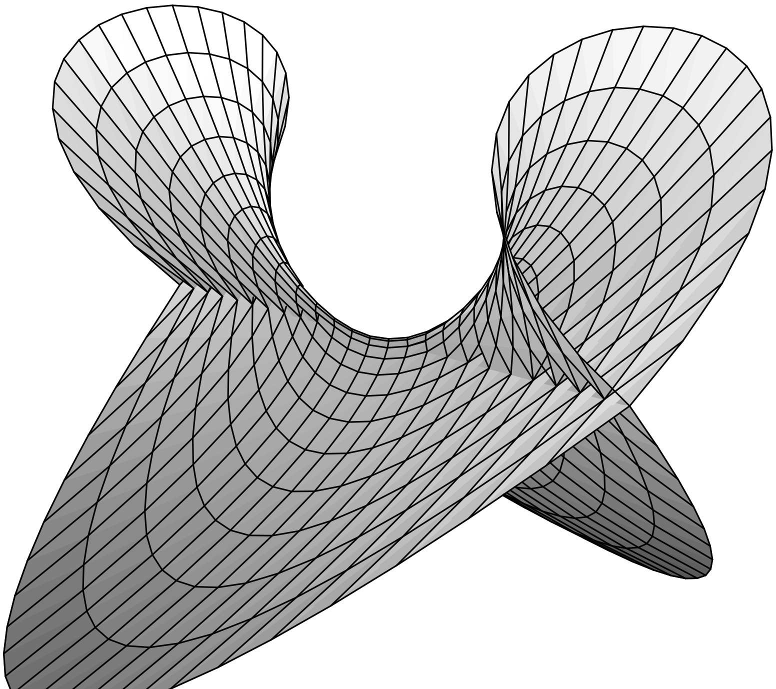
Jan Slovák

Geometrické algoritmy II.

Polynomiální objekty

zápisky z přednášek zpracoval Aleš Křenek



Obsah

Poznámka úvodem

Druhá část přednášky geometrické algoritmy je daleko bližší „čisté“ matematické teorii než část předchozí. S tím jistě souvisí pozorovaná nechuť podstatné části studentů informatiky tuto část studovat. Věřím však, že právě uvažování nad matematickým formalismem účinně tříbí analytické schopnosti, proto jsem po úvahách o vesměs lineárně zadaných objektech v první části přednášky zvolil právě matematicky podstatně náročnější teorii popisující algoritmický přístup k problémům spojeným s vzájemnou polohou objektů zadaných algebraickými rovnicemi.

Ústředním pojmem a nástrojem jsou zde tzv. Gröbnerovy báze a algoritmus pro jejich sestrojení. Tím zároveň podávám úvod do algoritmického přístupu ke komutativní algebře a elementární algebraické geometrii a představuje se tak jeden ze základních pilířů každé současné implementace tzv. počítačové algebry. Pro jednoduchost nevychází text z rámce okruhů polynomů více proměnných nad reálnými nebo komplexními skaláry. Užitečnost odvozených výsledků se snažím předvést na (algoritmickém) řešení praktických aplikací (řešení a řešitelnost systémů algebraických rovnic, implicitizace parametrických popisů variet, singularity a obálky algebraických křivek, algebraické (počítačové) důkazy geometrických tvrzení). Věřím, že studium těchto textů přispěje k vzdělání studentů, kteří si k této problematice najdou cestu.

Těžkého úkolu sepsání těchto učebních textů se ujal pan Aleš Křenek, touto cestou mu moc děkuji. Tak jako v předchozí části, texty vznikly na základě mých přednášek prakticky bez mojí další účasti a podle mého názoru se Aleš svého úkolu zhostil výborně. Samozřejmě, za obsahovou stránku musím ručit sám. Jakékoli komentáře, dotazy, výhrady apod. posílejte prosím na adresu `slovakmath.muni.cz`.

Brno 1995, Jan Slovák

1 Afinní variety

V této a několika následujících kapitolách se budeme zabývat formálním aparátem, který může mít mnoho aplikací všude, kde se pracuje s objekty nebo ději popsatelnými polynomy, resp. systémy polynomiálních rovnic.

Jedná se například o

- Hledání příslušnosti bodu k nějakému tělesu
- Hledání extrémů na ploše
- Analýza pohybů součástí nějakého stroje atd.

1.1 Základní pojmy

Přistupme nejprve k formálnímu aparátu, konkrétních aplikací se snad dočkáme později.

1.1 Definice. *Monomem* v proměnných $x_1, \dots, x_n$ nad polem k nazveme výraz $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, kde $\alpha_i \in \mathbb{N}$. Za stupeň tohoto monomu (značíme $\deg x_1^{\alpha_1} \cdots x_n^{\alpha_n}$) považujeme číslo $\alpha_1 + \cdots + \alpha_n$.

Zavádíme pojem *multiindexu* pro $\alpha = (\alpha_1, \dots, \alpha_n)$ a pro zjednodušŝení píšeme $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ a $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Polynomem v proměnných $x_1, \dots, x_n$ nad polem k rozumíme

$$\sum_\alpha a_\alpha x^\alpha \quad \text{kde } a_\alpha \in k \text{ a suma je konečná}$$

Množinu všech polynomů v proměnných $x_1, \dots, x_n$ nad polem k označíme $k[x_1, \dots, x_n]$. Sčítání na ní je vcelku zřejmé (u stejných monomů se sečtou koeficienty v k), násobení definujeme takto

$$(ax^\alpha) \cdot (bx^\beta) := (ab)x^{\alpha+\beta}$$

Tím jsme definovali strukturu okruhu[1]. Za stupeň polynomu považujeme maximum stupňů jeho monomů v daném uspořádání multiindexů.

To bylo jistě pouhé opakování z algebry, přistupme dále.

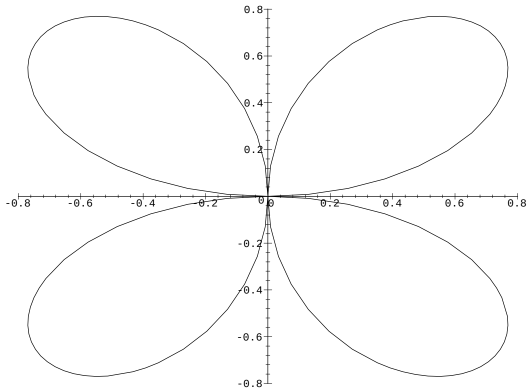
1.2 Definice. *Afinním n-rozměrným prostorem* rozumíme $k^n = \underbrace{k \times \cdots \times k}_{n}$ se standardní afinní strukturou.

Polynom $f = \sum_\alpha a_\alpha x^\alpha \in k[x_1 \dots, x_n]$ lze pochopitelně přirozeným způsobem chápat jako zobrazení $f\colon k^n \to k$ definované

$$f(u_1, \dots, u_n) := \sum_\alpha a_\alpha u^\alpha \quad \text{kde } u^\alpha = u_1^{\alpha_1} \cdots u_n^{\alpha_n}$$

Platí implikace, že pokud $f \in k[x_1, \dots, x_n]$ je identicky roven 0 (tj. z definice $a_\alpha = 0$ pro každé α), pak je $f\colon k^n \to k$ nulové zobrazení. Obrácení ale nemusí obecně platit,

[1] Nepřítel nechť si samostatně dokáže, že je tomu skutečně tak.



Obr. 1: $\mathfrak{V}((x^2+y^2)^3-4x^2y^2)$

uvažme třeba $k=\mathbb{Z}_2$, $f=x^2-x$. Zřejmě $f(x)=x(x-1)=0$ na $\mathbb{Z}_2$ pro každé x, ale f není nulový polynom.

Ve dvou proměnných stačí vzít $g(x,y)=x^2y+y^2x$. Obecně pro každé prvočíslo p a $a\neq 0$ platí $a^{p-1}=1$ v $\mathbb{Z}_p$, a tedy x^p-x je vždy nulové zobrazení.

1.3 Věta. *Nechť k je nekonečné pole, $f\in k[x_1\dots,x_n]$. Pak $f=0$ v $k[x_1\dots,x_n]$ právě tehdy, když $f\colon k^n\to k$ je nulové zobrazení.*

Důkaz: Indukcí podle n. Je-li $n=1$, pak má každý polynom stupně $r>0$ nejvýše r kořenů. Pokud je f nulové zobrazení, musel by polynom mít nekonečně mnoho kořenů, a tedy je stupně 0 nebo nulový. Konstantní polynom, který je nulovým zobrazením, ovšem musí být nutně nulový.

Indukční krok. Můžeme psát $f=\sum_i g_i(x_1,\dots,x_{n-1})x_n^i$. Pro pevně zvolené hodnoty $x_1,\dots,x_{n-1}$ je f polynom jedné proměnné, a tedy $g_i(x_1,\dots,x_{n-1})=0$. To platí pro libovolnou volbu $x_1,\dots,x_{n-1}$, tedy g_i jsou nulová zobrazení a podle indukčního předpokladu i nulové polynomy. $\square$

1.4 Důsledek. *Pro nekonečná pole a polynomy $f,g\in k[x_1,\dots,x_n]$ platí*

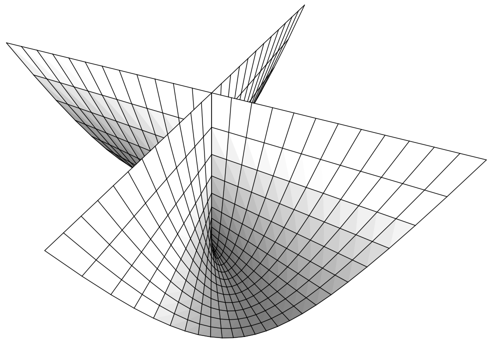
$$f=g \quad \textit{právě tehdy, když } f,g\colon k^n\to k \textit{ jsou stejná zobrazení}$$

1.5 Definice. Nechť $f_1,\dots,f_s\in k[x_1,\dots,x_n]$. *Afinní varietou* v k^n určenou polynomy $f_1,\dots,f_n$ nazveme množinu

$$\mathfrak{V}(f_1,\dots,f_s)=\Big\{(a_1,\dots,a_n)\in k^n \mid f_i(a_1,\dots,a_n)=0;\ i=1,\dots,s\Big\}$$

Afinní variety jsou například všechny kuželosečky, kvadriky a nadkvadriky singulární i regulární. Ze zajímavějších dvourozměrných uveďme čtyřlístek (obr. 1) – varietu $\mathfrak{V}((x^2+y^2)^3-4x^2y^2)$, z trojrozměrných pak obrázek z titulní strany – $\mathfrak{V}(x^2-y^2z^2+z^3)$, *Whitneyho deštník* (obr. 2) – $\mathfrak{V}(x^2z-y^2)$, který obsahuje celou přímku $\{x=0,y=0\}$, a konečně *Enneperovu plochu* (obr. 3).

Varieta určená více polynomy je pak průnik variet jednotlivých polynomů. Tedy například $\mathfrak{V}(x^2+y^2-1,z)$ je kružnice se středem $(0,0,0)$, poloměrem 1 ležící v rovině xy. Dále $\mathfrak{V}(xz,yz)$ je sjednocení přímky $x=0$, $y=0$ a roviny $z=0$, protože pro body těchto dvou útvarů jsou oba polynomy xz,yz nulové.



Obr. 2: Whitneyho deštník

1.6 Věta. *Nechť* $V = \mathfrak{V}(f_1, \ldots, f_s), W = \mathfrak{V}(g_1, \ldots, g_t) \subseteq k^n$ *jsou afinní variety. Potom i* $V \cup W, V \cap W$ *jsou afinní variety a platí*

$$\begin{aligned} V \cap W &= \mathfrak{V}(f_1, \ldots, f_s, g_1, \ldots, g_t) \\ V \cup W &= \mathfrak{V}(f_i g_j) \quad \textit{pro } 1 \leq i \leq s,\ 1 \leq j \leq t \end{aligned}$$

□

Na posledním příkladě se objevuje první problém – jak chápat dimenzi. Stačí zmíněná přímka, aby varieta byla třírozměrná, nebo ji ještě budeme považovat za dvojrozměrnou s jistou anomálií?

V následující části se mimo jiné pokusíme zodpovědět otázky, které se v souvislosti s varietami bezprostředně nabízejí.

1. Platí $\mathfrak{V}(f_1, \ldots, f_s) = \emptyset$?
2. Je $\mathfrak{V}(f_1, \ldots, f_s)$ konečná množina?
3. Jak lze chápat pojem dimenze v případě variet?

Jak se ukáže, tyto problémy lze „rozumně“ řešit pro variety v oboru komplexních čísel (resp. pro všechna algebraicky uzavřená pole), pro čísla reálná je to komplikovanější a velmi zlé pro obecná pole, tj. například racionální čísla[2].

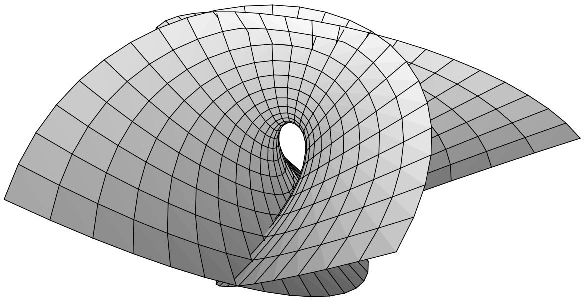
1.2 Parametrizace

Pro některé ryze praktické operace s varietami je vhodné používat implicitní reprezentaci (tedy až dosud používané vyjádření), např. pro zjištění, zda daný bod do variety patří či nikoli, jindy je naopak daleko užitečnější vyjádření parametrické. O co se přesně jedná, ukážeme na příkladech.

$\mathfrak{V}(x+y+z-1, x+2y-z-3)$ udává přímku (průnik dvou rovin). Řešíme-li systém

$$\begin{aligned} x + y + z - 1 &= 0 \\ x + 2y - z - 3 &= 0 \end{aligned}$$

[2]Takové rozhodnutí, zda $\mathfrak{V}(x^n + y^n - z^n) = \emptyset$ vede na velkou Fermatovu větu.



Obr. 3: Enneperova plocha

dostaneme přímo parametrické vyjádření této přímky

$$\begin{aligned} x &= -1 - 3t \\ y &= 2 - 2t \\ z &= t \end{aligned}$$

V následujícím se pokusíme o precizní a obecné vyjádření parametrizace.

1.7 Definice. Nechť k je pole a $f, g \in k[t_1, \dots, t_n]$ polynomy. Pak f/g nazveme *racionální funkcí* nad polem k.

Množina racionálních funkcí rozložená na třídy ekvivalence podle

$$f/g = h/l \iff f \cdot l = g \cdot h \quad \text{v } k[t_1, \dots, t_n]$$

tvoří podílové těleso okruhu polynomů $k[t_1, \dots, t_n]$; značíme $k(t_1, \dots, t_n)$.

1.8 Definice. *Racionální parametrickou reprezentací* variety $\mathfrak{V}(f_1, \dots, f_r) \subseteq k^n$ rozumíme racionální funkce $r_1, \dots, r_n \in k(t_1, \dots, t_s)$ splňující následující podmínky

- Je-li $x_i = r_i(t_1, \dots, t_s)$ pro $i = 1, 2, \dots, n$ pak $(x_1, \dots, x_n) \in \mathfrak{V}(f_1, \dots, f_r)$ pro libovolná $t_1, \dots, t_s$.
- $\mathfrak{V}(f_1, \dots, f_r)$ je minimální afinní varieta obsahující takto dané body $(x_1, \dots, x_n)$.

V této souvislosti se nabízí další otázky.

4. Existuje parametrizace dané variety, resp. lze ji nalézt?
5. Naopak, existuje (lze nalézt) k parametricky zadané varietě implicitní popis?

Obecná odpověď na první z těchto otázek je záporná. V podstatě lze tvrdit, že většinu afinních variet parametrizovat nelze, respektive neexistuje algoritmus parametrizace implicitního popisu. Ty, u kterých se to podaří, nazýváme *neiracionální*[3]. Opět obecně není jednoduché rozhodnout, zda daná varieta je neiracionální. Cesta opačným směrem je v nekonečných polích zvládnutelná, algoritmus předvedeme v kapitole 5.2.

Na první pohled je zřejmé, že pro jednu a tutéž varietu existuje více implicitních, případně i parametrických popisů. Opomeneme-li parametrický popis, nejednoznačnosti implicitního jsou způsobeny pro tento účel nevhodnou reprezentací pomocí několika „generujících“ polynomů.

[3]Přímý překlad anglického *unirational*.

1.3 Ideály

Připomeňme si trochu algebry.

1.9 Definice. Množinu $I \subseteq A$, kde A je okruh, nazveme *ideálem*, platí-li $0 \in I$ a zároveň

$$\begin{aligned} f, g \in I &\implies f + g \in I \\ f \in I, h \in A &\implies f \cdot h \in I \end{aligned}$$

Pojem *generátorů* ideálu je snad zřejmý, připomeňme jen značení $I = \langle a_1, \ldots, a_n \rangle$. Je-li generátorů konečný počet, říkame, že ideál je *konečně generovaný.* Pro varietu $V = \mathfrak{V}(f_1, \ldots, f_s)$ klademe

$$\mathfrak{I}(V) := \Big\{ f \in k[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ pro všechna } (a_1, \ldots, a_n) \in V \Big\}$$

1.10 Věta. *Nechť $f_1, \ldots, f_s, g_1, \ldots, g_t \in k[x_1, \ldots, x_n]$ jsou polynomy. Pak platí*

1. *Jestliže $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, pak $\mathfrak{V}(f_1, \ldots, f_s) = \mathfrak{V}(g_1, \ldots, g_t)$.*
2. *$\mathfrak{I}(V)$ je ideál a platí $\langle f_1, \ldots, f_s \rangle \subseteq \mathfrak{I}(V)$, kde $V = \mathfrak{V}(f_1, \ldots, f_s)$.*

Důkaz:

1. Uvažujme libovolný $(a_1, \ldots, a_n) \in \mathfrak{V}(f_1, \ldots, f_s)$. Pro něj platí

$$f_i(a_1, \ldots, a_n) = 0 \quad \text{pro } i = 1, 2, \ldots, s$$

Protože $g_1, \ldots, g_t \in \langle f_1, \ldots, f_s \rangle$, existují nějaké polynomy $h_{1,1}, \ldots, h_{t,s}$ v n proměnných tak, že

$$g_j = \sum_{i=1}^{s} h_{j,i} \cdot f_i \quad \text{pro } j = 1, 2, \ldots, t$$

Odtud $g_j(a_1, \ldots, a_n) = 0$ pro $j = 1, 2, \ldots, t$. Máme tedy

$$\mathfrak{V}(f_1, \ldots, f_s) \subseteq \mathfrak{V}(g_1, \ldots, g_t).$$

Opačná inkluze se dokáže zcela analogicky.

2. Nechť $g, g' \in \mathfrak{I}(V)$, $h \in k[x_1, \ldots, x_n]$. Potom pro zvolený bod $(a_1, \ldots, a_n) \in V$ platí $g(a_1, \ldots, a_n) = 0$, a tedy

$$\begin{aligned} (g \cdot h)(a_1, \ldots, a_n) = 0 &\implies g \cdot h \in \mathfrak{I}(V) \\ (g + g')(a_1, \ldots, a_n) = 0 &\implies g + g' \in \mathfrak{I}(V) \end{aligned}$$

Proto $\mathfrak{I}(V)$ je ideál. Uvažujme libovolný $f \in \langle f_1, \ldots, f_s \rangle$. Ten lze psát jako

$$f = \sum_{i=1}^{s} h_i \cdot f_i \quad \text{pro nějaká } h_1, \ldots, h_s \in k[x_1, \ldots, x_n]$$

Pro $(a_1, \ldots, a_n) \in V$ je tedy $f(a_1, \ldots, a_n) = 0$. Proto platí $\langle f_1, \ldots, f_s \rangle \subseteq \mathfrak{I}(V)$.

□

Jednoduché příklady:

$$\mathfrak{I}\Big(\{(0,0,\dots,0)\}\Big) = \langle x_1,\dots,x_n\rangle$$
$$\mathfrak{I}(k^n) = \{\ 0\} \quad \text{pro libovolné nekonečné pole } k$$

Inkluze opačná k druhé části věty obecně neplatí. Například varieta $\mathfrak{V}(x^2, y^2)$ má jediný bod – $(0,0)$. $\mathfrak{I}(V)$ je potom $\langle x, y\rangle \supset \langle x^2, y^2\rangle$.
Jsou-li $V, W \subseteq k^n$ variety, pak platí

$$V \subseteq W \implies \mathfrak{I}(V) \supseteq \mathfrak{I}(W)$$

Neboli polynomy, které se nulovaly na nějaké varietě se nutně musí nulovat i na její podmnožině.

Objevují se další problémy

6. Je každý ideál $I \in k[x_1,\dots,x_n]$ konečně generovaný?
7. Lze algoritmicky zjistit, zda $f \in \langle f_1,\dots,f_s\rangle$?
8. Jaký je přesný vztah mezi $\langle f_1,\dots,f_s\rangle$ a $\mathfrak{I}\Big(\mathfrak{V}(f_1,\dots,f_s)\Big)$?

1.4 Dimenze 1

Na všechny výše zmíněné otázky se pokusíme odpovědět nejprve ve zjednodušeném, ale názorném případě polynomů v jedné proměnné. Konvenčně používáme proměnnou x a koeficienty v polynomu značíme

$$f = a_0x^n + a_1x^{n-1} + \cdots + a_n \quad \text{kde } a_0 \neq 0.$$

Vedoucí člen polynomu (*leading term*) definujeme jako $LT(f) := a_0x^n$. Zřejmě platí

$$\deg f \leq \deg g \iff LT(f)|LT(g)$$

1.11 Věta ALGORITMUS DĚLENÍ SE ZBYTKEM. *Nechť k je pole a g nenulový polynom. Pak každé $f \in k[x]$ lze jednoznačně psát jako*

$$f = q\cdot g + r \quad \textit{kde } r = 0 \textit{ nebo } \deg r < \deg g$$

Důkaz: je pochopitelně konstruktivní, podíl q a zbytek r počítá následující algoritmus.
Algoritmus 1.1

1. $q := 0$, $r := f$
2. `while` $r \neq 0 \wedge LT(g)|LT(r)$
   2.1. $q := q + LT(r)/LT(g)$
   2.2. $r := r - LT(r)/LT(g)\cdot g$

Pro průchod cyklem platí invariant $f = q \cdot g + r$, algoritmus tedy dává správný výsledek. Stupeň r se každým průchodem zmenšuje, algoritmus tedy zastaví.

Připusťme, že existují ještě jiná q', r' tak, že $f = q' \cdot g + r'$. Protože stupně r a r' jsou ostře menší než stupeň g, musí platit i $\deg(r - r') < \deg g$ (protože $r \neq r'$, má smysl uvažovat $\deg(r - r')$). Zároveň ale platí

$$\deg(r - r') = \deg(q - q') + \deg g \geq \deg g$$

což je spor. Dvojice q, r je tedy určena jednoznačně. □

1.12 Důsledek. *Je-li k pole, má každý $f \in k[x]$ nejvýše* $\deg f$ *kořenů.*

Důkaz: Je-li $\deg f = 0$ (konstantní polynom), neexistuje žádný kořen. Nechť $\deg f = n > 0$ a f má kořen a. Potom podle věty 1.11 existují q, r tak, že

$$f = q(x - a) + r \quad \text{a zároveň } \deg r = 0 \text{ nebo } r = 0.$$

Protože a je kořen, r nemůže být konstantní a tudíž $f = q(x - a)$. Stupeň q je $n - 1$, podle indukčního předpokladu má nanajvýš $n - 1$ kořenů, a tedy f jich má nejvýše n.
□

1.13 Důsledek. *Nechť k je pole. Pak každý ideál v $k[x]$ je tvaru $\langle f \rangle$.*

Důkaz: Nechť $I \subseteq k[x]$. Pokud $I = \{0\}$, pak $I = \langle 0 \rangle$. Předpokládejme $I \supset \{0\}$ a nechť $f \in I$ je minimálního stupně. Pak zřejmě $\langle f \rangle \subseteq I$.

Naopak uvažujme nějaké $g \in I$. Podle věty 1.11 existují q, r takové, že $g = q \cdot f + r$ a zároveň $\deg r < \deg f$ nebo $r = 0$. Protože $g, f \in I$, platí $q \cdot f \in I$, a tedy $r \in I$. Polynom f byl vybrán s nejmenším stupněm z I, a proto $r = 0$. Odtud už plyne $g \in \langle f \rangle$, a tedy i $I \subseteq \langle f \rangle$. □

1.14 Definice. Nechť $f, g \in k[x]$. *Největším společným dělitelem* polynomů f, g, značíme $GCD(f, g)$, nazveme takový polynom h, že $h|f$, $h|g$ a platí

$$\forall p \in k[x] : p|f \wedge p|g \implies p|h$$

Největšího společného dělitele lze pochopitelně spočítat

Algoritmus 1.2

1. $h := f$, $s := g$
2. `while` $s \neq 0$
   - 2.1. $r :=$ zbytek po dělení h/s
   - 2.2. $h := s$
   - 2.3. $s := r$

Nechť $f = q \cdot g + r$ a $h = GCD(f, g)$. Potom $h|r, g$ a zároveň

$$\forall p \in k[x] : p|r, g \quad \text{tedy } p|f \text{ a } p|h$$

Odtud h je $GCD(r, g)$. Triviálně $GCD(h, 0) = h$, proto algoritmus počítá správně $GCD(f, g)$. Protože stupně r postupně klesají, algoritmus zastaví.

Největší společný dělitel dvou polynomů tedy existuje. Je určen jednoznačně až na násobek skalárem. Dva různé *GCD* se totiž musí dělit navzájem a to je u polynomů možné právě v tomto případě.

Pro korektnost následující věty ještě definujme největšího společného dělitele více než dvou polynomů. Je-li $s > 2$, potom

$$GCD(f_1, \dots, f_s) := GCD\Big(f_1, GCD(f_2, \dots, f_s)\Big)$$

1.15 Věta. *Pro polynomy $f_1, \dots, f_s$ platí $\langle GCD(f_1, \dots, f_s)\rangle = \langle f_1, \dots, f_s\rangle$.*

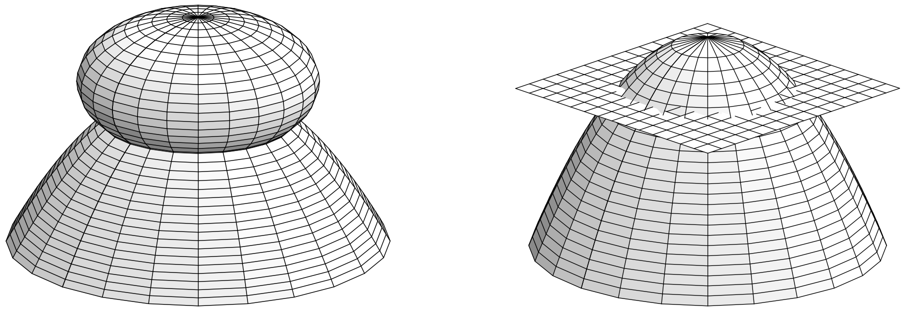
Důkaz: Protože $GCD(f_1, \dots, f_s) | f_1, \dots, f_s$, platí $\langle f_1, \dots, f_s\rangle \subseteq \Big\langle GCD(f_1, \dots, f_s)\Big\rangle$. Naopak přímo z algoritmu výpočtu *GCD* plyne *Bezoutova rovnost,* tj.

$$GCD(f_1, \dots, f_s) = h_1 f_1 + \dots + h_s f_s \quad \text{pro vhodná } h_1, \dots, h_s$$

Odtud již vyplývá opačná inkluze. □

Během kapitoly jsme položili několik otázek. Nyní máme již vše potřebné k jejich zodpovězení pro případ polynomů jedné proměnné.

1. Protože $\mathfrak{V}(f_1, \dots, f_s) = \mathfrak{V}(GCD(f_1, \dots, f_s))$ (důsledek věty 1.10), problém prázdnosti variety se redukuje na problém existence kořene polynomu.
2. Ze stejného důvodu je vždy konečnou množinou izolovaných bodů – kořenů $GCD(f_1, \dots, f_s)$ s jedinou vyjímkou $GCD(f_1, \dots, f_s) = 0$; to nastane pouze v případě, že $f_1 = f_2 = \dots = f_s = 0$. Pak je varietou celá množina k.
3. Pojem dimenze v tomto případě postrádá smysl.
4. Stejně tak není nijak účelné parametrizovat konečnou množinu.
6. Každý ideál je generovatelný jediným polynomem – důsledek věty 1.15.
7. $f \in \langle f_1, \dots, f_s\rangle \iff GCD(f_1, \dots, f_s) | f$ (důsledek věty 1.13).
8. Označíme-li $\langle f\rangle := \mathfrak{I}(\mathfrak{V}(f_1, \dots, f_s))$, pak f a $GCD(f_1, \dots, f_s)$ se mohou lišit pouze násobností kořenů.



Obr. 4: Stejná varieta?

2 Gröbnerovy báze

Jak už bylo řečeno, implicitní reprezentace variety není vždy nejvhodnější. Jen pro $k^3 = \mathbb{R}^3$ je při komplikovanějším zadání obtížné vůbec interpretovat, jak daná varieta vypadá. Znamenalo by to určit průnik obecně i dost komplikovaných útvarů. Demonstrujme na ještě poměrně jednoduchém příkladě. Varieta na obr. 4 vlevo je $\mathfrak{V}(x^2+y^2+z^2-1, x^2+y^2+z)$. V tomto případě lze ještě poměrně snadno určit, že průnikem koule a paraboloidu je kružnice ležící v rovině $z = \frac{1}{2}-\frac{1}{2}\sqrt{5}$, tedy varietu lze stejně dobře vyjádřit jako $\mathfrak{V}(x^2+y^2+z^2-1, z^2-z-1)$, případně $\mathfrak{V}(x^2+y^2+z, z-\frac{1}{2}+\frac{1}{2}\sqrt{5})$ a podobně.

Obrázek 4 a předchozí odstavec nabízí další problém. Jak rozhodnout, zda dvě implicitně zadané variety jsou stejné? Zrovna tak prázdnou varietu (opět v $\mathbb{R}^3$) lze popsat $\mathfrak{V}(x^2+1)$ i $\mathfrak{V}(1)$ nebo dokonce $\mathfrak{V}(x^2+y^2+z^2-1, x^2+y^2+z^2-2)$. Podobným problémem je i určení průniku, odvoláme-li se opět na obr. 4, průnik koule $\mathfrak{V}(x^2+y^2+z^2-1)$ a paraboloidu $\mathfrak{V}(x^2+y^2+z)$ lze vyjádřit jednodušeji jako průnik některého z těchto objektů a roviny.

Většinu těchto problémů poměrně uspokojivě řeší aparát prezentovaný v [1]. Jak se pokusíme ukázat, varietu je vhodnější reprezentovat generujícím ideálem a pro ten se podaří nalézt vyjádření nezávislé na volbě generátorů, resp. předvedeme algoritmus převádějící každou množinu generátorů na jistý jednoznačný kanonický tvar.

2.1 Dělení se zbytkem

U polynomů více proměnných je situace daleko komplikovanější než byla ve větě 1.11. Kupříkladu zde neexistuje přímý ekvivalent pojmu stupně, je nutné definovat ho podstatně opatrněji. Ani pojem vedoucího členu polynomu není zcela přímočarý, je zde nutné volit nějaké uspořádání na proměnných a monomech; celá teorie pak přestává být vůči proměnným symetrická.

Dělení se zbytkem zde znamená vyjádřit $f \in k[x_1, \ldots, x_n]$ jako

$$f = a_1 f_1 + \cdots + a_s f_s + r$$

Například mějme $f = x^2y + xy^2 + y^2$, $f_1 = xy - 1$ a $f_2 = y^2 - 1$. Prvním dělením získáme

$$f = (x + y) \cdot f_1 + (x + y^2 + y)$$

$LT(y^2 - 1)$ nedělí x (vedoucí člen zbytku), a tak bychom teoreticky nemohli pokračovat dál. Přesuneme-li však toto x do zbytku, dostáváme teprve výsledek

$$f = (x + y) \cdot f_1 + f_2 + (x + y + 1)$$

Zde již žádný člen zbytku není dělitelný žádným z $LT(f_1)$, $LT(f_2)$. To je také požadovaná vlastnost na výsledek dělení se zbytkem.

2.1 Definice. Úplné (lineární) dobré (tj. každá neprázdná podmnožina má nejmenší prvek) uspořádání $<$ na $\mathbb{N}_0^n$ splňující

$$\forall \alpha, \beta, \gamma \in \mathbb{Z}^n\colon \alpha < \beta \implies \alpha + \gamma < \beta + \gamma$$

nazveme *monomiálním uspořádáním* na $k[x_1, \ldots, x_n]$.

Takto položená definice není úplná. Uspořádání na $\mathbb{N}_0^n$ indukuje pouze uspořádání na monomech. Každý polynom lze však přeskládat jako klesající posloupnost monomů (na koeficienty teď nehledíme). Uspořádání se na polynomy rozšíří „lexikograficky", tedy větší je ten polynom, který má větší první monom, pokud tak nelze rozhodnou, bere se v potaz druhý monom atd.

Následující tři definice zavádějí nejběžněji užívaná monomiální uspořádání. Všechna se opírají o předem dané uspořádání jednotlivých proměnných, standardně $x_1 > x_2 > \cdots$.

2.2 Definice. *Lexikografické uspořádání* je takové $<_{\text{lex}}$, že pro každé $\alpha, \beta \in \mathbb{N}_0^n$ platí

$$\alpha >_{\text{lex}} \beta \iff \text{Nejlevější nenulový člen v } \alpha - \beta \text{ je kladný}$$

2.3 Definice. *Gradované lexikografické uspořádání* je takové $<_{\text{grlex}}$, že pro každé $\alpha, \beta \in \mathbb{N}_0^n$ platí:

$$\alpha >_{\text{grlex}} \beta \iff \begin{array}{ll} |\alpha| > |\beta| & \text{nebo} \\ |\alpha| = |\beta| & \text{a zároveň } \alpha >_{\text{lex}} \beta \end{array}$$

2.4 Definice. *Gradované opačné lexikografické uspořádání* je takové $<_{\text{grevlex}}$, že pro každé $\alpha, \beta \in \mathbb{N}_0^n$ platí:

$$\alpha >_{\text{grevlex}} \beta \iff \begin{array}{ll} |\alpha| > |\beta| & \text{nebo} \\ |\alpha| = |\beta| & \text{a zároveň nejpravější nenulový člen } (\alpha - \beta) \text{ je záporný} \end{array}$$

Tedy $x_1 >_{\text{grevlex}} x_2 >_{\text{grevlex}} \cdots >_{\text{grevlex}} x_n$, ale pokud $x > y > z$, pak $x^2yz^2 >_{\text{grlex}} xy^3z$, ale $x^2yz^2 <_{\text{grevlex}} xy^3z$.

2.5 Lemma. *$>_{lex}, >_{grlex}, >_{grevlex}$ jsou monomiální uspořádání.*

2.6 Definice. Nechť $f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ je nenulový a $<$ monomiální. Pak definujeme:

- Stupeň $\operatorname{multideg} f := \max\{\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0\}$

- Vedoucí koeficient $LC\,f := a_{\operatorname{multideg} f}$
- Vedoucí monom $LM\,f := x^{\operatorname{multideg} f}$
- Vedoucí člen $LT\,f := LC\,f \cdot LM\,f$

Tyto pojmy jsou tedy pro polynomy více proměnných vesměs silně závislé na volbě konkrétního uspořádání.

2.7 Lemma. *Nechť $f, g \in k[x_1, \ldots, x_n]$ a $<$ je monomiální. Pak*

1. $\operatorname{multideg}(f \cdot g) = \operatorname{multideg} f + \operatorname{multideg} g$
2. $f + g \neq 0 \implies \operatorname{multideg}(f + g) \leq \max\{\operatorname{multideg} f, \operatorname{multideg} g\}$

2.8 Věta Dělení se zbytkem. *Nechť $<$ je monomiální a $F = (f_1, \ldots, f_s)$ s-tice polynomů v $k[x_1, \ldots, x_n]$. Pak každý $f \in k[x_1, \ldots, x_n]$ lze vyjádřit jako*

$$f = a_1 f_1 + \cdots + a_s f_s + r \quad \textit{kde } a_i, r \in k[x_1, \ldots, x_n] \quad \textit{pro } i = 1, 2, \ldots, s$$

a navíc $r = 0$ nebo r je lineární kombinací monomů, z nichž žádný není dělitelný kterýmkoli z $LT\,f_1, \ldots, LT\,f_s$ a pokud $a_i f_i \neq 0$ pak $\operatorname{multideg} f \geq \operatorname{multideg} a_i f_i$ pro každé i. Polynom r nazýváme zbytkem po dělení f/F.

Je zřejmé, že narozdíl od jedné proměnné výsledek dělení se zbytkem není dán jednoznačně ani vzhledem k pevně zvolenému uspořádání monomů. Věta také nic o jednoznačnosti netvrdí, následující algoritmus dává jedno možné řešení. Nadále budeme výsledkem dělení se zbytkem chápat právě jeho výstup.

Algoritmus 2.1

1. $a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
2. `while` $p \neq 0$
   - 2.1. $i := 1$
   - 2.2. $d := \mathit{false}$
   - 2.3. `while` $i \leq s \wedge \mathrm{not}\, d$
     - 2.3.1. `if` $LT\,f_i | LT\,p$
       - 2.3.1.1. $a_i := a_i + LT\,p / LT\,f_i$
       - 2.3.1.2. $p := p - (LT\,p / LT\,f_i) \cdot f_i$
       - 2.3.1.3. $d := \mathit{true}$
     - 2.3.2. `else` $i := i + 1$
   - 2.4. `if` $\mathrm{not}\, d$
     - 2.4.1. $r := r + LT\,p$
     - 2.4.2. $p := p - LT\,p$

Důkaz: Při každém průchodu vnějším cyklem se právě jednou provede právě jeden z příkazů 2.3.1.2, 2.4.2, a tedy stupeň p klesne. Proto algoritmus skončí.

Platí invariant $f = a_1 f_1 + \cdots + p + r$ a přitom každý člen každého a_i je podílem $LT\,p / LT\,f_i$ z nějakého okamžiku. Proto stupeň těchto členů je menší než stupeň p v daném okamžiku a ten je nejvýše roven stupni f. Dohromady stupeň každého $a_i f_i$ je menší nebo roven stupni f. $\square$

V $k[x]$ byl každý ideál tvaru $I = \langle f \rangle$ a algoritmus dělení se zbytkem plně řešil příslušnost k ideálu. Oproti tomu v $k[x_1, \dots, x_n]$ platí pouze implikace

$$f = a_1 f_1 + \cdots + a_s f_s + 0 \implies f \in \langle f_1, \dots, f_s \rangle$$

Obrácení obecně neplatí, uvažujme $f = xy^2 - x$, $f_1 = xy + 1$, $f_2 = y^2 - 1$. Potom algoritmus dělení dá

$$f = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

ale přitom evidentně $f = x(y^2 - 1)$, a tedy $f \in \langle f_1, f_2 \rangle$.

2.2 Monomiální ideály

2.9 Definice. Ideál $I \subseteq k[x_1, \dots, x_n]$ nazýváme *monomiální,* existuje-li množina $A \subseteq \mathbb{N}_0^n$ tak, že I se sestává právě ze všech polynomů tvaru $\sum_{\alpha \in A} h_\alpha x^\alpha$, kde $h_\alpha \in k[x_1, \dots, x_n]$. Potom píšeme $I = \langle x^\alpha \mid \alpha \in A \rangle$.

Zřejmě pro monomiální ideál I platí

$$x^\beta \in I \iff \exists \alpha \in A \colon x^\alpha | x^\beta$$

2.10 Lemma. *Nechť $I \subseteq k[x_1, \dots, x_n]$ je monomiální ideál, $f \in k[x_1, \dots, x_n]$ polynom. Pak následující tvrzení jsou ekvivalentní*

1. *$f \in I$*
2. *Každý člen polynomu f je prvkem I.*
3. *Polynom f je lineární kombinací monomů z I s koeficienty z k.*

Důkaz: Implikace (3) $\implies$ (2) $\implies$ (1) je triviální. Zbývá ukázat (1) $\implies$ (3).

Platí $f = \sum_\alpha a_\alpha x^\alpha \in I$, kde $a_\alpha \in k$. Z předpokladu vyplývá, že lze vyjádřit $f = \sum_{\beta \in A} h_\beta x^\beta$, kde $h_\beta \in k[x_1, \dots, x_n]$. Každý člen $a_\alpha x^\alpha$ se musí rovnat některému členu z druhé rovnosti, tedy existují taková $d \in k, \delta \in \mathbb{N}_0^n$ tak, že $a_\alpha x^\alpha = dx^{\beta+\delta}$. Proto $x^\alpha \in I$, a tedy platí (3). □

2.11 Důsledek. *Dva monomiální ideály splývají právě tehdy, když obsahují stejné monomy.*

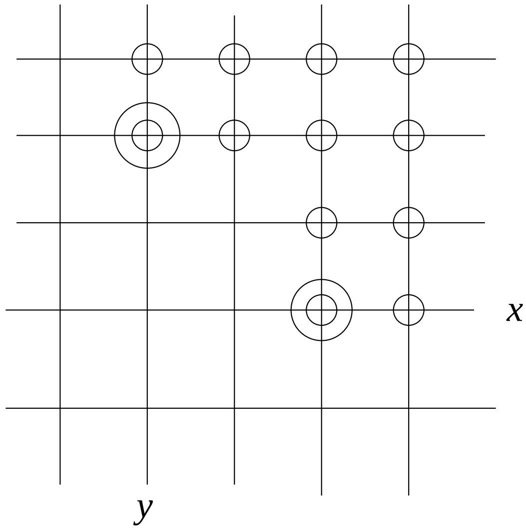
2.3 Dicksonovo lemma

2.12 Věta Dicksonovo lemma. *Každý monomiální ideál $I = \langle x^\alpha \mid \alpha \in A \rangle \subseteq k[x_1, \dots, x_n]$ lze psát ve tvaru $I = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$, kde $\alpha_1, \dots, \alpha_s \in A$.*

Důkaz: Důkaz vedeme indukcí podle počtu proměnných. Nechť $n = 1$. Pak $I \subseteq k[x]$, $I = \langle x^\alpha \mid \alpha \in A \subseteq \mathbb{N}_0 \rangle$. Položme $\beta := \min A$. Potom zřejmě $I = \langle x^\beta \rangle$.

Uvažujme tedy $n > 1$. Pro přehlednost označíme proměnné jako $x_1, \dots, x_{n-1}, y$, monomy potom budou tvaru $x^\alpha y^m$, kde $\alpha \in \mathbb{N}_0^{n-1}$, $m \in \mathbb{N}_0$, a množinu monomů x^β s $\beta \in A$ budeme značit I_A. Předpokládejme, že $I \subseteq k[x_1, \dots, x_{n-1}, y]$ je monomiální. Definujme $J \subseteq k[x_1, \dots, x_{n-1}]$ následovně

$$J := \langle x^\alpha \mid \exists m \in \mathbb{N}_0 \colon x^\alpha y^m \in I_A \rangle$$



Obr. 5: Monomy v ideálu $I = \langle x^3y, xy^3 \rangle \subset \mathbb{R}[x,y]$

Zřejmě J je monomiální ideál v $n-1$ proměnných, a tedy podle indukčního předpokladu lze psát $J = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$. Dále z definice J vyplývá, že existují taková minimální $m_i \in \mathbb{N}_0$ tak, že $x^{\alpha_i} y^{m_i} \in I_A$. Označme tedy $m := \max\{m_i\}$ a definujme analogicky systém ideálů $J_k \subseteq k[x_1, \ldots, x_{n-1}]$ pro $0 \le k \le m-1$

$$J_k := \langle x^\beta \mid x^\beta y^k \in I_A \rangle$$

Opět všechny J_k splňují indukční předpoklad, a tedy je lze vyjádřit

$$J_k = \langle x^{\alpha_{k,1}}, \ldots, x^{\alpha_{k,s_k}} \rangle.$$

Zbývá ukázat, že I je generovaný touto množinou monomů

$$\begin{gathered} x^{\alpha_1} y^m \ldots x^{\alpha_s} y^m \\ x^{\alpha_{0,1}} y^0 \ldots x^{\alpha_{0,s_0}} y^0 \\ \vdots \\ x^{\alpha_{m-1,1}} y^{m-1} \ldots x^{\alpha_{m-1,s_{m-1}}} y^{m-1} \end{gathered}$$

Uvažujme libovolný monom $x^\alpha y^p \in I_A$. Nastane jeden ze dvou případů

- $p \ge m$. Potom jistě $x^\alpha \in J$, a tedy některý z $x^{\alpha_1} y^m, \ldots, x^{\alpha_s} y^m$ dělí $x^\alpha y^p$.
- $p < m$. Potom analogicky $x^\alpha \in J_k$ a některý z $x^{\alpha_{k,1}} y^k, \ldots, x^{\alpha_{k,s_k}} y^k$ dělí $x^\alpha y^p$.

Podle lemmatu 2.10 lze každé $f \in I$ vyjádřit jako lineární kombinaci monomů z I_A, ty jsou již dělitelné některým ze zmíněných generátorů, a tedy f patří do ideálu jimi generovaného. Proto I je jeho podmnožinou.

Opačná inkluze je zcela triviální. $\square$

2.13 Důsledek. *Nechť $<$ je relace na $\mathbb{N}_0^n$ splňující podmínky*

1. *Relace $<$ je úplné uspořádání.*
2. $\alpha < \beta,\ \gamma \in \mathbb{N}_0^n \implies \alpha + \gamma < \beta + \gamma$

Pak $<$ je dobré uspořádání právě tehdy, když $\forall \alpha \in \mathbb{N}_0^n \colon \alpha \geq 0$

Důkaz:

"$\Longrightarrow$" Protože $<$ je dobré, existuje $\alpha_0 \in \mathbb{N}_0^n$ nejmenší. Předpokládejme $\alpha_0 < 0$. Podle podmínky (2) zkonstruujeme nekonečnou posloupnost $0 > \alpha_0 > 2\alpha_0 > \cdots$, což je spor s tím, že $<$ je dobré.

"$\Longleftarrow$" Nechť $\forall \alpha \in \mathbb{N}_0^n \colon \alpha \geq 0$. Uvažme libovolnou množinu $\emptyset \neq A \subseteq \mathbb{N}_0^n$. Potom $I = \langle x^\alpha \mid \alpha \in A \rangle$ je konečně generovaný nějakými monomy $x^{\alpha_1}, \ldots, x^{\alpha_s} \in A$. Bez újmy na obecnosti předpokládejme $\alpha_1 < \cdots < \alpha_s$.

Uvažujme libovolné $\alpha \in A$. Potom nutně $x^{\alpha_i} | x^\alpha$ pro vhodné $i = 1, \ldots, s$, tj. $\alpha = \alpha_i + \gamma$, kde $\gamma \geq 0$ (předpoklad této implikace). Potom ale platí

$$\alpha \geq \alpha_i + 0 \geq \alpha_1$$

a tedy α_1 je nejmenší v A. Protože A byla zvolena libovolně, je uspořádání $<$ dobré.

□

2.4 Hilbertova věta

Je-li $I \subseteq k[x_1, \ldots, x_n]$ nenulový, označme

$$LT\, I := \{ax^\alpha \mid \exists f \in I \colon\ LT\, f = ax^\alpha\}$$

Zřejmě $\langle LT\, I \rangle$ je monomiální, a tedy podle Dicksonova lemmatu lze psát $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$ pro nějaká vhodná $g_1, \ldots, g_s \in I$.

2.14 Věta HILBERTOVA. *Každý ideál $I \in k[x_1, \ldots, x_n]$ je konečně generovaný.*

Důkaz: Pokud by $I = \{0\}$, je tvrzení triviální. Uvažujme tedy $I \supset \{0\}$. Podle Dicksonova lematu a předchozí poznámky existují taková $g_1, \ldots, g_s \in I$, že $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$ Zřejmě $\langle g_1, \ldots, g_s \rangle \subseteq I$. Vezměme libovolné $f \in I$ a proveďme dělení se zbytkem s-ticí $g_1, \ldots, g_s$. Dostáváme

$$f = a_1 g_1 + \cdots + a_s g_s + r \quad \text{kde žádný člen } r \text{ není dělitelný } LT\, g_1, \ldots, LT\, g_s.$$

Protože $r = f - a_1 g_1 - \cdots - a_s g_s$, platí $r \in I$, a tedy $LT\, r \in LT\, I$. Zřejmě tedy $LT\, r \in \langle LT\, I \rangle$. Připusťme, že $r \neq 0$. Protože $\langle LT\, I \rangle$ je monomiální, musí být $LT\, r$ dělitelný některým z jeho generátorů, tj. $LT\, g_1, \ldots, LT\, g_s$. To je ovšem spor s výsledkem algoritmu dělení. Proto $r = 0$ a I je tedy generovaný $g_1, \ldots, g_s$. □

2.15 Definice. Konečná báze $g_1, \dots, g_s$ ideálu $I \subseteq k[x_1, \dots, x_n]$ se nazývá *Gröbnerova*, jestliže platí $\langle LT\, I \rangle = \langle LT\, g_1, \dots, LT\, g_s \rangle$.

Báze použitá v důkazu Hilbertovy věty byla Gröbnerova.

Jak už to na světě bývá, Gröbnerovy báze nevymyslel pan Gröbner, ale jeho aspirant B. Buchberger, který je tak údajně nazval na počest svého učitele. Ještě navíc nebyl první. V polovině šedesátých let popsal H. Hironaka „standardní báze", v podstatě se jednalo o totéž. Ke cti pana Buchbergera nutno podotknout, že o práci svého současníka patrně neměl ani ponětí a dovedl ji dále.

Ani pan Hilbert to neměl ve své době jednoduché. Větu, která byla ostatně jako hypotéza už zformulována dříve, dokázal podstatně komplikovanějším způsobem, než jsme uvedli. Navíc nekonstruktivní důkazy nebyly tenkrát příliš oblíbeny, a tak se od svých kolegů uznání nedočkal.

Inkluze $\langle LT\, I \rangle \supseteq \langle LT\, g_1, \dots, LT\, g_s \rangle$ platí pro libovolnou bázi $g_1, \dots, g_s$, a tedy se stačí omezit na dokazování opačné. Ta obecně platit nemusí. Uvažujme například $<_{\text{grlex}}$ a polynomy $x^3 - 2xy$ a $x^2y - 2y^2 + x$. Potom $x^2 = x(x^2y - 2y^2 + x) - y(x^3 - 2xy)$, a tedy $x^2 \in I$, ale zřejmě $x^2 \notin \langle x^3, x^2y \rangle$.

2.16 Důsledek. *Každý ideál $I \subseteq k[x_1, \dots, x_n]$ má Gröbnerovu bázi. Naopak každá množina polynomů $g_1, \dots, g_s \in I$ splňující $\langle LT\, I \rangle = \langle LT\, g_1, \dots, LT\, g_s \rangle$ je Gröbnerovou bází ideálu I.*

Na ilustraci uveďme jednoduchý případ, kdy generátory ideálu I budou polynomy stupně 1 a uspořádání bereme $<_{\text{lex}}$. Označme generátory $f_i = \sum_j a_{i,j}x_j + a_{i,0}$. Uvažujme matici $A = (a_{i,j})$, kde $i = 1, \dots, s$ a $j = 0, \dots, n$ a aplikujme na ni Gausovu eliminaci. Získáme $B = (b_{i,j})$ ve schodovitém tvaru, z ní navíc vypustíme nulové řádky. Máme novou bázi $g_1, \dots, g_t$, kde $t \leq s$. Vzhledem k provedeným úpravám je každé f_i vyjádřitelné jako lineární kombinace $g_1, \dots, g_t$, a tedy $\langle f_1, \dots, f_s \rangle = \langle g_1, \dots, g_t \rangle$ Tvrdíme, že $g_1, \dots, g_t$ je Gröbnerova báze.

Bez újmy na obecnosti předpokládejme, že proměnné jsou značeny tak, že $LM\, g_i = x_i$ pro $i = 1, \dots, t$. Uvažujme libovolný $f \in I$. Ten lze psát

$$f = h_1 f_1 + \dots + h_s f_s = h'_1 g_1 + \dots + h'_t g_t$$

Chceme, aby $LT\, f \in \langle LT\, g_1, \dots, LT\, g_t \rangle$, tj. $LT\, f$ má být dělitelný některým z $x_1, \dots, x_t$. Předpokládejme, že f je pouze v proměnných $x_{t+1}, \dots, x_n$. Pak ale $h'_1 = 0$, protože x_1 je vzhedem ke schodovitosti B pouze v g_1. Analogickým postupem získáme $h'_2 = \dots = h'_t = 0$, a tedy $f = 0$. Báze $g_1, \dots, g_t$ je tedy Gröbnerova.

Použití Gausovy eliminace zde není náhodné, v následující části ukážeme algoritmus počítající Gröbnerovy báze, který je v podstatě zobecněním Gausovy eliminace pro polynomy vyšších stupňů.

2.17 Věta Ascending Chain Condition. *Nechť $I_1 \subseteq I_2 \subseteq \cdots$ je neklesající nekonečná posloupnost ideálů v $k[x_1, \dots, x_n]$. Pak existuje $N \geq 1$ tak, že $I_N = I_{N+1} = \cdots$.*

Důkaz: Označme $I := \bigcup_{i=1}^{\infty} I_i$. Zřejmě I je ideál. Podle Hilbertovy věty existují $f_1, \dots, f_s$ tak, že $I = \langle f_1, \dots, f_s \rangle$. Jistě existuje takové N, že $f_1, \dots, f_s \in I_N$. Potom už $I = I_N = I_{N+1} = \cdots$. □

2.18 Definice. Nechť $I \subseteq k[x_1, \dots, x_n]$. Označme

$$V(I) := \{(a_1, \dots, a_n) \in k^n \mid \forall f \in I\colon f(a_1, \dots, a_n) = 0\}$$

Podle Hilbertovy věty je $I = \langle f_1, \dots, f_s \rangle$ a $V(I)$ je rovno varietě $\mathfrak{V}(f_1, \dots, f_s)$.

V obecné teorii se okruhy, kde je každý ideál konečně generovaný, nazývají *noetherovské.* Ukazuje se, že okruh je noetherovský, právě tehdy, když v něm platí tvrzení věty 2.17. V tomto kontextu má Hilbertova věta hlubší smysl. Dokazuje totiž, že okruh polynomů nad noetherovským okruhem je opět noetherovský.

3 Buchbergerův algoritmus

Pouhé tvrzení, že každý ideál má Gröbnerovu bázi (důsledek Hilberovy věty) by asi nebylo příliš prakticky použitelné. Proto se budeme dále zaměřovat na algoritmické nalezení takové báze, a protože pro daný ideál může Gröbnerových bází existovat více, pokusíme se identifikovat i jakousi jednoznačnou kanonickou formu.

3.1 Kritéria pro Gröbnerovy báze

3.1 Věta. *Nechť $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báze ideálu $I \subseteq k[x_1, \ldots, x_n]$ a f je polynom v $k[x_1, \ldots, x_n]$. Pak existuje právě jedno $r = \sum_\alpha a_\alpha x^\alpha \in k[x_1, \ldots, x_n]$ s těmito vlastnostmi*

1. *Žádný člen r není dělitelný žádným z $LT\, g_1, \ldots, LT\, g_t$, tj. $\forall \alpha \forall i\colon\ LT\, g_i \nmid a_\alpha x^\alpha$.*
2. *$\exists g \in I\colon f = g + r$*

Důkaz: Algoritmus pro dělení se zbytkem dá

$$f = a_1 g_1 + \cdots + a_t g_t + r \quad \text{kde } r \text{ splňuje podmínku 1.}$$

Za g už vezmeme $a_1 g_1 + \cdots + a_t g_t$, které triviálně padne do I.

Zbývá dokázat jednoznačnost. Předpokládejme $f = g + r = g' + r'$, kde $r \neq r'$. Zřejmě platí $r - r' = g' - g \in I$. Protože G je Gröebnerova, je $LT(r - r')$ dělitelný některým z $LT\, g_1, \ldots, LT\, g_t$. Diskutujme následující možnosti

- $LM\, r \neq LM\, r'$. Pak ten s vyšším stupněm musí být dělitelný některým z vedoucích členů $LT\, g_1, \ldots, LT\, g_t$, což je spor s prvním bodem.
- $LM\, r = LM\, r' \wedge LC\, r \neq LC\, r'$. Potom ale oba $LM\, r, LM\, r'$ musí být dělitelné některým z $LT\, g_1, \ldots, LT\, g_t$.

Proto tedy $LT\, r = LT\, r'$ a induktivní úvahou odtud plyne $r = r'$. □

Předchozí věta je vlastně zobecněním dělení se zbytkem, kde na místě dělitele vystupuje ideál. V případě jedné proměnné nebylo co zobecňovat, protože každý ideál byl generovaný jedním polynomem. Zajímá-li nás pouze zbytek, věta navíc říká, že nezáleží na pořadí polynomů v bázi. Proto má smysl zavést značení $\overline{f}^F$ pro zbytek po dělení f/F, pokud F je Gröbnerova báze.

3.2 Důsledek. *Nechť $G = \{g_1, \ldots, g_t\}$ je Gröbnerova báze ideálu $I \subseteq k[x_1, \ldots, x_n]$ a f je polynom v $k[x_1, \ldots, x_n]$. Pak platí*

$$f \in I \iff \text{zbytek po dělení } f/G \text{ je nulový}$$

Důkaz:

"$\Longleftarrow$" Nechť $f = g + r$ je rozklad z předchozí věty a $r = 0$. Potom triviálně $f \in I$.

"$\Longrightarrow$" $f \in I \implies f = f + 0$. Protože f vyhovuje podmínkám předchozí věty, a takový polynom podle jejího tvrzení existuje právě jeden, musí být zbytek po dělení f/G nutně nulový.

□

3.3 Definice. Pokud $\alpha = \operatorname{multideg} f$ a $\beta = \operatorname{multideg} g$, buď

$$\gamma := (\gamma_1, \ldots, \gamma_n) \quad \text{kde } \gamma_i = \max\{\alpha_i, \beta_i\}$$

Monom x^γ nazýváme *nejmenším společným násobkem (least common multiple)* monomů $LM\, f$ a $LM\, g$ a zavádíme poněkud matoucí označení $LCM(LM\, f, LM\, g) := x^\gamma$. Výraz

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

nazýváme S-polynomem[4] polynomů f, g.

Jedná se o nástroj k jakési eliminaci vedoucích členů, Gaussova eliminace je speciálním případem tohoto postupu pro stupeň 1. Narozdíl od ní ale může dojít ke zvýšení stupně, i když původní vedoucí členy odstraní.

Vezměme například $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$, tedy polynomy stupně 5 v $\mathbb{R}[x,y]$ a uspořádání $<_{\mathrm{grlex}}$. Pak $\gamma = (4,2)$ a

$$S(f,g) = \frac{x^4y^2}{x^3y^2} f - \frac{x^4y^2}{3x^4y} g = xf - \frac{1}{3} yg = -x^3y^3 + x^2 - \frac{1}{3} y^3$$

což je polynom stupně 6.

Následuje lemma technického rázu, které je nutné pro důkaz stěžejní věty.

3.4 Lemma. *Uvažme polynom* $f = \sum_{i=1}^t c_i x^{\alpha_i} g_i$, *kde* $c_1, \ldots, c_t \in k$ *a* $\alpha_i + \operatorname{multideg} g_i = \delta$ *pro nějaké pevné* δ *kdykoli* $c_i \neq 0$. *Pokud* $\operatorname{multideg} f < \delta$, *pak existují taková* $c_{i,j}$, *že*

$$\sum_{i=1}^t c_i x^{\alpha_i} g_i = \sum_{j,k=1}^t c_{j,k} x^{\delta - \gamma_{j,k}} S(g_j, g_k) \quad \textit{kde } x^{\gamma_{j,k}} = LCM(LM\, g_j, LM\, g_k)$$

a dále každý $x^{\delta-\gamma_{j,k}} S(g_j, g_k)$ *má stupeň menší než* δ.

Důkaz: Označme $d_i := LC\, g_i$ a $p_i = x^{\alpha_i} g_i / d_i$. Určitě $c_i d_i = LC(c_i x^{\alpha_i} g_i)$ a $LC\, p_i = 1$. Protože $\operatorname{multideg}(c_i x^{\alpha_i} g_i) = \delta$ a zároveň $\operatorname{multideg} f < \delta$, musí nutně platit $\sum_{i=1}^t c_i d_i = 0$. Pokusme se teď f vyjádřit jako kombinaci S-polynomů.

$$\begin{aligned} f = \sum_{i=1}^t c_i d_i p_i &= c_1 d_1 (p_1 - p_2) + (c_1 d_1 + c_2 d_2)(p_2 - p_3) + \cdots \\ &\quad + (c_1 d_1 + \cdots + c_{t-1} d_{t-1})(p_{t-1} - p_t) + (\underbrace{c_1 d_1 + \cdots + c_t d_t}_{0}) p_t \end{aligned}$$

Každý rozdíl $p_j - p_k$ lze vyjádřit v S-polynomech

$$\frac{x^\delta}{d_j x^{\delta - \alpha_j}} g_j - \frac{x^\delta}{d_k x^{\delta - \alpha_k}} g_k = x^{\delta - \gamma_{j,k}} \left(\frac{x^{\gamma_{j,k}}}{LT\, g_j} g_j - \frac{x^{\gamma_{j,k}}}{LT\, g_k} g_k \right) = x^{\delta - \gamma_{j,k}} S(g_j, g_k)$$

Z obou rovností se už snadno odvodí jednotlivé koeficienty $c_{j,k}$. □

[4] Ze *syzygy* neboli spřežení, více kapitola 3.4.

3.5 Věta. *Nechť $I \subseteq k[x_1, \dots, x_n]$ je ideál. Pak jeho báze $G = \{g_j, \dots, g_t\}$ je Gröbnerova právě tehdy, když pro každé $i \neq j$ je zbytek po dělení $S(g_i, g_j)/G$ nulový.*

Důkaz:

"$\Longrightarrow$" Plyne bezprostředně z důsledku 3.2.

"$\Longleftarrow$" Uvažujme $0 \neq f \in I$. Potřebujeme $LT\,f \in \langle LT\,g_1, \dots LT\,g_t\rangle$. Podaří-li se zaručit, aby pro $f = \sum_{i=1}^t h_i g_i$ platilo

$$\operatorname{multideg} f = \max\Big\{\operatorname{multideg}(h_i g_i)\Big\}$$

bude $LT\,f$ nutně dělitelný některým $LT\,g_i$, a tedy G bude Gröbnerova.

Označme $m_i := \operatorname{multideg}(h_i g_i)$, $\delta := \max\{m_1, \dots, m_t\}$. Zřejmě $\operatorname{multideg} f \leq \delta$. Nechť $h_1, \dots, h_t$ jsou zvolena tak, že δ je minimální. Protože pracujeme s monomiálním uspořádáním, které je dobré, takové δ existuje.

Dokažme tedy, že $\operatorname{multideg} f = \delta$. Lze psát

$$(1)\ \ f = \sum_{m_i=\delta} h_i g_i + \sum_{m_i<\delta} h_i g_i = \sum_{m_i=\delta} (LT\,h_i) g_i + \sum_{m_i=\delta} (h_i - LT\,h_i) g_i + \sum_{m_i<\delta} h_i g_i$$

Všechny sčítance druhé a třetí sumy mají jistě stupeň menší než δ. Připustíme-li, že $\operatorname{multideg} f < \delta$, potom nutně

$$\operatorname{multideg}\left(\sum_{m_i=\delta} (LT\,h_i) g_i\right) < \delta$$

Označme nyní $c_i x^{\alpha_i} := LT\,h_i$ a aplikujme lemma 3.4.

$$\sum_{m_i=\delta} (LT\,h_i) g_i = \sum_{m_i=\delta} c_i x^{\alpha_i} g_i = \sum_{j,k} c_{j,k} x^{\delta-\gamma_{j,k}} S(g_j, g_k)$$

Z předpokladu věty a algoritmu o dělení se zbytkem získáváme

$$S(g_j, g_k) = \sum_{i=1}^t a_{i,j,k} g_i$$

a navíc $\operatorname{multideg}(a_{i,j,k} g_i) \leq \operatorname{multideg} S(g_j, g_k)$. Označíme-li $b_{i,j,k} := x^{\delta-\gamma_{j,k}} a_{i,j,k}$, dostáváme

$$x^{\delta-\gamma_{j,k}} S(g_j, g_k) = \sum_{i=1}^t b_{i,j,k} g_i$$

Podle druhé části lemmatu 3.4 platí

$$\operatorname{multideg}(b_{i,j,k} g_i) \leq \operatorname{multideg}\Big(x^{\delta-\gamma_{j,k}} S(g_j, g_k)\Big) < \delta$$

a dosazením

$$\sum_{m_i=\delta} (LT\,h_i) g_i = \sum_{j,k} c_{j,k} \left(\sum_{i=1}^t b_{i,j,k} g_i\right) = \sum_{i=1}^t \left(\sum_{j,k} c_{j,k} b_{i,j,k}\right) g_i$$

přičemž platí

$$\operatorname{multideg}\left(\sum_{j,k} c_{j,k} b_{i,j,k} g_i\right) < \delta \quad \text{pro } i = 1, \ldots, t$$

Dosazením do rovnosti (1) získáváme vyjádření f jako kombinace $g_1, \ldots, g_t$, kde všechny sčítance jsou stupně menšího než δ. To je spor s minimální volbou δ, a tedy $\operatorname{multideg} f = \delta$, odkud $LT\, f \in \langle LT\, g_1, \ldots, LT\, g_t \rangle$ a báze G je Gröbnerova.

□

3.2 Algoritmus

Věta 3.5 poskytuje už účinný prostředek pro zjištění, zda nějaká báze je Gröbnerova. Uvažujme například $I = \langle x + y, y - z \rangle$. Jediný S-polynom, který připadá v úvahu je

$$S(x + y, y - z) = \frac{xy}{x}(x + y) - \frac{xy}{y}(y - z) = xz + y^2$$

Dělením získáme $xz + y^2 = z(x + y) + y(y - z)$, a tedy daná báze je Gröbnerova.

Spolu s větou 2.17 získáváme také návod k naivnímu algoritmu pro výpočet Gröbnerovy báze. V každém jeho kroku k již zkonstruované bázi $G = \{f_1, \ldots, f_s\}$ přidáme všechny nenulové $\overline{S(f_i, f_j)}^G$. Získáme tak bázi G'. Zřejme jsme nic nového nepřidali, a tak $\langle G' \rangle = \langle G \rangle$. Navíc $\langle LT\, G \rangle \subseteq \langle LT\, G' \rangle$.

Pokud ovšem $G \subset G'$, pak také $\langle LT\, G \rangle \subset \langle LT\, G' \rangle$, protože přidáváme zbytky po dělení G a ty nemohou být dělitelné žádným z $LT\, f_1, \ldots, LT\, f_s$, a tedy $\langle LT\, G \rangle$ obohatí. Máme tedy neklesající posloupnost ideálů

$$\langle LT\, G_1 \rangle \subseteq \langle LT\, G_2 \rangle \subseteq \cdots$$

A ta má podle věty 2.17 jistý index, od kterého je stabilní. Připustíme-li, že přidávání zbytků k bázím nikdy neskončí, dostáváme se tak do sporu. Následující algoritmus počítající Gröbnerovu bázi G ideálu $\langle F \rangle$ je tedy korektní

Algoritmus 3.1

1. $G := F$, $G' := \emptyset$
2. `while` $G \neq G'$
   - 2.1. $G' := G$
   - 2.2. $\forall p, g \in G' : p \neq g$ `do`
     - 2.2.1. $s := \overline{S(p, q)}^{G'}$
     - 2.2.2. `if` $s \neq 0$
       - 2.2.2.1. $G := G \cup \{s\}$

Tento algoritmus ovšem není zdaleka ideální. Lze vymyslet velmi jednoduše vypadající vstupy, pro něž vrací divoké výsledky. Dále výstupní báze se přímo odvíjí od vstupní, a tedy pro tentýž ideál zadaný různými bázemi dá také různé výsledky. Z hlediska čistě rutinního algoritmus také není optimální, mnoho výpočtů zbytků zbytečně opakuje, i když je zřejmé, že jakmile byly zbytky jednou vynulovány, budou nulové i v následujících krocích.

3.3 Redukované báze

Jak již bylo řečeno, Gröbnerových bází daného ideálu existuje více. Zaměříme se tedy na nalezení jednoznačné kanonické podoby, která daný ideál bude identifikovat.

3.6 Lemma. *Nechť G je Gröbnerova báze ideálu I a $p \in G$ takový, že $LT\,p \in \langle LT(G - \{p\})\rangle$. Pak $G - \{p\}$ je také Gröbnerova báze I.*

Důkaz: Z definice Gröbnerovy báze platí $\langle LT\,I\rangle = \langle LT\,G\rangle$. Protože $LT\,p \in \langle LT(G - \{p\})\rangle$, platí $\langle LT(G - \{p\})\rangle = \langle LT\,G\rangle$. Odsud již, podle důsledku 2.16, plyne tvrzení. □

Následující definice je tedy smysluplná.

3.7 Definice. *Minimální Gröbnerovou bází* ideálu I je taková Gröbnerova báze G, že pro všechna $p \in G$ platí $LC\,p = 1$ a zároveň $LT\,p \notin \langle LT(G - \{p\})\rangle$

Například mějme $k[x, y]$ a $<_{\text{grlex}}$, $I = \langle f_1, f_2\rangle = \langle x^3 - 2xy, x^2y - 2y^2 + x\rangle$. Zmíněný algoritmus dá

$$(f_1, \ldots, f_5) = (x^3 - 2xy, x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x)$$

Přitom platí $LT\,f_1 = x^3 = -x\,LT\,f_3$ a $LT\,f_2 = -\frac{1}{2}x\,LT\,f_4$ a tedy f_1 a f_2 jsou podle lematu 3.6 zbytečné.

Minimální Gröbnerova báze ještě stále není to, co hledáme, protože ideál může mít více minimálních bází. Například pro každé a je $\{x^2 + axy, xy, y^2 - 1/2x\}$ minimální Gröbnerovou bází uvedeného ideálu. Proto následující definice

3.8 Definice. Polynom $g \in G$ nazveme *redukovaný* pro bázi G pokud žádný z jeho monomů neleží v $\langle LT(G - \{g\})\rangle$. *Redukovanou Gröbnerovou bází* ideálu I potom nazveme takovou Gröbnerovu bázi G, že pro všechna $p \in G$ platí $LC\,p = 1$ a zároveň p je redukovaný pro G.

Zejména každá redukovaná Gröbnerova báze je minimální.

3.9 Lemma. *Je-li polynom g redukovaný pro nějakou minimální Gröbnerovu bázi G ideálu I, pak je také redukovaný pro každou minimální Gröbnerovu bázi G' téhož ideálu, která jej obsahuje.*

Důkaz: Tvrzení dokážeme sporem. Uvažme $G = \{g_1, \ldots, g_s\}$, $G' = \{g'_1, \ldots, g'_t\}$ a $g = \cdots + m + \cdots$ kde $m \in \langle LT(G' - \{g\})\rangle$ (tj. g není redukovaný pro G'). Potom $m = a_1\,LT\,g'_1 + \cdots + a_t\,LT\,g'_t$ pro nějaké vhodné polynomy $a_1, \ldots, a_t$. Protože G i G' jsou Gröbnerovy báze téhož ideálu, platí $\langle LT\,G\rangle = \langle LT\,G'\rangle$, a tedy každé $LT\,g'_i$ lze vyjádřit jako kombinaci $LT\,g_1, \ldots, LT\,g_s$. Odtud už plyne $m \in \langle LT\,G\rangle$ a protože je G' minimální, je $m \in \langle LT(G \setminus \{g\})\rangle$, což je spor s předpokládanou redukovaností g pro G. □

3.10 Věta. *Nechť $I \subseteq k[x_1, \ldots, x_n]$ je nenulový. Pak pro každé monomiální uspořádání existuje právě jedna redukovaná Gröbnerova báze ideálu I. Navíc každou Gröbnerovu bázi lze algoritmicky redukovat.*

Důkaz: Předpokládejme, že $\langle G\rangle = I$, G je Gröbnerova. S ohledem na lemma 3.6 lze předpokládat, že G je i minimální. (Algoritmus minimalizace je zřejmý, stačí testovat pouze dělitelnost vedoucích monomů.)

Nechť $g \in G$ není redukovaný. Při dělení $g/(G - \{g\})$ se tedy $LT\, g$ nutně dostane do zbytku, protože nemá čím být dělitelný (báze je minimální). Tedy $LT(\overline{g}^{G-\{g\}}) = LT\, g$, protože nic jiného už nemůže být vedoucím členem zbytku. Označme

$$g' := \overline{g}^{G-\{g\}} \quad \text{a} \quad G' := \Big(G - \{g\}\Big) \cup \{g'\}$$

G' je opět minimální Gröbnerovou bází ideálu I, protože $\langle LT\, G' \rangle = \langle LT\, G \rangle$, tj. také platí $\langle LT\, G' \rangle = \langle LT\, I \rangle$. Polynom g' je zřejmě redukovaný pro G' díky vlastnostem algoritmu pro dělení. Byl-li nějaký $h \neq g$ redukovaný pro G, zůstává podle předchozího lemmatu redukovaný i pro G'. Tím je dán algoritmus pro redukci Gröbnerovy báze.

Zbývá dokázat jednoznačnost. Předpokládejme dvě redukované Gröbnerovy báze $G, \widetilde{G}$ nenulového ideálu I. Platí tedy $\langle LT\, G \rangle = \langle LT\, I \rangle = \langle LT\, \widetilde{G} \rangle$. Protože tento ideál je monomiální, lze pro něj aplikovat Dicksonovo lemma. S odvoláním na konstrukci báze v jeho důkazu lze tvrdit, že existuje právě jedna monomiální báze monomiálního ideálu tak, že koeficienty jejích členů jsou rovny jedné a žádný z členů této báze nedělí jiný.

Podle definice minimality musí být $LT\, G$ i $LT\, \widetilde{G}$ právě takovou bází. Tedy $LT\, G = LT\, \widetilde{G}$. Ke každému $g \in G$ tedy exisuje právě jedno $\tilde{g} \in \widetilde{G}$ takové, že $LT\, g = LT\, \tilde{g}$.

Platí $g - \tilde{g} \in I$. Protože G je Gröbnerova, platí $\overline{g - \tilde{g}}^G = 0$. Členy $LT\, g, LT\, \tilde{g}$ se odečtou už v $g - \tilde{g}$. Protože obě báze jsou redukované, nemůže být žádný ze zbývajících členů $g - \tilde{g}$ dělitelný kterýmkoli z $LT\, G = LT\, \widetilde{G}$. Musí se tedy dostat do zbytku. Platí tedy

$$g - \tilde{g} = \overline{g - \tilde{g}}^G = 0$$

Tím je jednoznačnost dokázána. □

Algoritmus konstrukce redukované Gröbnerovy báze vyplývající z předchozí věty sice vede k cíli, ale zdaleka není optimální. Jeho první část, algoritmus uvedený za větou 3.5 totiž může dát výsledek z mnoha polynomů, resp. polynomů vysokých stupňů či koeficientů. Optimalizace[5] spočívá v půběžném aplikování minimalizace, normování a redukce na mezivýsledky. Sice jsme neukázali, že si to můžeme dovolit, v důkaze předchozí věty se silně využívalo toho, že báze, která je redukována, byla minimální Gröbnerova, v jistých případech ale tento postup aplikovat lze. Bohužel není jednoduché rozhodnout, kdy a který ze tří zmíněných kroků použít. Všechny dostupné algoritmy se tedy opírají o nějakou heuristiku, nicméně ke každému lze zkonstruovat „rozumně vypadající“ vstup, pro který na soudobé technice zhavaruje pro nedostatek paměti. Nepříliš povzbudivé, ale pro většinu běžných aplikací naštěstí algoritmy příliš neselhávají.

V tuto chvíli máme odpovědi na dvě z dříve položených otázek.

- $f \in I \iff \overline{f}^G = 0$ pro Gröbnerovu bázi G ideálu I (důsledek 3.2).
- Dva ideály jsou stejné právě tehdy, když mají stejné redukované Gröbnerovy báze.

V obou případech nezáleží na zvoleném monomiálním uspořádání.

[5]Tento termín chápeme ve smyslu informatickém, matematici by snad raději viděli vylepšení – meliorace.

3.4 Zefektivnění algoritmu

Podstatným kritériem použitým v naivní verzi algoritmu je tvrzení věty 3.5. Výpočet S-polynomu a následné dělení se zbytkem je nejbolestivější místo algoritmu z hlediska časové náročnosti. Pokusíme se nalézt ekvivalentní kritérium, které bude snadněji implementovatelné.

3.11 Definice. Zvolme pevné monomiální uspořádání. Nechť $G = \{g_1, \ldots, g_t\} \subseteq k[x_1, \ldots, x_n]$. Řekneme, že $f \in k[x_1, \ldots, x_n]$ se *redukuje na g modulo G* (píšeme $f \to_G g$), pokud existují nějaká $a_1, \ldots, a_t \in k[x_1, \ldots, x_n]$ tak, že

$$f = a_1 g_1 + \cdots + a_t g_t + g$$

a zároveň $\operatorname{multideg} f \geq \operatorname{multideg} a_i g_i$ pro každé $i = 1, \ldots, t$.

Polynomy $a_1, \ldots, a_t$ v definici jsou veskrze libovolné, nemusí se jednat o výsledek dělení se zbytkem.

3.12 Lemma. *Nechť $G = (g_1, \ldots, g_s) \in (k[x_1, \ldots, x_n])^s$, $f \in k[x_1, \ldots, x_n]$. Platí implikace*

$$\overline{f}^G = 0 \implies f \to_G 0$$

Opak obecně neplatí. □

Například $f = xy^2 - x$, $G = (xy + 1, y^2 - 1)$. Potom $\overline{f}^G = -x - y$, ale přitom $f = x(y^2 - 1)$.

V důkazu stěžejního kritéria (věta 3.5) se ale využívá pouze vlastnosti $f \to_G 0$. Odtud plyne následující

3.13 Důsledek. *Báze $G = \{g_1, \ldots, g_t\}$ je Gröbnerova právě tehdy, když $S(g_i, g_j) \to_G 0$ pro všechna i, j.*

3.14 Věta. *Nechť $G \subset k[x_1, \ldots, x_n]$ je konečná, $f, g \in G$. Nechť navíc $LCM(LM\, f, LM\, g) = LM\, f \cdot LM\, g$. Potom $S(f, g) \to_G 0$.*

Důkaz: Bez újmy na obecnosti můžeme předpokládat $LC\, f = LC\, g = 1$. Potom lze vyjádřit

$$f = LM\, f + p$$
$$g = LM\, g + q$$

Počítejme

$$S(f, g) = LM\, g \cdot f - LM\, f \cdot g = (g - q)f - (f - p)g = gp - fq$$

Přitom stupně gp i fq jsou jistě menší než stupeň $S(f, g)$. □

3.15 Definice. Nechť $F = (f_1, \ldots, f_s) \in (k[x_1, \ldots, x_n])^s$. *Syzygy*[6] vedoucích členů nazýváme s-tici polynomů $S = (h_1, \ldots, h_s)$ takovou, že

$$\sum_{i=1}^{s} h_i\, LT\, f_i = 0$$

Symbolem $S(F)$ značíme množinu všech s-tic, které danou podmínku splňují.

[6] Česky „spřažení“, zachycuje algebraické relace mezi vedoucími členy.

Označíme-li e_i jednotkové vektory ve volném modulu[7] $(k[x_1,\dots,x_n])^s$, každou syzygy lze vyjádřit

$$S = \sum_{i=1}^{s} h_i e_i$$

Každý S-polynom nad $\{f_i, f_j\} \subseteq F$ odpovídá prvku volého modulu

$$S_{i,j} := \frac{x^\gamma}{LT\, f_i} e_i - \frac{x^\gamma}{LT\, f_j} e_j \quad \text{kde } x^\gamma = LCM(LM\, f_i, LM\, f_j)$$

který vždy patří do $S(F)$. Termín S-polynom pochází právě z této korespondence. Na druhé straně každou syzygy $S \in S(F)$ lze vyjádřit jako lineární kombinaci výrazů $S_{i,j}$.

3.16 Věta. *Nechť $F = (f_1,\dots,f_s) \in (k[x_1,\dots,x_n])^s$ a $S \in S(F)$. Potom lze vyjádřit*

$$S = \sum_{i<j} u_{i,j} S_{i,j} \quad \textit{kde } u_{i,j} \textit{ jsou vhodné polynomy}$$

Důkaz je analogický důkazu lemmatu 3.4 a pro velkou ošklivost ho raději vypustíme.□

3.17 Definice. *Homogenní syzygy* $S \in S(F)$ stupně $\alpha \in \mathbb{N}_0{}^n$ je tvaru

$$c_1 x^{\alpha_1} e_1 + \dots + c_s x^{\alpha_s} e_s$$

kde $c_i \in k$ a $\alpha_i + \operatorname{multideg} f_i = \alpha$ pro všechna taková i, kde $c_i \neq 0$.

3.18 Lemma. *Nechť $F = (f_1,\dots,f_s) \in (k[x_1,\dots,x_n])^s$. Platí*

1. *Každou syzygy $S \in S(F)$ lze vyjádřit jednoznačně jako součet homogenních syzygy z $S(F)$.*
2. *$S(F)$ je podmodul ve volném modulu $(k[x_1,\dots,x_n])^s$ s bází vybranou z homogenních syzygy $S_{i,j}$.*

□

Podmodul $S(F)$ pro netriviální F není volný. Pro bázi $S(F)$ nejsou nutně třeba všechny $S_{i,j}$. Například v lexikografickém uspořádání $x < y < z$ pro $F = \{x^2y^2+z, xy^2-y, x^2y+yz\}$ dostáváme $S_{1,2} = (1,-x,0)$, $S_{1,3} = (1,0,-y)$, $S_{2,3} = (0,x,-y)$, tj. $S_{2,3} = S_{1,3} - S_{1,2}$.

3.19 Věta. *Báze $G = \{g_1,\dots,g_t\}$ ideálu $I \subseteq k[x_1,\dots,x_n]$ je Gröbnerova právě tehdy, když pro každou syzygy $S = h_1e_1 + \dots + h_te_t$ v homogenní bázi $S(G)$ platí*

$$S \cdot G \to_G 0 \quad \textit{kde } S \cdot G = \textstyle\sum_{i=1}^t h_i g_i$$

Důkaz je opět analogický větě 3.5. □

Jako kritérium pro zjištění, zda daná báze je Gröbnerova tedy stačí testovat redukovatelnost jistých velmi speciálních syzygy (pouze prvků homogenní báze podmodulu $S(G)$) na 0.

[7]Zobecnění vektorového prostoru. Definice modulu je zcela stejná, jen pole skalárů zaměníme libovolným okruhem. Volné moduly jsou právě kartézské mocniny okruhu skalárů s operacemi definovanými po komponentách. Všechny vektorové prostory jsou volné díky invertibilitě nenulových skalárů.

3.20 Věta. *Nechť $G = (g_1, \ldots, g_t)$ a $\mathfrak{S} \subseteq \{S_{i,j} \mid 1 \leq i < j \leq t\}$ je báze $S(G)$. Předpokládejme, že pro nějaké různé g_i, g_j, g_k platí $LT\, g_k |\, LCM(LM\, g_i, LM\, g_j)$. Jestliže $S_{i,k}, S_{j,k} \in \mathfrak{S}$, pak $\mathfrak{S} - \{S_{i,j}\}$ je také báze $S(G)$.*

Důkaz: Označme $x^{\gamma_{i,j}} := LCM(LM\, g_i, LM\, g_j)$. Předpokládáme, že $x^{\gamma_{i,k}}, x^{\gamma_{j,k}} | x^{\gamma_{i,j}}$. Odtud zřejmě

$$S_{i,j} = \frac{x^{\gamma_{i,j}}}{x^{\gamma_{i,k}}} S_{i,k} - \frac{x^{\gamma_{i,j}}}{x^{\gamma_{j,k}}} S_{j,k}$$

Tedy $S_{i,j}$ je v bázi $\mathfrak{S}$ zbytečný. □

Důsledek 3.13 poskytuje náhradní kritérium pro výpočet Gröbnerovy báze, navíc věty 3.14 a 3.20 dává zefektivnění. V tuto chvíli již můžeme formulovat algoritmus, který je vylepšenou podobou naivního Buchbergerova. Vstupem je nějaká báze $F = (f_1, \ldots, f_s)$, výstupem Gröbnerova báze G.

Algoritmus 3.2

1. $B := \{(i,j) \mid 1 \leq i < j \leq s\}$, $G := F$, $t := s$
2. `while` $B \neq \emptyset$
   - 2.1. vezmi libovolné $(i,j) \in B$
   - 2.2. `if` $LCM(LT\, f_i, LT\, f_j) \neq LT\, f_i \cdot LT\, f_j$ `and` not $Test(f_i, f_j, B)$
     - 2.2.1. $S := \overline{S(f_i, f_j)}^G$
     - 2.2.2. `if` $S \neq 0$
       - 2.2.2.1. $t := t + 1$
       - 2.2.2.2. $f_t := S$
       - 2.2.2.3. $G := G \cup \{f_t\}$
       - 2.2.2.4. $B := B \cup \{(i,t) \mid 1 \leq i < t\}$
   - 2.3. $B := B - \{(i,j)\}$

Funkce *Test* ověřuje podmínku věty 3.20, tj. vrací *true,* pokud existuje nějaké $k \notin \{i,j\}$ takové, že $(i,k), (j,k) \in B$ (při vhodném pořadí dvojic) a přitom zároveň platí $LT\, f_k |\, LCM(LT\, f_i, LT\, f_j)$. Invarientem algoritmu je tvrzení, že B neobsahuje ty dvojice, o nichž víme, že se S-polynom redukuje na nulu (buď je to patrné z testu 2.2, nebo si to zaručíme krokem 2.2.2.3). Algoritmus zastaví v důsledku věty 2.17 (Ascending Chain Condition) a výstupem je skutečně Gröbnerova báze.

Testy jsou v souhrnu podstatně méně pracné, než výpočty S-polynomů v původním algoritmu a následné opakované dělení. Problémy okolo vhodnosti minimalizace a redukce Gröbnerovy báze v daném okamžiku výpočtu ovšem zůstávají.

Jako vedlejší produkt algoritmu získáme informace o algebraických relacích mezi polynomy vzniklé Gröbnerovy báze. Zaměřme se o něco podrobněji na manipulaci algoritmu se syzygy. Označíme-li I množinu všech dvojic (i,j) takových, že *Test*$(f_i, f_j, B) =$ *false* v okamžiku zastavení, je množina

$$\mathfrak{S} := \left\{ S_{i,j} \mid (i,j) \in I \right\}$$

taková báze $S(G)$, že pro všechny její prvky $S_{i,j}$ platí

$$S_{i,j} \cdot G = S(f_i, f_j) \to_G 0$$

Toto tvrzení plyne ze zpětné rekonstrukce výpočtu algoritmu, dvojice (i,j) byla totiž odstraněna z B buď tehdy, bylo-li možné $S_{i,j}$ vyjádřit z ostatních, nebo při platnosti výše uvedené podmínky. Tedy algoritmus navíc produkuje bázi $S(G)$.

Nějaká verze Buchbergerova algoritmu je naimplementována ve všech programových systémech zahrnujících počítačovou algebru, většinou je na něm podstatná část algebraických manipulací založena. Jako příklad uveďme systém MAPLE, který je patrně v naší síti nejdostupnější, a MATHEMATICA (ten je bohužel dostupný pouze na stroji `princ.math.muni.cz`).

Velice stručnou ukázku můžete vidět na obr. 6. První příkaz slouží k načtení knihovny `grobner`, druhý vyvolá nápovědu týkající se této knihovny, třetí počítá redukovanou Gröbnerovu bázi pro ideál uvedený za definicí 3.7 v gradovaném lexikografickém uspořádání (tdeg je zkratka pro total degree), další totéž v lexikografickém uspořádání (plex=pure lexicographic). Následující příkazy ilustrují různé chování použitých uspořádání (`leadmon` dává vedoucí koeficient a monom, `spoly` je S-polynom v zadaném uspořádání, `normalf` je v podstatě zbytek po dělení).

Snadná modifikace předchozí teorie (od začátku kapitoly 2) vede k rozšíření na podmoduly ve volných modulech. Pak lze aplikovat předchozí algoritmus na vlastní výsledek, dostaneme příslušnou Gröbnerovu bázi podmodulu $S(G)$ atd. Lze ukázat, že tento postup také zastaví. Počty generátorů v získaných Gröbnerových bázích mají mimo jiné topologickou interpretaci, lze z nich odvodit např. počty k-rozměrných „děr“ ve varietě apod.

Případný zájemce může najít více podrobností v diplomové práci Zorky Velenové, která je k dispozici ve stejném adresáři, jako tyto texty.[8]

[8]Zorka uvádí obecné vlastnosti modulů nad komutativními okruhy, Buchbergerův algoritmus v této obecné situaci včetně zmíněné iterace a ukazuje, že tato se musí zastavit nejpozději po tolika krocích, kolik je volných proměnných. Navíc představuje specializovaný software – Macaulay.

```
> with(grobner);
```

$$[finduni, finite, gbasis, gsolve, leadmon, normalf, solvable, spoly]$$

```
> ?grobner
> gbasis([x^3-2*x*y,x^2*y-2*y^2+x],[x,y],tdeg);
```

$$\left[x\,y, x^2, -x + 2\,y^2\right]$$

```
> gbasis([x^3-2*x*y,x^2*y-2*y^2+x],[x,y],plex);
```

$$\left[x - 2\,y^2, y^3\right]$$

```
> leadmon(x-2*y^2, [x,y],plex);
```

$$[1, x]$$

```
> leadmon(x-2*y^2, [x,y],tdeg);
```

$$\left[-2, y^2\right]$$

```
> spoly(x-2*y^2,y^3, [x,y],plex);
> normalf(spoly(x-2*y^2,y^3, [x,y],plex),[x-2*y^2,y^3],
> [x,y],plex);
```

$$-2\,y^5$$

$$0$$

```
> spoly(x-2*y^2,y^3, [x,y],tdeg);
> normalf(spoly(x-2*y^2,y^3, [x,y],tdeg),[x-2*y^2,y^3],
> [x,y],tdeg);
```

$$x\,y$$

$$x\,y$$

```
>
```

Obr. 6: Ukázka zápisníku systému MAPLE

4 Teorie eliminací proměnných

Pro úvahy o polynomech v různých počtech proměnných budeme považovat okruh $k[x_{p+1}, \ldots, x_n]$ za podokruh $k[x_1, \ldots, x_n]$. Jedná se o polynomy, v nichž se nevyskytují proměnné $x_1, \ldots, x_p$. Je to skutečně podokruh, ale už ne ideál.

4.1 Eliminace

4.1 Definice. Nechť $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$. Pro $p = 1, \ldots, n$ definujeme

$$I_p := I \cap k[x_{p+1}, \ldots, x_n]$$

Tuto množinu nazveme *p-tým eliminačním ideálem.*

Samozřejmě I_p je ideálem pouze v $k[x_{p+1}, \ldots, x_n]$. Na úrovni polynomiálních rovnic I_p obsahuje všechny rovnice, které jsou důsledky systému $f_1 = 0, \ldots, f_s = 0$ a v kterých vystupují pouze proměnné $x_{p+1}, \ldots, x_n$.

4.2 Věta ELIMINAČNÍ. *Nechť $I \subseteq k[x_1, \ldots, x_n]$ je ideál, $G = \{g_1, \ldots, g_m\}$ jeho Gröbnerova báze vzhledem k $<_{\mathrm{lex}}$. Proměnné nechť jsou uspořádány $x_1 >_{\mathrm{lex}} x_2 >_{\mathrm{lex}} \cdots$. Potom pro každé $p = 0, \ldots, n$ je $G_p := G \cap k[x_{p+1}, \ldots, x_n]$ Gröbnerovou bází ideálu I_p.*

Důkaz: Bez újmy na obecnosti můžeme uvažovat $G_p = \{g_1, \ldots, g_r\}$. Protože $G \subseteq I$, je i $G_p \subseteq I_p$. Inkluze $\langle G_p \rangle \subseteq I_p$ platí triviálně. Dokážeme opačnou. Nechť $f \in I_p$, chceme

$$f = h_1 g_1 + \cdots + h_r g_r$$

Provedeme dělení původní Gröbnerovou bází G. Protože $f \in I$, platí $\overline{f}^G = 0$, a tedy

$$f = h_1 g_1 + \cdots + h_r g_r + h_{r+1} g_{r+1} \cdots + h_m g_m$$

Každý z polynomů $g_{r+1}, \ldots, g_m$ musí obsahovat nějakou z proměnných $x_1, \ldots, x_p$, jinak by byl prvkem G_p. Vzhledem k vlastnostem lexikografického uspořádání takovou proměnnou obsahují i $LT\, g_{r+1}, \ldots, LT\, g_m$. Uvědomíme-li si postup algoritmu pro dělení se zbytkem a skutečnost, že v f není žádný monom obsahující některou z $x_1, \ldots, x_p$, musí být $h_{r+1} = \cdots = h_m = 0$. Tedy $f \in \langle G_p \rangle$.

Dokázali jsme nejen požadovanou inkluzi, ale i fakt, že dělení f/G dopadne na I_p stejně jako f/G_p. Pro $1 \leq i < j \leq r$ uvažujme S-polynomy $S(g_i, g_j)$. Platí

$$\overline{S(g_i, g_j)}^{G_p} = \overline{S(g_i, g_j)}^{G} = 0$$

a tedy G_p je Gröbnerova báze ideálu I_p. □

Zřejmě aplikací eliminační věty na minimální resp. redukovanou Gröbnerovu bázi získáme opět bázi minimální resp. redukovanou.

Jediná v důkazu využitá vlastnost lexikografického uspořádání je tvrzení, že z některých proměnných objevujících se v polynomu se ta, která je v daném uspořádání největší, objeví i ve vedoucím členu. To je ovšem podstatně slabší požadavek, než definice lexikografického uspořádání. Proto lze při skutečných implementacích používat uspořádání v podstatě gradované s touto vlastností zajištěnou. Dosáhne se tak většinou efektivnějších výpočtů, protože čisté lexikografické uspořádání zpravidla vede k nepříjemnému nárůstu exponentů.

4.2 Věta o rozšíření

Společnou myšlenkou následujících úvah je chápání $k[x_1, \dots, x_n]$ jako $k[x_2, \dots, x_n][x_1]$, tedy polynom v proměnných $x_1, \dots, x_n$ považujeme za polynom v jedné proměnné x_1 a koeficientech z $k[x_2, \dots, x_n]$. To ovšem není pole, ale pouze okruh. Proto místo něj pro účely důkazů použijeme odpovídající podílové těleso $k(x_2, \dots, x_n)$ a na závěr vždy ukážeme, že se vše podstatné stejně odehrálo v $k[x_2, \dots, x_n]$.

4.3 Věta O ROZŠÍŘENÍ. *Nechť $I = \langle f_1, \dots, f_s \rangle \subseteq \mathbb{C}[x_1, \dots, x_n]$. Pro každé $i = 1, \dots, s$ položme*

$$f_i := g_i(x_2, \dots, x_n)x_1^{N_i} + \text{ členy nižšího stupně v } x_1$$

kde $g_i \in \mathbb{C}[x_2, \dots, x_n]$ je nenulový. Nechť $(a_2, \dots, a_n)$ je prvek variety $V(I_1)$ dané prvním eliminačním ideálem. Pak platí

$$(a_2, \dots, a_n) \notin \mathfrak{V}(g_1, \dots, g_s) \implies \exists a_1 \in \mathbb{C}\colon (a_1, a_2, \dots, a_n) \in V(I)$$

Ke korektnímu důkazu se časem propracujeme (kapitola 4.4), zatím jen ilustrativní příklad. Nechť $f = xy - 1$, $g = xz - 1$, $I = \langle f, g \rangle$. Gröbnerova báze je $y - z, xz - 1$, proto podle eliminační věty $I_1 = \langle y - z \rangle$. Pro každé $a \in \mathbb{C}$ platí $(a, a) \in V(I_1)$. Vyjádříme polynomy $y - z, xz - 1$ podle stupně v x

$$\begin{aligned} y - z &= (y - z)x^0 \\ xz - 1 &= zx^1 - 1 \end{aligned}$$

Zřejmě pro $a \neq 0$ existuje rozšíření $(1/a, a, a) \in V(I)$.

Rozšíření znamená postup do značné míry opačný k eliminaci. K varietě prvního eliminačního ideálu (předpokládáme, že tu už určíme snáz) hledáme hodnoty pro x_1, aby výsledný bod padl do původní variety. Celý problém lze chápat jako hledání společného kořene polynomů po dosazení už známých $n - 1$ složek.

4.3 Existence společných kořenů

4.4 Definice. Nechť k je pole. Polynom $f \in k[x_1, \dots, x_n]$ nazveme *ireducibilní nad k*, platí-li $f \notin k$ a f není součinem nekonstantních polynomů.

4.5 Lemma. *Nechť $f \in k[x_1, \dots, x_n]$ a platí $f|gh$. Pokud je f ireducibilní, pak $f|h$ nebo $f|g$.*

Důkaz je jednoduchý ale technicky zdlouhavý a opírá se o zmíněnou myšlenku rozšíření na podílové těleso. Vede se indukcí k počtu proměnných. □

4.6 Lemma. *Nechť f, g mají kladný stupeň v x_1. Potom mají společný faktor v $k[x_2, \dots, x_n][x_1]$ s kladným stupněm v x_1 právě tehdy, když mají takový faktor v $k(x_2, \dots, x_n)[x_1]$.*

Důkaz: Implikace od případu v $k[x_2, \dots, x_n][x_1]$ k $k(x_2, \dots, x_n)[x_1]$ je zcela zřejmá. Zaměřme se tedy na opačnou. Pišme $f = \tilde{h}\tilde{f}_1$, $g = \tilde{h}\tilde{g}_1$ kde $\tilde{h}, \tilde{f}_1, \tilde{g}_1 \in k(x_2, \dots, x_n)[x_1]$. Dále za d označme společný jmenovatel „zlomků“ $\tilde{h}, \tilde{f}_1, \tilde{g}_1$ a položme

$$h := d\tilde{h},\ f_1 := d\tilde{f}_1,\ g_1 := d\tilde{g}_1$$

Ty už nutně padnou do $k[x_2,\dots,x_n][x_1]$. Platí $d^2f = hf_1$, $d^2g = hg_1$ a opět se pohybujeme v $k[x_2,\dots,x_n][x_1]$. Protože $\tilde{h} = h/d$ a $d \in k[x_2,\dots,x_n]$, musí nutně existovat ireducibilní faktor h_1 v h s kladným stupněm v x_1.

Víme, že $h_1|d^2f$. Protože je ireducibilní, musí dělit d nebo f. Ale d nemá s x_1 nic společného, a tak nutně $h_1|f$. Dělitelnost $h_1|g$ se ukáže analogicky. □

4.7 Věta. *Každý nekonstantní polynom $f \in k[x_1,\dots,x_n]$ lze psát jako $f = f_1\cdots f_r$ součin ireducibilních polynomů. Toto vyjádření je jednoznačné až na permutaci faktorů a násobky skalárem.*

Důkaz: Tvrzení v případě polynomů jedné proměnné je všeobecně známé. Na základě předchozího lemmatu lze zobecnit i do okruhu polynomů více proměnných. □

4.8 Lemma. *Nechť $f,g \in k[x]$, $\deg f = l > 0$, $\deg g = m > 0$. Polynomy f,g mají společný faktor právě tehdy, když $\exists A,B \in k[x]$ tak, že*

- *A,B nejsou oba nulové*
- $\deg A < m$, $\deg B < l$
- $Af + Bg = 0$

Důkaz:

"$\Longrightarrow$" Pišme $f = hf_1$, $g = hg_1$. Pak $\deg f_1 < l$, $\deg g_1 < m$. Platí

$$0 = g_1f_1 - f_1g_1 = g_1hf_1 - f_1hg_1 = g_1f - f_1g$$

což bylo třeba dokázat.

"$\Longleftarrow$" Sporem. Předpokládejme, že f,g nemají společný faktor. Nechť například $B \neq 0$. Platí $GCD(f,g) = 1$. Z Bezoutovy rovnosti dostáváme

$$\tilde{A}f + \tilde{B}g = 1 \implies B = (\tilde{A}f + \tilde{B}g)B = \tilde{A}Bf - \tilde{B}Af = (\tilde{A}B - \tilde{B}A)f$$

a tedy $\deg B \geq l$, což je spor.

□

Označme členy polynomů A,B z předchozího lemmatu

$$\begin{aligned} A &= c_0x^{m-1} + \cdots + c_{m-1} \\ B &= d_0x^{l-1} + \cdots + d_{l-1} \end{aligned}$$

Porovnáme-li koeficienty u jednotlivých mocnin x při tomto vyjádření třetí podmínky lemmatu, dostáváme homogenní systém rovnic

$$\begin{aligned} a_0c_0 + b_0d_0 &= 0 \\ a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 &= 0 \\ &\vdots \\ a_lc_{m-1} + b_md_{l-1} &= 0 \end{aligned}$$

Ten má nenulové řešení (v proměnných $c_0,\dots c_{m-1}, d_0,\dots,d_{l-1}$) právě tehdy, když je jeho matice singulární. Pro ni zavádíme zvláštní označení.

4.9 Definice. Nechť $f, g \in k[x]$ jsou kladného stupně. Označme

$$f = a_0x^l + \cdots + a_l$$
$$g = b_0x^m + \cdots + b_m$$

Sylvesterovou maticí polynomů f, g rozumíme matici $Syl(f, g, x)$ řádu $m + l$ tvaru

$$\left(\begin{array}{cccc|cccc}
a_0 & 0 & \cdots & 0 & b_0 & 0 & \cdots & 0 \\
a_1 & a_0 & & \vdots & b_1 & b_0 & & \vdots \\
a_2 & a_1 & \ddots & 0 & b_2 & b_1 & \ddots & 0 \\
\vdots & & & a_0 & \vdots & & & b_0 \\
a_l & & & & b_m & & & \\
0 & a_l & & \vdots & 0 & b_m & & \vdots \\
\vdots & & \ddots & & \vdots & & \ddots & \\
0 & \cdots & 0 & a_l & 0 & \cdots & 0 & b_m
\end{array}\right)$$

Rezultantem polynomů f, g vzhledem k proměnné x nazveme její determinant. Značíme $Res(f, g, x)$.

Pro $f, g \in k[x]$ kladných stupňů je $Res(f, g, x)$ zřejmě prvkem pole k. Lze jej chápat jako polynom v proměnných $a_0, \ldots, a_l, b_0, \ldots, b_m$ s celočíselnými koeficienty.

4.10 Důsledek. *Polynomy $f, g \in k[x]$ mají společný faktor (tedy i kořen pro algebraicky uzavřené k) právě tehdy, když $Res(f, g, x) = 0$.*

Důkaz: Plyne bezprostředně z lemmatu 4.8 a definice rezultantu. □

4.11 Lemma. *Nechť $f, g \in k[x]$ jsou polynomy kladného stupně. Pak existují taková $A, B \in k[x]$ tak, že platí*

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

Důkaz: Pro $Res(f, g, x) = 0$ je tvrzení přímým důsledkem lemmatu 4.8. Uvažujme tedy případ $Res(f, g, x) \neq 0$. Z Bezoutovy rovnosti plyne existence $\tilde{A}, \tilde{B}$, takových, že $\tilde{A}f + \tilde{B}g = 1$. Označme jednotlivé členy těchto polynomů

$$\tilde{A} = c_0x^{m-1} + \cdots + c_{m-1}$$
$$\tilde{B} = d_0x^{l-1} + \cdots + d_{l-1}$$

Porovnáme-li koeficienty u jednotlivých mocnin proměnné x v Bezoutově rovnosti, získáme systém

$$\begin{aligned}
a_0c_0 + b_0d_0 &= 0 \\
a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 &= 0 \\
&\vdots \\
a_lc_{m-1} + b_md_{l-1} &= 1
\end{aligned}$$

Chápeme-li tento systém v proměnných $c_0, \dots, c_{m-1}, d_0, \dots, d_{l-1}$, je jeho matice právě $Syl(f, g, x)$. Protože předpokládáme nenulovost rezultantu, lze aplikovat Cramerovo pravidlo a získáváme

$$\tilde{A} = \frac{A}{Res(f,g,x)} \qquad \tilde{B} = \frac{B}{Res(f,g,x)}$$

pro nějaká vhodná A, B. Odtud již plyne požadovaná rovnost. □

Rezultant lze poměrně efektivně vypočítat modifikací Euklidova algoritmu. Zřejmě platí

$$Res(f,g,x) = (-1)^{lm}\, Res(g,f,x)$$

Dá se ukázat, že pokud $f = qg + r$, kde $\deg r < \deg g$ (krok algoritmu), pak

$$Res(f,g,x) = Res(r,g,x) \cdot b_0^{l-\deg r} \quad \text{kde } b_0 = LC\, g$$

Návod k důkazu je uveden v rámci cvičení ke kapitole týkající se rezultantů v [2].

S ohledem na myšlenku předloženou na začátku kapitoly můžeme zobecnit definici rezultantu na polynomy ve více proměnných. $Res(f, g, x_1)$ definujeme zcela analogicky, jen polynomy f, g chápeme jako polynomy v proměnné x_1 a koeficientech z $k[x_2, \dots, x_n]$.

4.12 Věta. *Nechť $f, g \in k[x_1, \dots, x_n]$ jsou kladného stupně v x_1. Pak*

1. *$Res(f, g, x_1) \in I_1$, kde I_1 je první eliminační ideál $\langle f, g\rangle$.*
2. *$Res(f, g, x_1) = 0$ právě tehdy, když f, g mají společný faktor kladného stupně v x_1.*

Důkaz: Uvažujme opět $f, g \in k[x_2, \dots, x_n][x_1] \subseteq k(x_2, \dots, x_n)[x_1]$. To už je pole, a tak lze aplikovat důsledek 4.10 a lemma 4.11.

1. Pokud $Res(f, g, x_1) = 0$, je tvrzení zřejmé. Přímo z definice rezultantu plyne $Res(f, g, x_1) \in k[x_2, \dots, x_n]$. Podle lemmatu 4.11 existují nějaká $A, B \in k(x_2, \dots, x_n)[x_1]$ tak, že $Res(f, g, x_1) = Af + Bg$, což už je i prvek $\langle f, g\rangle$. Zbývá ukázat, že $A, B \in k[x_2, \dots, x_n][x_1]$. Ale tyto polynomy jsou konstruovány v důkazu lemmatu 4.11 tak, že tuto podmínku splňují.
2. Lemma 4.6 umožňuje pohybovat se bez problémů mezi okruhem $k[x_2, \dots, x_n]$ a polem $k(x_2, \dots, x_n)$. V poli je ale druhá část tvrzení zřejmá.

□

4.4 Důkaz věty o rozšíření

Nyní máme k dispozici nástroje dostatečně silné pro důkaz věty o rozšíření (4.3). Pro jednoduchost ho detailně provedeme pouze pro ideály generované jen dvěma polynomy.

Důkaz 4.3: Uvažujme $f, g \in \mathbb{C}[x_1, \dots, x_n] \subseteq \mathbb{C}(x_2, \dots, x_n)[x_1]$ s vedoucími koeficienty a_0, b_0. Tradičně označíme $I_1 := \langle f, g\rangle \cap \mathbb{C}[x_2, \dots, x_n]$. Chceme ukázat, že pro každé $(c_2, \dots, c_n) \in V(I_1) - \mathfrak{V}(a_0, b_0)$ existuje $c_1 \in \mathbb{C}$ tak, že $(c_1, \dots, c_n) \in V(\langle f, g\rangle)$.

Označme $\mathbf{c} := (c_2, \dots, c_n)$ a konvenčně pišme $f(x_1, \mathbf{c}) = f(x_1, c_2, \dots, c_n)$. Stačí ukázat

$$Res\Big(f(x_1, \mathbf{c}), g(x_1, \mathbf{c})\Big) = 0$$

Potom už podle předchozího bude existovat společný kořen $c_1 \in \mathbb{C}$ a $(c_1, \ldots, c_n)$ padne do $\mathfrak{V}(f, g)$.

Předpokládejme nejprve, že $a_0(\mathbf{c}) \neq 0$ a zároveň $b_0(\mathbf{c}) \neq 0$. Označme $h := Res(f, g, x_1)$. Podle věty 4.12 platí $h \in I_1$, a tedy zejména $h(\mathbf{c}) = 0$. Dosazením $\mathbf{c}$ za $(x_2, \ldots, x_n)$ získáváme

$$Res\big(f(x_1, \mathbf{c}), g(x_1, \mathbf{c})\big) = h(\mathbf{c}) = 0$$

Uvažujme nyní např. $b_0(\mathbf{c}) = 0$, $a_0(\mathbf{c}) \neq 0$. Potom stupeň $g(x_1, \mathbf{c})$ v x_1 je menší než m a $h(c)$ nelze použít jako v předchozím případě. Můžeme ovšem uvážit jinou bázi ideálu $\langle f, g\rangle$, např. $\langle f, g + x_1^N f\rangle$ a volit N tak velké, aby stupeň $x_1^N f$ v x_1 byl větší, než stupeň g. Potom bude vedoucí koeficient $g + x_1^N f$ roven a_0 a je možno aplikovat první část důkazu. $\square$

Uvažme například ideál $I = \langle x^2y - 1, x^2z - 1\rangle$. První eliminační ideál je potom $\langle y - z\rangle$. Varieta $V(I)$ je „jakási hyperbola" o dvou větvích položená v rovině $y = z$. Tato rovina je vlastně $V(I_1)$. Věta o rozšíření tvrdí, že ke každé dvojici $(y, z) \in V(I_1)$ s vyjímkou jistých bodů nalezneme hodnotu pro x, abychom získali bod původní variety. Jinými slovy na téměř každé přímce dané dvojicí y, z (tedy volné v x) lze najít bod patřící do původní variety. Problematickým bodem v tomto příkladě je právě $y = z = 0$, k němuž rozšíření neexistuje. Obecně se jedná právě o ty body, které neleží v projekci původní variety podle proměnné x_1, ale padnou do nejmenší afinní variety, která tuto projekci obsahuje (viz. kapitola 4.6).

Obecný důkaz věty o rozšíření je v podstatě analogický předchozímu, je však technicky náročný. Pro ideál $I = \langle f_1, \ldots, f_s\rangle$ se vytvoří polynom $g = u_2f_2 + \cdots + u_sf_s \in \mathbb{C}[u_2, \ldots, u_s, x_1, \ldots, x_m]$. Uvažuje se rezultant

$$Res(f_1, g, x_1) = \sum_\alpha h_\alpha(x_2, \ldots, x_n) \cdot u^\alpha \quad \text{kde } u = (u_2, \ldots, u_s)$$

a porovnávají se koeficienty u^α. Věřme a detaily přenechejme jen vážným zájemcům.

4.5 Hilbertova věta o nulách

4.13 Věta Hilbertova o nulách. *Nechť pole k je algebraicky uzavřené, $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Platí*

$$f \in \mathfrak{I}\big(\mathfrak{V}(f_1, \ldots, f_s)\big) \iff f^m \in \langle f_1, \ldots, f_s\rangle \quad \textit{pro vhodné } m \in \mathbb{N}_0$$

Důkaz: Nejprve dokážeme, že každý ideál $I \subseteq k[x_1, \ldots, x_n]$ splňuje

$$V(I) = \emptyset \iff I = k[x_1, \ldots, x_n] \tag{2}$$

To je bezprostřední důsledek věty pro $f = 1$. V závěru ukážeme, že se jedná o ekvivalentní tvrzení.

Každé algebraicky uzavřené pole je nekonečné. Jinak by stačilo uvažovat polynom $(x - a_1) \cdots (x - a_n) + 1$, který nemá kořen – spor. Proto implikace zprava doleva platí triviálně. Důkaz zleva doprava vedeme indukcí. Předpokládejme $V(I) = \emptyset$.

1. Nechť $n = 1$. Pak $I = \langle f_1 \rangle$ podle důsledku 1.13. Protože f_1 nemá kořeny a k je algebraicky uzavřené, musí být f_1 konstanta. Tedy $\langle f_1 \rangle = k[x_1]$.
2. Nechť $I = \langle f_1, \ldots, f_s \rangle$. Je-li některý z $f_1, \ldots, f_s$ konstanta, je tvrzení zřejmé. Předpokládejme tedy nekonstantní polynomy. Předpokládejme navíc, že f_1 je velmi speciálního tvaru
$$f_1(x_1, \ldots, x_n) = cx_1^N + \text{členy s nižším stupněm v } x_1$$
kde $c \in k$, $c \neq 0$ je konstanta. Posléze ukážeme, že si tento předpoklad můžeme dovolit. Z věty o rozšíření (4.3) díky speciálnímu tvaru f_1 plyne $\pi_1(V(I)) = V(I_1)$. Předpokládáme $V(I) = \emptyset$, a tedy i $\pi_1(V(I)) = \emptyset$. I_1 už je pouze v $n-1$ proměnné, a tedy podle indukčního předpokladu $1 \in I_1$. Odtud zřejmě i $1 \in I$.

Zbývá ukázat, že v obecném případě umíme problém redukovat tak, abychom mohli předpokládat speciální tvar f_1. K tomu užijeme homomorfismus $k[x_1, \ldots, x_n] \to k[\tilde{x}_1, \ldots, \tilde{x}_n]$
$$\begin{aligned} x_1 &:= \tilde{x}_1 \\ x_2 &:= \tilde{x}_2 + a_2\tilde{x}_1 \\ &\vdots \\ x_n &:= \tilde{x}_n + a_n\tilde{x}_1 \end{aligned}$$
Pokud neexistuje řešení systému rovnic po této transformaci, neexistovalo ani před ní, pokud patří 1 do obrazu nějaké množiny, patří i do vzoru (vše jsou vlastnosti homomorfismu).

Tyto transformační rovnice s neznámými parametry dosadíme do f_1. Chtěli bychom, aby koeficient členu nejvyššího stupně v x_1 byl konstantní. Přitom monom s nejvyšším stupněm v $\tilde{x}_1$ může vzniknout z monomu s nejvyšším součtem stupňů ve všech proměnných x_i. Požadavek, aby jeho koeficient nezávisel na ostatních proměnný je polynomiálních podmínka na parametry $a_2, \ldots, a_n$.

Tím je dokázáno tvrzení (2). Zbývá ukázat, že implikuje dokazovanou větu. Nejprve směr tvrzení zprava doleva. Pokud $f^m \in \langle f_1, \ldots, f_s \rangle$, také $f^m \in \mathfrak{I}(\mathfrak{V}(f_1, \ldots, f_s))$, to znamená $(f(\mathbf{a}))^m = 0$ pro všechna $\mathbf{a} \in \mathfrak{V}(f_1, \ldots, f_s)$. Protože k je obor integrity, musí nutně i $f(\mathbf{a}) = 0$, a tedy $f \in \mathfrak{I}(\mathfrak{V}(f_1, \ldots, f_s))$.

Obráceně chceme $f^m = \sum_{i=1}^s h_i f_i$. Uvažme ideál
$$\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset k[x_1, \ldots, x_n, y].$$
Zvolme $\mathbf{a} = (a_1, \ldots, a_{n+1})$ libovolné. Pokud $(a_1, \ldots, a_n) \notin V(I)$, pak zřejmě $\mathbf{a} \notin V(\tilde{I})$. Pokud naopak $(a_1, \ldots, a_n) \in V(I)$, platí i $f(a_1, \ldots, a_n) = 0$, a tedy $1 - yf$ se určitě nenuluje na $\mathbf{a}$. Dohromady $V(\tilde{I}) = \emptyset$, tedy $1 \in \tilde{I}$ a lze psát
$$1 = \sum_{i=1}^s p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$
Za y dosadíme $1/f(x_1, \ldots, x_n)$. Potom v $k(x_1, \ldots, x_n)$ dostáváme rovnost
$$1 = \sum_{i=1}^s p_i\Big(x_1, \ldots, x_n, \tfrac{1}{f(x_1, \ldots, x_n)}\Big) f_i$$
Vynásobením f^m s m dostatečně velkým získáme požadovanou rovnost. □

4.6 Věta o uzávěru

Připomeňme, že projekci „odřezávající“ prvních k souřadnic značíme π_k.

4.14 Lemma. *Nechť $I_k = \langle f_1, \ldots, f_s\rangle \cap \mathbf{C}[x_{k+1}, \ldots, x_n]$. Potom*

$$\pi_k\Big(\mathfrak{V}(\langle f_1, \ldots, f_s\rangle)\Big) \subseteq V(I_k)$$

Důkaz: Nechť $f \in I_k$ je libovolný. Je to polynom pouze v proměnných $x_{k+1}, \ldots, x_n$. Uvažme libovolné $(a_1, \ldots, a_n) \in \mathfrak{V}(\langle f_1, \ldots, f_s\rangle)$. Protože $f \in \langle f_1, \ldots, f_s\rangle$, jistě platí $f(a_{k+1}, \ldots, a_n) = 0$, a tedy $f(\pi_k(a_1, \ldots, a_n)) = 0$. Tím je inkluze dokázána. □

Obecně $\pi_k(V)$ nemusí být varieta, tj. inkluze je ostrá. Viz příklad u věty o rozšíření.

4.15 Lemma. *Nechť $V = \mathfrak{V}(f_1, \ldots, f_s) \subseteq \mathbb{C}^n$, I_1 je první eliminační ideál a g_i jako ve větě o rozšíření. Pak v $\mathbb{C}^{n-1}$ platí*

$$V(I_1) = \pi_1(V) \cup \Big(\mathfrak{V}(g_1, \ldots, g_n) \cap V(I_1)\Big)$$

□

Tedy varieta daná prvním eliminačním ideálem se skládá právě z projekce původní variety a oné „méně rozměrné“ množiny vymykajících se bodů, které dotvoří projekci na afinní varietu.

S právě diskutovanými vlastnostmi souvisí pojem *Zariského topologie.* To je taková topologie na k^n, kde k je pole, že uzavřené množiny jsou právě nulové množiny systémů racionálních lomených funkcí.

4.16 Věta O UZÁVĚRU. *Nechť $V = \mathfrak{V}(f_1, \ldots, f_s) \subseteq \mathbb{C}^n$ a I_k je k-tý eliminační ideál. Potom platí*

1. *$V(I_k)$ je nejmenší afinní varieta obsahující $\pi_k(V)$, tedy uzávěr v Zariského topologii.*
2. *Pokud $V \neq \emptyset$, pak existuje afinní varieta $W \subset V(I_k)$ tak, že $V(I_k) - W \subseteq \pi_k(V)$.*

Důkaz: Potřebujeme dokázat $V(I_k) = V(\mathfrak{I}(\pi_k(V)))$. Uvažme libovolný $f \in \mathfrak{I}(\pi_k(V)) \subseteq \mathbb{C}[x_{k+1}, \ldots, x_n]$. Zřejmě $f(a_{k+1}, \ldots, a_n) = 0$ pro všechna $(a_{k+1}, \ldots, a_n) \in \pi_k(V)$, a tedy také $f(a_1, \ldots, a_n) = 0$ v $\mathbb{C}[x_1, \ldots, x_n]$ pro všechna $(a_1, \ldots, a_n) \in V$. Podle Hilbertovy věty o nulách tedy existuje m tak, že $f^m \in \langle f_1, \ldots, f_s\rangle$. Protože f nezávisí na $x_1, \ldots, x_k$, nezávisí na nich ani f^m.

Uvažujme nyní libovolné $\mathbf{a} \in V(I_k)$. Víme, že ke každému polynomu $f \in \mathfrak{I}(\pi_k(V))$ existuje m tak, že $f^m \in I_k$. Pokud $f^m(\mathbf{a}) = 0$ musí i $f(\mathbf{a}) = 0$, a tedy i $\mathbf{a} \in V(\mathfrak{I}(\pi_k(V)))$. Opačná inkluze je zřejmá, protože $I_k \subseteq \mathfrak{I}(\pi_k(V))$.

Důkaz druhé části věty patří k netriviálním a opět formálně komplikovaným. Provedeme ho jen pro případ $k = 1$. Podle lemmatu 4.15 můžeme vyjádřit

$$V(I_1) = \pi_1(V) \cup \underbrace{\Big(\mathfrak{V}(g_1, \ldots, g_s) \cap V(I_1)\Big)}_{W}$$

Toto W je zřejmě afinní varieta. Pokud $W \subset V(I_1)$, je vše v pořádku. Pro případ $W = V(I_1)$ lze, podobně jako v důkazu věty 4.3, „zlepšit“ generátory, aby použitá báze indukovala požadovanou vlastnost. K tomu budeme potřebovat následující lemma.

4.17 Lemma. *Pokud $W = V(I_1)$, pak $V = \mathfrak{V}(f_1, \dots, f_s, g_1, \dots, g_s)$.*

Důkaz: Protože se jedná o variety, je zřejmě $\mathfrak{V}(f_1, \dots, f_s, g_1, \dots, g_s) \subseteq V$. Zvolme libovolně $(a_1, \dots, a_n)$. Protože $\pi_1(V) \subseteq V(I_1)$, je $(a_2, \dots, a_n) \in V(I_1) = W$. Tedy nutně z definice W platí $g_i(a_2, \dots, a_n) = 0$ pro všechna i. Odtud opačná inkluze. □

Vraťme se k vlastnímu důkazu věty. Definujme nový ideál $\tilde{I} := \langle f_1, \dots, f_s, g_1, \dots, g_s \rangle$. Ten podle lemmatu určuje stejnou varietu. Polynomy g_i už mají nulový stupeň v x_1, f_i můžeme nahradit $\tilde{f}_i := f_i - g_i x_1^{N_i}$, které mají ostře menší stupeň v x_1.

Podle lemmatu 4.15 získáme nový rozklad a nové $\widetilde{W}$. Pokud bude opět $W = V(I_1)$, celý postup zopakujeme. Po konečném počtu kroků buď dojdeme k žádané vlastnosti anebo vynulujeme stupeň v x_1. To ale znamená $\pi_1(V) = V(I_1)$ a můžeme volit $W = \emptyset$, což je také afinní varieta. □

V příkladu na straně 33 je varieta W právě bod $y = z = 0$. Věta byla sice pro jednoduchost dokázána pro okruhy polynomů nad $\mathbb{C}$, ale zřejmě platí pro libovolné algebraicky uzavřené pole.

4.7 Korespondence ideálů a variet

Sumarizujme na závěr výsledky celé teorie s ohledem na korespondenci algebraických struktur (ideály) a geometrických objektů (variety) a na odpovídající si operace na nich.

4.18 Definice. Radikálovým ideálem ideálu $I \subseteq k[x_1, \dots, x_n]$ nazveme

$$\sqrt{I} := \langle f \in k[x_1, \dots, x_n] \mid \exists m \in \mathbb{N}\colon\ f^m \in I \rangle$$

Jako důsledek Hilbertovy věty o nulách dostáváme

4.19 Důsledek. *Je-li k algebraicky uzavřenmé, pak pro každou varietu $\mathfrak{V}(f_1, \dots, f_s)$ platí*

$$\mathfrak{I}(\mathfrak{V}(f_1, \dots, f_s)) = \sqrt{\langle f_1, \dots, f_s \rangle}$$

4.20 Definice. Ideál $I \subseteq k[x_1, \dots, x_n]$ nazýváme *prvoideálem,* jestliže pro každé $f \cdot g \in I$ je už $f \in I$ nebo $g \in I$. Ideál je *vlastní,* pokud $\{0\} \neq I \subset k[x_1, \dots, x_n]$, *maximální,* není-li obsažen v žádném ostře větším vlastním ideálu.

4.21 Definice. Afinní varieta $V \subseteq k^n$ se nazývá *ireducibilní,* jestliže kdykoli $V = V_1 \cup V_2$, kde V_1, V_2 jsou afinní variety, platí už $V = V_1$ nebo $V = V_2$.

To je vcelku přirozený pojem. Například varieta $\mathfrak{V}(xy) \subseteq \mathbb{R}^2$ není ireducibilní, tvoří ji dvě přímky, které jsou pochopitelně afinní variety. V tuto chvíli se nabízí hypotéza, dokázaná v následující větě.

4.22 Věta. *Afinní varieta $V \subseteq k^n$ je ireducibilní právě tehdy, když $\mathfrak{I}(V)$ je prvoideál.*

Důkaz:

"$\Longrightarrow$" Nechť $f \cdot g \in \mathfrak{I}(V)$ a označme

$$V_1 := V \cap \mathfrak{V}(f)$$
$$V_2 := V \cap \mathfrak{V}(g)$$

To jsou zřejmě afinní variety. Platí $V = V_1 \cup V_2$, protože na každém bodě V se musí nulovat alespoň jeden z f, g. Předpokládáme, že V je ireducibilní, nechť tedy například $V = V_1$. Určitě $f \in \mathfrak{I}(V_1)$, a tedy i $f \in \mathfrak{I}(V)$. To znamená, že $\mathfrak{I}(V)$ je prvoideál.

"$\Longleftarrow$" Předpokládejme naopak, že $\mathfrak{I}(V)$ je prvoideál, $V = V_1 \cup V$ a například $V_1 \neq V$. Odtud ostrá inkluze $\mathfrak{I}(V) \subset \mathfrak{I}(V_1)$. Určitě také $\mathfrak{I}(V) \subseteq \mathfrak{I}(V_2)$. Zvolme $f \in \mathfrak{I}(V_1) - \mathfrak{I}(V)$, $g \in \mathfrak{I}(V_2)$. Protože $V = V_1 \cup V_2$, platí $f \cdot g \in \mathfrak{I}(V)$. To je prvoideál, a tedy $f \in \mathfrak{I}(V)$, což jsme vyloučili volbou f, anebo $g \in \mathfrak{I}(V)$. Ukázali jsme $\mathfrak{I}(V_2) \subseteq \mathfrak{I}(V)$. Tedy tyto ideály se rovnají a musí se rovnat i variety V a V_2.

$\square$

Všechny závěry jsou shrnuty v tabulce 1. K ní je nutné jen poznamenat, že při projekci musíme uvažovat uzávěr, protože, jak již víme, projekce samotná nemusí ještě být varieta.

Algebraické objekty		Geometrické objekty
radikálový ideál		varieta
I	$\longrightarrow$	$V(I)$
$\mathfrak{I}(V)$	$\longleftarrow$	V
součet ideálů		průnik variet
$I + J$	$\longrightarrow$	$V(I) \cap V(J)$
$\sqrt{\mathfrak{I}(V) + \mathfrak{I}(W)}$	$\longleftarrow$	$V \cap W$
součin ideálů		sjednocení variet
$I \cdot J$	$\longrightarrow$	$V(I) \cup V(J)$
$\sqrt{\mathfrak{I}(V) \cdot \mathfrak{I}(W)}$	$\longleftarrow$	$V \cup W$
eliminace proměnných		projekce variety
$\sqrt{I \cap k[x_{k+1}, \dots, x_n]}$	$\longleftrightarrow$	$\overline{\pi_k(V(I))}$
prvoideál		ireducibilní varieta
maximální ideál		jednobodová varieta
Ascending Chain Condition		Descending Chain Condition

Tabulka 1: Korespondence ideálů a variet

5 Aplikace

5.1 Řešitelnost systémů rovnic

5.1 Věta. *Systém $f_1 = 0, \dots, f_s = 0$, kde $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ a k je algebraicky uzavřené pole, nemá řešení právě tehdy, když $1 \in \langle f_1, \dots, f_s \rangle$, tj. redukovaná Gröbnerova báze tohoto ideálu je $\{1\}$.*

Důkaz: Pokud je varieta prázdná, lze tvrdit, že libovolný polynom se nuluje na všech jejích bodech[9], tedy i polynom 1. Potom ale, podle Hilbertovy věty o nulách (4.13), platí $1^m \in \langle f_1, \dots, f_s \rangle$ pro nějaké m.

Naopak je-li $1 \in \langle f_1, \dots, f_s \rangle$, musí to být nutně celý okruh. Protože pole k předpokládáme algebraicky uzavřené a tedy nekonečné, varieta, kde se nulují všechny polynomy, je už triviálně prázdná. □

Tedy o daném systému algebraických rovnic lze algoritmicky rozhodnout, zda má nebo nemá řešení. Alternativní metodou pro tohoto rozhodnutí je přímé použití aparátu rezultantů, patrně se tak dosáhne i lepší časové složitosti. Tato problematika ale není naším cílem, a tak případné zájemce odkazujeme na literaturu.

5.2 Věta. *Nechť $V = V(I) \subseteq \mathbb{C}^n$ je afinní varieta a $<$ libovolné monomiální uspořádání. Pak následující tvrzení jsou ekvivalentní.*

1. *V je konečná*
2. *$\forall i = 1, \dots, n\ \exists m_i \in \mathbb{N}_0 \colon x_i^{m_i} \in \langle LT\, I \rangle$*
3. *Nechť G je redukovaná Gröbnerova báze I. Pak*
$$\forall i = 1, \dots, n\ \exists m_i \in \mathbb{N}_0 \colon x_i^{m_i} = LM\, g \quad \text{pro některé } g \in G$$
4. *Faktorokruh[10] $\mathbb{C}[x_1, \dots, x_n]/I$ nad $\mathbb{C}$ je konečně rozměrný vektorový prostor.*

Důkaz:

"$1 \Longrightarrow 2$" Pokud je $V = \emptyset$, potom $1 \in I$ a můžeme brát $m_i = 0$ pro každé i.

Předpokládejme tedy $V \neq \emptyset$ a zvolme i. Nechť $a_j \in \mathbb{C}$ pro $j = 1, \dots, k$ jsou různé i-té souřadnice bodů V. Polynom

$$f(x_i) := \prod_{j=1}^{k} (x_i - a_j)$$

je nulový ve všech bodech V. Podle Hilberovy věty o nulách existuje m tak, že $f^m \in I$. Odtud už $x_i^{km} \in \langle LT\, I \rangle$ a stačí položit $m_i = km$.

"$2 \Longrightarrow 3$" Předpokládáme, že $x_i^{m_i} \in \langle LT\, I \rangle$. Protože G je Gröbnerova, platí $\langle LT\, I \rangle = \langle LT\, G \rangle$. Ovšem jedná se o monomiální ideály, a tak musí existovat $g \in G$ takové, že $LT\, g | x_i^{m_i}$ (přímo z definice 2.9). Tedy pro nějaké vhodné m_i' musí být $LT\, g = x_i^{m_i'}$.

[9]Poněkud krkolomné, ale podrobným rozebráním důkazu Hilbertovy věty o nulách pro tento případ tvrzení skutečně dostaneme

[10]Připomeňme, že faktorokruh $\mathbb{C}[x_1, \dots, x_n]/I$ nad $\mathbb{C}$ je množina tříd ekvivalence $f \sim g \iff f - g \in I$.

"3 $\Longrightarrow$ 2" je zcela triviální.

"2 $\Longrightarrow$ 4" Nechť $x_i^{m_i} \in \langle LT\, I\rangle$. Definujme vektorový prostor nad $\mathbb{C}$

$$S := \left\langle x^\alpha \mid x^\alpha \notin \langle LT\, I\rangle \right\rangle$$

Zde je na místě podotknout, že se nejedná o tytéž „zobáky". Vnější znamenají generování vektorového prostoru, tedy máme k použití sčítání uvnitř a násobení skalárem (tj. komplexním číslem), vnitřní generují ideál, tedy se sčítá uvnitř a násobí zvenku polynomem.

Například pro $I = \langle x^2, y^2\rangle$ je $S = \langle 1, x, y, xy\rangle$. Vzhledem k předpokladu je S konečněrozměrný nanejvýš dimenze $m_1 \cdots m_n$. Ukážeme, že zobrazení

$$\begin{aligned} S &\to \mathbb{C}[x_1, \ldots, x_n]/I \\ x^\alpha &\mapsto [x^\alpha] \end{aligned}$$

přirozeně rozšířené na polynomy je izomorfismus vektorových prostorů.

- Nechť x^β je také vzorem $[x^\alpha]$. Potom $x^\beta \in [x^\alpha]$, tedy $x^\alpha - x^\beta \in I$. Protože oba jsou prvky S, není ani jeden z nich prvkem $LT\, I$. Kdyby rozdíl byl nenulový, jeho vedoucí monom, tj. jeden z x^α, x^β by patřil do $LT\, I$. Proto jejich rozdíl musí být nulový. To znamená $x^\alpha = x^\beta$, tj. zobrazení je prosté.
- Nechť $f = \sum_\alpha a_\alpha x^\alpha$ je libovolný. Jsou-li všechny monomy $x^\alpha \in S$, pak třída $[f]$ je jeho obrazem. Pokud nejsou, vezmeme z jeho monomů $x^\alpha \notin S$ největšího stupně. Pak určitě existuje $g \in I$ takové, že $LT\, g = a_\alpha x^\alpha$. Zřejmě $[f] = [f - g]$ a problematický monom v $f - g$ je ostře nižšího stupně. Po konečném počtu kroků získáme reprezentanta $[f]$ tvořeného pouze monomy S. Zobrazení je tedy surjektivní.
- Sčítání i násobení skalárem je zřejmě zachováno.

"4 $\Longrightarrow$ 1" Stačí ukázat, že pro dané i existuje pouze konečně mnoho možných i-tých souřadnic bodů z V.

Uvažme proto třídy $[x_i^j] \in \mathbb{C}[x_1, \ldots, x_n]/I$. Dimenze je konečná, a tedy, pro dostatečně velké m, existuje nenulová lineární kombinace

$$\sum_{j=0}^{m} c_j [x_i^j] = [0]$$

což lze psát

$$\left[\sum_{j=0}^{m} c_j x_i^j\right] = [0]$$

Odtud $\sum_{j=0}^{m} c_j x_i^j \in I$, což je nenulový polynom v x_i a ten má nejvýše konečně mnoho kořenů.

$\square$

V obou větách nezáleželo na volbě monomiálního uspořádání. V praxi to znamená, že pokud výpočet zhavaruje pro nějaké, je možné jej provést s jiným uspořádáním a pravděpodobnost úspěchu se tak zvyšuje.

5.2 Polynomiální a racionální implicitizace

Připomeňme, že parametrická reprezentace variety v k^n je dána systémem n racionálních funkcí (viz. 1.8). Uvažme množinu definovanou parametricky systémem polynomů $F = (f_1, \ldots, f_n)$, kde $f_1, \ldots, f_n \in k[t_1, \ldots, t_m]$. F je možno chápat jako zobrazení $k^m \to k^n$ takto

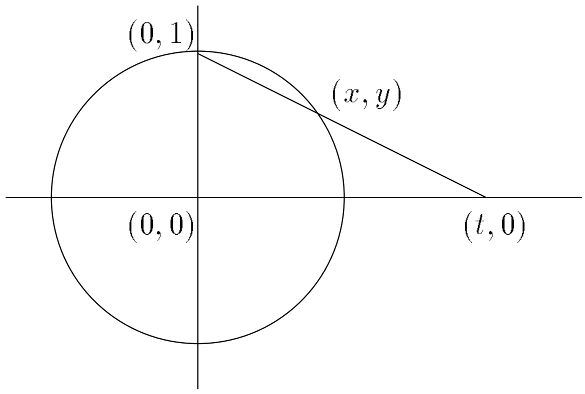
$$x_1 = f_1(t_1, \ldots, t_m)$$
$$\vdots$$
$$x_n = f_n(t_1, \ldots, t_m)$$

Cílem implicitizace je nalézt varietu $\mathfrak{V}(g_1, \ldots, g_s)$ parametricky zadanou systémem F, tj. nejmenší afinní varietu $V \subseteq k^n$ obsahující $F(k^m)$. Podobně pro racionální parametrizace.

Například kružnice (obrázek 7) $\mathfrak{V}(x^2 + y^2 = 1)$ je implicitizací parametrického vyjádření

$$y = \frac{1 - t^2}{1 + t^2} \quad x = \frac{2t}{1 + t^2}$$

Bodu $(0, 1)$ ovšem parametrickým vyjádřením nikdy nedosáhneme, bez něj by ale $F(\mathbb{R}^2)$ nebyla varieta.

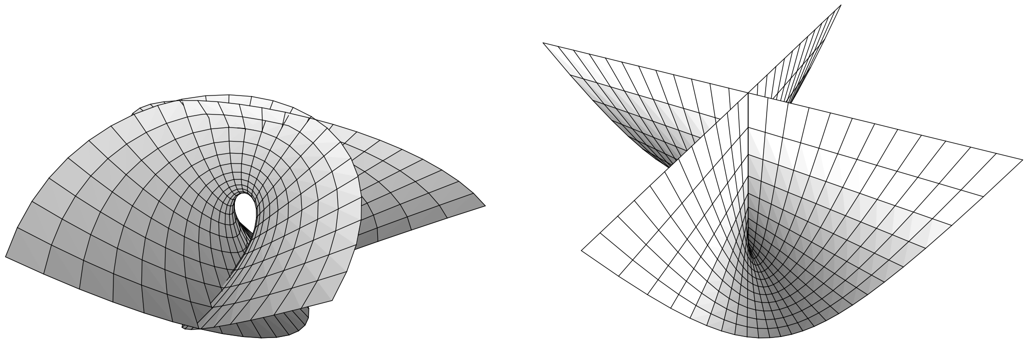


Obr. 7: Implicitizace kružnice

5.3 Věta O POLYNOMIÁLNÍ IMPLICITIZACI. *Nechť k je nekonečné pole, $F\colon k^m \to k^n$ polynomiální zobrazení $F = (f_1, \ldots, f_n)$ a $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subseteq k[t_1, \ldots, t_m, x_1, \ldots, x_n]$. Pak $V(I_m)$ m-tého eliminačního ideálu je nejmenší afinní varieta v k^n obsahující $F(k^m)$.*
Tedy sestrojíme-li varietu $V = \mathfrak{V}(x_1 - f_1, \ldots, x_n - f_n)$, a „vyeliminujeme“ z příslušných polynomů hodnoty parametrů $t_1, \ldots, t_m$, dostaneme právě implicitní popis hledané variety – uzávěru $F(k^m)$. *Důkaz:* Označme $p_m : k^{m+n} \to k^n$ projekci zapomínající prvních m komponent. Přímo z definice I je $F(k^m) = p_m\big(\mathfrak{V}(I)\big)$. Proto pro algebraicky uzavřené pole k plyne tvrzení přímo z věty o uzávěru (4.16).

Uvažujme tedy algebraicky uzavřené rozšíření $K \supset k$, označme $\bar{I} = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subseteq K[t_1, \ldots, t_m, x_1, \ldots, x_n]$. Přímo z definice I a $\bar{I}$ je

$$F(k^m) = p_m\big(\mathfrak{V}(I)\big) \subseteq V(I_m)$$



Obr. 8: Enneperova plocha a Whitneyho deštník

Uvažme tedy nějakou jinou varietu $Z = \mathfrak{V}(g_1, \ldots, g_s) \subseteq k^n$ tak, že $F(k^m) \subseteq Z_k$. Odsud $g_i \circ F = 0$ na každém $(t_1, \ldots, t_m) \in k^m$. Stejná vlastnost platí i v K^m, a tedy i varieta Z_K generovaná stejnými polynomy $g_1, \ldots, g_s$ v K^n obsahuje $F(K^m)$. Lze tedy aplikovat větu o uzávěru a dostáváme $V(\bar{I}_m) \subseteq Z_K$. Zpětným zúžením na k získáme žádané $V(I_m) \subseteq Z$. $\square$

Z předchozí věty už vyplývá podoba algoritmu pro implicitizaci. Spočteme redukovanou Gröbnerovu bázi ideálu $\langle x_1 - f_1, \ldots, x_n - f_n \rangle$ v lexikografickém uspořádání, kde $t_i > x_j$ pro každé i, j. Dále snadno stanovíme I_m a to je přesně hledaný ideál.

Respektive stačí takové uspořádání, které zaručí převahu všech t_i nad x_j, aby se algoritmem pro výpočet Gröbnerovy báze eliminovala t_i, jinak může být uspořádání libovolné. Máme tak naději dosáhnout efektivnějšího výpočtu, než s čistým lexikografickým uspořádáním.

Jako příklady můžeme uvést už dříve zobrazené variety v $\mathbb{R}^3$ nazývané Enneperova plocha a Whitneyho deštník, viz. obr. 8. Jejich parametrický popis je $x = 3u + 3uv^2 - u^3$, $y = 3v + 3u^2v - v^3$, $z = 3u^2 - 3v^2$, resp. $x = uv$, $y = v$, $z = u^2$. Aplikace eliminační procedury (např. v systému MAPLE za použití `gbasis` s uspořádáním `plex`) dá odpovídající implicitní popisy. V případě Enneperovy plochy je to odpudivý polynom:

$-59049z - 104976z^2 - 6561y^2 - 72900z^3 - 18954y^2z - 23328z^4 + 32805z^2x^2 + 14580z^3x^2 + 3645z^4x^2 - 1296y^4z - 16767y^2z^2 - 6156y^2z^3 - 783y^2z^4 + 39366zx^2 + 19683x^2 - 1296y^4 - 2430z^5 + 432z^6 + 108z^7 + 486z^5x^2 - 432y^4z^2 + 54y^2z^5 + 27z^6x^2 - 48y^4z^3 + 15y^2z^6 - 64y^6 - z^9$

Výsledný implicitní popis Whitneyho deštníku je jednodušší: $x^2 - y^2z$

Racionální implicitizací rozumíme analogický postup pro racionální lomené funkce

$$x_i = \frac{f_i(t_1, \ldots, t_m)}{g_i(t_1, \ldots, t_m)}$$

Přímočaře se nabízející řešení dosadit do předchozí věty ideál $\langle x_1g_1 - f_1, \ldots, x_ng_n - f_n \rangle$ nefunguje. Například uvažujme

$$x = \frac{u^2}{v} \quad y = \frac{v^2}{u} \quad z = u$$

Dostáváme $I = \langle vx - u^2, uy - v^2, z - u \rangle$ a po eliminaci $I_2 = \langle z(x^2y - z^3) \rangle$. Správný výsledek je ale jenom $\mathfrak{V}(x^2y - z^3)$, tedy postup přidal navíc celou rovinu.

Řešení vypadá tak, že zavedeme varietu nulových bodů jmenovatelů $W = \mathfrak{V}(g_1, \ldots, g_n)$ a zobrazení F chápeme jako $(k^m - W) \to k^n$. Pro implicitizaci použijeme ideál

$$I = \langle g_1 x_1 - f_j, \ldots, g_n x_n - f_n, 1 - g_1 \cdots g_n y \rangle \subseteq k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$$

Potom $V(I_{m+1})$ je minimální afinní varieta obsahující $F(k^m - W)$. Důkaz už se vede v podstatě analogicky předchozí větě. Stěžejním bodem je ověření, že pokud se polynom nuluje na $k^m - W$, nuluje se už na celém k^m. Viz. [2], str. 132.

5.3 Algebraické křivky

5.4 Definice. Nechť $f \in k[x, y]$. Varietu $\mathfrak{V}(f)$ nazveme *algebraickou křivkou* v k^2 (v rovině).

V následující části půjde především o postižení pojmu tečny a singulárního bodu, tj. takového bodu na křivce, kde je pojem tečny těžko definovatelný.

5.5 Definice. Nechť $m \in \mathbb{N}$, $(a, b) \in \mathfrak{V}(f)$ a L je přímka taková, že $(a, b) \in L$. Řekneme, že L protíná $\mathfrak{V}(f)$ v (a, b) *s násobností m,* jestliže L lze parametrizovat

$$\begin{aligned} x &= a + ct \\ y &= b + dt \end{aligned}$$

tak, že $t = 0$ je m-násobný kořen polynomu $f(a + ct, b + dt) \in k[t]$.
Označme

$$\nabla f(p, q) := \left(\frac{\partial f}{\partial x}(p, q), \frac{\partial f}{\partial y}(p, q) \right)$$

5.6 Lemma. *Nechť $f \in k[x, y]$ a $(a, b) \in \mathfrak{V}(f)$. Pak platí*

1. *Je-li $\nabla f(a, b) \neq (0, 0)$, pak existuje právě jedna přímka L procházející bodem (a, b), která v něm protíná $\mathfrak{V}(f)$ s násobností alespoň 2.*

2. *Je-li $\nabla f(a, b) = (0, 0)$, pak každá přímka procházející (a, b) v něm protíná $\mathfrak{V}(f)$ s násobností alespoň 2.*

Důkaz: Označme $g(t) := f(a + ct, b + dt)$. Protože $(a, b) \in \mathfrak{V}(f)$, je $t = 0$ kořen g. Derivujme podle proměnné t

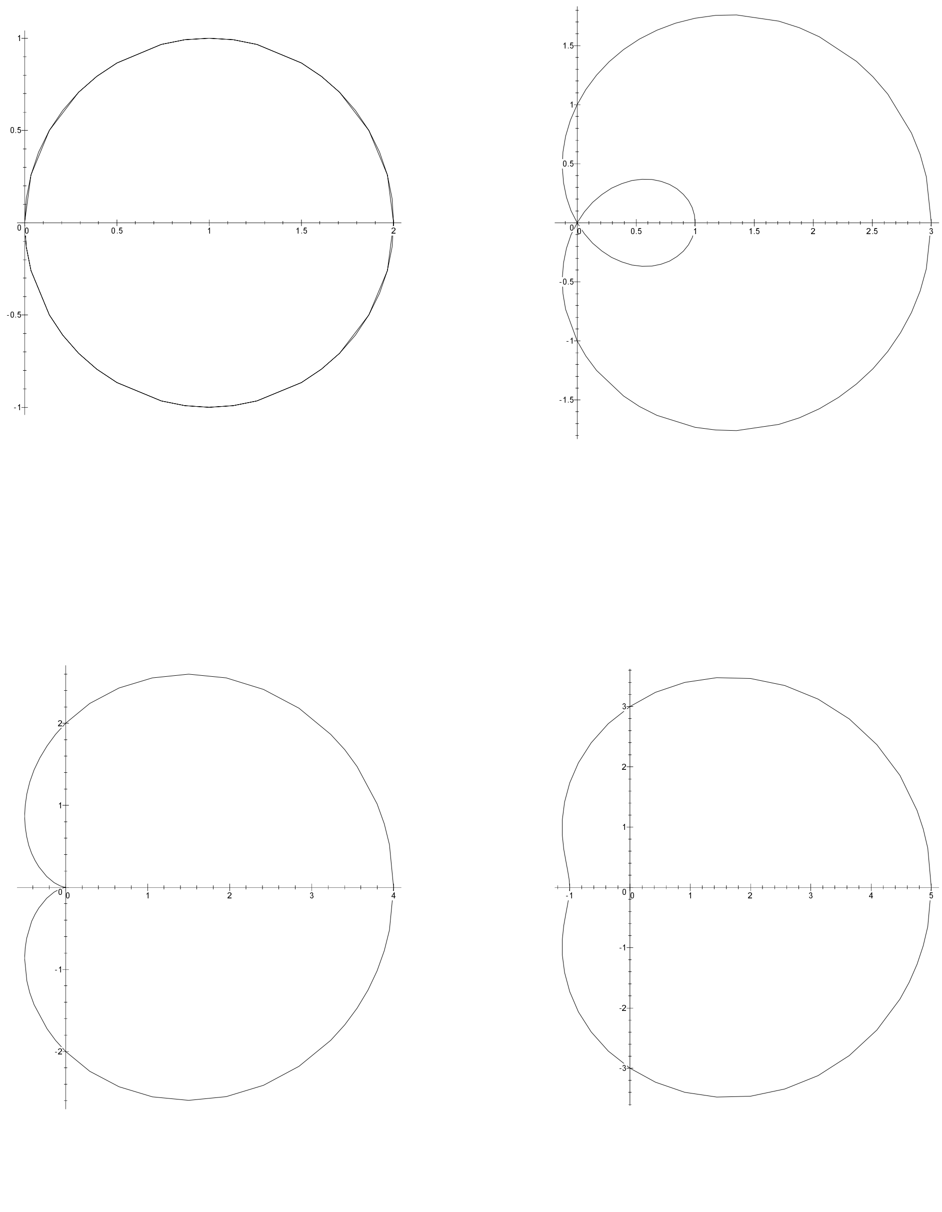
$$g'(t) = \frac{\partial f}{\partial x}(a + ct, b + dt) \cdot c + \frac{\partial f}{\partial y}(a + ct, b + dt) \cdot d$$

V bodě $t = 0$ potom

$$g'(0) = \frac{\partial f}{\partial x}(a, b) \cdot c + \frac{\partial f}{\partial y}(a, b) \cdot d$$

Tedy pokud $\nabla f(a, b) = (0, 0)$, je $g'(0) = 0$, a tedy $t = 0$ je alespoň dvojnásobný – druhá část tvrzení.

Pokud $\nabla f(a, b) \neq (0, 0)$, dostaneme z podmínky $g'(0) = 0$ jednorozměrný prostor řešení pro dvojici (c, d). To spolu s požadavkem $(a, b) \in L$ udává přímku jednoznačně. □



Obr. 9: Křivky $\mathfrak{V}(f)$ s $f(x, y) = (x^2 + y^2 - 2x)^2 - a^2(x^2 + y^2)$, $a = 0, 1, 2, 3$

5.7 Definice. Nechť $f \in k[x,y]$. Body $(a,b) \in \mathfrak{V}(f)$ s vlastností $\nabla f(a,b) = (0,0)$ se nazývají *singulární* body křivky $\mathfrak{V}(k)$, ostatní *regulární.* Přímka protínající $\mathfrak{V}(f)$ v regulárním bodě s násobností alespoň 2 se nazývá *tečna.*

Singulární body mohou velmi zajímat inženýry. Pokud křivka popisuje pohyb nějaké součásti, singulární bod je vždy podezřelé místo – jedná se o bod zvratu, křížení apod. Jejich určení má tedy bezprostřední praktický význam.

Množina singulárních bodů dané křivky je zřejmě právě varieta

$$\mathfrak{V}\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right)$$

Existence singulárních bodů je tedy na základě předchozí teorie problém algoritmicky řešitelný (nad $\mathbb{C}$), mnohdy se podaří je přímo nalézt.

Například pro křivky z obr. 9 dostaneme (třeba aplikací procedury `gsolve` v MAPLE), že pro každou hodnotu parametru a existuje vždy právě jeden singulární bod $(0,0)$. Pro $a > 1$ je to izolovaný bod, pro $a = 1$ je to „bod vratu“, pro menší dochází k samoprotnutí křivky.

5.4 Obálky systému křivek

Polynom $F \in k[x,y,t]$ budeme chápat jako proměnnou t parametrizovaný systém křivek $\mathfrak{V}(F_t)$ v $k[x,y]$ daných rovnicemi $F(x,y,t) = 0$. Například

$$(x-t)^2 + \left(y - 2t^2\right)^2 - 1 = 0$$

definuje systém kružnic o poloměru 1, jejichž střed se pohybuje po parabole $y = 2x^2$, viz. obr. 10.

5.8 Definice. Říkáme, že dvě křivky mají *dotyk řádu m,* jestliže je lze lokálně parametrizovat[11] hladkým zobrazením tak, aby parametrizace v bodě dotyku měly stejné derivace až do řádu m včetně. Maximální křivka, kterou lze lokálně parametrizovat tak, aby každý bod v této parametrizaci byl prvkem právě jedné z křivek daného systému a měl s ní v něm dotyk alespoň řádu 1, se nazývá *obálka* daného systému.

5.9 Věta. *Obálka systému křivek $F \in k[x,y,t]$ je obsažena ve varietě*

$$\mathfrak{V}\left(F, \frac{\partial F}{\partial t}\right)$$

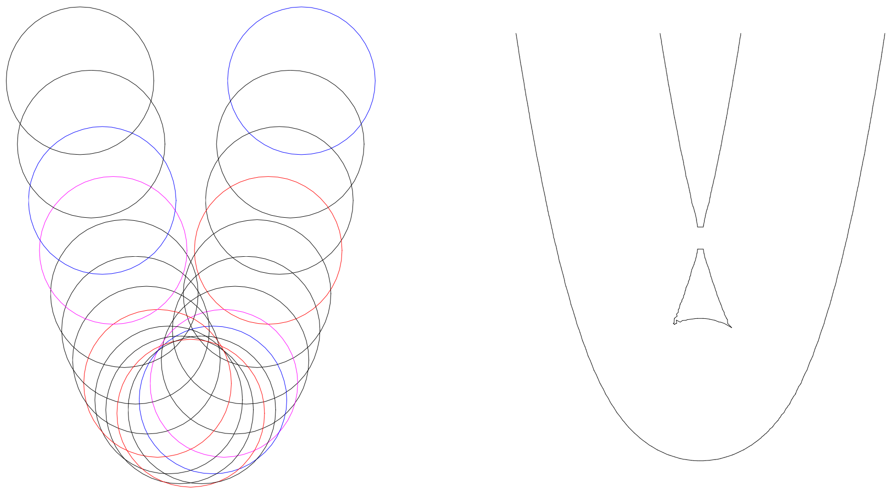
Důkaz: Nechť je obálka parametrizována $x = f(t)$, $y = g(t)$. Pro každé $t \in k$ požadujeme příslušnost ke křivce, tj.

$$(f(t), g(t)) \in \mathfrak{V}(F_t)$$

Navíc, aby křivka byla obálka, musí být ∇F_t v bodě $(f(t), g(t))$ kolmý na $(f'(t), g'(t))$. Kdo nevěří, ať si zopakuje analýzu. Kolmost znamená nulovou hodnotu skalárního součinu, tj.

$$\frac{\partial F}{\partial x}(f(t), g(t), t) \cdot f'(t) + \frac{\partial F}{\partial y}(f(t), g(t), t) \cdot g'(t) = 0 \tag{3}$$

[11] Křivku nemusí nutně jít parametrizovat, ale pro nějaké dostatečně malé okolí daného bodu se to podaří.



Obr. 10: Systém křivek $(x-t)^2 + (y-2t^2)^2 - 1 = 0$ a jejich obálka

Pouhým derivováním složené funkce $t \mapsto F(f(t), g(t), t)$ a následným dosazením za t dostaneme

$$\frac{\partial}{\partial t}\bigg|_{t=s} F(f(t), g(t), t) = \frac{\partial F}{\partial x}(f(s), g(s), s) \cdot f'(s) + \frac{\partial F}{\partial y}(f(s), g(s), s) \cdot g'(s) + \frac{\partial F}{\partial t}(f(s), g(s), s)$$

Funkce F je na všech bodech tvaru $(f(s), g(s), s)$ nulová (vlastnost obálky), a tedy musí být nulová i její derivace podle t. O prvních dvou členech pravé strany víme, že jsou dohromady nulové, pokud uvažovaná křivka je obálka. Dohromady tedy dostáváme

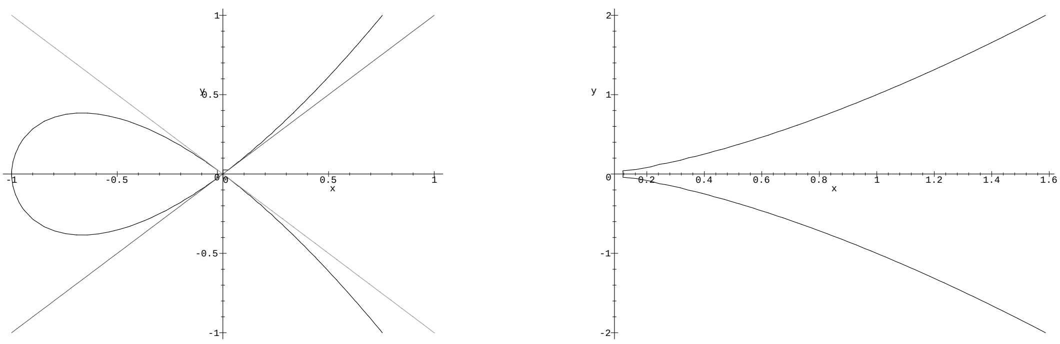
$$\frac{\partial F}{\partial t}(f(s), g(s), s) = 0$$

□

Pro všechny singulární body křivek systému je rovnost 3 splněna triviálně, a tedy i singulární body budou zahrnuty do výsledné variety.

Obálku systému kružnic se středy na parabole vidíme na obr. 10. K jejímu zadání jako afinní variety lze dospět v MAPLE např. posloupností příkazů h := **proc**(x, y, t) $(x-t)^2 + (y - 2 * t^2)^2 - 1$ **end**; **gbasis**$([h(x, y, t),$ **diff**$(h(x, y, t), t)], [t, x, y],$ **plex**), přičemž polynom definující hledanou obálku je generátor prvního eliminačního ideálu (poslední z výsledného seznamu). Vyjde $256x^6 + 256x^4y^2 - 320x^4y - 764x^4 - 256x^2y^3 - 384x^2y^2 + 60x^2y + 688x^2 + 64y^4 - 272y^3 + 225y^2 + 272y - 289$.

5.10 Tečny v singulárních bodech. Právě studium chování křivky v okolí singulárních bodů nám podá dobrou informaci o celé křivce. Všechny přímky procházející takovým bodem sice mají dotyk vyššího řádu, jistě je ale všechny nechceme považovat



Obr. 11: Tečný kužel křivek $\mathfrak{V}(x^3+x^2-y^2)$ a $\mathfrak{V}(X^3-y^2)$ v singulárním bodě

za tečny. Podle Taylorovy věty (snad dobře známé z matematické analýzy) má polynom f rozvoj v singulárním bodě (a,b)

$$f(x,y) = \underbrace{f(a,b)}_{=0 \text{ protože } (a,b\in K)} + \underbrace{\frac{\partial f}{\partial x}(a,b)(x-a) + \frac{\partial f}{\partial y}(y-b)}_{=0 \text{ protože je } (a,b) \text{ singulární}} +$$
$$+\frac{\partial^2 f}{\partial x^2}(a,b)(x-a)^2 + \frac{\partial^2 f}{\partial x \partial y}(a,b)(x-a)(y-b) + \frac{\partial^2 f}{\partial y^2}(a,b)(y-a)^2 + \dots$$

Předpokládejme, že $f_r(x-a,y-b) = \sum_{i=1}^{r} \frac{\partial^r f}{\partial x^i \partial y^{r-i}}(a,b)(x-a)^i(y-a)^{r-i}$ je první nenulová homogenní část. Pak množina všech řešení $(u:v)$ rovnice $f_r(u,v)=0$ dává směrové vektory *tečen v singulárním bodě* (a,b). Množinu všech těchto tečen nazýváme *tečný kužel křivky* K v singulárním bodě (a,b).

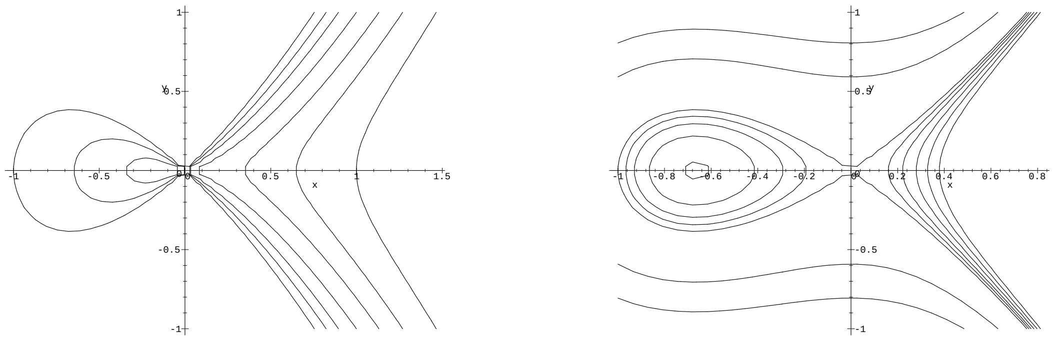
5.11 Příklad. Pro kubickou křivku $K = \mathcal{V}(x^3+x^2-y^2)$ snadno spočteme, že její jediný singulární bod je $(0,0)$, první nenulová homogenní část polynomu je x^2-y^2, tečný kužel je tedy tvořen dvěma přímkami $x \pm y = 0$, viz. obrázek 11.

5.12 Deformace singularit. Jednoduchý postup jak zjistit chování křivky v okolí regulárního bodu je spočíst její tečnu v tomto bodě. Pro singulární body je to sice s tečnami složitější, často však stačí libovolně málo pozměnit vhodný parametr (tj. koeficient) definujícího polynomu a singularita vymizí. Z chování tečen pro blízké hodnoty parametru můžeme usuzovat na typ původní singularity. Již jsme se potkali se singularitou v počátku u křivek $\mathcal{V}(x^3-y^2)$ (násobná tečna – osa x) a $\mathcal{V}(x^3+x^2-y^2)$. Uvažme polynomy

$$f_\varepsilon = x^3-y^2-\varepsilon,\ g_\delta = x^3+\delta x^2-y^2,\ h_{\varepsilon,\delta} = x^3+\delta x^2-y^2-\varepsilon.$$

Polynomy f_0 a g_0 dávají první z našich křivek, g_1 dá druhou.

Podívejme se nejprve na chování křivek $\mathcal{V}(g_\delta)$. Snadno spočteme, že vždy mají pouze jeden singulární bod $(0,0)$, jeho typ je ovšem zcela odlišný pro $\delta<0$ a $\delta>0$.



Obr. 12: Deformace singularit křivek

Je-li δ kladné, pak nám vyjdou dvě reálné tečny ve směrech $(1 : \pm\sqrt{\delta})$, zatímco pro $\delta < 0$ vyjdou obě tečny imaginární, je proto počátek izolovaným bodem křivky, viz. levý obrázek na 12.

Při deformacích f_ε je situace ještě daleko jednodušší. Pro nenulové ε totiž budou všechny body křivky regulární, viz. pravý obrázek na 12.

V obou případech získáváme jasnou představu o typu singularity Neilovy paraboly $\mathcal{V}(x^3 - y^2)$. Diskusí současných deformací $h_{\varepsilon,\delta}$ dospějeme ke křivce hodnot parametrů $\mathcal{V}(\varepsilon) \cup \mathcal{V}(\varepsilon - \frac{4\delta^3}{27})$, pro které křivky obsahují nějaký singulární bod, pro všechny hodnoty vně této křivky jsou všechny body regulární. Tvar křivky se přitom podstatně mění pouze při přechodech mezi uvedenými čtyřmi oblastmi. Hodnoty odpovídající Neilově parabole jsou právě jediným bodem společným všem čtyřem oblastem.

6 Algebraické důkazy geometrických tvrzení

Některá geometrická tvrzení lze poměrně jednoduše převést na algebraická a použít algebraické metody k jejich důkazu. Takových postupů je k dispozici několik, my se soustředíme pouze na jednu metodu, která využívá k důkazům již vybudovaného aparátu.

6.1 Metoda Gröbnerových bazí

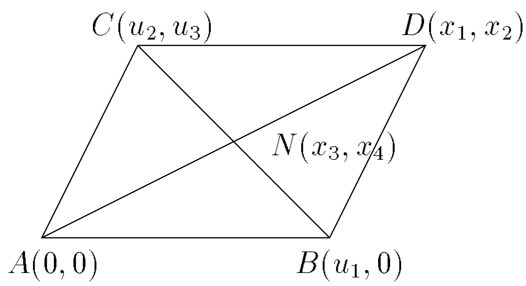
Začněme příkladem. Budeme cvičně uvažovat tvrzení, že uhlopříčky rovnoběžníka se navzájem půlí. Uvažujme rovnoběžník se souřadnicemi vrcholů podle obrázku 13. Proměnné u_1, u_2, u_3 jsou volné, zadávají rovnoběžník, $x_1, \dots, x_4$ jsou na nich závislé.

Sformulujme nejprve předpoklad, že se jedná o rovnoběžník. Přímka $\overline{CD}$ musí být rovnoběžná s $\overline{AB}$, tedy $h_1 := x_2 - u_3 = 0$. Podobně se musí rovnat směrnice $\overline{AC}$ a $\overline{BD}$

$$\frac{u_3}{u_2} = \frac{x_2}{x_1 - u_1} \quad \text{tedy } h_2 := u_3(x_1 - u_1) - u_2 x_2 = 0$$

Varieta $\mathfrak{V}(h_1, h_2)$ dává podmínky na rovnoběžník. Požadujeme kolinearitu bodů A, N, D, tedy dostáváme $h_3 := x_1x_4 - x_2x_3 = 0$. Analogicky z kolinearity B, N, C získáme polynom $h_4 := x_4(u_2 - u_1) - (x_3 - u_1)u_3$. Tím jsme popsali, že N je průsečík uhlopříček. Samozřejmě, že jsme mohli zvolit i jiný (dokonce jednodušší) systém polynomů popisující stejný geometrický objekt. Ten náš je v jistém smyslu co nejprimitivnější, využívající jen popis rovnosti směrů a rovnosti vzdáleností bodů.

Chceme ukázat, že se uhlopříčky půlí, tedy $x_3^2 + x_4^2 = (x_3 - x_1)^2 + (x_4 - x_2)^2$. Podobně pro druhou uhlopříčku $(x_3 - u_1)^2 + x_4^2 = (x_3 - u_2)^2 + (x_4 - u_3)^2$. Dostaneme tak polynomy g_1, g_2 jejichž vynulování máme odvodit za předpokladu vynulování předpokladů h_1, h_2, h_3, h_4.



Obr. 13: Označení bodů v rovnoběžníku

Zdá se tedy, že vše co potřebujeme je přesně zachyceno v následující definici.

6.1 Definice. Řekneme, že $g \in \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$ *silně vyplývá* z $h_1, \dots, h_r$, jestliže $g \in \mathfrak{I}(\mathfrak{V}(h_1, \dots, h_r))$.

6.2 Věta. *Je-li $g \in \sqrt{\langle h_1, \dots, h_r \rangle}$, pak g silně vyplývá z $h_1, \dots, h_r$.*

Důkaz: Z definice radikálového ideálu plyne $g^s \in \langle h_1, \dots, h_r \rangle$ pro vhodné s. Tedy g^s se nuluje na všech bodech dané variety, a tedy nutně i $g \in \mathfrak{I}(\mathfrak{V}(h_1, \dots, h_r))$. □

Obrácení věty v případě algebraicky uzavřeného pole plyne z Hilbertovy věty o nulách.

Příslušnost polynomu g k radikálovému ideálu se určí snadno výpočtem redukované Gröbnerovy báze (dokonce pro libovolné nekonečné pole k):

6.3 Věta. *Nechť k je libovolné nekonečné pole a $g, h_1, \dots, h_r \in k[x_1, \dots, x_n]$. Pak $g \in \sqrt{\langle h_1, \dots, h_r \rangle}$ právě když je $\{1\}$ redukovaná Gröbnerova báze ideálu $I = \langle h_1, \dots, h_r, 1 - yg \rangle \subset k[x_1, \dots, k_n, y]$.*

Důkaz: Předpokládejme nejprve, že konstantní polynom 1 patří do I. Pak stejně jako v závěru důkazu Hilbertovy věty o nulách dostáváme 1 jako lineární kombinaci polynomů h_i a $1 - yg$ a v $k(x_1, \dots, x_n)[y]$ můžeme za y dosadit $1/g$ a ověříme tak příslušnost g^m do $\langle h_1, \dots, h_r \rangle$. K tomuto kroku jsme ale nepotřebovali algebraickou uzavřenost k.

Naopak, je-li $g^m \in \langle h_1, \dots, h_r \rangle$, pak

$$1 = y^m g^m + (1 - y^m g^m) = y^m g^m + (1 - yg)(1 + yg + \dots + (yg)^{m-1}) \in I.$$

□

Spočítáme-li Gröbnerovu bázi ideálu $\langle h_1, \dots, h_4, 1 - yg_1 \rangle$ z předchozího případu, nezískáme $\{1\}$, tedy g_1 z předpokladů $h_1, \dots, h_4$ nevyplývá silně. Je-to díky případům, kdy $u_1 = 0$ nebo $u_3 = 0$ a rovnoběžník degeneruje na úsečku. Potom průsečíkem uhlopříček je dokonce nekonečně mnoho bodů a ty všechny nesplňují podmínku půlení.

Zkuste si spočíst Gröbnerovu bázi polynomů h_1, h_2, h_3, h_4 (v lex. uspořádání). Z ní bude jasně vidět, že v našem příkladě získáme ve skutečnosti čtyři komponenty diskutované variety $V \subset \mathbb{R}^7$. Můžeme je zapsat například jako

$$\begin{aligned}
V' &= \mathfrak{V}(x_1 - u_1 - u_2, x_2 - u_3, x_3 - \frac{u_1 + u_2}{2}, x_4 - \frac{u_3}{2}) \\
U_1 &= \mathfrak{V}(x_2, x_4, u_3) \\
U_2 &= \mathfrak{V}(x_1, x_2, u_1 - u_2, u_3) \\
U_3 &= \mathfrak{V}(x_1 - u_2, u_2 - u_3, x_3 u_3 - x_4 u_2, u_1)
\end{aligned}$$

Obecně jsou problémy tohoto rázu způsobeny právě neireducibilními varietami. Jediná možná cesta z těchto komplikací je revize pojmu důsledku. Budeme požadovat, aby dokazované tvrzení platilo pouze na těch komponentách, kde jsou námi zvolené volné parametry u_i skutečně nezávislé:

6.4 Definice. Nechť $W \subseteq \mathbb{R}^{m+n}$ je ireducibilní varieta, souřadnice značíme $u_1, \dots, u_m, x_1, \dots, x_n$. Řekneme, že souřadné funkce $u_1, \dots, u_m$ jsou *algebraicky nezávislé* na W, jestliže neexistuje polynom v $\mathbb{R}[u_1, \dots, u_n]$ patřící do $\mathfrak{I}(W)$.

6.5 Definice. Řekneme, že hypotéza g vyplývá *genericky* z předpokladů $h_1, \dots, h_r$, jestliže

$$g \in \mathfrak{I}(V') \subseteq \mathbb{R}[u_1, \dots, u_m, x_1, \dots, x_n]$$

kde $V' \subseteq \mathbb{R}^{m+n}$ je sjednocení těch ireducibilních komponent variety $V = \mathfrak{V}(h_1, \dots, h_r)$, na kterých jsou $u_1, \dots, u_m$ algebraicky nezávislé.

Rozklad variety na ireducibilní komponenty lze provést algoritmicky. Jde však o komplikovanou proceduru, je naimplementovaná například v systému Axiom. Není však nezbytně nutný, jak ukážeme v následujícím.

6.6 Věta. *Hypotéza g vyplývá genericky z $h_1, \ldots, h_r$, jestliže existuje nenulový polynom $c \in \mathbb{R}[u_1, \ldots, u_m]$ tak, že*

$$c \cdot g \in \sqrt{\langle h_1, \ldots, h_r \rangle}.$$

Je-li pole k algebraicky uzavřené, pak platí i obrázená implikace

Důkaz: Nechť V_j je nějaká z komponent V' dle definice 6.5. Protože cg se nuluje na V, musí se nulovat i na V_j, tedy $cg \in \mathfrak{I}(V_j)$. To je prvoideál podle věty 4.22, ale $c \notin \mathfrak{I}(V_j)$ (požadováno v definici 6.5), a tedy $g \in \mathfrak{I}(V_j)$.

Předpokládejme nyní, že g vyplývá genericky z $h_1, \ldots, h_r$ a k je algebraicky uzavřené. Nechť $V_1, \ldots, V_k$ jsou všechny ireducibilní komponenty na kterých jsou $u_1, \ldots, u_m$ algebraicky závislé, tjèxistují polynomy $c_1, \ldots, c_k \in k[u_1, \ldots, u_m]$, $c_i \in \mathfrak{I}(V_j)$. Nyní stačí zvolit $c = c_1 c_2 \ldots c_k$ a z definice plyne, že $cg \in \mathfrak{I}(V)$. Protože je k algebraicky uzavřené, plyne odtud příslušnost do radikálnového ideálu. □

Pro praktické použití předchozí věty je vhodné formulovat ekvivalentní kritéria. Jako obvykle, budeme uvažovat

$$\mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n] \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n].$$

6.7 Věta. *Následující tvrzení jsou ekvivalentní*

1. *Existuje $c \in \mathbb{R}[u_1, \ldots, u_m]$ nenulový tak, že $cg \in \sqrt{\langle h_1, \ldots, h_r \rangle}$.*
2. *$g \in \sqrt{H}$, kde $H = \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$.*
3. *$\{1\}$ je redukovaná Gröbnerova báze $\langle h_1, \ldots, h_r, 1 - yg \rangle$ opět v okruhu polynomů $\mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$.*

Důkaz: Ukážeme nejprve (1) ⇔ (2). Předpokládejme, že platí (1), tj. $(cg)^s = \sum_{j=1}^n a_j h_j$ pro vhodné polynomy $a_j \in \mathbb{R}[u_1, \ldots, u_m, x_1, \ldots, x_n]$ a $s \geq 1$. Odtud

$$g^s = \sum_{j=1}^n \frac{a_j}{c^s} h_j$$

což značí právě $g^s \in \langle h_1, \ldots, h_r \rangle \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$, neboli g patří do příslušného radikálu.

Naopak, patří-li g do $\sqrt{\langle h_1, \ldots, h_r \rangle} \subset \mathbb{R}(u_1, \ldots, u_m)[x_1, \ldots, x_n]$, pak $g^s = \sum_{j=1}^n b_j h_j$. Vynásobením mocninou společného násobku všech jmenovatelů racionálních funkcí lomených b_j dostaneme výraz tvaru $(cg)^s = \sum_{j=n} b'_j h_j$, kde koeficienty b'_j jsou již polynomy.

Ekvivalenci druhého a třetího tvrzení jsme již ukázali, viz. 6.3 □

Tedy opět vystačíme s počítámím Gröbnerových bází, rozklad na ireducibilní komponenty není pro tyto účely třeba.

6.2 Příklady

Závěrem ukážeme aplikaci předchozích úvah při důkazu jedné z Apolloniových vět. Vraťme se ale nejprve k úvodnímu příkladu.

Již jsme zmínili rozklad $\mathfrak{V}(h_1, \ldots, h_4)$ na variety

$$\begin{aligned} V' &= \mathfrak{V}(x_1 - u_1 - u_2, x_2 - u_3, x_3 - (u_1 + u_2)/2, x_4 - u_3/2) \\ U_1 &= \mathfrak{V}(x_2, x_4, u_3) \\ U_2 &= \mathfrak{V}(x_1, x_2, u_1 - u_2, u_3) \\ U_3 &= \mathfrak{V}(x_1 - u_2, u_2 - u_3, x_3 u_3 - x_4 u_2, u_1) \end{aligned}$$

Jedině na komponentě V' jsou u_1, u_2, u_3 algebraicky nezávislé, zbývající komponenty popisují degenerované případy. V_1 a V_2 znamenají, že bod C leží na přímce $\overline{AB}$, V_3 znamená splynutí bodů A a B.

Ověřme si výsledek nalezením příslušné Gröbnerovy báze. V systému MAPLE to vypadá takto:

```
with(grobner):
> g1:=x1^2 - 2*x1*x3 - 2*x4*x2 + x2^2:
> g2:=2*x3*u1 - 2*x3*u2 - 2*x4*u3 - u1^2 + u2^2 + u3^2:
> gbasis([x1-u1-u2, x2-u3,x3-(u1+u2)/2,x4-u3/2,1-y*g1],
[u1,u2,u3,x1,x2,x3,x4,y]);
```

$$[1]$$

```
> gbasis([x1-u1-u2, x2-u3,x3-(u1+u2)/2,x4-u3/2,1-y*g2],
[u1,u2,u3,x1,x2,x3,x4,y]);
```

$$[1]$$

Odtud je vidět, že na komponentě V' opravdu g_1 i g_2 skutečně silně vyplývá z předpokladů. Pro původní polynomy h_i ovšem dostaneme něco jiného:

```
> gbasis([x2-u3, (x1-u1)*u3- x2*u2, x1*x4 - x2*x3, x4*(u2-u1) -
(x3-u1)*u3, 1-y*g1],[u1,u2,u3,u4,x1,x2,x3,x4,y]);
```

$$\begin{gathered}[-x1\,x4 + x4\,u2, x4\,u1, -1 + y\,x1^2 - 2\,y\,x1\,x3 - 2\,y\,x4\,x2 + y\,x2^2, \\ -x2 + u3, -x1\,x4 + x2\,x3, x2\,u1, x2\,u2 - x2\,x1]\end{gathered}$$

Pokud ovšem použijeme původní polynomy, ale test pro generické implikování, dostáváme opět potřebnou bázi:

```
> gbasis([x2-u3, (x1-u1)*u3- x2*u2, x1*x4 - x2*x3, x4*(u2-u1) -
(x3-u1)*u3, 1-y*g1],[x1,x2,x3,x4,y]);
```

$$[1]$$

```
> gbasis([x2-u3, (x1-u1)*u3- x2*u2, x1*x4 - x2*x3, x4*(u2-u1) -
(x3-u1)*u3, 1-y*g2],[x1,x2,x3,x4,y]);
```

$$[1]$$

Nyní slíbená Apolloniova úloha. Chceme dokázat, že pro pravoúhlý trojúhelník jsou středy všech tří stran a pata výšky nad přeponou na jediné kružnici. K formulaci zadání budeme potřebovat osm polynomů $h_1, \ldots, h_8$, obsahující dva volné parametry (délky odvěsen) a osm volných proměnných $x_1, \dots, x_8$ (poslední dvě jsou souřadnice středu kružnice procházející středy stran trojúhelníka). Dokazované tvrzení je pak vyjádřeno jediným polynomem g:

```
> h1:= 2*x1 - u1: h2 := 2*x2 - u2: h3 := 2*x3 - u1: h4 := 2*x4 - u2:
> h5:= x5*u1 - x6*u2 : h6:= x5*u2 + x6*u1 - u1*u2:
> h7 := (x1-x7)^2 + x8^2 - x7^2 - (x8 - x2)^2:
> h8:= (x1-x7)^2 + x8^2 - (x3-x7)^2 - (x4-x8)^2:
> g := (x5-x7)^2 + (x6-x8)^2 - (x1-x7)^2 - x8^2:
> x:= seq(x.i, i=1..8): u:= u1,u2: h:= seq(h.i, i=1..8):
```

Nakreslete si sami obrázek! Potřebný test ověřující, že g genericky vyplývá z $h_1, \dots, h_8$ je positivní:

```
> gbasis([h,1-y*g],[x,y]);
```

$$[1]$$

Silně ovšem tvrzení nevyplývá:

```
> gbasis([h,1-y*g],[u,x,y]);
```

$[x1, x3, x4, x2, u2, -1 + y\,x5^2 - 2\,y\,x5\,x7 + y\,x6^2 - 2\,y\,x6\,x8, u1]$

Všimněme si ještě, že často vystačíme i s jednodušším testem. Může se totiž stát, že g patří přímo do ideálu generovaného h_i (v okruhu polynomů v nezávislých proměnných nad podílovým tělesem $\mathbb{R}(u_1, u_2)$). Stačí pak provést dělení se zbytkem podle Gröbnerovy baze:

```
> F:= gbasis([h], [x],plex);
```

$$F := [2\,x1 - u1, 2\,x2 - u2, 2\,x3 - u1, 2\,x4 - u2, -u2^2\,u1 + (\,u2^2 + u1^2\,)\,x5,$$
$$-u1^2\,u2 + (\,u2^2 + u1^2\,)\,x6, -u1 + 4\,x7, -u2 + 4\,x8]$$

```
> normalf(g, F, [x],plex);
```

$$0$$

Zájemcům doporučuji zkusit si další jednoduché (či složitější) úlohy samostatně.

Literatura

[1] B. Buchberger. Groebner bases: an algorithmic method in polynomial ideal theory. In N. K. Bose, editor, *Multidimensional Systems Theory*, pages 184–232. D. Reidel Publishing Company, Dordrecht, 1985.

[2] David Cox, John Little, and Donal O'Shea. *Ideals, Varieties, and Algorithms.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, Inc., 1992.