1. Algebraické vlastnosti polynomiálních oborů

1.1. Gaussova věta.

Polynom nazýváme *primitivní*, pokud není dělitelný žádným neinvertibilním konstantním polynomem. 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 1.1. *Buď $\mathbf{R}$ 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) $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ *existuje a je roven primitivnímu polynomu $h \in R[x]$ splňujícímu $h = \mathrm{NSD}_{\mathbf{Q}[x]}(f, g)$.*

Takový polynom h v části (3) 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.

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 1.2 (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 $u \in R$, 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:

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

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

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

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

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

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. □

Důkaz Tvrzení 1.1. (1) Pokud že $f \mid g$ v $\mathbf{R}[x]$, tj. že existuje $h \in R[x] \subseteq Q[x]$ splňující $g = fh$, pak tato rovnost platí i v $\mathbb{Q}[x]$. Opačná implikace je těžší. Předpokládejme, že $f \mid g$ v $\mathbf{Q}[x]$, 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 $b \mid a$ (využíváme Tvrzení **??**). 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 $\mathbf{Q}[x]$. ($\Rightarrow$) Protože je f primitivní, jakýkoliv vlastní dělitel je primitivní a má stupeň aspoň 1. Tedy jde zároveň o vlastního dělitele v $\mathbf{Q}[x]$.

($\Leftarrow$) Nechť g je vlastní dělitel f v $\mathbf{Q}[x]$. Pak existuje $q \in Q$ 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 $\mathbf{R}[x]$. □

Z Tvrzení 1.1 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

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

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

Věta 1.3. *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* $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ *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* $h = \mathrm{NSD}_{\mathbf{Q}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$.

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 $\mathrm{NSD}_{\mathbf{R}}(\mathrm{c}(f), \mathrm{c}(g))$ dělí $\mathrm{c}(f)$ i $\mathrm{c}(g)$, a zároveň $\mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$ dělí $\mathrm{pp}(f)$ i $\mathrm{pp}(g)$, 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 $\mathrm{c}(h)$ dělí $\mathrm{c}(f)$ i $\mathrm{c}(g)$, tedy $\mathrm{c}(h) \mid \mathrm{NSD}_{\mathbf{R}}(\mathrm{c}(f), \mathrm{c}(g))$; analogicky $\mathrm{pp}(h) \mid \mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$ a dostáváme $h \mid r$. □

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

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 $\mathrm{NSD}_{\mathbb{Z}[x]}(4x^2 + 8x + 4, -6x^2 + 6) = 2(x + 1)$.

Věta 1.3 nejen zaručuje existenci NSD v $\mathbf{R}[x]$, ale také dává návod, jak je spočítat. Např. vypočet NSD v $\mathbb{Z}[x]$ se redukuje na dva výpočty NSD, jeden v $\mathbb{Z}$ a druhý v $\mathbb{Q}[x]$. Oba lze provést pomocí Eukleidova algoritmu.

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

Důkaz. Použijeme charakterizaci z Věty **??**. NSD v $\mathbf{R}[x]$ existují podle Věty 1.3. A je-li $f_1, f_2, f_3, \ldots$ posloupnost vlastních dělitelů, 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 a_i vedoucí koeficient polynomu f_i, pak $a_n, a_{n+1}, \ldots$ je 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. **Hilbertova věta o bázi.**

Definice. Komutativní okruh $\mathbf{R}$ se nazývá *noetherovský*, pokud má každý ideál v $\mathbf{R}$ konečnou bázi.

Příklad.

- Obory integrity hlavních ideálů jsou noetherovské, každý ideál má jednoprvkovou bázi. OIHI jsou např. tělesa, obor $\mathbb{Z}$ a obory $\mathbf{T}[x]$, $\mathbf{T}$ těleso.
- Obory $\mathbb{Z}[x_1, \ldots, x_k]$ a $\mathbf{T}[x_1, \ldots, x_k]$, $\mathbf{T}$ těleso, nejsou OIHI, ale jsou noetherovské (viz Hilbertova věta o bázi 1.6).
- Obory $\mathbf{R}[X]$, kde X je nekonečná množina, noetherovské nejsou: např. ideál I sestávající z polynomů s absolutním členem 0 nemá konečnou bázi.

Lemma 1.5. *Buď $\mathbf{R}$ je komutativní okruh. Pak $\mathbf{R}$ je noetherovský právě tehdy, když v $\mathbf{R}$ neexistuje nekonečná rostoucí posloupnost ideálů $I_1 \subset I_2 \subset I_3 \subset \ldots$*

Důkaz. ($\Rightarrow$) Uvažujme takovou posloupnost $I_1 \subset I_2 \subset I_3 \subset \ldots$ a položme $I = \bigcup_{j=1}^{\infty} I_j$. Pak I je také ideál a předpokládejme, že $a_1, \ldots, a_n$ je jeho konečná báze (taková existuje, neboť $\mathbf{R}$ je noetherovský). Pak $a_1, \ldots, a_n \in I = \bigcup_{j=1}^{\infty} I_j$, takže pro každé i existuje nějaké j_i splňující $a_i \in I_{j_i}$. Označme $k = \max_{i=1,\ldots,n} j_i$. Pak $a_1, \ldots, a_n \in I_k$, a tedy $\langle a_1, \ldots, a_n \rangle = I_k = I_{k+1} = \ldots = I$, spor.

($\Leftarrow$) Předpokládejme, že nějaký ideál I nemá konečnou bázi. Definujme následující posloupnost ideálů: položme $I_1 = \langle a_1 \rangle$, kde $a_1 \in I$ je zvoleno libovolně. Dále, indukcí, zvolme a_{i+1} tak, aby $a_{i+1} \in I \setminus I_i$ a položme $I_{i+1} = \langle a_1, \ldots, a_{i+1} \rangle$ – takové a_{i+1} existuje, protože $I \neq \langle a_1, \ldots, a_i \rangle$. Získali jsme nekonečnou posloupnost ideálů $I_1 \subset I_2 \subset I_3 \subset \ldots$, spor. □

Věta 1.6 (Hilbertova věta o bázi)**.** *Buď $\mathbf{R}$ komutativní noetherovský okruh. Pak $\mathbf{R}[x]$ je také noetherovský.*

Důkaz. Pro spor předpokládejme, že ideál I v okruhu $\mathbf{R}[x]$ nemá konečnou bázi. Zvolme f_1 některý z polynomů nejmenšího stupně v I. Dále, indukcí, zvolme f_{i+1} některý z polynomů v $I \setminus \langle f_1, \ldots, f_i \rangle$ nejmenšího možného stupně. Zřejmě bude $\deg f_1 \leq \deg f_2 \leq \deg f_3 \leq \ldots$ Pro každé i definujme a_i jako vedoucí koeficient polynomu f_i, a položme

$$J_i = \langle a_1, \ldots, a_i \rangle.$$

Dostali jsme tedy posloupnost $J_1 \subseteq J_2 \subseteq J_3 \subseteq \ldots$ ideálů v $\mathbf{R}$. Protože je okruh $\mathbf{R}$ noetherovský, nemůže tato posloupnost obsahovat ostře rostoucí podposloupnost, a tedy existuje k splňující $J_k = J_{k+1} = J_{k+2} = \ldots$ Čili $a_{k+1} \in J_k$ a můžeme psát

$$a_{k+1} = \sum_{i=1}^{k} r_i a_i$$

pro nějaká $r_i \in R$. Definujme polynom $\tilde{f}_i = x^s f_i$ pro takové s, aby platilo $\deg \tilde{f}_i = \deg f_{k+1}$, a uvažujme polynom

$$f = \sum_{i=1}^{k} r_i \tilde{f}_i.$$

Ten má stejný vedoucí člen jako f_{k+1}, takže polynom $f_{k+1} - f$ má menší stupeň než f_{k+1}. Přitom $f \in \langle f_1 \ldots, f_k \rangle$, takže polynom $f_{k+1} - f \in I \setminus \langle f_1, \ldots, f_k \rangle$. To je ve sporu s volbou f_{k+1} jako polynomu s touto vlastností nejmenšího stupně. □

Vícenásobnou aplikací Hilbertovy věty o bázi dostáváme, že okruhy polynomů konečně mnoha proměnných nad noetherovským okruhem jsou noetherovské.