



**MATEMATICKO-FYZIKÁLNÍ
FAKULTA**
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Lukáš Kubej

Řešení soustav polynomiálních rovnic

Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Štovíček, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná Matematika

Praha 2017

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 má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V Praze dne 20. 7. 2017

Lukáš Kubej

Chtěl bych poděkovat vedoucímu mé bakalářské práce doc. RNDr. Janu Štovíčkovi, Ph.D. za rady, pomoc a čas věnovaný při tvorbě této práce.

Název práce: Řešení soustav polynomiálních rovnic

Autor: Lukáš Kubej

Katedra: Katedra algebry

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

Abstrakt: Práce se zabývá teorií kolem soustav polynomiálních rovnic. Jejím cílem je především předvést a dokázat Tvrzení o eliminaci a Tvrzení o rozšíření, přičemž Tvrzení o eliminaci pomáhá řešit zadané polynomiální soustavy a Tvrzení o rozšíření nám umožňuje určit, která z částečných řešení půjde s jistotou doplnit na řešení kompletní. Pro formulaci a důkaz těchto tvrzení vyložíme teorii zabývající se mimo jiné monomickým uspořádáním, algoritmem dělení polynomů a především klíčového pojmu Groebnerovy báze. Nakonec jsou uvedeny řešené příklady ukazující aplikaci teorie popsané v této práci.

Klíčová slova: Algebraická geometrie, Groebnerovy báze, Eliminační teorie

Title: Solving systems of polynomial equations

Author: Lukáš Kubej

Department: Department of Algebra

Supervisor: doc. RNDr. Jan Štovíček, Ph.D., Department of Algebra

Abstract: This work is about theory of systems of polynomial equations. Its main purpose is to prove the Elimination theorem and the Extension theorem, where the Elimination theorem helps us to solve a given systems of polynomial equations and the Extension theorem tells us, which partial solutions can be extended into a complete solutions. To formulate and prove those theorems, we will explain theory including monomial orders, division algorithm for polynomial and mainly the key concept of Groebner basis. At the end are solved examples showing application of explained theory.

Keywords: Algebraic geometry, Groebner bases, Elimination theory

Obsah

Úvod	2
1 Základní pojmy	3
1.1 Okruh $k[x_1, \dots, x_n]$	3
1.2 Algebraická geometrie	3
2 Dělení polynomů se zbytkem	6
2.1 Monomické uspořádání	6
2.2 Algoritmus dělení v $k[x_1, \dots, x_n]$	7
3 Groebnerovy báze	10
3.1 Groebnerovy báze a jejich existence	10
3.2 Vlastnosti Groebnerovýchází	11
3.3 Algoritmus nalezení Groebnerovy báze	11
4 Teorie eliminace	13
4.1 Tvzení o eliminaci a rozšíření	13
4.2 Resultanty	13
4.3 Důkaz tvrzení o rozšíření	17
5 Příklady	21
5.1 Řešení polynomiálních soustav	21
5.2 Implicitace	23
Závěr	26
Seznam použité literatury	27

Úvod

Tato práce se bude zabývat teorií kolem soustav polynomiálních rovnic více proměnných. Jejím hlavním cílem bude předvést a dokázat Tvrzení o eliminaci a Tvrzení o rozšíření. Tvrzení o eliminaci nám pomůže při řešení soustav polynomiálních rovnic tím, že eliminuje proměnné a umožní nám řešit jednoduší soustavu. Tvrzení o rozšíření nám bude nástrojem jak určit, která z částečných řešení půjde s doplnit na řešení kompletní.

Nejprve v první kapitole uvedeme základní pojmy a věty které budeme používat. V druhé kapitole zavedeme pojem monomického uspořádání a s jeho pomocí zavedeme algoritmus pro dělení polynomů. Ten bude základním nástrojem pro upravování polynomů do vhodnější formy. Ve třetí kapitole představíme klíčový pojem Groebnerovy báze a algoritmus pro její nalezení. Ve čtvrté kapitole dokážeme Tvrzení o eliminaci, zavedeme pojem resultantu a pomocí něho dokážeme i Tvrzení o rozšíření. V poslední kapitole ilustrujeme probranou teorii na příkladech.

Tato práce je z většiny inspirována knihou *Ideals, Varieties and Algorithms* Cox a kol. (1996), kde je toto téma pokryto v prvních třech kapitolách.

1. Základní pojmy

V této kapitole nejprve uvedeme několik tvrzení o okruhu polynomů více proměnných nad tělesem k . Jsou to známá algebraická tvrzení, jejichž studium není předmětem této práce a proto je uvedu bez důkazu. Dále definujeme základní pojmy a tvrzení z algebraické geometrie, která bude použita napříč celou prací.

V celé práci budeme předpokládat, že k je těleso (nebude-li řečeno jinak).

1.1 Okruh $k[x_1, \dots, x_n]$

Důkazy následujících tvrzení jsou známé a lze je nalézt například v Fulton (1969), Stanovský (2009) a Cox, Little a O'Shea (1996).

Tvrzení 1 (Důsledek Hilbertovi věty o bázi). *Okruh $k[x_1, \dots, x_n]$ je noetherovský. Tedy každý ideál $I \subset k[x_1, \dots, x_n]$ je konečně generovaný nebo ekvivalentně neexistuje nekonečná ostře rostoucí posloupnost ideálů v $k[x_1, \dots, x_n]$.*

Tvrzení 2 (Důsledek Gaussovy věty). *Okruh $k[x_1, \dots, x_n]$ je Gaussův obor. Tedy každý nekonstantní polynom f má (až na pořadí a skalární násobky) jednoznačný rozklad na ireducibilní činitele.*

Tvrzení 3. $\mathbb{C}$ je algebraicky uzavřené těleso. Tedy každý nekonstantní polynom $f \in \mathbb{C}[x]$ má kořen v $\mathbb{C}$.

Tvrzení 4. Necht $f, g \in k[x]$. Pak $\text{GCD}(f, g)$ je generátor ideálu $\langle f, g \rangle$.

Tvrzení 5. Necht $f, g \in k[x_1, \dots, x_n]$ jsou nekonstantní v x_1 . Pak f a g mají společného dělitele v $k[x_1, \dots, x_n]$, který je nekonstantní v x_1 , právě když mají společného nekonstantního dělitele v $k(x_2, \dots, x_n)[x_1]$.

Tvrzení 6. Necht k je nekonečné těleso a $f, g \in k[x_1, \dots, x_n]$. Pak $f = g$ v $k[x_1, \dots, x_n]$, právě když $f, g : k^n \rightarrow k$ jsou stejné funkce.

Definice 1. Necht $f \in k[x_1, \dots, x_n]$. Řekneme, že f je monom, pokud $f = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots x_n^{\alpha_n}$. Pro $\alpha = (\alpha_1, \dots, \alpha_n)$ budeme značit $x^\alpha = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \dots x_n^{\alpha_n}$.

1.2 Algebraická geometrie

Definice 2. Necht $f_1, \dots, f_k \in k[x_1, \dots, x_n]$. Pak řekneme, že

$$V(f_1, \dots, f_k) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \text{ pro všechna } 1 \leq i \leq k\}$$

je algebraická množina definovaná $f_1, \dots, f_k$.

Lemma 7. Necht $V = V(f_1, \dots, f_k)$ a $W = V(g_1, \dots, g_l)$ jsou algebraické množiny v k^n . Pak

$$\begin{aligned} V \cap W &= V(f_1, \dots, f_k, g_1, \dots, g_l) \\ V \cup W &= V(f_i g_j : 1 \leq i \leq k, 1 \leq j \leq l) \end{aligned}$$

a tedy jsou také algebraickými množinami.

Důkaz. První rovnost je zřejmá, obě strany obsahují právě ty body, ve kterých se nulují všechna $f_1, \dots, f_k, g_1, \dots, g_l$. Pro druhou rovnost zřejmě platí $V \subset \mathbf{V}(f_i g_j)$ a $W \subset \mathbf{V}(f_i g_j)$. Tedy máme $V \cup W \subset \mathbf{V}(f_i g_j)$. Pro důkaz opačné inkluze zvolme $(a_1, \dots, a_n) \in \mathbf{V}(f_i g_j)$. Pokud leží ve V , máme hotovo, pokud ne, pak $f_{i_0}(a_1, \dots, a_n) \neq 0$ pro nějaké i_0 . Protože se však v $(a_1, \dots, a_n)$ nulují $f_{i_0} g_j$ pro všechna j , tak se musejí nulovat všechna g_j a $(a_1, \dots, a_n) \in W$. Tedy $\mathbf{V}(f_i g_j) \subset V \cup W$. □

Definice 3. Necht $I \subset k[x_1, \dots, x_n]$ je ideál. Budeme značit

$$\mathbf{V}(I) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0 \text{ pro všechna } f \in I\}.$$

Lemma 8. $\mathbf{V}(I)$ je algebraická množina. Speciálně pokud $I = \langle f_1, \dots, f_s \rangle$, pak $\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_s)$.

Důkaz. Protože $k[x_1, \dots, x_n]$ je noetherovský, platí $I = \langle f_1, \dots, f_s \rangle$ pro nějaké $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Dokážeme $\mathbf{V}(I) = \mathbf{V}(f_1, \dots, f_s)$. Zvolme $f \in \langle f_1, \dots, f_k \rangle$. Pak $f = \sum_{i=1}^k h_i f_i$ pro $h_i \in k[x_1, \dots, x_n]$. Pokud se v nějakém bodě nulují všechna f_i , tak se v něm nuluje i f . Tedy platí $\mathbf{V}(f_1, \dots, f_k) \subset \mathbf{V}(I)$. Druhá inkluze je zřejmá. □

Definice 4. Necht $X \subset k^n$. Pak řekneme, že

$$\mathbf{I}(X) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ pro všechna } (a_1, \dots, a_n) \in X\}$$

je ideál množiny X .

Lemma 9. Necht $X \subset k^n$. Pak $\mathbf{I}(X)$ je ideál.

Důkaz. Zřejmě platí, že $0 \in \mathbf{I}(X)$. Dále necht $f, g \in \mathbf{I}(X)$ a $h \in k[x_1, \dots, x_n]$. Pak

$$\begin{aligned} f(a_1, \dots, a_n) + g(a_1, \dots, a_n) &= 0 + 0 = 0 \\ h(a_1, \dots, a_n)f(a_1, \dots, a_n) &= h(a_1, \dots, a_n) \cdot 0 = 0. \end{aligned}$$

Tedy $\mathbf{I}(X)$ je ideál. □

Pozorování. Necht $I \subset k[x_1, \dots, x_n]$ je ideál. Pak $I \subset \mathbf{I}(\mathbf{V}(I))$.

Lemma 10. Necht V, W jsou algebraické množiny v k^n . Pak $V \subset W$, právě když $\mathbf{I}(W) \subset \mathbf{I}(V)$.

Důkaz. $\Rightarrow$: Každé $f \in \mathbf{I}(W)$ se nuluje na celém W , a protože $V \subset W$ tak i na celém V . Tedy $f \in \mathbf{I}(V)$.

$\Leftarrow$: Necht W je algebraická množina definovaná polynomy $f_1, \dots, f_k$. Pak $f_1, \dots, f_k \in \mathbf{I}(W) \subset \mathbf{I}(V)$ a tedy se všechna f_i nulují na V . Protože však W je tvořena všemi body kde se všechna f_i nulují, tak $V \subset W$. □

Důsledek 11. *Nechť V, W jsou algebraické množiny v k^n . Pak $V = W$, právě když $\mathbf{I}(W) = \mathbf{I}(V)$.*

2. Dělení polynomů se zbytkem

V následujících kapitolách budeme potřebovat algoritmus pro dělení polynomu $f \in k[x_1, \dots, x_n]$ polynomy $f_1, \dots, f_k \in k[x_1, \dots, x_n]$. Ten bude mít za cíl dát nám rozklad $f = a_1 f_1 + \dots + a_k f_k + r$, kde $a_1, \dots, a_k, r \in k[x_1, \dots, x_n]$ a kde „zbytek“ r je v nějakém smyslu menší. Toto formalizujeme zavedením pojmu monomického uspořádání a následně pomocí něho popíšeme algoritmus dělení. Vhodných uspořádání však bude existovat víc a výsledek algoritmu bude záviset na volbě konkrétního z nich.

2.1 Monomické uspořádání

Definice 5. *Monomické uspořádání na $k[x_1, \dots, x_n]$ je každá relace $>$ na $\mathbb{N}_0^n$ splňující:*

- (i) $>$ je lineární uspořádání.
- (ii) Pokud $\alpha > \beta$ pak $\alpha + \gamma > \beta + \gamma$, kde $\alpha, \beta, \gamma \in \mathbb{N}_0^n$.
- (iii) $>$ je dobré uspořádání (každá neprázdná podmnožina $\mathbb{N}_0^n$ má nejmenší prvek vzhledem k $>$).

Monomické uspořádání uspořádává monomy tak, že $x^\alpha > x^\beta$, právě když $\alpha > \beta$.

Lemma 12. *Uspořádání $>$ na $\mathbb{N}_0^n$ je dobré uspořádání, právě když každá ostře klesající posloupnost prvků z $\mathbb{N}_0^n$*

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

je konečná.

Důkaz. $\Rightarrow$: Pokud by posloupnost byla nekonečná, tak pro množinu jejich členů neexistuje minimální prvek, tedy $>$ není dobré uspořádání.

$\Leftarrow$: Pokud $>$ není dobré uspořádání, pak existuje $M \subseteq \mathbb{N}_0^n$ bez minimálního prvku. Zvolíme $\alpha(1) \in M$ libovolné. Protože $\alpha(1)$ není minimální nelezne $\alpha(2) \in M$ takové, že $\alpha(1) > \alpha(2)$. Protože $\alpha(2)$ není minimální prvek M existuje $\alpha(3) \in M$ takové, že $\alpha(2) > \alpha(3)$. Tímto postupem sestrojíme nekonečnou ostře klesající posloupnost. □

Definice 6. *Nechť $f = \sum_{\alpha} a_{\alpha} x^{\alpha}$ je nenulový polynom v $k[x_1, \dots, x_n]$ a necht $>$ je monomické uspořádání.*

- (i) *Multistupeň f je*

$$\text{multideg}(f) = \max(\alpha \in \mathbb{N}_0^n : a_{\alpha} \neq 0).$$

- (ii) *Vedoucí koeficient f je*

$$LC(f) = a_{\text{multideg}(f)}.$$

(iii) Vedoucí monom f je

$$LM(f) = x^{\text{multideg}(f)}.$$

(iv) Vedoucí člen f je

$$LT(f) = LC(f) \cdot LM(f).$$

Definice 7 (Lexikografické uspořádání). *Nechť $\alpha = (\alpha_1, \dots, \alpha_n)$ a $\beta = (\beta_1, \dots, \beta_n) \in \mathbb{N}_0^n$. Řekneme, že $\alpha >_{lex} \beta$ pokud je v rozdílu $\alpha - \beta$ nejlevější nenulová složka kladná.*

Tvrzení 13. *Lexikografické uspořádání na $\mathbb{N}_0^n$ je monomické uspořádání*

Důkaz. (i) Zřejmé. (ii) Protože $\alpha - \beta = (\alpha + \gamma) - (\beta + \gamma)$, tak se rovná i jejich nejlevější nenulová složka. (iii) Předpokládejme pro spor, že $>_{lex}$ není dobré uspořádání. Pak podle Lemmatu 12 existuje nekonečná ostře klesající posloupnost $\alpha(1) >_{lex} \alpha(2) >_{lex} \alpha(3) >_{lex} \dots$ prvků z $\mathbb{N}_0^n$. Uvažme první složky prvků $\alpha(i) \in \mathbb{N}_0^n$. Ty tvoří nerostoucí posloupnost nezáporných čísel. Jelikož běžné číselné uspořádání je dobrým uspořádáním na $\mathbb{N}_0$, tak posloupnost prvních členů musí někde přestat klesat. Tedy musí existovat k takové, že všechny první složky $\alpha(i)$ se rovnají pro $i > k$. Nyní uvažme posloupnost druhých složek prvků $\alpha(k), \alpha(k+1), \dots$ ze stejného důvodu musí i tato posloupnost přestat klesat. Tímto způsobem nakonec dostaneme l takové, že $\alpha(i)$ se rovnají ve všech složkách pro $i > l$. To je však spor s tím, že daná posloupnost je ostře klesající. $\square$

Pokud mocniny proměnných zapíšeme do vektoru popořadě, pak platí $x_1 > x_2 > \dots > x_n$. Pokud však chceme jiné uspořádání proměnných, stačí zapsat jejich mocniny do vektoru v jiném pořadí a proměnné budou uspořádané v tomto pořadí. Každé uspořádání proměnných tedy určuje vlastní lexikografické uspořádání.

Monomických uspořádání existuje mnohem víc, ale pro potřeby této práce si vystačíme pouze s lexikografickým uspořádáním.

2.2 Algoritmus dělení v $k[x_1, \dots, x_n]$

V této části nejprve popíšeme samotný algoritmus, dokážeme některé jeho vlastnosti a nakonec uvedeme jeho nedostatky, které se budeme snažit vyřešit v další kapitole.

Algoritmus používá pojem vedoucího členu, tedy musíme mít předem dané monomické uspořádání.

Input: $f, f_1, \dots, f_s$
Output: $r, a_1, \dots, a_s$
 $a_1 := 0; \dots; a_s := 0; r := 0;$
 $p := f;$
while $p \neq 0$ **do**
 $i := 1;$
 $\text{dělilo_se} := \text{false};$
 while $i < s$ **and** $\text{dělilo_se} = \text{false}$ **do**
 if $LT(f_i)$ dělí $LT(p)$ **then**
 $a_i := a_i + LT(p)/LT(f_i);$
 $p := p - (LT(p)/LT(f_i))f_i;$
 $\text{dělilo_se} := \text{true};$
 else
 $i := i + 1;$
 end
 end
 if $\text{dělilo_se} = \text{false}$ **then**
 $r := r + LT(p);$
 $p := p - LT(p);$
 end
end

Algoritmus 1: Algoritmus dělení v $k[x_1, \dots, x_n]$

Tvrzení 14. *Nechť $f, f_1, \dots, f_n \in k[x_1, \dots, x_n]$ a $a >$ je monomické uspořádání na $\mathbb{N}_0^n$. Pak algoritmus dělení vrátí $r, a_1, \dots, a_r \in k[x_1, \dots, x_n]$ takové, že platí*

$$f = a_1 f_1 + \dots + a_n f_n + r,$$

kde buď $r = 0$ nebo r je lineární kombinací monomů takových, že žádný není dělitelný ani jedním z $LT(f_1), \dots, LT(f_n)$. Polynom r nazveme zbytek f po dělení $f_1, \dots, f_n$. Navíc pokud $a_i f_i \neq 0$, pak

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i).$$

Důkaz. V každém průběhu hlavního while cyklu nastane právě jedna ze dvou možností. Buď existuje i takové, že $LT(f_i)$ dělí $LT(p)$ a pak se provede daná část algoritmu pro nejmenší takové i („krok s dělením“), nebo takové i neexistuje a následuje „krok se zbytkem“.

Nejprve ukážeme, že v každém korku platí

$$f = a_1 f_1 + \dots + a_n f_n + r + p. \quad (2.1)$$

Toto je zřejmě pravda pro inicializované hodnoty $p, r, a_1, \dots, a_s$. Dále předpokládejme, že v nějakém korku platí (2.1). Pokud je následující krok „krok s dělením“ podle i , pak platí

$$a_i f_i + p = (a_i + LT(p)/LT(f_i))f_i + (p - (LT(p)/LT(f_i))f_i)$$

a jelikož ostatní proměnné zůstanou nezměněné, tak (2.1) zůstane pravdivá. Pokud je další krok „krok se zbytkem“, pak všechna a_i zůstanou stejná a

$$r + p = (r + LT(p)) + (p - LT(p)),$$

tedy (2.1) zustane opět pravdivá. Tedy (2.1) je pravdivá v každém kroku algoritmu.

Jelikož algoritmus skončí v okamžiku, kdy $p = 0$, tak

$$f = a_1 f_1 + \cdots + a_n f_n + r$$

a protože jsme k r přidávali pouze členy, které nebyly dělitelné žádným z $LT(f_i)$, tak má r požadované vlastnosti.

Dále dokážeme, že algoritmus vždy skončí v konečném počtu kroků. Ukážeme, že v každém kroku se stupeň p buď zmenší, nebo $p = 0$. Jelikož pracujeme s dobrým uspořádáním, tak nemůžeme dostat nekonečnou posloupnost klesajících multistupňů a algoritmus pak skončí v konečném počtu kroků.

Pokud je následující krok „krok s dělením“ pak p je předefinováno na

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

A platí

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p)$$

Pokud je následující krok „krok se zbytkem“ pak p je předefinováno na

$$p' = p - LT(p).$$

Tedy v obou případech p' má menší multistupeň než p a nebo $p' = 0$

Zbývá ukázat, že pokud $a_i f_i \neq 0$, pak $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$. Každý člen v a_i je tvaru $LT(p)/LT(f_i)$ pro nějakou hodnotu p a vždy platí $LT(p) < LT(f)$. Tedy $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$. □

Nedostatkem tohoto algoritmu je, že pokud na vstupu přeházíme pořadí polynomů kterými dělíme, můžeme dostat odlišný zbytek. Také nemusí platit, že pokud $f \in \langle f_1, \dots, f_n \rangle$, tak je zbytek polynomu f po dělení polynomy $f_1, \dots, f_n$ nulový. Oba nedostatky však mizí při použití Groebnerových bází, které popíšeme v další kapitole.

3. Groebnerovy báze

V této kapitole zdefinujeme pojem Groebnerovýchází a algoritmus pro jejich nalezení. Pomocí nich a algoritmu dělení získáme postup, jak pro libovolný polynom určit, zda náleží do daného ideálu. Nakonec zavedeme pojem redukované Groebnerovy báze která bude pro každý ideál jednoznačně určena.

V celé kapitole budeme uvažovat pevně zvolené monomické uspořádání.

3.1 Groebnerovy báze a jejich existence

Věta 15 (Dickinsonovo lemma). *Nechť $A \subset \mathbb{N}_0^n$ a $I = \langle x^\alpha : \alpha \in A \rangle \subset k[x_1, \dots, x_n]$ je ideál. Pak existují $\alpha_1, \dots, \alpha_s \in A$ tak, že $I = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$.*

Důkaz této věty nebudeme uvádět. Lze ho případně nálezt v Cox a kol. (1996)

Definice 8. *Nechť $I \subset k[x_1, \dots, x_n]$ je nenulový ideál. Množinu všech vedoucích členů prvků z I označíme $LT(I)$.*

Definice 9. *Konečnou podmnožinu $\{g_1, \dots, g_s\}$ ideálu I nazveme Groebnerovou bází, pokud*

$$\langle LT(g_1), \dots, LT(g_s) \rangle = \langle LT(I) \rangle.$$

Věta 16. *Nechť $I \subset k[x_1, \dots, x_n]$ je nenulový ideál. Pak I má Groebnerovu bází.*

Důkaz. Protože $\langle LT(I) \rangle$ je generovaný monomy $LM(g)$ pro nenulové $g \in I$, tak z Dickinsonova lemmatu dostáváme, že existují $g_1, \dots, g_s \in I$ takové, že $\langle LT(I) \rangle = \langle LM(g_1), \dots, LM(g_s) \rangle$. Jelikož $LM(g_i)$ se liší od $LT(g_i)$ násobek konstantou, tak $\langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. □

Lemma 17. *Nechť $I = \langle x^{\alpha_1}, \dots, x^{\alpha_k} \rangle$ je ideál generovaný monomy. Pak $x^\alpha \in I$, právě když x^α je dělitelné některým x^{α_i} .*

Důkaz. Pokud $x^\alpha \in I$, tak $x^\alpha = \sum_{i=1}^k h_i x^{\alpha_i}$, kde $h_i \in k[x_1, \dots, x_n]$. Rozepíšeme všechna h_i jako lineární kombinaci monomů. Každý člen na pravé straně je dělitelný nějakým x^{α_i} a navíc se na pravé straně musí vyrušit všechny sčítance jiných monomů než x^α . Zbývající sčítance musí být tvaru $c x^{\alpha - \alpha_i} x^{\alpha_i}$, kde $c \in k$. Jelikož musí na pravé straně zbývat alespoň jeden sčítanec, tak zřejmě $x_i^{\alpha_i}$ dělí x^α . Opačná implikace plyne přímo z definice ideálu. □

Věta 18. *Groebnerova báze ideálu je jeho bází.*

Důkaz. Mějme nenulový ideál I a $\{g_1, \dots, g_s\}$ jeho Groebnerovu bází. Ukážeme, že $I = \langle g_1, \dots, g_s \rangle$.

Zřejmě platí $\langle g_1, \dots, g_s \rangle \subset I$. Pro důkaz opačné inkluze mějme $f \in I$. Použitím algoritmu dělení na vydělení polynomu f polynomy $g_1, \dots, g_s$, dostaneme vyjádření

$$f = a_1g_1 + \dots + a_sg_s + r,$$

kde žádný člen v r není dělitelný ani jedním z $LT(g_1), \dots, LT(g_s)$. Dále platí

$$r = f - a_1g_1 - \dots - a_sg_s \in I.$$

Tedy pokud $r \neq 0$, tak $LT(r) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. Tedy dle lemmatu 17 musí $LT(r)$ být dělitelné nějakým $LT(g_i)$, což je spor s tím, že r je zbytek. Tedy $r = 0$ a

$$f = a_1g_1 + \dots + a_sg_s \in \langle g_1, \dots, g_s \rangle.$$

□

3.2 Vlastnosti Groebnerovýchází

Tvrzení 19. *Nechť $G = \{g_1, \dots, g_s\}$ je Groebnerova báze ideálu $I \subset k[x_1, \dots, x_n]$ a $f \in k[x_1, \dots, x_n]$. Pak existuje právě jedno $r \in k[x_1, \dots, x_n]$ s následujícími vlastnostmi:*

- (i) *Žádný z členů v r není dělitelný ani jedním z $LT(g_1), \dots, LT(g_s)$.*
- (ii) *Existuje $g \in I$ takový, že $f = g + r$.*

Důkaz. Použitím dělicího algoritmu dostaneme $f = a_1g_1 + \dots + a_sg_s + r$ kde r splňuje (i). Položíme $g = a_1g_1 + \dots + a_sg_s$, čímž je splněna i podmínka (ii).

Stačí tedy dokázat už jen jednoznačnost. Nechť $f = g_a + r_a = g_b + r_b$ a jsou splněny podmínky (i) a (ii). Pak $r_b - r_a = g_a - g_b \in I$. Tedy pokud $r_a \neq r_b$, tak $LT(r_b - r_a) \in \langle LT(I) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$. Dle 17 je $LT(r_b - r_a)$ dělitelné některým $LT(g_i)$. To však nemůže nastat, protože ani jeden z členů v r_a, r_b není dělitelný žádným $LT(g_i)$. Tedy $r_b - r_a = 0$ a jednoznačnost je dokázána.

□

Toto tvrzení ukazuje, že pokud v algoritmu dělení dělíme prvky Groebnerovy báze, tak nezáleží na pořadí, ve kterém dělíme, jelikož zbytek je určen jednoznačně.

Důsledek 20. *Nechť $f \in k[x_1, \dots, x_n]$ a $G = \{g_1, \dots, g_s\}$ je Groebnerova báze ideálu $I \subset k[x_1, \dots, x_n]$. Pak $f \in I$ právě tehdy, když zbytek po dělení f podle G je nula.*

3.3 Algoritmus nalezení Groebnerovy báze

V této sekci popíšeme algoritmus na nalezení Groebnerovy báze a speciální druh Groebnerovy báze který bude jednoznačný. U tvrzení z této sekce však nebudeme uvádět důkazy, neboť nebudou potřeba pro další teorii a budou uvedeny pouze informativně. Důkazy lze nalézt v Cox a kol. (1996) (2. kapitola, §6 a §7)

Definice 10. Budeme značit $\bar{f}^F$ zbytek po dělení polynomu f uspořádanou s -ticí $F = (f_1, \dots, f_s)$.

Pokud je F Groebnerovou bází ideálu $\langle f_1, \dots, f_s \rangle$, pak díky Tvzení 19 stačí F uvažovat jako množinu.

Definice 11. Necht $f, g \in k[x_1, \dots, x_n]$ jsou nenulové, $\alpha = \text{multideg}(f)$ a $\beta = \text{multideg}(g)$. Označme $\gamma = (\gamma_1, \dots, \gamma_n)$ kde $\gamma_i = \max(\alpha_i, \beta_i)$. S -polynomem f a g nazveme kombinaci

$$S(f, g) = \frac{x^\gamma}{LT(f)} \cdot f - \frac{x^\gamma}{LT(g)} \cdot g.$$

S -polynom je zadefinován tak, aby vyrušil vedoucí členy a je hlavním nástrojem v dále uvedeném algoritmu.

Tvrzení 21. Necht I je ideál $k[x_1, \dots, x_n]$ a $G = \{g_1, \dots, g_s\}$ je báze I . Pak G je Groebnerovou bází ideálu I právě tehdy, když pro každou dvojici $i \neq j$ platí $\overline{S(g_i, g_j)}^G = 0$.

Input: $F = (f_1, \dots, f_s)$
Output: $G = (g_1, \dots, g_t)$
 $G := F$;
repeat
 $G' := G$;
 foreach $\{p, q\}, p \neq q \in G'$ **do**
 $S := \overline{S(p, q)}^{G'}$;
 if $S \neq 0$ **then**
 $G := G \cup \{S\}$
 end
 end
until $G = G'$;

Algoritmus 2: Buchbergerův algoritmus

Tvrzení 22. Necht $I = \langle f_1, \dots, f_s \rangle$ je ideál $k[x_1, \dots, x_n]$. Pak Buchbergerův algoritmus se vstupem $F = (f_1, \dots, f_s)$ vrátí v konečném počtu kroků Groebnerovu bázi $G = (g_1, \dots, g_t)$ ideálu I a $F \subset G$.

Definice 12. Redukovanou Groebnerovou bází ideálu I nazveme takovou Groebnerovu bázi G pro kterou platí:

(i) $LC(p) = 1$ pro každé $p \in G$.

(ii) Pro každé $p \in G$, žádný člen polynomu p neleží v $\langle LT(G - \{p\}) \rangle$.

Tvrzení 23. Necht I je nenulový ideál. Pak I má (pro dané monomické uspořádání) jednoznačně určenou redukovanou Groebnerovu bázi.

Uvedená základní verze Buchbergerova algoritmu produkuje zbytečně velké báze a je výpočetně náročná. Existují ale jeho vylepšení, která výrazně zrychlí výpočet. Navíc lze už v průběhu algoritmu upravovat polynomy tak, že algoritmus bude vracet redukovanou Groebnerovu bázi. Více lze najít například v Cox a kol. (1996) 2. kapitola §9 nebo Buchberger (1985).

4. Teorie eliminace

4.1 Tvzení o eliminaci a rozšíření

Definice 13. *Nechť $I = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$. Ideál*

$$I_l = I \cap k[x_{l+1}, \dots, x_n]$$

nazveme l -tým eliminačním ideálem I_l .

Tvrzení 24 (Tvrzení o eliminaci). *Nechť $I \subset k[x_1, \dots, x_n]$ je ideál a G je Groebnerova báze ideálu I vzhledem k lexikografickému uspořádání, kde $x_1 > \dots > x_n$. Pak pro každé $0 \leq l \leq n$ je množina*

$$G_l = G \cap k[x_{l+1}, \dots, x_n]$$

Groebnerovou bází l -tého eliminačního ideálu I_l .

Důkaz. Zvolme l mezi 0 a n . Protože $G_l \subset I_l$, stačí ukázat, že $\langle LT(I_l) \rangle = \langle LT(G_l) \rangle$, přičemž inkluze „ $\supset$ “ je zřejmá. Chceme tedy dokázat, že pro libovolné $f \in I_l$, existuje $g \in G_l$ takové, že $LT(f)$ je dělitelné $LT(g)$. Pak $LT(I_l) \subset \langle LT(G_l) \rangle$ a tedy $\langle LT(I_l) \rangle \subset \langle LT(G_l) \rangle$.

Zvolme tedy $f \in I_l$. Jelikož $f \in I$, tak $LT(f)$ je dělitelné $LT(g)$ pro nějaké $g \in G$. Protože $f \in I_l$, tak $LT(g)$ obsahuje pouze proměnné $x_{l+1}, \dots, x_n$. Jelikož jsme však použili lexikografické uspořádání kde $x_1 > \dots > x_n$, tak $LT(g) \in k[x_{l+1}, \dots, x_n]$ implikuje $g \in k[x_{l+1}, \dots, x_n]$. Tedy $g \in G_l$. □

Tvrzení 25 (Tvrzení o rozšíření). *Nechť k je algebraicky uzavřené těleso a $I = \langle f_1, \dots, f_s \rangle$ je ideál $k[x_1, \dots, x_n]$. Pro každé $1 \leq i \leq s$ napišme f_i ve tvaru*

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{členy, ve kterých má } x_1 \text{ stupeň } < N_i,$$

kde $N_i \geq 0$ a $g_i \in k[x_2, \dots, x_n]$ je nenulové. Dále necht máme částečné řešení $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$. Pokud $(c_2, \dots, c_n) \notin \mathbf{V}(g_1, \dots, g_s)$, pak existuje $c_1 \in k$ takové, že $(c_1, \dots, c_n) \in \mathbf{V}(I)$.

Důkazu tohoto tvrzení budeme věnovat zbytek kapitoly. Nejprve však zavedeme pojem resultantu dvou polynomů, který bude pro důkaz zásadním nástrojem.

4.2 Resultanty

V této části budeme často používat pojem společného dělitele. Jelikož ale konstantní polynomy dělí libovolný polynom a všude bysme museli psát společného nekonstantního dělitele, tak pro zjednodušení formulací budeme společným dělitelem uvažovat pouze nekonstantní polynomy.

Tvrzení 26. *Nechť $f, g \in k[x]$ jsou polynomy stupňů $l, m > 0$. Pak f, g mají společného dělitele právě tehdy, když existují polynomy $A, B \in k[x]$ takové, že:*

- (i) A a B nejsou oba nulové.
- (ii) A má stupeň nejvýše $m - 1$ a B má stupeň nejvýše $l - 1$.
- (iii) $Af + Bg = 0$.

Důkaz. Nejprve předpokládejme, že mají společného dělitele $h \in k[x]$. Pak $f = hf_1$ a $g = hg_1$, kde $f_1, g_1 \in k[x]$. Zřejmě platí $\deg(f_1) \leq l - 1$ a $\deg(g_1) \leq m - 1$. Pak

$$g_1 \cdot f + (-f_1) \cdot g = g_1 hf_1 - f_1 hg_1 = 0.$$

Stačí tedy položit $A = g_1$ a $B = -f_1$.

Pro důkaz opačné implikace mějme A, B splňující výše zmíněné vlastnosti. Bez újmy na obecnosti předpokládejme, že díky (i) je $B \neq 0$. Pro spor předpokládejme, že $GCD(f, g) = 1$. Díky Tvrzení 4 pak existují polynomy $C, D \in k[x]$ takové, že $Cf + Dg = 1$. Použitím (iii) dostáváme:

$$B = (Cf + Dg)B = BCf + BDg = BCf - ADf = (BC - AD)f.$$

Protože B je nenulové, musí být $\deg(B) \geq \deg(f) = l$ což je ve sporu s (ii). Tedy $GCD(f, g) \neq 1$ a f, g mají společného dělitele. □

Otázkou zůstává, jak polynomy A a B nalézt. Necht

$$\begin{aligned} A &= c_0 x^{m-1} + \cdots + c_{m-1}, \\ B &= d_0 x^{l-1} + \cdots + d_{l-1}, \end{aligned}$$

kde koeficienty $c_0, \dots, c_{m-1}, d_0, \dots, d_{l-1}$ budeme uvažovat jako neznámé. Cílem je nalézt $c_i, d_i \in k$ takové, že alespoň jedno je nenulové a $Af + Bg = 0$. Pak budeme mít A a B splňující podmínky Tvrzení 26. Dále necht

$$\begin{aligned} f &= a_0 x^l + \cdots + a_l, & a_0 &\neq 0, \\ g &= b_0 x^m + \cdots + b_m, & b_0 &\neq 0, \end{aligned}$$

Dosazením do vzorce $Af + Bg = 0$ a porovnáním koeficientů dostáváme následující soustavu $l + m$ rovnic o $l + m$ neznámých:

$$\begin{aligned} a_0 c_0 + b_0 d_0 &= 0 && \text{koeficient u } x^{l+m-1} \\ a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 &= 0 && \text{koeficient u } x^{l+m-2} \\ &\vdots && \vdots \\ a_l c_{m-1} + b_m d_{l-1} &= 0 && \text{koeficient u } x^0. \end{aligned} \tag{4.1}$$

Jelikož má tato soustava lineárních rovnic stejně rovnic jako neznámých, tak má nenulové řešení právě tehdy, když je její determinant nulový.

Definice 14. Mějme nekonstantní polynomy $f, g \in k[x]$ tvaru

$$\begin{aligned} f &= a_0x^l + \cdots + a_l, & a_0 &\neq 0, \\ g &= b_0x^m + \cdots + b_m, & b_0 &\neq 0. \end{aligned}$$

Pak Sylvestrovou maticí polynomů f a g vzhledem k x rozumíme matici koeficientů systému lineárních rovnic 4.1 značenou symbolem $Syl(f, g, x)$. Tedy je to následující $(l+m) \times (l+m)$ matice:

$$Syl(f, g, x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ & a_1 & \cdots & & & b_1 & \cdots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & b_m & & & \vdots \\ & & \ddots & & & \ddots & & \\ & & & a_l & & & & b_m \end{pmatrix},$$

kde koeficienty a_i se vyskytují v prvních m sloupcích a koeficienty b_i v posledních l sloupcích.

Resultantem f a g vzhledem k x nazveme determinant Sylvestrové matice. Tedy

$$Res(f, g, x) = \det(Syl(f, g, x)).$$

Tvrzení 27. Mějme nekonstantní polynomy $f, g \in k[x]$. Pak $Res(f, g, x) \in k$ je celočíselný polynom v koeficientech f a g . Navíc f a g mají společného dělitele právě tehdy, když $Res(f, g, x) = 0$.

Důkaz. První část je zřejmá z definice determinantu. Pro druhou část platí: resultant je nula $\Leftrightarrow$ soustava 4.1 má nenulové řešení $\Leftrightarrow$ existuje A a B z Tvrzení 26 $\Leftrightarrow f$ a g mají společného dělitele, přičemž první ekvivalence plyne z definice resultantu a druhá z úvahy před ní.

□

Tvrzení 28. Mějme nekonstantní polynomy $f, g \in k[x]$. Pak existují polynomy $A, B \in k[x]$ takové, že

$$Af + Bg = Res(f, g, x)$$

a navíc koeficienty A a B jsou celočíselné polynomy v koeficientech f a g .

Důkaz. Pokud $Res(f, g, x) = 0$, tak stačí položit $A = B = 0$. Uvažujme tedy $Res(f, g, x) \neq 0$.

Nejprve nalezneme taková $C, D \in k[x]$, že $Cf + Dg = 1$. Necht

$$\begin{aligned} f &= a_0x^l + \cdots + a_l, & a_0 &\neq 0, \\ g &= b_0x^m + \cdots + b_m, & b_0 &\neq 0, \\ C &= c_0x^{m-1} + \cdots + c_{m-1}, \\ D &= d_0x^{l-1} + \cdots + d_{l-1}, \end{aligned}$$

kde koeficienty $c_0, \dots, c_{m-1}, d_0, \dots, d_{l-1}$ jsou neznámé v k . Pokud tyto formule dosadíme do rovnice $Cf + Dg = 1$ a porovnáme koeficienty, dostaneme následující soustavu:

$$\begin{aligned} a_0 c_0 + b_0 d_0 &= 0 && \text{koeficient u } x^{l+m-1} \\ a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 &= 0 && \text{koeficient u } x^{l+m-2} \\ &\vdots && \vdots \\ a_l c_{m-1} + b_m d_{l-1} &= 1 && \text{koeficient u } x^0. \end{aligned} \tag{4.2}$$

Takto soustava je stejná jako soustava 4.1 až na poslední rovnici která má na pravé straně 1. Tedy matice koeficientů je Sylvestrova matice polynomů f a g vzhledem k x a jelikož $\text{Res}(f, g, x) \neq 0$, tak má soustava 4.2 právě jedno řešení.

Za těchto podmínek můžeme použít Cramerovo pravidlo. To nám dává předpis pro každou proměnnou ve tvaru, kde v čitateli je determinant nějaké matice s koeficienty $0, 1, a_0, \dots, a_l, b_0, \dots, b_m$ (tedy celočíselný polynom v těchto koeficientech) a ve jmenovateli $\text{Res}(f, g, x)$. Jelikož $C = c_0 x^{m-1} + \dots + c_{m-1}$, můžeme vytknout jmenovatel $\text{Res}(f, g, x)$ a dostaneme

$$C = \frac{A}{\text{Res}(f, g, x)},$$

kde $A \in k[x]$ a koeficienty A jsou celočíselné polynomy v a_i, b_i . Stejně tak dostaneme

$$D = \frac{B}{\text{Res}(f, g, x)},$$

kde $B \in k[x]$ má stejné vlastnosti jako A . Rovnici $Cf + Dg = 1$ vynásobíme $\text{Res}(f, g, x)$ a dostáváme $Af + Bg = \text{Res}(f, g, x)$, kde A i B mají požadované vlastnosti. □

Nyní zobecníme pojem resultantu pro polynomy více proměnných.

Definice 15. *Mějme nekonstantní polynomy $f, g \in k[x_1, \dots, x_n]$ tvaru*

$$\begin{aligned} f &= a_0 x_1^l + \dots + a_l, & a_0 &\neq 0, \\ g &= b_0 x_1^m + \dots + b_m, & b_0 &\neq 0, \end{aligned}$$

kde $a_i, b_i \in k[x_2, \dots, x_n]$. Pak resultantem f a g vzhledem k x_1 nazveme determinant

$$\text{Res}(f, g, x_1) = \det \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ & a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & \ddots & a_0 & \vdots & & \ddots & b_0 \\ & \vdots & & a_1 & & \vdots & & b_1 \\ a_l & & & & b_m & & & \\ & a_l & & \vdots & & b_m & & \vdots \\ & & \ddots & & & & \ddots & \\ & & & a_l & & & & b_m \end{pmatrix},$$

kde koeficienty a_i se vyskytují v prvních m sloupcích a koeficienty b_i v posledních l sloupcích.

Tvrzení 29. *Nechť $f, g \in k[x_1, \dots, x_n]$ jsou nekonstantní v x_1 . Pak:*

$$(i) \operatorname{Res}(f, g, x_1) \in \langle f, g \rangle \cap k[x_2, \dots, x_n].$$

(ii) $\operatorname{Res}(f, g, x_1) = 0$ právě tehdy, když f a g mají společného dělitele který je nekonstantní v x_1 .

Důkaz. Nechť $a_i, b_i \in k[x_2, \dots, x_n]$ jsou koeficienty f, g rozepsaných jako polynomy v x_1 . Jelikož resultant je celočíselný polynom v a_i, b_i tak $\operatorname{Res}(f, g, x_1) \in k[x_2, \dots, x_n]$. Také víme, že $\operatorname{Res}(f, g, x_1) = Af + Bg$, kde A a B jsou polynomy v x_1 jejichž koeficienty jsou celočíselné polynomy v a_i, b_i . Tedy $A, B \in k[x_1, \dots, x_n]$ a z $\operatorname{Res}(f, g, x_1) = Af + Bg$ plyne $\operatorname{Res}(f, g, x_1) \in \langle f, g \rangle$.

Pro důkaz druhé části použijeme Tvrzení 27 na $f, g \in k(x_2, \dots, x_n)[x_1]$. Použitím Tvrzení 5 pak dostáváme (ii). □

Důsledek 30. *Nechť k je algebraicky uzavřené těleso a $f, g \in k[x]$. Pak $\operatorname{Res}(f, g, x) = 0$ právě tehdy, když f a g mají společný kořen v k .*

Tvrzení 31. *Nechť k je algebraicky uzavřené těleso a $f, g \in k[x_1, \dots, x_n]$, kde*

$$\begin{aligned} f &= a_0 x_1^l + \dots + a_l, & a_0 &\neq 0, \\ g &= b_0 x_1^m + \dots + b_m, & b_0 &\neq 0, \end{aligned}$$

pro $a_i, b_i \in k[x_2, \dots, x_n]$. Pokud se resultant $\operatorname{Res}(f, g, x_1) \in k[x_2, \dots, x_n]$ nuluje na $(c_2, \dots, c_n) \in k^{n-1}$, pak nastane jedna z následujících možností:

(i) a_0 nebo b_0 se nuluje na $(c_2, \dots, c_n)$.

(ii) Existuje $c_1 \in k$ takové, že f i g se nulují na $(c_1, \dots, c_n) \in k^n$.

Důkaz. Označme $c = (c_2, \dots, c_n)$, $f(x_1, c) = f(x_1, c_2, \dots, c_n)$ a $h = \operatorname{Res}(f, g, x_1)$. Stačí si uvědomit, že pokud se na c nenuluje ani jedno z a_0, b_0 , pak $h(c) = \operatorname{Res}(f(x_1, c), g(x_1, c), x_1)$. Obě strany jsou pak totiž determinantem stejné matice, kde se pouze dosadí buď přímo do matice nebo až do determinantu jako polynomu. Máme tedy $0 = h(c) = \operatorname{Res}(f(x_1, c), g(x_1, c), x_1)$ a díky Důsledku 30 má $f(x_1, c)$ a $g(x_1, c)$ společný kořen. □

4.3 Důkaz tvrzení o rozšíření

Nejprve dokážeme tvrzení o rozšíření pro případ, kdy je ideál generovaný dvěma polynomy.

Tvrzení 32 (tvrzení o rozšíření pro dva polynomy). *Nechť k je algebraicky uzavřené těleso a $I = \langle f, g \rangle \subset k[x_1, \dots, x_n]$. Dále nechť*

$$\begin{aligned} f &= a_0 x_1^l + \dots + a_l, & a_0 &\neq 0, \\ g &= b_0 x_1^m + \dots + b_m, & b_0 &\neq 0, \end{aligned}$$

kde $a_i, b_i \in k[x_2, \dots, x_n]$. Předpokládejme, že máme částečné řešení $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$. Pokud $(c_2, \dots, c_n) \notin \mathbf{V}(a_0, b_0)$, pak existuje $c_1 \in k$ takové, že $(c_1, \dots, c_n) \in \mathbf{V}(I)$.

Důkaz. Označme $c = (c_2, \dots, c_n)$. Z Tvzení 29 víme, že $\text{Res}(f, g, x_1) \in I_1$, tedy se nuluje na c . Z předpokladu víme, že $c \notin \mathbf{V}(a_0, b_0)$, tedy bez újmy na obecnosti předpokládejme, že $a_0(c) \neq 0$. Pokud $b_0(c) \neq 0$ pak použijeme Tvzení 31 a máme dokázáno.

Pokud $b_0(c) = 0$, tak nalezneme N dostatečně velké, aby $x_1^N f$ mělo větší stupeň v x_1 než g . Pak vedoucí koeficient polynomu $g + x_1^N f$ vzhledem k x_1 je a_0 . Použijeme Tvzení 31 na polynomy f a $g + x_1^N f$ a dostaneme $c_1 \in k$ takové, že $(c_1, c) \in \mathbf{V}(f, g + x_1^N f)$. Jelikož ale $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$, tak $(c_1, c) \in \mathbf{V}(f, g)$ a máme dokázáno. $\square$

Tvrzení 33 (tvrzení o rozšíření). *Nechť k je algebraicky uzavřené těleso a $I = \langle f_1, \dots, f_s \rangle$ je ideál $k[x_1, \dots, x_n]$. Pro každé $1 \leq i \leq s$ napišme f_i ve tvaru*

$$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} + \text{členy, ve kterých má } x_1 \text{ stupeň} < N_i,$$

kde $N_i \geq 0$ a $g_i \in k[x_2, \dots, x_n]$ je nenulové. Dále necht' máme částečné řešení $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$. Pokud $(c_2, \dots, c_n) \notin \mathbf{V}(g_1, \dots, g_s)$, pak existuje $c_1 \in k$ takové, že $(c_1, \dots, c_n) \in \mathbf{V}(I)$.

Důkaz. Označme $c = (c_2, \dots, c_n)$. Chceme nalézt společný kořen c_1 pro všechny $f_1(x_1, c), \dots, f_s(x_1, c)$. Díky předchozímu tvrzení zbývá dokázat pro případ $s \geq 3$.

Jelikož $c \notin \mathbf{V}(g_1, \dots, g_s)$ tak můžeme bez újmy na obecnosti předpokládat, že $g_1(c) \neq 0$.

Uvažme polynom $u_2 f_2 + \dots + u_s f_s \in k[u_2, \dots, u_s, x_1, \dots, x_n]$. Pak platí, že $\text{Res}(f_1, u_2 f_2 + \dots + u_s f_s, x_1)$ je polynom v $k[u_2, \dots, u_s, x_2, \dots, x_n]$. Rozepíšme ho tedy podle mocnin u_i a dostaneme

$$\text{Res}(f_1, u_2 f_2 + \dots + u_s f_s, x_1) = \sum_{\alpha} h_{\alpha} u^{\alpha},$$

kde $h_{\alpha} \in k[x_2, \dots, x_n]$. Ukážeme, že $h_{\alpha} \in I$, tedy bude platit $h_{\alpha} \in I_1$.

Máme, že

$$A f_1 + B(u_2 f_2 + \dots + u_s f_s) = \text{Res}(f_1, u_2 f_2 + \dots + u_s f_s, x_1), \quad (4.3)$$

kde $A, B \in k[u_2, \dots, u_s, x_1, \dots, x_n]$. Rozložíme $A = \sum_{\alpha} A_{\alpha} u^{\alpha}$ a $B = \sum_{\beta} B_{\beta} u^{\beta}$, kde $A_{\alpha}, B_{\beta} \in k[x_1, \dots, x_n]$. Označme $e_i \in k^{s-1}$ vektor samých nul s jedničkou pozici $i - 1$. Pak můžeme psát $u_2 f_2 + \dots + u_s f_s = \sum_{i \geq 2} u^{e_i} f_i$. Dosazením do rovnice 4.3

dostáváme:

$$\begin{aligned}
\sum_{\alpha} h_{\alpha} u^{\alpha} &= \left(\sum_{\alpha} A_{\alpha} u^{\alpha} \right) f_1 + \left(\sum_{\beta} B_{\beta} u^{\beta} \right) \left(\sum_{i \geq 2} u^{e_i} f_i \right) \\
&= \sum_{\alpha} (A_{\alpha} f_1) u^{\alpha} + \sum_{i \geq 2, \beta} B_{\beta} f_i u^{\beta + e_i} \\
&= \sum_{\alpha} (A_{\alpha} f_1) u^{\alpha} + \sum_{\alpha} \left(\sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_{\beta} f_i \right) u^{\alpha} \\
&= \sum_{\alpha} \left(A_{\alpha} f_1 + \sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_{\beta} f_i \right) u^{\alpha}.
\end{aligned}$$

Porovnáním koeficientů dostáváme

$$h_{\alpha} = A_{\alpha} f_1 + \sum_{\substack{i \geq 2, \beta \\ \beta + e_i = \alpha}} B_{\beta} f_i,$$

tedy $h_{\alpha} \in I$ pro všechna α .

Jelikož $c \in \mathbf{V}(I_1)$, tak $h_{\alpha}(c) = 0$ pro všechna α . Tedy pokud označíme $h = \text{Res}(f_1, u_2 f_2 + \dots + u_s f_s, x_1)$, tak $h(c, u_2, \dots, u_s) = 0$.

Nyní předpokládejme bez újmy na obecnosti, že $g_2(c) \neq 0$ a f_2 má v x_1 větší stupeň než $f_3, \dots, f_s$. Pokud by předpoklad neplatil tak místo f_2 uvažíme polynom $f_2 + x_1^N f_1$ pro N dostatečně velké, aby splňovalo tento předpoklad. Pokud nalezneme společný kořen pro $f_1(x_1, c), f_2(x_1, c) + x_1^N f_1(x_1, c), f_3(x_1, c), \dots, f_s(x_1, c)$ pak ten samý prvek je společným kořenem pro všechna $f_i(x_1, c)$.

Díky tomuto předpokladu máme

$$h(c, u_2, \dots, u_s) = \text{Res}(f_1(x_1, c), u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c), x_1).$$

Platí totiž, že jsou-li oba vedoucí koeficienty polynomů z resultantu vzhledem k x_1 nenulové, tak obě strany jsou determinantom stejné matice, kde se pouze dosadí buď přímo do matice nebo až do determinantu jako polynomu.

Celkově tedy máme

$$\text{Res}(f_1(x_1, c), u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c), x_1) = 0,$$

kde $f_1(x_1, c), u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c), x_1 \in k[x_1, u_2, \dots, u_s]$. Dle Tvzení 29 mají tyto polynomy společného dělitele F nekonstantního v x_1 . Protože F dělí $f_1(x_1, c)$, tak $F \in k[x_1]$. Protože F dělí $u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c)$ tak máme

$$F(x_1) A(x_1, u_2, \dots, u_s) = u_2 f_2(x_1, c) + \dots + u_s f_s(x_1, c),$$

kde $A \in k[x_1, u_2, \dots, u_s]$. Pokud rozepíšeme A podle mocnin u_i a porovnáme koeficienty, tak snadno vidíme, že F dělí všechna $f_i(x_1, c)$.

Nyní stačí vzít libovolný kořen F , jehož existenci nám zaručuje předpoklad, že k je algebraicky uzavřené, a tento kořen je kořenem pro všechna $f_i(x_1, c)$. □

Jako poslední věc uvedeme jednoduchý, ale užitečný důsledek tvrzení o rozšíření.

Tvrzení 34. *Nechť k je algebraicky uzavřené těleso a $I = \langle f_1, \dots, f_s \rangle$ je ideál $k[x_1, \dots, x_n]$. Necht' pro nějaké $1 \leq i \leq s$ je f_i tvaru*

$$f_i = cx_1^{N_i} + \text{členy, ve kterých má } x_1 \text{ stupeň} < N_i,$$

kde $c \in k$ je nenulové a $N_i \geq 0$. Dále necht' máme částečné řešení $(c_2, \dots, c_n) \in \mathbf{V}(I_1)$. Pak existuje $c_1 \in k$ takové, že $(c_1, \dots, c_n) \in \mathbf{V}(I)$.

Důkaz. Aplikujeme-li podmínku na znění tvrzení o rozšíření, dostáváme $g_i = c \neq 0$. Tedy nutně $\mathbf{V}(g_1, \dots, g_s) = \emptyset$ a každé částečné řešení má rozšíření.

□

5. Příklady

V této kapitole ilustrujeme na řešených příkladech aplikaci studované teorie. Protože výpočet Groebnerovy báze je početně náročný, předvedeme ho pouze v prvním příkladu a v ostatních příkladech použijeme k výpočtu matematický software (konkrétně Wolfram Mathematica 10.4).

5.1 Řešení polynomiálních soustav

Jako první příklad vyřešíme soustavu tří polynomů o třech neznámých pomocí tvrzení o eliminaci.

Příklad 1. *Najděte všechna řešení soustavy*

$$\begin{aligned}x^2 + y^2 + z^2 &= 4, \\x^2 + 2y^2 &= 5, \\xz &= 1,\end{aligned}$$

nad tělesem $\mathbb{C}$.

Nejprve pro zjednodušení odečteme od druhé rovnice první. Označme

$$\begin{aligned}f_1 &= x^2 + y^2 + z^2 - 4, \\f_2 &= y^2 - z^2 - 1, \\f_3 &= xz - 1\end{aligned}$$

a nalezneme Grobnerovu bázi ideálu $I = \langle f_1, f_2, f_3 \rangle$. Budeme postupovat podle Buchbergerova algoritmu, tedy nejprve spočteme S-polynomy pro všechny dvojice f_i a jejich zbytky po dělení f_1, f_2, f_3 . Nejprve spočteme

$$S(f_1, f_2) = \frac{x^2 y^2}{x^2} f_1 - \frac{x^2 y^2}{y^2} f_2 = x^2 z^2 + x^2 + y^4 + y^2 z^2 - 4y^2.$$

Odečtením násobku f_1 dostáváme

$$S(f_1, f_2) - (z^2 + 1)f_1 = y^4 - 5y^2 - z^4 + 3z^2 + 4.$$

Odečtením násobku f_2 dostáváme

$$S(f_1, f_2) - (z^2 + 1)f_1 - (y^2 + z^2 - 4)f_2 = 0.$$

Tedy $S(f_1, f_2) \in I$ a nemusíme ho přidávat do báze.

Dále spočteme

$$S(f_2, f_3) = \frac{xzy^2}{y^2} f_2 - \frac{xzy^2}{xz} f_3 = xz + xz^3 - y^2.$$

Stejným postupem dostaneme

$$S(f_2, f_3) = f_2 - (z^2 + 1)f_3$$

Tedy i $S(f_1, f_2) \in I$ a nemusíme ho přidávat do báze.

Nakonec spočtíme

$$S(f_1, f_3) = \frac{x^2 z}{x^2} f_1 - \frac{x^2 z}{xz} f_3 = x - y^2 z + z^3 - 4z.$$

Po odečtení násobku f_2

$$S(f_1, f_3) - z f_2 = x - 3z + 2z^2,$$

už není žádný člen dělitelný vedoucími koeficienty f_1, f_2, f_3 , tedy označíme

$$f_4 = x - 3z + 2z^2,$$

a přidáme ho do báze.

Dále si všimneme, že f_1 se po vydělení ostatními polynomy rozkládá na

$$f_1 = x f_4 + 3 f_3 - 2 z^2 f_3 + f_2,$$

tedy leží v ideálu generovaném f_2, f_3, f_4 a můžeme ho tedy z báze vynechat. Navíc úpravou $f_3 - z f_4 = -2z^4 + 3z^2 - 1$ můžeme odstranit x z polynomu f_3 . Označme

$$\begin{aligned} g_1 &= f_4 = x - 3z + 2z^2, \\ g_2 &= f_2 = y^2 - z^2 - 1, \\ g_3 &= -f_3 + z f_4 = 2z^4 - 3z^2 + 1. \end{aligned}$$

Stejným postupem jako výše bychom zjistili, že všechny S-polynomy leží v $I = \langle g_1, g_2, g_3 \rangle$, tedy $G = \{g_1, g_2, g_3\}$ je Groebnerova báze ideálu I .

Použitím Tvzení o eliminaci 24 dostáváme $I \cup k[z] = \langle g_3 \rangle = \langle (z^2 - 1)(z^2 - \frac{1}{2}) \rangle$. Tedy $z \in \{\pm 1, \pm 1 \setminus \sqrt{2}\}$. Dosazením do zbývajících rovnic snadno dostáváme, že všechna řešení jsou tvaru:

$$\left[1, \pm\sqrt{2}, -1\right], \left[-1, \pm\sqrt{2}, 1\right], \left[\frac{\sqrt{2}}{2}, \pm\frac{\sqrt{6}}{2}, \sqrt{2}\right], \left[-\frac{\sqrt{2}}{2}, \pm\frac{\sqrt{6}}{2}, -\sqrt{2}\right].$$

Příklad 2. Určte maximum a minimum funkce $f(x, y, z) = xyz$ na množině určené podmínkami

$$x^2 + y^2 + z^2 = 1, \quad x + y + z = 0.$$

Označme $f_1(x, y, z) = x^2 + y^2 + z^2 - 1$ a $f_2(x, y, z) = x + y + z$. Bez ověření uvedeme, že zadaná množina je kompaktní. Funkce f, f_1, f_2 mají parciální derivace všech řádů. Máme

$$\nabla f_1 = (2x, 2y, 2z), \nabla f_2 = (1, 1, 1),$$

tedy gradienty jsou lineárně závislé pouze pokud $x = y = z$. Taková situace však nastává díky druhé rovnosti pouze v případě, že jsou rovny nule a tento bod nesplňuje první rovnost. Všechna přípustná řešení jsou tedy stacionární body funkce

$$xyz - \lambda_1 f_1 - \lambda_2 f_2.$$

Parciálním derivováním tedy dostáváme následující soustavu:

$$\begin{aligned}yz - 2\lambda_1 x - \lambda_2 &= 0, \\xz - 2\lambda_1 y - \lambda_2 &= 0, \\xy - 2\lambda_1 z - \lambda_2 &= 0.\end{aligned}$$

Polynomy z této soustavy spolu s f_1, f_2 tvoří ideál $I \subset \mathbb{C}[\lambda_1, \lambda_2, x, y, z]$. Groebnerova báze ideálu I je tvořena následujícími polynomy:

$$\begin{aligned}g_1 &= 4\lambda_1 - 6z^3 + 3z, \\g_2 &= 6\lambda_2 + 1, \\g_3 &= x + y + z, \\g_4 &= 2y^2 + 2yz + 2z^2 - 1, \\g_5 &= 12yz^2 - 2y + 6z^3 - z, \\g_6 &= 18z^4 - 15z^2 + 2.\end{aligned}$$

Díky Tvrzení o eliminaci 24 víme, že $I_4 = \langle g_6 \rangle$. Protože $g_6 = (3z^2 - 2)(6z^2 - 1)$, tak $z \in \{\pm 1/\sqrt{6}, \pm 2/\sqrt{6}\}$. Dosazením do g_5 a g_6 dostáváme

$$\begin{aligned}g_5(y, \pm 1/\sqrt{6}) &= \pm\sqrt{6} + 6y, \\g_5(y, \pm 2/\sqrt{6}) &= 0, \\g_6(y, \pm 1/\sqrt{6}) &= 1/3 \pm 4/\sqrt{6}y + 2y^2, \\g_6(y, \pm 2/\sqrt{6}) &= -2/3 \pm 2/\sqrt{6}y + 2y^2,\end{aligned}$$

přičemž společná řešení jsou právě

$$\begin{aligned}\left[-\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}\right], \left[-\frac{1}{\sqrt{6}}, \frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}}\right], \left[\frac{2}{\sqrt{6}}, -\frac{1}{\sqrt{6}}, -\frac{1}{\sqrt{6}}\right], \\ \left[\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}}\right], \left[\frac{1}{\sqrt{6}}, -\frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}}\right], \left[-\frac{2}{\sqrt{6}}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}\right],\end{aligned}$$

kde x jsme dopočítali z g_3 . Z tvaru g_1, g_2 je zřejmé, že k těmto řešením existují příslušné λ_1, λ_2 , tedy toto jsou právě všechna řešení původní soustavy.

Tedy první tři řešení jsou maxima funkce xyz o hodnotě $1/(3\sqrt{6})$ a zbylé tři jsou minima o hodnotě $-1/(3\sqrt{6})$.

Řešit tuto soustavu běžným způsobem by bylo mnohem snažší. Tento způsob má však výhodu, že ho lze automatizovat a lze použít i při větších soustavách, které by byly pro člověka neupočitatelné.

5.2 Implicitace

V této části předvedeme příklady na aplikaci Tvrzení o rozšíření 33. K těmto příkladům však budeme nejprve potřebovat následující tvrzení které uvedeme bez důkazu.

Tvrzení 35. *Nechť k je nekonečné těleso a $F : k^m \longrightarrow k^n$ funkce definovaná polynomiální parametrizací*

$$\begin{aligned}x_1 &= f_1(t_1, \dots, t_m), \\&\vdots \\x_n &= f_n(t_1, \dots, t_m).\end{aligned}$$

Dále necht' $I = \langle x_1 - f_1, \dots, x_n - f_n \rangle$ je ideál $k[t_1, \dots, t_m, x_1, \dots, x_n]$. Pak $\mathbf{V}(I_m)$ je nejmenší algebraická množina v k^n obsahující $F(k^m)$.

Příklad 3. *Nechť S je parametrická plocha*

$$\begin{aligned}x &= uv, \\y &= uv^2, \\z &= u^2.\end{aligned}$$

Najděte nad $\mathbb{C}$ nejmenší algebraickou množinu V obsahující S . Nalezněte všechny body V které nenáleží S .

Označme $f_1 = x - uv$, $f_2 = y - uv^2$, $f_3 = z - u^2$ a $I = \langle f_1, f_2, f_3 \rangle$. Groebnerova báze ideálu I vzhledem k $u > v > x > y > z$ je

$$\begin{aligned}g_1 &= u^2 - z, \\g_2 &= uv - x, \\g_3 &= ux - vz, \\g_4 &= uy - x^2, \\g_5 &= v^2z - x^2, \\g_6 &= vx - y, \\g_7 &= vyz - x^3, \\g_8 &= x^4 - y^2z.\end{aligned}$$

Tedy $I_2 = \langle g_8 \rangle = \langle x^4 - y^2z \rangle$ a dle Tvrzení 35 je $V = \mathbf{V}(x^4 - y^2z)$ nejmenší algebraická množina obsahující S .

Chceme nalézt body z V , které nelze rozšířit tak, aby náležely $\mathbf{V}(I)$. Nejprve se pokusíme, pomocí Tvrzení o rozšíření 33, nalézt body které nelze rozšířit na $\mathbf{V}(I_1)$. Jelikož $I_1 = \langle v^2z - x^2, vx - y, vyz - x^3, x^4 - y^2z \rangle$, tak g_i z tvrzení jsou z, x a yz . Pouze body V ležící v $\mathbf{V}(x, yz, z) = [0, c, 0]$, kde $c \in \mathbb{C}$, nemají zaručené rozšíření. Díky g_6 víme, že pokud $x = 0$ tak $y = 0$. Pro $c \neq 0$ tedy neexistuje rozšíření a pro $c = 0$ funguje například rozšíření $[0, 0, 0, 0]$.

Pro rozšíření na celé $V(I)$ stačí použít Důsledek 33, protože g_1 má konstantní koeficient před nejvyšší mocninou u .

Jediné body V co nepatří do S jsou tedy body tvaru $[0, c, 0]$ pro c nenulové.

Příklad 4. *Enneprova plocha S je definována parametricky rovnicemi*

$$\begin{aligned}x &= 3u + 3uv^2 - u^3, \\y &= 3v + 3u^2v - v^3, \\z &= 3u^2 - 3v^2.\end{aligned}$$

Najděte nad $\mathbb{C}$ nejmenší algebraickou množinu V obsahující S . Ukažte, že všechny body V náležejí S .

Označme $f_1 = 3u + 3uv^2 - u^3$, $f_2 = 3v + 3u^2v - v^3$, $f_3 = 3u^2 - 3v^2$ a $I = \langle f_1, f_2, f_3 \rangle$. Groebnerova báze ideálu I vzhledem k $u > v > x > y > z$ je

$$\begin{aligned}
g_1 &= 3u^2 - 3v^2 - z, \\
g_2 &= 9u + 6uv^2 - 3x - uz, \\
g_3 &= -9v^2x + 9uvy + 18uz - 6xz - 2uz^2, \\
g_4 &= 3vx - 3uy + 4uvz, \\
g_5 &= 9ux - 9vy - 9z + 6v^2z + z^2, \\
g_6 &= -27vxy + 27uy^2 - 36v^2xz + 72uz^2 - 24xz^2 - 8uz^3, \\
g_7 &= 3v + 2v^3 - y + vz, \\
g_8 &= 648x^2 + 243v^2x^2 - 648y^2 - 243v^2y^2 - 1944z - 1296v^2z + 108x^2z + \\
&\quad 324vyz + 135y^2z + 108z^2 - 108vyz^2 + 48z^3 - 4z^4, \\
g_9 &= 27vx^2 - 27vy^2 - 27yz + 54v^2yz + 72vz^2 - 9yz^2 + 8vz^3, \\
g_{10} &= -27x^2 + 27y^2 + 81z + 54v^2z - 54vyz - 18z^2 + 18v^2z^2 + z^3, \\
g_{11} &= 69984vx^2 + 2187vx^4 + 69984x^2y - 729x^4y - 69984vy^2 - 69984y^3 + \\
&\quad 5832x^2y^3 - 2187vy^4 - 5103y^5 - 279936yz - 23328x^2yz + 139968vy^2z + \\
&\quad 5832y^3z + 8748vy^4z + 186624vz^2 + 93312yz^2 - 7047x^2yz^2 - 11664vy^2z^2 + \\
&\quad 1215y^3z^2 + 20736vz^3 + 5184yz^3 - 189x^2yz^3 + 3240vy^2z^3 - 945y^3z^3 - \\
&\quad 15552vz^4 + 216yz^4 + 648vy^2z^4 - 3456vz^5 + 288yz^5 - 192vz^6 + 8yz^6, \\
g_{12} &= -729x^4 + 4374vx^2y + 5832x^2y^2 - 4374vy^3 - 5103y^4 + 2187x^2z - \\
&\quad 19683y^2z + 8748vy^3z - 2430x^2z^2 + 17496vyz^2 + 972y^2z^2 + 5832z^3 - \\
&\quad 189x^2z^3 + 5184vyz^3 - 945y^2z^3 - 648z^4 + 648vyz^4 - 72z^5 + 8z^6, \\
g_{13} &= 81vx^2 + 81x^2y - 81vy^2 - 81y^3 + 27vx^2z - 324yz + 135vy^2z + 216vz^2 + \\
&\quad 96vz^3 - 12yz^3 + 8vz^4, \\
g_{14} &= -2187x^4 + 4374x^2y^2 - 2187y^4 + 6561x^2z - 729x^4z - 6561y^2z + \\
&\quad 5832x^2y^2z - 5103y^4z - 5103x^2z^2 + 17496vyz^2 - 16767y^2z^2 + 8748vy^3z^2 + \\
&\quad 17496z^3 - 2997x^2z^3 + 17496vyz^3 + 81y^2z^3 + 3888z^4 - 189x^2z^4 + \\
&\quad 5832vyz^4 - 945y^2z^4 - 864z^5 + 648vyz^5 - 48z^6 + 8z^7, \\
g_{15} &= 19683x^6 - 59049x^4y^2 + 59049x^2y^4 - 19683y^6 - 59049x^4z + 118098x^2y^2z - \\
&\quad 59049y^4z + 118098x^4z^2 - 118098y^4z^2 - 314928x^2z^3 + 10935x^4z^3 - \\
&\quad 314928y^2z^3 + 56862x^2y^2z^3 + 10935y^4z^3 + 174960x^2z^4 - 174960y^2z^4 - \\
&\quad 419904z^5 + 34992x^2z^5 + 34992y^2z^5 + 1296x^2z^6 - 1296y^2z^6 + 10368z^7 - \\
&\quad 64z^9.
\end{aligned}$$

Jediný polynom neobsahující ani u , ani v , je g_{15} . Tedy $I_1 = \langle g_{15} \rangle$ a dle Tvrzení 35 je $V = \mathbf{V}(g_{15})$ nejmenší algebraická množina obsahující S .

Polynom g_7 má konstantní koeficient 2 před nejvyšší mocninou v a polynom g_1 má konstantní koeficient 3 před nejvyšší mocninou u . Tedy dvakrát po sobě použijeme Důsledek 33 a máme, že každý bod z V má rozšíření v $\mathbf{V}(I)$. Tedy všechny body V náležejí S .

Závěr

Pomocí základů algebraické geometrie, obecných algebraický vět a resultantů jsme ve čtvrté kapitole formulovali a dokázali Tvzení o rozšíření. Pomocí monomických uspořádání, algoritmu dělení a především pojmu Groebnerovy báze jsme v téže kapitole dokázali Tvzení o eliminaci. Nakonec jsme obě tvrzení využili dohromady při řešení úloh v poslední kapitole.

Seznam použité literatury

BUCHBERGER, B. (1985). *Groebner bases: an algorithmic method in polynomial ideal theory*.

COX, D., LITTLE, J. a O'SHEA, D. (1996). *Ideals, varieties and algorithms*. Springer.

FULTON, W. (1969). *Algebraic curves*.

STANOVSKÝ, D. (2009). *Základy Algebry*. matfyzpress.