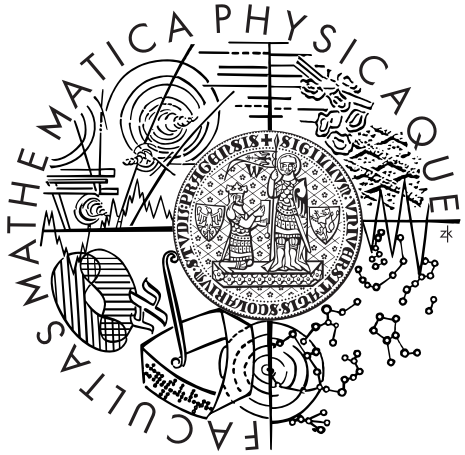
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Adam Stejskal

Jak poznat prvoideál?

Katedra algebry

Vedoucí bakalářské práce: RNDr. Jan Šťovíček, Ph.D.
Studijní program: Matematika
Studijní obor: Obecná matematika

Praha 2014

Rád bych na tomto místě poděkoval zejména vedoucímu mé bakalářské práce za cenné rady, které mi poskytl.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Jak poznat prvoideál?

Autor: Adam Stejskal Katedra: Katedra algebry

Vedoucí bakalářské práce: RNDr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: Formulujeme algoritmus rozpoznávající prvoideály v okruhu polynomů s koeficienty z určitých okruhů. Jako hlavní nástroj k počítání s ideály používáme metodu Gröbnerových bází. Předvedeme analogii Buchbergerova algoritmu pro výpočet Gröbnerovy báze pro ideály polynomů s koeficienty nad okruhem, který není nutně těleso. Také ukážeme vztah mezi prvoideály v okruhu polynomů nad okruhem R a prvoideály v okruhu polynomů nad kvocientem R a jeho prvoideálu. V práci je kladen důraz převážně na otázky teoretické správnosti, ale výpočetní aspekt také není zcela zanedbán.

Klíčová slova: Gröbnerovy báze, prvoideál, polynomiální okruh, Gröbnerovy báze nad okruhem

Title: Determining primeness of an ideal

Author: Adam Stejskal

Department: Department of Algebra

Supervisor: RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: We present an algorithm for determining whether an ideal in a polynomial ring is prime or not. We use the Gröbner bases as a main tool for operations with ideals. We show an analogue of Buchberger's algorithm for computing a Gröbner basis for an ideal in polynomials over a ring, which not need to be a field. We also show a relation between prime ideals in polynomials over a ring R and prime ideals in polynomials over a quotient ring of R modulo a prime ideal. We are primarilly discussing the issues of theoretical corectness, but we also present the conditions of actual computability.

Keywords: Gröbner basis, prime ideal, polynomial ring, Gröbner basis over ring

Obsah

0 Úvod

Práce má za cíl popsat algoritmus, který rozpoznává prvoideály nad polynomiálním okruhem. Algoritmus byl popsán v roce 1988 v [GZT] jako aplikace metody Gröbnerových bází. V [GZT] je ovšem kladen důraz pouze na teoretickou správnost. Naopak [IGB] je mnohem podrobnější a předkládá konkrétní postupy při většině výpočtů. V práci se snažíme zkombinovat oba přístupy. Většina důkazů je převzatá z [IGB], naopak zavedení aparátu Gröbnerových bází z [GZT].

Jako hlavní nástroj pro práci s ideály jsou použity Gröbnerovy báze. Je ovšem otázkou, jak spočítat Gröbnerovu bázi ideálu polynomiálního okruhu. Nelze totiž použít známý Buchbergerův algoritmus, protože předpokládá, že koeficienty polynomů leží v tělese. Je třeba tedy najít nějakou analogii pro polynomy nad okruhy. V první kapitole jsou uvedeny základní definice aparátu Gröbnerových bazí. Dále v ní specifikujeme, za jakých podmínek je možné Gröbnerovy báze spočítat, a odkazujeme na algoritmus, který Gröbnerovu bázi ideálu polynomiálního okruhu spočítá. Dále jsou v první kapitole předvedeny metody, jak pomocí Gröbnerových bází spočítat generátory ideálů speciálního tvaru, tzv. saturací.

Ve druhé kapitole uvedeme charakterizaci prvoideálů v okruhu polynomů nad R pomocí prvoideálů v polynomech nad R/P, kde $P \subseteq R$ je prvoideál. V kombinaci s výsledky první kapitoly dostaneme hledaný algoritmus, který je na konci ilustrován formou vyřešeného cvičení z [IGB].

V práci budeme používat značení obvyklé na MFF UK, s výjimkou množiny $\mathbb{N}$. Tento symbol bude v práci označovat přirozená čísla s nejmenším prvkem 0. Dále budeme bez důkazu uvádět tvrzení dokázaná na předmětech bakalářského studia.

1 Gröbnerovy báze

1.1 Základní definice

V této sekci zavedeme vše potřebné, abychom mohli definovat Gröbnerovu bázi ideálu nad polynomiálním okruhem. Dále uvedeme dvě ekvivalentní definice Gröbnerovy báze ideálu.
Nejprve je třeba specifikovat okruh, nad nímž se bude vše odehrávat.

Definice 1. *Řekneme, že v okruhu R jsou lineární rovnice řešitelné, pokud platí obě z následujících podmínek:*

(a) Pro dané $a_1,\dots,a_k, a \in R$ lze rozhodnout, zda a je prvkem ideálu $\langle a_1,\dots,a_k\rangle R$. Pokud $a \in \langle a_1,\dots,a_k\rangle R$, můžeme navíc spočítat $b_1,\dots,b_k \in R$ takové, že $a = \sum_{i=1}^{k} a_i b_i$.

(b) Pro dané $a_1,\dots,a_m \in R$ lze spočítat konečnou množinu generátorů R-modulu $\{(b_1,\dots,b_m) \in R^m : \sum_{i=1}^{m} a_i b_i = 0\}$.

V následujícím textu budeme okruhem R myslet komutativní okruh s jed notkou, který je noetherovský a v němž jsou lineární rovnice řešitelné. Dále písmenem A budeme označovat okruh $R[x_1,\dots,x_n]$.

Poznámka. Podle Hilbertovy věty o bázi [IGB,Theorem 1.1.3] je A také noetherovský okruh.

Termem (v n proměnných) rozumíme polynom $1.x_1^{k_1}x_2^{k_2}.\cdots.x_n^{k_n}$, zkráceně budeme psát $x^{\mathbf{B}}$, kde $\mathbf{B} = (k_1,\dots,k_n) \in \mathbb{N}^{\mathbf{n}}$. Množinu všech termů v n proměnných označíme $\mathbb{T}^n$.

Definice 2. *Uspořádání $\geq$ na $\mathbb{T}^n$ nazveme vyhovující, pokud platí:*

(a) $x^{\mathbf{B}} \geq 1$ pro všechna $\mathbf{B} \in \mathbb{N}^{\mathbf{n}}$

(b) Pokud $x^{\mathbf{C}} \geq x^{\mathbf{D}}$, potom je $x^{\mathbf{C}+\mathbf{B}} \geq x^{\mathbf{D}+\mathbf{B}}$ pro všechna $\mathbf{B},\mathbf{C},\mathbf{D} \in \mathbb{N}^{\mathbf{n}}$.

Podle [IGB, Theorem 1.4.6] je každé vyhovující uspořádání na $\mathbb{T}^n$ dobré uspořádání (míněno, že uspořádání je úplné a existují nejmenší prvky neprázdných podmnožin).

Příklad. Příkladem vyhovujícího uspořádání je lexikografické uspořádání $\geq$ definované následovně: Pro termy $x^{\mathbf{C}}, x^{\mathbf{B}} \in \mathbb{T}^n$, kde $\mathbf{C} = (c_1,\dots,c_n) \in \mathbb{N}^{\mathbf{n}}$ a $\mathbf{B} = (b_1,\dots,b_n) \in \mathbb{N}^{\mathbf{n}}$ položíme $x^{\mathbf{C}} \geq x^{\mathbf{B}}$ právě tehdy, když existuje $i < n$ takové, že $c_1 = b_1, \dots c_i = b_i$ a současně $c_{i+1} > b_{i+1}$.

Další příklady vyhovujících uspořádání lze nalézt třeba v [IGB, sekce 1.4]. V této práci nebude obvykle záležet na konkrétním uspořádání termů, proto budeme implicitně předpokládat uspořádání lexikografické. Bude-li třeba, na změnu uspořádání termů upozorníme.

Definice 3. *Pro libovolné $f \in A$ napišme $f = cx^{\mathbf{B}} + g$, kde $c \neq 0$ a pro všechny nenulové monočleny $c'x^{\mathbf{D}}$ polynomu g platí $\mathbf{B} \geq \mathbf{D}$ a současně neplatí $\mathbf{D} \geq \mathbf{B}$. Potom*

- *$lm(f) = cx^{\mathbf{B}}$ budeme nazývat vedoucí monočlen f*
- *$lt(f) = x^{\mathbf{B}}$ budeme nazývat vedoucí term f*
- *$lc(f) = c$ budeme nazývat vedoucí koeficient f*

Dále pro $S \subseteq A$ definujeme $Lm(S)$ jako ideál generovaný množinou $\{lm(f) : f \in S\}$.

Definice 4. *Buď $f \in A$, $G \subseteq A$. Řekneme, že f je redukovatelný modulo G, pokud f je nenulový a $lm(f) \in Lm(G)$. Řekneme, že f je redukovaný modulo G, pokud není redukovatelný modulo G.*

Tvrzení 1. *Pro daný polynom $f \in A$ a množinu $G \subseteq A$ lze spočítat polynom g takový, že $f - g \in \langle G \rangle$ a g je redukovaný modulo G. Říkáme, že polynom f se redukuje modulo G na g, a píšeme $f \xrightarrow{G} g$.*

Důkaz. Viz [IGB, Theorem 4.1.10] pro důkaz existence g, viz [IGB, Algorithm 4.1.1] (dělení se zbytkem polynomů více proměnných) pro důkaz spočítatelnosti g.

❑

Nyní již můžeme definovat ústřední pojem této kapitoly.

Definice 5. *Buď $I \subseteq A$ ideál a $G \subseteq I$. Řekneme, že G je Gröbnerova báze pro I, pokud $Lm(G) = Lm(I)$.*

Následující věta charakterizuje Gröbnerovy báze.

Věta 2. *Nechť I je ideál A a $G = \{g_1, \ldots, g_m\}$ je množina nenulových polynomů z I. Pak jsou následující podmínky ekvivalentní:*

i) G je Gröbnerova báze pro I.

ii) Pro každý polynom $f \in A$ platí: $f \in I$ právě tehdy, když $f \xrightarrow{G} 0$.

iii) Pro každý polynom $f \in I$ platí: $f = h_1 g_1 + \cdots + h_m g_m$, kde $h_1, \ldots, h_m \in A$ takové, že $lt(f) = \max_{1 \leq j \leq m} (lt(h_i) lt(g_i))$.

Důkaz. Viz [IGB, Theorem 4.1.12].

❑

Důsledek 1. *Máme-li Gröbnerovu bázi G pro ideál I, potom*

1) lze rozhodnout, zda $f \in I$ pro libovolný $f \in A$,

2) $I = \langle G \rangle$.

1.2 Počítání Göbnerových bází

Nyní se důkladněji zaměříme na to, jak spočítat Gröbnerovu bázi pro daný ideál. Budeme vycházet ze sekcí 3.2 a 4.2 z [IGB], uvedeme bez důkazu další charakterizaci Gröbnerovy báze pro ideál polynomiálního okruhu. Dále formulujeme analogii Buchbergerova algoritmu, který funguje nad okruhy. Nakonec odkážeme na tvrzení, které zavadí další užitečnou vlastnost Gröbnerovy báze.
Budeme používat jisté podmoduly modulu $(R[x_1,\dots,x_n])^s$.Nejprve zavedeme značení a terminologii. Ať $X_1,\dots,X_s$ jsou termy v n proměnných, $c_1,\dots,c_s \in R$. Dále buď L ideál v $R[x_1,\dots,x_n]$ generovaný množinou $\{c_1X_1,\dots,c_sX_s\}$. Označíme $Syz(L) = \{(h_1,\dots,h_s) \in (R[x_1,\dots,x_n])^s : \sum_{i=1}^s h_ic_iX_i = 0\}$. $Syz(L)$ je podmodul $(R[x_1,\dots,x_n])^s$, neboť se jedná o jádro homomorfismu

$$\varphi : (R[x_1,\dots,x_n])^s \longrightarrow L$$

definovaného přiřazením

$$(h_1,\dots,h_s) \mapsto \sum_{i=1}^{s} h_ic_iX_i.$$

Dále nechť X je nějaký term v n proměnných. Řekneme, že $h = (h_1,\dots,h_s) \in Syz(L)$ je homogenní stupně X, pokud jsou h_i monočleny (tj. $h_i = lc(h_i)lt(h_i)$) takové, že $X_ilt(h_i) = X$ pro všechna i.
Z Hilbertovy věty o bázi víme, že $R[x_1,\dots,x_n]$ je noetherovský okruh. Dá se ukázat [IGB, Theorem 3.1.1], že $(R[x_1,\dots,x_n])^s$ je noetherovský modul, tedy každý jeho podmodul je konečně generovaný. Pro podmodul $Syz(L)$ dokonce platí, že má konečnou množinu homogenních generátorů [IGB, Lemma 4.2.2]. Pro výpočet Gröbnerovy báze je zásadní následující věta [IGB, Theorem 4.2.3].

Věta 3. *Nechť $G = \{g_1,\dots,g_t\}$ je množina nenulových polynomů z $R[x_1,\dots,x_n]$. $\mathcal{B}$ buď konečná množina homogenních generátorů modulu $Syz(lm(g_1),\dots,lm(g_t))$. Pak G je Gröbnerova báze pro ideál $\langle G\rangle$ právě tehdy, když pro každé $(h_1,\dots,h_t)\in\mathcal{B}$ platí*

$$h_1g_1 + \cdots + h_tg_t \xrightarrow{G} 0.$$

Jak ale spočítat množinu homogenních generátorů? Neformálně řečeno lze tuto úlohu převést na výpočet generátorů $Syz(M)$ jako R-modulu pro nějakou konečnou množinu M (viz [IGB Theorem 4.2.6]). To umíme, neboť předpokládáme, že v R jsou řešitelné lineární rovnice (Definice 1, podmínka b).

Nyní již lze formulovat algoritmus, který spočítá Gröbnerovu bázi ideálu I $\subseteq R[x_1,\dots,x_n]$, kde R je noetherovský okruh, v němž jsou lineární rovnice řešitelné.

ALGORITMUS (výpočet Gröbnerovy báze)

VSTUP: $F = \{f_1, \ldots, f_t\} \subseteq R[x_1, \ldots, x_n]$, kde $f_i \neq 0$ pro $i \in \{1,...t\}$

VÝSTUP: $G = \{g_1, \ldots, g_m\}$ Gröbnerova báze pro $\langle f_1, \ldots, f_t \rangle$

0.krok $G := \emptyset, G' := F$;

1.krok WHILE $(G \neq G')$ DO

$G := G'$;

označíme prvky G jako $g_1, \ldots, g_k$;

Spočti $\mathcal{B}$ množinu homogenních generátorů $Syz(lm(g_1),...,lm(g_k))$;

FOR $(h = (h_1, \ldots, h_k) \in \mathcal{B})$ DO

spočti $g_1h_1 + \cdots + g_kh_k \xrightarrow{G'} r$;

IF $(r \neq 0)$ THEN $G' := G' \cup \{r\}$;

Správnost algoritmu plyne zejména z Věty 3, pro detailnější důkaz viz [IGB,Theorem 4.2.8.]
Na závěr uvedeme, jak se chová Gröbnerova báze, pokud některé proměnné upřednostníme před ostatními. To nám poskytne způsob, jak induktivně zmenšovat ideál okruhu A vzhledem k počtu proměnných.

Věta 4. *Nechť I je ideál v okruhu $A[y_1, \ldots, y_m] = R[x_1, \ldots, x_n, y_1, \ldots, y_m]$. Dále nechť máme vyhovující uspořádání $\geq_1$ a $\geq_2$ na množinách termů v n x-ových proměnných, respektive v m y-ových. Definujme nové uspořádání $\geq$ na $\mathbb{T}^{n+m}$ následovně: $x^{\boldsymbol{B}}y^{\boldsymbol{D}} \geq x^{\boldsymbol{B'}}y^{\boldsymbol{D'}}$ právě tehdy, když $y^{\boldsymbol{D}} \geq_2 y^{\boldsymbol{D'}}$, nebo $y^{\boldsymbol{D}} = y^{\boldsymbol{D'}}$ a $x^{\boldsymbol{B}} \geq_1 x^{\boldsymbol{B'}}$. Pokud G je Gröbnerova báze ideálu I vzhledem k $\geq$, pak platí:*

1) *G je Gröbnerova báze pro I vzhledem k $\geq_2$ v okruhu polynomů m proměnných s koeficienty v A.*

2) *$G \cap A$ je Gröbnerova báze ideálu $I \cap A$ vzhledem k $\geq_1$.*

Důkaz. Viz [GZT, Prop.3.1]

❑

Další tvrzení bude často používáno jako fakt v následující sekci.

Tvrzení 5. *Pro ideály I a J okruhu A dané konečnou množinou generátorů lze spočítat množinu generátorů $I \cap J$.*

Důkaz. Viz [GZT, Corrolary 3.2]

❑

1.3 Gröbnerovy baze a operace s ideály

V této části práce uvedeme, jak lze aplikovat Gröbnerovy báze na manipulaci s ideály polynomiálního okruhu. Konkrétně použijeme Gröbnerovy báze pro ideál $I \subseteq A$ na výpočet generátorů tzv. *saturace* ideálu $S^{-1}I \cap A$, kde S je multiplikativní množina. Ukáže se, že pokud budeme vhodně volit multiplikativní množinu S, budeme schopni redukovat problém rozpoznání prvoideálu v A na rozpoznávání prvoideálů v polynomech s méně proměnnými. Tvrzení z této sekce jsou vybraná z [IGB,sekce 4.4]
Protože v následujících tvrzeních budeme pracovat s podílovými tělesy, je třeba v nich předpokládat, že R je navíc obor integrity. Nakonec se ale ukáže, že původní okruh být obor integrity nemusí. Písmenem A budeme i nadále značit okruh $A = R[x_1, \ldots, x_n]$. Platí tedy, že pokud R je obor integrity pak A je rovněž obor integrity (a tedy lze také zkonstruovat jeho podílové těleso).

Definice 6. *Buď $S \subset R$, kde R je libovolný okruh. Řekneme, že S je multiplikativní, pokud $1 \in S$, $0 \notin S$, a pokud r,$s \in S$, pak $rs \in S$.*
Je-li $S \subset A$ multiplikativní množina, A obor integrity, K podílové těleso oboru A, pak definujeme okruh zlomků A vzhledem k S jako $S^{-1}A = \{\frac{r}{s} \in K : r \in A, s \in S\}$.

Pokud použijeme značení z předcházející definice, je vidět, že $S^{-1}A$ je podokruh tělesa K. Dále je navíc A podokruh $S^{-1}A$, protože 1 je v každé multiplikativní množině. Nyní definujeme jeden z nejdůležitějších pojmů této sekce.

Definice 7. *Nechť $I \subseteq A$ je ideál a $S \subset A$ je multiplikativní množina. Potom saturaci ideálu I v A vzhledem k S definujeme jako:*

$$S^{-1}I \cap A,$$

kde $S^{-1}I = \{\frac{r}{s} \in K : r \in I, s \in S\}$.

Je zřejmé, že $S^{-1}I$ je ideálem v $S^{-1}A$. Nyní nás bude zajímat, jak spočítat generátory saturací nějakého ideálu vzhledem ke speciálním multiplikativním množinám S. Pokud za S vezmeme $S = \{g^n : n \in \mathbb{N}\}$ pro nějaké $g \in A$, následující tvrzení dává návod, jak spočítat generátory saturace.

Tvrzení 6. *Nechť R je obor integrity, $g \in A$ je nenulový polynom, $I \subseteq A$ je ideál. Buď $S = \{g^n : n \in \mathbb{N}\}$ multiplikativní množina. Dále uvažme novou proměnnou w, okruh $A[w]$, v něm ideál $\langle I, wg - 1\rangle$. Potom platí*

$$S^{-1}I \cap A = \langle I, wg - 1\rangle \cap A.$$

Důkaz. Nejprve vezměme $f \in S^{-1}I \cap A$. Jistě existuje $n \in \mathbb{N}$ takové, že $g^n f \in I$, a potom i $w^n g^n f \in IA[w] \subseteq \langle I, wg - 1\rangle$. Navíc lze psát

$$f = w^n g^n f + (1 - w^n g^n) f = w^n g^n f + (1 - wg)(1 + wg + \cdots + w^{n-1} g^{n-1}) f \in \langle I, wg - 1\rangle.$$

Nechť naopak $f \in \langle I, wg - 1\rangle \cap A$. Potom

$$A \ni f = \sum_{i=1}^{t} p_i q_i + (wg - 1)h,$$

kde $p_1, \ldots, p_t \in A$ je nějaká konečná množina generátorů I, $q_1, \ldots, q_t, h \in A[w]$. Dále uvažme dosazovací homomorfismus $\varphi : A[w] \to S^{-1}A$, kde $w \mapsto g^{-1}$. Protože v f se nevyskytuje proměnná w, platí $f = \varphi(f) = \sum_{i=1}^{t} p_i q_i' g^{-k_i} \in S^{-1}I \cap A$ (k_i je mocnina u w v q_i, tedy nyní již $q_i' \in A$).

❑

Jak se dá použít tvrzení na výpočet generátorů saturace daného ideálu $I \subseteq A$ vzhledem k $S = \{g^n : n \in \mathbb{N}\}$ ("daným ideálem" je míněno, že známe jeho konečnou množinu generátorů)? Nejprve uvážíme nějaké vyhovující uspořádání $\geq$ na termech v proměnných $x_1, \ldots, x_n, w$, takové, že $w \geq x_n \geq \cdots \geq x_1$. Potom spočteme Gröbnerovu bázi G ideálu $\langle I, wg - 1\rangle$. Podle Věty 4 z předchozí sekce pak $G \cap A$ je Gröbnerova báze pro $\langle I, wg - 1\rangle \cap A$, ale to je dle Tvrzení 6 přesně $S^{-1}I \cap A$. A samozřejmě $S^{-1}I \cap A = \langle G \cap A\rangle$.
Dále nás zajímá, jak spočítat generátory saturace vzhledem k multiplikativní množině $S = R - \{0\}$. To bude mírně obtížnější.

Tvrzení 7. *Nechť R je obor intergrity. Buď $S \subset R$ nějaká multiplikativní množina, $I \subseteq A$ nenulový ideál. Dále nechť $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báze pro I. Potom G je Gröbnerova báze pro ideál $S^{-1}I$ v $S^{-1}A$.*

Důkaz. Použijeme ekvivalentní definici *iii*) z Věty 2. Nechť $f \in S^{-1}I$. Pak existuje $s \in S$ takové, že $sf \in I$, a tedy lze psát $sf = \sum_{i=1}^{t} h_i g_i$, kde $h_1, \ldots, h_t \in A$ takové že $lt(sf) = lt(f) = \max\limits_{1 \leq j \leq m} (lt(h_i)lt(g_i))$. Dále jistě $f = (\frac{1}{s})sf = \sum_{i=1}^{t} (\frac{h_i}{s}) g_i$. Ale protože R je obor integrity, platí $lt(sf) = lt(f)$ a také $lt(\frac{h_i}{s}) = lt(h_i)$ pro všechna $i \leq t$. Tedy množina G vyhovuje podmínce *iii*) z Věty 2 pro ideál $S^{-1}A$ a je jeho Gröbnerovou bází.

❑

Další lemma je přímým důsledkem charakterizace Gröbnerových bází.

Lemma 8. *Nechť $I \subseteq J$ jsou ideály okruhu A takové, že $Lm(J) \subseteq Lm(I)$. Potom I=J.*

Důkaz. Nechť $m \in Lm(I)$ je vedoucí monočlen nějakého polynomu $f \in I$. Potom $m \in Lm(J)$, neboť $I \subseteq J$. Tedy $Lm(J) = Lm(I)$ a dle definice je J Gröbnerova báze pro I (nekonečná). Z Důsledku 1, bodu 2) dostáváme, že $I = \langle J\rangle$, ovšem jistě i $J = \langle J\rangle$.

❑

Je-li R obor integrity s podílovým tělesem k, můžeme si všimnout, že pokud vezmeme multiplikativní množinu $S \subset R$, potom pro ideál $I \subseteq A$ je $S^{-1}I$ přesně ideál $\langle I\rangle_{S^{-1}R[x_1, \ldots, x_n]} = I(S^{-1}R)[x_1, \ldots, x_n]$, kde $S^{-1}R$ je podokruh k.

Tvrzení 9. *Nechť R je obor integrity s podílovým tělesem k. Dále nechť $I \subseteq R[x_1, \ldots, x_n]$ je nenulový ideál s Gröbnerovou bazí $G = \{g_1, \ldots, g_t\}$. Položme $s = \prod_{i=1}^{t} lc(g_i) \in R$ a $S = \{s^n : n \in \mathbb{N}\}$. Potom platí*

$$Ik[x_1, \ldots, x_n] \cap R[x_1, \ldots, x_n] = I(S^{-1}R)[x_1, \ldots, x_n] \cap R[x_1, \ldots, x_n]. \qquad (*)$$

Důkaz. V důkazu budeme značit ideály generované vedoucími monočleny v okruhu $R[x_1,\dots,x_n]$ jako Lm, v okruhu $(S^{-1}R)[x_1,\dots,x_n]$ jako Lm_S. K důkazu tvrzení postačí dokázat rovnost

$$Lt_S(Ik[x_1,\dots,x_n]\cap(S^{-1}R)[x_1,\dots,x_n])\subseteq Lt_S(I(S^{-1}R)[x_1,\dots,x_n]),\qquad (**)$$

neboť zřejmě $I(S^{-1}R)[x_1,\dots,x_n]\subseteq Ik[x_1,\dots,x_n]\cap(S^{-1}R)[x_1,\dots,x_n]$ a tedy s použitím lemmatu 8 dostaneme rovnici $I(S^{-1}R)[x_1,\dots,x_n]=Ik[x_1,\dots,x_n]\cap$ $\cap(S^{-1}R)[x_1,\dots,x_n]$, průnikem obou stran s $R[x_1,\dots,x_n]$ vyjde rovnice $(*)$.
Fakt: Platí

$$Lm(I)(S^{-1}R)[x_1,\dots,x_n]\cap R[x_1,\dots,x_n]=Lm(I)k[x_1,\dots,x_n]\cap R[x_1,\dots,x_n].$$

Předpokládejme, že Fakt platí, a nechť $f\in Ik[x_1,\dots,x_n]\cap(S^{-1}R)[x_1,\dots,x_n]$. Chceme ukázat, že $lm(f)\in Lm_S(I(S^{-1}R)[x_1,\dots,x_n])$. Podle Tvrzení 7 je G Gröbnerova báze pro $Ik[x_1,\dots,x_n]$ a dle Věty 2 lze psát

$$f=\sum_{i=1}^{t}h_ig_i,$$

kde $h_1,\dots,h_t\in k[x_1,\dots,x_n]$ takové, že $lt(f)=\max\limits_{1\le j\le m}(lt(h_i)lt(g_i))$. Označme $V=$ $=\{i:lt(f)=lt(h_i)lt(g_i)\}$. Pak jistě $lm(f)=\sum_{i\in V}lm(h_i)lm(g_i)$. Víme, že $f\in(S^{-1}R)[x_1,\dots,x_n]$ proto existuje $n\in\mathbb{N}$ takové, že $s^nf\in R[x_1,\dots,x_n]$. A protože $Lm(I)=Lm(G)$ (G je Gröbnerova báze pro I), víme, že platí

$$lm(s^nf)=\sum_{i\in V}lm(s^nh_i)lm(g_i)\in Lm(I)k[x_1,\dots,x_n]\cap R[x_1,\dots,x_n]$$

s požitím Faktu dostaneme

$$lm(s^nf)\in Lm(I)(S^{-1}R)[x_1,\dots,x_n]\cap R[x_1,\dots,x_n],$$

dále opět s použitím $Lm(I)=Lm(G)$ můžeme psát

$$lm(s^nf)=\sum_{i=1}^{t}a_ilm(g_i)\frac{c_iX_i}{s^{k_i}}=\sum_{i=1}^{t}\frac{d_iX_ilm(g_i)}{s^{k_i}},$$

kde $d_i=a_ic_i\in R$, $k_i\in\mathbb{N}$, $X_i\in R[x_1,\dots,x_n]$ je term takový, že $lt(f)=$ $=X_i\ lt(g_i)$ pro všechna i, kde $d_i\neq0$. Podle Tvrzení 7 je G Gröbnerova báze i pro $I(S^{-1}R)[x_1,\dots,x_n]$ v $(S^{-1}R)[x_1,\dots,x_n]$, tedy dle definice je $Lm_S(G)=$ $=Lm_S(I(S^{-1}R)[x_1,\dots,x_n]))$. Ale $lm(g_i)\in Lm_S(G)$, to implikuje

$$lm(f)=\sum_{i=1}^{t}\frac{d_iX_ilm(g_i)}{s^{k_i+n}}\in Lm_S(I(S^{-1}R)[x_1,\dots,x_n]),$$

což dokazuje rovnost $(**)$.
Zbývá ukázat, že Fakt skutečně platí. Dokážeme, že obě strany rovnosti jsou rovny ideálu $\langle\{lt(g_i):1\le i\le t\}\rangle_{R[x_1,\dots,x_n]}$.
Všimneme si, že platí $Lm(I)(S^{-1}R)[x_1,\dots,x_n]\cap R[x_1,\dots,x_n]\subseteq Lm(I)k[x_1,\dots,x_n]\cap$

$\cap R[x_1,\ldots,x_n]$. To je zřejmé, neboť $S^{-1}R \subseteq k$. Dále vyjádříme $lm(g_i) = c_i lt(g_i)$, kde $c_i = lc(g_i) \in R$. Jistě tedy $c_i | s = \prod_{i=1}^{t} lc(g_i)$ pro všechna i a tedy existují $d_i \in R$ takové, že $s = d_i c_i$. Potom pro každé i lze psát

$$lt(g_i) = \frac{d_i}{s} c_i lt(g_i) \in Lm(I)(S^{-1}R)[x_1,\ldots,x_n].$$

Z toho plyne

$$\langle \{lt(g_i) : 1 \leq i \leq t\} \rangle_{R[x_1,\ldots,x_n]} \subseteq Lm(I)(S^{-1}R)[x_1,\ldots,x_n] \cap R[x_1,\ldots,x_n].$$

Nyní ukážeme, že

$$Lm(I)k[x_1,\ldots,x_n] \cap R[x_1,\ldots,x_n] \subseteq \langle \{lt(g_i) : 1 \leq i \leq t\} \rangle_{R[x_1,\ldots,x_n]}.$$

To je vidět z toho, že $Lm(I) = Lm(G)$, a tedy pro libovolné $f \in Lm(I)k[x_1,\ldots,x_n] \cap$ $\cap R[x_1,\ldots,x_n]$ můžeme psát $f = \sum_{i=1}^{t} a_i c_i lt(g_i) h_i$, kde $h_i \in k[x_1,\ldots,x_n]$, $a_i, c_i \in R$, přičemž ale koeficienty f jsou prvky R. Zřejmě je každý term polynomu f dělitelný termem $lt(g_i)$ pro nějaké i. Tedy skutečně platí i tato inkluze.

❑

Důsledek. Nechť jsou v R řešitelné lineární rovnice. Potom pro libovolný ideál $I \subseteq A = R[x_1,\ldots,x_n]$ a multiplikativní množinu $S = R - \{0\}$ umíme spočítat generátory ideálu $S^{-1}I \cap A$.

Důkaz. Zřejmé z Tvrzení 9 a 5.

❑

2 Rozpoznání prvoideálu

V této kapitole nejprve dokážeme kritérium, které převede problém rozpoznání prvoideálu v $R[x]$ na rozpoznání prvoideálu v R a ireducibilního polynomu z $k[x]$, kde k je podílové těleso oboru integrity R/P pro nějaký (prvo)ideál $P \subseteq R$. Posléze formulujeme algoritmus na rozpoznání prvoideálu okruhu $R[x_1,\ldots,x_n]$, který vyplyne z kritéria. Rutinní operace s ideály budou prováděny metodou Gröbnerových bází.

2.1 Kritérium

Uvažme okruh R, $P \subseteq R$ prvoideál a k podílové těleso R/P. Označme π přirozenou projekci $R \to R/P$ definovanou přiřazením $r \mapsto r + P$. Rozkladovou třídu prvku r budeme někdy značit také $\overline{r}$. Projekcí $R[x] \longrightarrow (R/P)[x]$ myslíme homomorfismus definovaný přiřazením $f = \sum_{i=1}^{t} a_i x^i \mapsto \sum_{i=1}^{t} \pi(a_i)x^i$ a budeme tuto projekci značit rovněž π. Dále si všimneme, že pro ideál $I \subseteq R[x]$ je $\pi(I)$ ideál v $(R/P)[x]$.

Lemma 10. *Nechť $I \subseteq R[x_1,\ldots,x_n]$ je ideál. Označme $T = {}^{R}\!/_{I \cap R}$. Potom I je prvoideál právě tehdy, když $\pi(I)$ je prvoideál v $T[x_1,\ldots,x_n]$.*

Důkaz. Nechť $\varphi : T[x_1,\ldots,x_n] \longrightarrow {}^{R[x_1,\ldots,x_n]}\!/_{I}$ je zobrazení a pro $f = \sum_{i=1}^{m}(a_i + I \cap R)x^i$ položíme $\varphi(f) = \sum_{i=1}^{m} a_i x^i + I$. Nejdříve ukážeme, že je zobrazení dobře definované. Nechť pro libovolné $a_i, b_i \in R$ platí $a_i - b_i = c_i \in I \cap R$. Potom

$$\varphi\Big(\sum_{i=1}^{m}(a_i + I \cap R)x^i\Big) = \sum_{i=1}^{m}(a_i)x^i + I = \sum_{i=1}^{m}(c_i + b_i)x^i + I =$$
$$= \sum_{i=1}^{m} b_i x^i + \sum_{i=1}^{m} c_i x^i + I = \sum_{i=1}^{m} b_i x^i + I,$$

přičemž poslední rovnost platí, protože $c_i \in I$ a tedy také $c_i x^i \in I$ pro všechna i. Zřejmě se také jedná o surjektivní homomorfisus. Dále si všimněme, že

$$\sum_{i=1}^{m}(a_i)x^i \in I \iff \sum_{i=1}^{m}(a_i + I \cap R)x^i \in \pi(I)$$

a tedy $ker(\varphi) = \pi(I)$. Podle první věty o izomorfismu máme

$${}^{T[x_1,\ldots,x_n]}\!/_{\pi(I)} \cong {}^{R[x_1,\ldots,x_n]}\!/_{I}.$$

Vidíme, že I je prvoideál $\iff {R[x_1,\dots,x_n]}/{I}$ je obor integrity $\iff$
$\iff {T[x_1,\dots,x_n]}/{\pi(I)}$ je obor integrity $\iff \pi(I)$ je prvoideál.
Tím je lemma dokázáno.

❑

Poznámka. Pokud je ideál I z Lemmatu 10 prvoideál, pak je $I \cap R$ prvoideál v R.

Důkaz. Buď $fg \in I \cap R$ pro $f,g \in R$. I je prvoideál, tedy například $f \in I \Rightarrow f \in I \cap R$.

❑

Lemma 11. *Nechť R je obor integrity s podílovým tělesem k. Buď $I \subseteq R[x_1,\dots,x_n]$ ideál takový, že $I \cap R = 0$. Potom I je prvoideál v $R[x_1,\dots,x_n]$, právě když jsou splněny obě následující podmínky:*

- *$Ik[x_1,\dots,x_n]$ je prvoideál v $k[x_1,\dots,x_n]$,*
- *$I = Ik[x_1,\dots,x_n] \cap R[x_1,\dots,x_n]$.*

Důkaz. Předpokládejme, že I je prvoideál v $R[x_1,\dots,x_n]$, a $f,g \in k[x_1,\dots,x_n]$ takové, že $fg \in Ik[x_1,\dots,x_n]$. Potom ale $fg = \frac{h}{r}$, kde $h \in I$ a $0 \neq r \in R$. Současně existují nenulové $d,e \in R$ takové, že $df,\ eg \in R[x_1,\dots,x_n]$. Tedy $r(df)(eg) = rde(\frac{h}{r}) = deh \in I$. Tedy $(rdf)(eg) \in I$, a protože I je prvoideál, dostáváme $rdf \in I$ nebo $eg \in I$. A proto $f \in Ik[x_1,\dots,x_n]$ nebo $g \in Ik[x_1,\dots,x_n]$ (v k existují $(rd)^{-1}$ i e^{-1}). Tedy $Ik[x_1,\dots,x_n]$ je prvoideál v $k[x_1,\dots,x_n]$. Nechť dále $\frac{h}{r} \in Ik[x_1,\dots,x_n] \cap R[x_1,\dots,x_n]$ pro libovolné $h \in I$ a $0 \neq r \in R$. Ukážeme, že $\frac{h}{r} \in I$. Zřejmě totiž $r(\frac{h}{r}) \in I$, ale $I \cap R = 0$, tedy musí platit $\frac{h}{r} \in I$. Opačná inkluze zřejmě platí, a proto $I = Ik[x_1,\dots,x_n] \cap R[x_1,\dots,x_n]$.
Nechť nyní platí, že $Ik[x_1,\dots,x_n]$ je prvoideál v $k[x_1,\dots,x_n]$ a $I = Ik[x_1,\dots,x_n] \cap$
$\cap R[x_1,\dots,x_n]$. Buďte $f,g \in R[x_1,\dots,x_n]$ takové, že $fg \in I$. Pak $fg \in Ik[x_1,\dots,x_n]$. Předpokládejme, že $f \in Ik[x_1,\dots,x_n]$. Pak ale $f \in Ik[x_1,\dots,x_n] \cap R[x_1,\dots,x_n] = I$ a I je prvoideál.

❑

Následující kritérium je shrnutí dvou uvedených lemmat.

Kritérium rozpoznání prvoideálu. *Nechť $I \subseteq R[x]$ je ideál. Potom I je prvoideál právě tehdy, když platí*

1) $I \cap R$ je prvoideál v R, a současně

2) pro $T = {R}/{I \cap R}$, k podílové těleso T a $J = \pi(I)$ platí: $Jk[x]$ je prvoideál v $k[x]$ a $J = Jk[x] \cap T[x]$.

Důkaz. Předpokládejme, že platí 1). Potom T je obor integrity. Dále nechť $f \in J \cap T$. Pak $\pi^{-1}(f) \subseteq R$ (protože $f \in T$) a $\pi^{-1}(f) \subseteq I$ (protože $f \in J$) a tedy $\pi^{-1}(f) \subseteq I \cap R$. Proto $J \cap T = 0$. Z lemmatu 11 máme, že 2) platí právě

když I je prvoideál.
Pokud předpokládáme, že I je prvoideál, platnost podmínky 1 plyne z lemmatu 10.

❑

2.2 Algoritmus

Nyní již můžeme formulovat algoritmus na rozpoznávání prvoideálů v $R[x_1,\ldots,x_n]$. Je ovšem třeba předpokládat, že R noetherovský a jsou v něm řešitelné lineární rovnice, abychom mohli počítat Gröbnerovy báze ideálů. Dále musíme předpokládat, že jsme schopni rozpoznat prvoideál v R. Také je třeba předpokládat, že umíme testovat ireducibilitu polynomů z $F[x]$, kde F je podílové těleso kvocientu polynomiálního okruhu nad R a nějakého prvoideálu. Dle [IGB] jsou tyto předpoklady splněny například pro $\mathbb{Z}$ a $\mathbb{Q}$. Nyní formulujeme algoritmus.

ALGORITMUS (rozpoznání provideálu)

VSTUP: Ideál $I = \langle f_1,\ldots,f_k\rangle \subseteq R[x_1,\ldots,x_n]$

VÝTUP: TRUE, pokud I je prvideál, FALSE jinak

0.krok FOR $i = 1,\ldots n$ DO $R_i := R[x_i,\ldots,x_n]$
$R_{n+1} := R$
FOR $i = 1\ldots.,n+1$: spočti $J_i = I \cap R_i$

1.krok IF (J_{n+1} není prvoideál) THEN $result$:=FALSE
ELSE jdi na 2.krok

2.krok $result$:=TRUE
$i := n+1$
WHILE ($i > 1$ AND $result$==TRUE) DO
$R' := R_i/J_i$
$J' := \pi(J_{i-1})$, kde π je projekce $R_i[x_{i-1}] \longrightarrow R'[x_{i-1}]$
$k' :=$ podílové těleso R'
Spočti polynom f takový, že $J'k'[x_{i-1}] = \langle f\rangle$
IF (f není ireducibilní nebo $f \neq 0$) THEN $result$:=FALSE
ELSE
spocti $J'k'[x_{i-1}] \cap R'[x_i]$
IF ($J'k'[x_{i-1}] \cap R'[x_i] \neq J'$) THEN $result$:=FALSE
ELSE $i := i-1$

3.krok retrun $result$

Tvrzení 12. *Algoritmus dává správný výsledek.*

Důkaz. Budeme postupovat indukcí podle počtu proměnných. Začneme s ideálem $I \subseteq R[x]$, zadaným jeho množinou generátorů. Spočteme pro něj $J = I \cap R$ (to lze dle Tvrzení 5) a rozhodneme, zda je J prvoideál. Pokud ne, podle Kritéria není prvoideál ani I. Pokud ano, položíme $T = {}^{R}\!/_{R \cap I}$ a $J = \pi(I)$. T je tedy obor integrity, a lze zkonstruovat jeho podílové těleso K. Nyní je $K[x]$ obor integrity hlavních ideálu (dokonce Eukleidovský), tedy má ideál $JK[x]$ jeden generátor f, který lze nalézt pomocí Eukleidova algoritmu. Podle předpokladu umíme rozhodnout, zda je f ireducibilní (a tedy $JK[x]$ je prvoideál). Pokud ano, zbývá ověřit, zda $J = JK[x] \cap T[x]$, což umíme, protože na pravé straně rovnosti je saturace J vzhledem k multiplikativní množině $T - \{0\}$(viz Tvrzení 9). Nyní nám Kritérium bod 2) říká, zda je I prvoideál.
Dále pokud máme ideál I v okruhu $R[x_1, \ldots, x_{n+1}]$, lze na něj pohlížet jako na ideál okruhu $(R[x_1, \ldots, x_n])[x_{n+1}]$, a podle indukčního předpokladu umíme poznat prvoideál v $R[x_1, \ldots, x_n]$ i ireducibilní polynomy v podílových tělesech příslušných faktorokruhů.

❑

Následující příklad [IGB, Exercise 4.4.4] ilustruje běh algoritmu.

Příklad. Dokažte, že ideál $I = \langle y^4 - z^3, y^2 - xz, xy^2 - z^2, x - z^2 \rangle$ je prvoideál v $\mathbb{Q}[x,y,z]$.

Řešení. Použijeme lexikografické uspořádání, kde $z > y > x$, tedy budeme počítat spíše v okruhu $\mathbb{Q}[z,y,x]$. Nejprve spočítáme (pomocí Mathematicy) Gröbnerovu bázi G pro ideál I. Výsledkem je $G = \{y^2 - x^3, z - x^2\}$. Dále přistoupíme k inicializačnímu kroku a položíme $R_1 := \mathbb{Q}[z,y,x], R_2 := \mathbb{Q}[y,x], R_3 := \mathbb{Q}[x]$, $R_4 := \mathbb{Q}$, spočteme ideály $J_i = I \cap R_i$, tedy $J_3 = J_4 = 0, J_2 = \langle y^2 - x^3 \rangle, J_1 = I$.
Pro $i = 4$ je průběh triviální, přistupme tedy rovnou k $i = 3$. Nyní máme $R' = R_3/J_3 = \mathbb{Q}[x]/0 = \mathbb{Q}[x]$. $J' = J_2 R'[y] = \langle y^2 - x^3 \rangle \mathbb{Q}[x,y]$, $k' = \mathbb{Q}(x)$ (tedy k' je těleso racionálních lomených funkcí s koeficienty v $\mathbb{Q}$). Máme spočítat (jediný) generátor ideálu $J'k'[y]$, to je polynom $f = y^2 - x^3$. Ten je ireducibilní, protože zřejmě v k' nemá kořen. Dále máme zkontrolovat, zda $J'k'[y] \cap (\mathbb{Q}[x])[y] = J'$. To ale platí díky Tvrzení 9. Pokud dosadíme za R z Tvrzení 9 okruh $\mathbb{Q}[x]$, za I ideál J' (množina $\{y^2 - x^3\}$ je zřejmě Gröbnerovou bází pro J'), vyjde $s = 1$ a multiplikativní množina S tedy obsahuje jen prvek 1. Dostáváme tedy

$$J'k'[y] \cap (\mathbb{Q}[x])[y] = J'(\mathbb{Q}[x] \cap \mathbb{Q}[x,y] = J',$$

což jsme chtěli. Hodnota *result* tedy zůstává na TRUE.
Dostáváme se k $i = 2$. Nyní je $R' = {}^{\mathbb{Q}[y,x]}\!/_{\langle y^2 - x^3 \rangle}$, $J' = IR'[z], k'$ je podílové těleso okruhu R'. Připomeňme, že máme projekci

$$\mathbb{Q}[z,y,x] \longrightarrow R'[z],$$

kde $f = \sum_{i=1}^{t} h_i z^i \in \mathbb{Q}[z,y,x], h_1, \ldots, h_t \in \mathbb{Q}[y,x]$, se zobrazí na polynom $\overline{f} = \sum_{i=1}^{t} \overline{h_i} z^i \in R'[z]$, kde $\overline{h_i}$ jsou polynomy h_i redukované modulo $\langle y^2 - x^3 \rangle$. Jak vypadá projekce ideálu $I = \langle y^2 - x^3, z - x^2 \rangle$ do okruhu $R'[z]$? Polynom $y^2 - x^3 \in \langle y^2 - x^3 \rangle$, tedy při projekci do R' přejde na 0. Ideál J' je tedy generován jedním prvkem, a to polynomem $\overline{z - x^2}$. Ten je stupně 1 a je tedy ireducibilní.

Navíc je $\{\overline{z - x^2}\}$ Gröbnerova báze pro J'. Použitím Tvrzení 9 jako v případě $i = 3$ tedy získáváme rovnost

$$J'k'[z] \cap R[z] = J',$$

a algoritmus vrátí TRUE, jak se mělo dokázat.

Literatura

[IGB] Adams, W. W., Loustaunau, P. (1994), *An Introduction to Grobner Bases*, Graduate Studies in Mathematics 3., American Mathematical Society, ISBN-0821872168

[GZT] Gianni,P., Zacharias,G., Trager,B.(1988) *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comp. 6, strany 149-167