POLYNOMY

DAVID STANOVSKÝ

1. Polynomy nad gaussovskými obory

1.1. Gaussova věta.

Polynomy jedné proměnné nad tělesem tvoří eukleidovský obor, a tedy jsou gaussovské. Polynomy více proměnných, nebo třeba polynomy nad $\mathbb{Z}$, eukleidovské nejsou. Jak to je s jejich gaussovskostí? Odpověď dává Gaussova věta.

Věta 1.1 (Gaussova věta)**.** *Je-li* $\mathbf{R}$ *gaussovský obor, pak je* $\mathbf{R}[x]$ *také gaussovský obor.*

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

Důkaz. Použijeme charakterizaci z Věty **??**. Existenci NSD v $\mathbf{R}[x]$ dokážeme ve Větě 1.2. Je-li $f_1, f_2, f_3, \dots$ nekonečná posloupnost vlastních dělitelů, pak $\deg f_1 \geq \deg f_2 \geq \deg f_3 \geq \dots \geq 0$, a tedy existuje n takové, že $\deg f_n = \deg f_{n+1} = \dots$ Označíme-li u_i absolutní člen polynomu f_i, pak $u_n, u_{n+1}, u_{n+2} \dots$ tvoří nekonečnou posloupnost vlastních dělitelů v $\mathbf{R}$, spor. □

Ve zbytku sekce vyjasníme vztah mezi dělitelností polynomů v $\mathbf{R}[x]$ a v $\mathbf{Q}[x]$, kde $\mathbf{Q}$ je podílvé těleso oboru $\mathbf{R}$. Cílem je Věta 1.2, na níž stojí důkaz věty Gaussovy, která převádí výpočty v oboru $\mathbf{R}[x]$ na výpočty v oboru $\mathbf{R}$ a v oboru $\mathbf{Q}[x]$. K její formulaci se nám budou hodit následující definice.

Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom z $\mathbf{R}[x]$. Definujeme

$$\mathrm{c}(f) = \mathrm{NSD}(a_0, \dots, a_n) \qquad \text{a} \qquad \mathrm{pp}(f) = f / \mathrm{c}(f).$$

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

Věta 1.2. *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* $\mathbf{Q}[x]$*.*

Date: 21. prosince 2017.

Pracovní materiál pro zimní semestr předmětu Algebra I 2017/18. Text není hotový a nejspíš obsahuje chyby. Jeho finální verze bude součástí nového vydání skript.

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 $\mathbf{R}[x]$ použít, protože výsledek je dělitelný 2, ale ani jeden z polynomů 2 dělitelný není. Druhou odpověď nemůžeme použít, protože výsledek ani neleží v $\mathbf{R}[x]$. Věta říká, že použít máme primitivní výsledek, tj. v našem případě $x+1$ nebo $-x-1$. Takový polynom h jistě existuje: stačí vzít libovolný $\mathrm{NSD}(f,g)$ v $\mathbf{Q}[x]$ a přenásobit ho prvkem $q = \frac{a}{b} \in Q$, kde a je NSN jmenovatelů všech koeficientů, a b je NSD všech čitatelů koeficientů.

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 $\mathbb{Z}[x]$.

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

Lemma 1.3 (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. Tedy existuje ireducibilní prvek $p \in R$, který dělí součin fg, tj. všechny koeficienty tohoto součinu. 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 kromě $a_j b_k$. Ten naopak p dělitelný není, protože p je ireducibilní a nedělí ani a_j, ani b_k (zde využíváme gaussovskost). Dostáváme, že $p \nmid c_{j+k}$, spor. □

Parafrází dostaneme následující důsledek, který je stěžejní ingrediencí Věty 1.2.

Důsledek 1.4. *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 dokážeme tu opačnou. Mějme takový polynom $h \in Q[x]$ a zvolme $q \in Q$ tak, aby byl qh primitivní polynom z $\mathbf{R}[x]$. Pak $qg = f \cdot qh$, 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 $h \in R[x]$. □

Důkaz Věty 1.2. (1) Nejprve dokážeme, že pro primitivní polynomy f, g existuje $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ je roven primitivnímu polynomu $h \in R[x]$ splňujícímu $h = \mathrm{NSD}_{\mathbf{Q}[x]}(f, g)$. Polynom h dělí f, g v $\mathbf{Q}[x]$ a je primitivní, tedy díky Důsledku 1.4 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 Důsledku 1.4 $d \mid h$ 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 Důsledku 1.4 vlastním dělitelem v $\mathbf{R}[x]$. □

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

Připomeňte si důkaz Gaussova lemmatu 1.3. 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 $a_1 r s^{n-1}, \ldots, a_n r^n$, musí dělit i první člen $a_0 s^n$. Protože jsou r, s nesoudělné, musí r dělit a_0 (zde využíváme gaussovskost, konkrétně Tvrzení **??** aplikované na všechny ireducibilní prvku 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 $-\frac{3}{2}$.

Tvrzení 1.6 (Eisensteinovo kritérium)**.** *Buď* $\mathbf{R}$ *gaussovský obor a* $f = \sum_{i=0}^{n} a_i x^i$ *primitivní polynom z* $\mathbf{R}[x]$. *Pokud existuje ireducibilní prvek* $p \in R$ *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* $\mathbf{R}[x]$.

Důkaz. 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 $p \mid a_0 = b_0 c_0$, podle Tvrzení **??** 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. Protože $p \mid a_1 = b_0 c_1 + b_1 c_0$ a $p \nmid c_0$, podle Tvrzení **??** 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 $p \mid b_2$. Tímto způsobem zjistíme, že p dělí všechny koeficienty b_i, tedy $p \mid gh = f$, což je spor s primitivitou. □

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

2. Symetrické polynomy

V této sekci se budeme zabývat polynomy více proměnných nad libovolným oborem $\mathbf{R}$. Polynom f 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 $\mathbf{R}[x_1, x_2, x_3]$:

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

Všechny koeficienty jsou nutně symetrické polynomy vzhledem k x_1, x_2, x_3, protože v původním součinu nezáleží na pořadí, ve kterém násobíme.

Předchozí příklad lze očividně zobecnit na n činitelů. Dostáváme

$$(y - x_1) \cdot \ldots \cdot (y - x_n) = y^n - s_1 y^{n-1} + s_2 y^{n-2} - s_3 y^{n-3} + \ldots + (-1)^n s_n,$$

kde

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

Těmto polynomům se říká *elementární symetrické polynomy.* Z výše uvedené rovnosti pak plynou známé *Viètovy vztahy.*

Tvrzení 2.1 (Viètovy vztahy)**.** *Buď* $\mathbf{T}$ *těleso a* $f = \sum a_i x^i$ *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*

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

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 $x_1^2 + \ldots + x_n^2 = s_1^2 - 2s_2$. Z Viètových vztahů plyne, že součet čtverců všech kořenů daného polynomu $\sum a_i x^i$ je roven $s_1(u_1, \ldots, u_n)^2 - 2s_2(u_1, \ldots, u_n) = (-\frac{a_1}{a_n})^2 - 2\frac{a_2}{a_n}$, tj.

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

Je zřejmé, že součet a součin symetrických polymů je symetrický polynom. Čili například polynom $2s_1^2 s_3 + 3s_2^3 - 1$ je symetrický. V předchozím příkladě jsme viděli, že součet čtverců lze získat sčítáním a násobením z elementárních symetrických polynomů $s_1, \ldots, s_n$. Stěžejním poznatkem je, že každý symetrický polynom lze získat tímto způsobem.

Věta 2.2 (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* $g \in R[y_1, \ldots, y_n]$ *takový, že* $f = g(s_1, \ldots, s_n)$.

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 2.3. *Buď* $\mathbf{T}$ *těleso a* f *monický 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* $g \in T[x_1, \ldots, x_n]$ *platí* $g(u_1, \ldots, u_n) \in T$.

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 2.2 existuje polynom $h \in T[y_1, \ldots, y_n]$ splňující $g = h(s_1, \ldots, s_n)$, čili $g(u_1, \ldots, u_n)$ je rovno hodnotě polynomu h na n-tici prvků z T, což je opět prvek T. □

Ve zbytku sekce dokážeme Větu 2.2. Předvedeme si Gaussův důkaz založený na algoritmu, 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.

Zavedeme tzv. *lexikografické uspořádání* na členech polynomu:

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

pokud existuje $i \geq 0$ takové, že $k_1 = l_1$, …, $k_i = l_i$ a $k_{i+1} \geq l_{i+1}$ (konstanty $a, b \in R \setminus \{0\}$ nehrají žádnou roli). Je snadné nahlédnout, že

(1) jde skutecně o uspořádání (velmi podobné uspořádání ve slovníku),
(2) $t_1 \geq t_2$ a $s_1 \geq s_2$ implikuje $t_1 s_1 \geq t_2 s_2$,
(3) v tomto uspořádání neexistuje nekonečný klesající řetězec $t_1 > t_2 > t_3 > \ldots$

Vedoucím členem polynomu $f \in R[x_1, \ldots, x_n]$ se pak rozumí ten člen, který je lexikograficky největší. Díky vlastnosti (2) platí, že vedoucí člen součinu dvou polynomů je roven součinu jejich vedoucích členů (protože jsme v oboru integrity, koeficient nebude nulový).

Příklad. Platí $2x^2y > -5x^2z^2 > 100z^{10}$. V polynomu $2x^2y - 5x^2z^2 + 100z^{10}$ tedy bude vedoucím členem $2x^2y$.

Všimněte si, že v symetrickém polynomu má vedoucí člen klesající exponenty, tj. je tvaru $ax_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$, kde $k_1 \geq k_2 \geq \ldots \geq k_n$. Kdyby totiž $k_i < k_j$, mohli bychom prohodit proměnné x_i, x_j, ze symetrie bychom dostali ten samý polynom, ale najednou bychom měli větší člen.

Lemma 2.4. *Buď $k_1 \geq k_2 \geq \ldots \geq k_n$ přirozená čísla. Pak existuje* právě jedna *n-tice nezáporných čísel $l_1, \ldots, l_n$ taková, že vedoucí člen polynomu $s_1^{l_1}s_2^{l_2}\cdots s_n^{l_n}$ je roven $x_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$.*

Důkaz. Spočteme vedoucí člen polynomu $s_1^{l_1}s_2^{l_2}\cdots s_n^{l_n}$: ten je roven součinu jednotlivých vedoucích členů, čili

$$x_1^{l_1}\cdot(x_1x_2)^{l_2}\cdot(x_1x_2x_3)^{l_3}\cdot\ldots\cdot(x_1\cdots x_n)^{l_n} = x_1^{l_1+\ldots+l_n}x_2^{l_2+\ldots+l_n}\cdots x_{n-1}^{l_{n-1}+l_n}x_n^{l_n}.$$

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 algoritmus na výpočet reprezentace symetrického polynomu pomocí elementárních.

- `VSTUP:` $f \in R[x_1, \ldots, x_n]$ symetrický
- `VÝSTUP:` $g \in R[y_1, \ldots, y_n]$ takový, že $f = g(s_1, \ldots, s_n)$
- $f_1 = f$, $g_1 = 0$
- Jsou-li definovány f_i, g_i, pak:
  najdi $l_1, \ldots, l_n$ takové, že vedoucí člen f_i je roven c-násobku vedoucího členu polynomu $s_1^{l_1}\cdots s_n^{l_n}$, pro n2jaké $c \in R$
  $f_{i+1} = f_i - c\cdot s_1^{l_1}\cdots s_n^{l_n}$
  $g_{i+1} = g_i + c\cdot y_1^{l_1}\cdots y_n^{l_n}$
  Pokud je $f_{i+1} \in R$ (konstantní polynom), odpověz $g_{i+1} + f_{i+1}$.

Nyní dokážeme správnost algoritmu: všimněte si, že

- taková $l_1, \ldots, l_n$ lze najít, protože každý polynom f_i je symetrický (f_1 je a f_{i+1} vznikne jako rozdíl dvou symetrických polynomů), čili exponenty jeho vedoucího členu jsou sestupné a důkaz Lemmatu 2.4 dává návod, jak taková $l_1, \ldots, l_n$ najít;
- $f_i + g_i(s_1, \ldots, s_n) = f$ pro každé i: pro $i = 1$ to platí triválně a v každém dalším kroku, co jsme odečetli od f_i, to přičteme ke g_i; čili algoritmus skutečně odpoví správný výsledek;
- vedoucí členy f_i se zmenšují, tedy po konečně mnoha krocích musí skončit konstantním polynomem (buď nulou, nebo polynomem, jehož jediný a tedy vedoucí člen je $x_1^0\cdots x_n^0$), a algoritmus se zastaví.

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

- $f_1 = x_1^3 + \ldots + x_n^3$, $g_1 = 0$.

- Vedoucí člen f_1 je x_1^3, což je zároveň vedoucí člen polynomu s_1^3, čili: $f_2 = f_1 - s_1^3 = -3\sum_{i\neq j} x_i^2 x_j - 6\sum_{i<j<k} x_i x_j x_k$, $g_2 = g_1 + y_1^3 = y_1^3$.
- Vedoucí člen f_2 je $-3x_1^2x_2$, což je zároveň vedoucí člen polynomu $-3s_1s_2$, čili: $f_3 = f_2 - (-3)s_1s_2 = 3\sum_{i<j<k} x_i x_j x_k$, $g_3 = g_2 + (-3)y_1y_2 = y_1^3 - 3y_1y_2$.
- Vedoucí člen f_3 je $3x_1x_2x_3$, což je zároveň vedoucí člen polynomu $3s_3$, čili: $f_4 = f_3 - 3s_3 = 0$, $g_4 = g_2 + 3y_3 = y_1^3 - 3y_1y_2 + 3y_3$.

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

Důkaz Věty 2.2. Existence byla prokázána výše uvedeným algoritmem. Jednoznačnost dokážeme sporem: kdybychom měli dvě vyjádření $f = g_1(s_1, \ldots, s_n) = g_2(s_1, \ldots, s_n)$, $g_1 \neq g_2$, pak bychom mohli vyjádřit nulový polynom netriviálním způsobem jako $0 = h(s_1, \ldots, s_n)$, kde $h = g_1 - g_2 \neq 0$. Označme $h = \sum a_i h_i$, kde h_i jsou jednotlivé členy tvary $y_1^{l_1} \cdots y_n^{l_n}$. Tyto členy jsou různé, a tedy díky jednoznačnosti v Lemmatu 2.4 mají polynomy $h_i(s_1, \ldots, s_n)$ různé vedoucí koeficienty. Uvažujte ten lexikograficky největší z nich. Tím, že je striktně větší než všechny ostatní členy, se nikdy nemůže pokrátit, a tedy $h(s_1, \ldots, s_n)$ nikdy nemůže vyjít 0, spor. □

3. Počítání modulo polynom a konstrukce těles

3.1. **Faktorokruh modulo polynom.**

Připomeňme konstrukci oborů $\mathbb{Z}_m$. Začali jsme s oborem celých čísel, zvolili $m > 0$ a uvažovali všechny možné zbytky po dělení m, čísla $0, \ldots, m-1$, a na nich operace modulo m. Pokud bylo m prvočíslo, dostali jsme těleso. Podobný postup lze provést i pro 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 $n > 0$. *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,

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

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 práci s násobením je třeba si připomenout, že $f \equiv g \pmod m$ právě tehdy, když $f \bmod m = g \bmod m$, a že $f \bmod m \equiv f \pmod m$. Pak lze všechny identity přeložit do kongruencí, kde je platnost zřejmá. Například pro asocitivitu dokazujeme

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

čili dokazujeme

$$\underbrace{(f \cdot g \bmod m)}_{\equiv fg \pmod m} \cdot h \equiv f \cdot \underbrace{(g \cdot h \bmod m)}_{\equiv gh \pmod m} \pmod m,$$

a po substituci dostáme očividně platnou rovnost $(fg)h = f(gh)$.

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:

$$(a+b\alpha)\cdot(c+d\alpha) = ac + (ad+bc)\alpha + bd\alpha^2 \equiv (ac-bd) + (ad+bc)\alpha \pmod{\alpha^2+1}.$$

Všimněte si, že jsme dostali stejné vzorce, jako platí pro sčítání a násobení komplexních čísel, tj. při ztotožnění 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 $\mathbb{Q}(i)$. Pro konečná tělesa je situace zajímavější. Např. faktorokruh $\mathbb{Z}_2[\alpha]/(\alpha^2+1)$ má čtyři prvky, ale není to těleso, dokonce ani obor integrity, protože

$$(\alpha+1)\cdot(\alpha+1) = \alpha^2+1 \equiv 0 \pmod{\alpha^2+1}.$$

Naopak faktorokruh $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$ má 9 prvků a lze ukázat, že to je těleso. Tyto jevy vysvětluje následující tvrzení.

Tvrzení 3.1. *Buď* $\mathbf{T}$ *těleso a* $m \in T[\alpha]$ *stupně* > 0. *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). Kdyby v $\mathbf{T}[\alpha]$ platilo $m = f\cdot g$, kde $\deg(f), \deg(g) < \deg(m)$, pak by v $\mathbf{T}[\alpha]/(m)$ platilo $f\cdot g = m \equiv 0 \pmod{m}$.

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

Pomocí faktorokruhů lze konstruovat konečná tělesa.

Příklad. Buď p prvočíslo a uvažujme ireducibilní polynom $m \in \mathbb{Z}_p[\alpha]$ stupně k. Faktorokruh $\mathbb{Z}_p[\alpha]/(m)$ je podle Tvrzení 3.1 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 $\mathbb{Z}_2[\alpha]/(\alpha^3+\alpha+1)$, devítiprvkové jako $\mathbb{Z}_3[\alpha]/(\alpha^2+1)$. Pozor, p^k-prvkové těleso není ani $\mathbb{Z}_{p^k}$, ani $(\mathbb{Z}_p)^k$! V dalších kapitolách si ukážeme, že

(1) každé konečné těleso lze sestrojit tímto způsobem (speciálně, každé konečné těleso má velikost mocniny prvočísla),
(2) pro každé p, k existuje ireducibilní polynom stupně k nad $\mathbb{Z}_p$,
(3) na jeho volbě nezáleží, tj. různé volby m dají tělesa, která „vypadají stejně" (formálně, jsou *izomorfní*).

3.2. Kořenová a rozkladová nadtělesa.

Cílem této části je dokázat, že pro každé těleso $\mathbf{T}$ a každý polynom $f \in T[x]$ stupně > 0 existuje rozšíření $\mathbf{S}$, kde se f rozkládá na lineární činitele, tj. součin polynomů stupně 1. Pro $\mathbf{T} = \mathbb{Q}$ se věc zdá jasná, tímto tělesem je $\mathbb{C}$, ale tento fakt je předmětem Základní věty algebry, kterou zatím nemáme dokázanou. Naopak, existence rozkladového nadtělesa je stěžejním krokem k jejímu důkazu. A pro konečná tělesa žádná analogie použít nelze.

Definice. Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně > 0.

(1) *Kořenovým nadtělesem* polynomu f rozumíme rozšíření $\mathbf{S} \geq \mathbf{T}$ takové, že $f(a) = 0$ a $\mathbf{S} = \mathbf{T}(a)$.
(2) *Rozkladovým nadtělesem* polynomu f rozumíme rozšíření $\mathbf{S} \geq \mathbf{T}$ takové, že v $\mathbf{S}[x]$ platí $f \parallel (x - a_1) \cdot \ldots \cdot (x - a_n)$ a $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$.

Příklad. Příklady kořenových a rozkladových nadtěles; uvedena jsou všechna, která jsou obsažena v tělese $\mathbb{C}$:

f	kořenová nadtělesa f nad $\mathbb{Q}$	rozkladové nadtěleso f nad $\mathbb{Q}$
x^2+1	$\mathbb{Q}(i)$	$\mathbb{Q}(i)$
x^2-1	$\mathbb{Q}$	$\mathbb{Q}$
x^3-1	$\mathbb{Q},\ \mathbb{Q}(e^{2\pi i/3})$	$\mathbb{Q}(e^{2\pi i/3})$
x^3-2	$\mathbb{Q}(\sqrt[3]{2}),\ \mathbb{Q}(\sqrt[3]{2}\cdot e^{2\pi i/3})$	$\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}\cdot e^{2\pi i/3})$

Dokážeme, že pro každý polynom stupně > 0 existuje kořenové i rozkladové nadtěleso. Klíčovým krokem je konstrukce rozšíření, kde má daný polynom aspoň *nějaký* kořen. Dále pak stačí postupovat indukcí.

Tvrzení 3.2. *Buď* $\mathbf{T}$ *těleso a* $f \in T[x]$ *stupně* ≥ 1. *Pak existuje kořenové nadtěleso polynomu* f *nad* $\mathbf{T}$.

Důkaz. Buď m nějaký ireducibilní dělitel polynomu f. Stačí najít kořenové nadtěleso pro polynom m, v něm bude mít kořen i f. Uvažujme faktorokruh $\mathbf{S} = \mathbf{T}[\alpha]/(m(\alpha))$. Podle Tvrzení 3.1 je $\mathbf{S}$ těleso. Vyhodnotíme-li v $\mathbf{S}$ polynom m na prvku α, dostaneme $m(\alpha) \bmod m(\alpha) = 0$. Prvek α je tedy kořenem polynomu m v $\mathbf{S}$. Přitom nejmenší podtěleso $\mathbf{S}$ obsahující $T \cup \{\alpha\}$ je celé $\mathbf{S}$, čili $\mathbf{S} = \mathbf{T}(\alpha)$ je hledaným kořenovým nadtělesem. □

Stěžejním krokem důkazu bylo dosazení prvku α do polynomu m, což si možná zaslouží podrobnější komentář. Označme $m = \sum_{i=0}^{n} a_i x^i$ a dosaďme do polynomu m prvek α. Mocniny α^i, $i < n$, jsou přímo prvky faktorokruhu, ale mocninu α^n je potřeba vzít modulo $m(\alpha)$. Ale přitom $a_n\alpha^n \equiv -\sum_{i=0}^{n-1} a_i\alpha^i \pmod{m(\alpha)}$, a tedy

$$m(\alpha) = \sum_{i=0}^{n-1} a_i\alpha^i + (a_n\alpha^n \bmod m(\alpha)) = \sum_{i=0}^{n-1} a_i\alpha^i - \sum_{i=0}^{n-1} a_i\alpha^i = 0.$$

Věta 3.3. *Buď* $\mathbf{T}$ *těleso a* $f \in T[x]$ *stupně* ≥ 1. *Pak existuje rozkladové nadtěleso polynomu* f *nad* $\mathbf{T}$.

Důkaz. Budeme postupovat indukcí podle stupně polynomu f. Je-li f stupně 1, $f = ax - b$, pak $\mathbf{S} = \mathbf{T} = \mathbf{T}(a^{-1}b)$. V opačném případě uvažujme kořenové nadtěleso $\mathbf{T}(a) \geq \mathbf{T}$ polynomu f a polynom $g \in T(a)[x]$ takový že $f = g \cdot (x - a)$. Pak $\deg g < \deg f$, tedy podle indukčního předpokladu existuje jeho rozkladové nadtěleso $\mathbf{S} = \mathbf{T}(a)(b_1, \ldots, b_m) = \mathbf{T}(a, b_1, \ldots, b_m)$ nad $\mathbf{T}(a)$. Protože se polynom g rozkládá v $\mathbf{S}[x]$ na lineární činitele, rozkládá se tam i $f = g \cdot (x - a)$. □

4. Základní věta algebry

Cílem této sekce je dokázat, že každý komplexní polynom má komplexní kořen. Tomuto faktu se říká Základní věta algebry (název je poněkud zastaralý a odpovídá době vzniku, tedy přelomu 18. a 19. století, kdy se algebra zabývala především řešením polynomiálních rovnic, což už dávno není pravda). Snadným důsledkem je, že všechny kořeny jsou komplexní: máme-li jeden, u, vydělíme monočlenem $x - u$ a použijeme větu znovu.

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. Důkazů základní věty algebry existuje celá řada, ať už čistě analytické (pomocí komplexní analýzy), geometrické, či částečně algebraické. Ukážeme si Gaussův důkaz z roku 1816, který je poměrně jednoduchý a pěkně odděluje analytické a algebraické principy potřebné k důkazu. Z algebry jsou stěžejním nástrojem

- existence rozkladových nadtěles (Věta 3.3),
- teorie symetrických polynomů (klíčový krok důkazu je založen na úvaze podobné Důsledku 2.3).

Z reálné analýzy pak stěžejním způsobem využijeme

- větu o středním bodě,

která implikuje, 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 počtů s komplexně sdruženými čísly.

Lemma 4.1. *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 $a_i \bar{a}_j + a_j \bar{a}_i \in \mathbb{R}$. Čili podle předpokladu má polynom g komplexní kořen u. Čili $f(u) = 0$ nebo $\bar{f}(u) = 0$. 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 4.2. *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 se snadno dokáže ze spojitosti funkce $x \mapsto x^2$. □

Lemma 4.3. *Reálný polynom lichého stupně má reálný kořen.*

Důkaz. Reálný polynom f dává spojitou 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, kde $f(u) = 0$. □

Věta 4.4 (Základní věta algebry)**.** *Každý komplexní polynom stupně ≥ 1 má nějaký komplexní kořen.*

Důkaz. Díky Lemmatu 4.1 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 4.3. 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 2.2 existuje polynom $g \in \mathbb{R}[y_1, \ldots, y_n]$ 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 $u_i + u_j + z u_i u_j \in \mathbb{C}$. 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.

$$u_i + u_j + z_1 u_i u_j \in \mathbb{C} \quad \text{a} \quad u_i + u_j + z_2 u_i u_j \in \mathbb{C}.$$

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

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

a podle Lemmatu 4.2 víme, že komplexní kvadratický polynom má nutně komplexní kořeny. □