

GAUSSOVA VĚTA

Polynom nazýváme *primitivní*, pokud není dělitelný žádným neinvertibilním konstantním polynomm. Ekvivalentně (pro gaussovské obory), je-li NSD jeho koeficientů 1. Uvažujme nějaký obor integrity \mathbf{R} a jeho podílové těleso \mathbf{Q} . Dělitelnost v oborech $\mathbf{R}[x]$ a $\mathbf{Q}[x]$ se pro primitivní polynomy chová velmi podobně.

Tvrzení 1. *Bud' \mathbf{R} gaussovský obor, \mathbf{Q} jeho podílové těleso a f, g primitivní polynomy z $\mathbf{R}[x]$. Pak*

- (1) $f \mid g$ v $\mathbf{R}[x]$ právě tehdy, když $f \mid g$ v $\mathbf{Q}[x]$;
- (2) f je ireducibilní v $\mathbf{R}[x]$ právě tehdy, když f je ireducibilní v $\mathbf{Q}[x]$;
- (3) $\text{NSD}_{\mathbf{R}[x]}(f, g)$ existuje a je roven primitivnímu polynomu $h \in R[x]$ splňujícímu $h = \text{NSD}_{\mathbf{Q}[x]}(f, g)$.

Takový polynom h v části (3) jistě existuje: stačí vzít libovolný $\text{NSD}(f, g)$ 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 čísel koeficientů.

Je zřejmé, že pokud $f \mid g$ a g je primitivní, pak je i f primitivní. Klíčovým krokem k důkazu uvedeného tvrzení je fakt, že platí také opačné tvrzení: součin fg je primitivní právě tehdy, když jsou oba polynomy f, g primitivní.

Lemma 2 (Gaussovo lemma). *Bud' \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 $u \in R$, který dělí součin fg , tj. všechny koeficienty tohoto součinu. Zvolme nejmenší j takové, že $u \nmid a_j$, a nejmenší k takové, že $u \nmid b_k$ (protože jsou polynomy f, g primitivní, u nemůže dělit všechny jejich koeficienty). Podívejme se na $(j+k)$ -tý koeficient polynomu fg :

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

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

$$u \mid a_0 b_{j+k} + \dots + a_{j-1} b_{k+1}.$$

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

$$u \mid a_{j+1} b_{k-1} + \dots + a_{j+k} b_0.$$

Tedy u dělí všechny členy kromě $a_j b_k$. Ten naopak u dělitelný není, protože u je ireducibilní a nedělí ani a_j , ani b_k . Dostáváme, že $u \nmid c_{j+k}$, spor. \square

Důkaz Tvrzení 1. (1) Pokud $f \mid g$ v $\mathbf{R}[x]$, tj. že existuje $h \in R[x] \subseteq Q[x]$ splňující $g = fh$, pak tato rovnost platí i v $Q[x]$. Opačná implikace je těžší. Předpokládejme, že $f \mid g$ v $Q[x]$, tj. že existuje $h \in Q[x]$ splňující $g = fh$. Zvolme $q \in Q$ tak, aby qh byl 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 $\mathbf{R}[x]$. Označme $q = \frac{a}{b} \in Q$. Platí $ag = b(qg)$, přitom oba polynomy g, qg jsou primitivní, takže z $a \mid b(qg)$ plyne $a \mid b$, a z $b \mid aq$ plyne $b \mid a$. Tedy $a \parallel b$ a $1 \parallel q \in R$ a dostáváme $h \in R[x]$.

(2) Dokážeme následující ekvivalentní tvrzení: f má vlastního dělitele v $\mathbf{R}[x]$ právě tehdy, když má vlastního dělitele v $Q[x]$. (\Rightarrow) Protože je f primitivní, jakýkoliv vlastní dělitel je primitivní a má stupeň aspoň 1. Tedy jde zároveň o vlastního

dělitele v $\mathbf{Q}[x]$. (\Leftarrow) Necht g je vlastní dělitel f v $\mathbf{Q}[x]$. Pak existuje $q \in \mathbf{Q}$ takové, že qg je primitivní polynom z $\mathbf{R}[x]$. Přitom $qg \mid f$ v $\mathbf{Q}[x]$, tedy podle (1) je qg vlastní dělitel f v $\mathbf{R}[x]$.

(3) Polynom h dělí f, g v $\mathbf{Q}[x]$ a je primitivní, tedy podle (1) 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, podle (1) $d \mid f, g$ v $\mathbf{Q}[x]$, tedy $d \mid h$ v $\mathbf{Q}[x]$, a opět podle (1) $d \mid h$ i v $\mathbf{R}[x]$. \square

Z Tvrzení 1 lze snadno odvodit podobná tvrzení pro obecné polynomy, ne nutně primitivní. Buď $f = \sum_{i=0}^n a_i x^i$ polynom z $\mathbf{R}[x]$. Definujeme

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

Polynom $\text{pp}(f)$ je očividně primitivní a nazývá se *primitivní částí* polynomu f .

Věta 3. *Buď \mathbf{R} gaussovský obor, \mathbf{Q} jeho podílové těleso a f, g polynomy z $\mathbf{R}[x]$. Pak*

- (1) *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 $\mathbf{Q}[x]$.
- (2) *Pak $\text{NSD}_{\mathbf{R}[x]}(f, g)$ existuje a je roven součinu $c \cdot h$, kde $c = \text{NSD}_{\mathbf{R}}(c(f), c(g))$ a h je primitivní polynom z $\mathbf{R}[x]$ splňující $h = \text{NSD}_{\mathbf{Q}[x]}(\text{pp}(f), \text{pp}(g))$.*

Důkaz. (1) Pokud není f primitivní, pak se rozkládá na součin neinvertibilního konstantního polynomu a primitivního polynomu. Jinak je buď konstantní (první položka), nebo primitivní (druhá položka).

(2) Označme pravou stranu r . Protože $\text{NSD}_{\mathbf{R}}(c(f), c(g))$ dělí $c(f)$ i $c(g)$, a zároveň $\text{NSD}_{\mathbf{R}[x]}(\text{pp}(f), \text{pp}(g))$ dělí $\text{pp}(f)$ i $\text{pp}(g)$, tak jejich součin r dělí oba polynomy f, g , čili r je společný dělitel. Dokážeme, že je to největší společný dělitel: pokud nějaký h dělí f i g , pak $c(h)$ dělí $c(f)$ i $c(g)$, tedy $c(h) \mid \text{NSD}_{\mathbf{R}}(c(f), c(g))$; analogicky $\text{pp}(h) \mid \text{NSD}_{\mathbf{R}[x]}(\text{pp}(f), \text{pp}(g))$ a dostáváme $h \mid r$. \square

Příklady.

- Polynom $2x - 2$ je ireducibilní v $\mathbf{Q}[x]$, ale není ireducibilní v $\mathbf{Z}[x]$, protože není primitivní: rozkládá se jako $2 \cdot (x - 1)$.
- Polynom 2 není ireducibilní v $\mathbf{Q}[x]$, protože je invertibilní, ale je ireducibilní v $\mathbf{Z}[x]$.

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

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

Pak $c = \text{NSD}_{\mathbf{Z}}(4, -6) = 2$, $h = \text{NSD}_{\mathbf{Q}[x]}(x^2 + 2x + 1, x^2 - 1) = x + 1$, a tedy $\text{NSD}_{\mathbf{Z}[x]}(4x^2 + 8x + 4, -6x^2 + 6) = 2(x + 1)$.

Věta 3 nejen zaručuje existenci NSD v $\mathbf{R}[x]$, ale také dává návod, jak je spočítat. Např. výpočet NSD v $\mathbf{Z}[x]$ se redukuje na dva výpočty NSD, jeden v \mathbf{Z} a druhý v $\mathbf{Q}[x]$. Oba lze provést pomocí Eukleidova algoritmu.

Věta 4 (Gaussova). *Je-li \mathbf{R} gaussovský obor, pak je $\mathbf{R}[x]$ také gaussovský obor.*

Důkaz. Použijeme větu charakterizující gaussovské obory pomocí existence NSD. NSD v $\mathbf{R}[x]$ existují podle Věty 3. A je-li f_1, f_2, f_3, \dots 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 a_i vedoucí koeficient polynomu f_i , pak a_n, a_{n+1}, \dots je posloupnost vlastních dělitelů v \mathbf{R} , spor. \square

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