na znaménku vedoucího koeficientu buď $\lim_{x\to-\infty} = -\infty$ a $\lim_{x\to\infty} = \infty$, nebo naopak, tedy existují body a, b takové, že $f(a) < 0$ a $f(b) > 0$. Z věty o středním bodě plyne, že existuje bod $u \in \mathbb{R}$, kde $f(u) = 0$. □

Důkaz Věty 5.1. Díky Lemmatu 5.2 stačí uvažovat reálný polynom f stupně $n = 2^k m$, kde m je liché. Budeme postupovat indukcí podle k. Je-li $k = 0$, odpověď dává Lemma 5.4. V indukčním kroku uvažujme rozkladové nadtěleso $\mathbf{T}$ pro polynom f nad $\mathbb{R}$, označme $u_1, \ldots, u_n$ kořeny f v $\mathbf{T}$ (včetně násobnosti). Chceme dokázat, že aspoň jeden z těchto kořenů je v $\mathbb{C}$. Pro každý parametr $z \in \mathbb{Z}$ definujeme polynom

$$h_z = \prod_{i<j} (x - (u_i + u_j + z u_i u_j)) \in T[x].$$

Klíčovým krokem je ukázat, že to je ve skutečnosti reálný polynom. Uvažujte polynom

$$\tilde{h}_z = \prod_{i<j} (x - (y_i + y_j + z y_i y_j)) \in \mathbb{R}[x][y_1, \ldots, y_n].$$

Ten je symetrický v proměnných $y_1, \ldots, y_n$ s koeficienty v $\mathbb{R}[x]$ a $h_z = \tilde{h}_z(u_1, \ldots, u_n)$. Podle Věty 4.2 existuje polynom $g \in \mathbb{R}[x][y_1, \ldots, y_n]$ takový, že $\tilde{h}_z = g(s_1, \ldots, s_n)$. Z Viètových vztahů plyne, že $s_i(u_1, \ldots, u_n) \in \mathbb{R}$, a tedy

$$h_z = g(s_1(u_1, \ldots, u_n), \ldots, s_n(u_1, \ldots, u_n)) \in \mathbb{R}[x].$$

Přitom stupeň polynomu h_z je

$$\deg h_z = \binom{n}{2} = \frac{2^m q \cdot (2^m q - 1)}{2} = 2^{m-1} q (2^m q - 1),$$

takže můžeme použít indukční předpoklad a dostáváme, že h_z má kořen v $\mathbb{C}$. Shrnuto, dokázali jsme, že pro každé $z \in \mathbb{Z}$ existují nějaká $i < j$ taková, že $u_i + u_j + zu_iu_j \in \mathbb{C}$. Takových z je nekonečně mnoho, ale dvojic indexů je jen konečně mnoho, musí tedy existovat dvojice $i < j$, která se opakuje aspoň dvakrát (dokonce nekonečněkrát). Označme příslušná čísla z_1, z_2, tj.

$$u_i + u_j + z_1u_iu_j \in \mathbb{C} \quad \text{a} \quad u_i + u_j + z_2u_iu_j \in \mathbb{C}.$$

Odečtením obou rovníc vidíme, že $(z_1 - z_2)u_iu_j \in \mathbb{C}$, čili také $u_iu_j \in \mathbb{C}$ a $u_i + u_j \in \mathbb{C}$. Z toho plyne, že oba kořeny u_i, u_j jsou komplexní, neboť

$$(x - u_i)(x - u_j) = x^2 - (u_i + u_j)x + u_iu_j$$

a podle Lemmatu 5.3 víme, že komplexní kvadratický polynom má nutně komplexní kořeny. □

Důsledkem je, že polynom $f \in \mathbb{C}[x]$ stupně n má právě n komplexních kořenů (včetně násobnosti) a rozkládá se v $\mathbb{C}[x]$ na součin

$$f \parallel (x - u_1) \cdot \ldots \cdot (x - u_n),$$

kde $u_1, \ldots, u_n \in \mathbb{C}$. Důkaz provedeme snadno indukcí: máme-li jeden komplexní kořen, u, vydělíme f polynomem $x - u$ a použijeme větu znovu, na polynom menšího stupně.