Diskrétní matematika B – 10. (zkrácený) týden
Systémy polynomiálních rovnic

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

1. Polynomy více proměnných
   - Těleso racionálních funkcí
2. Variety a ideály
   - Dimenze 1
3. Dělení se zbytkem
4. Monomiální ideály a Hilbertova věta
   - Hilbertova věta (Hilbert basis theorem)
5. Gröbnerovy báze a eliminace proměnných

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Jiří Rosický, *Algebra*, PřF MU, 2002.
- Peter J. Cameron. *Introduction to algebra*, Oxford University Press, 2001, 295 s. (Dostupné v knihovně PřF).

Podílové těleso

Naší snahou nyní bude zobecnit způsob konstrukce racionálních čísel jakožto zlomků čísel celých.
Nechť R je obor integrity. Jeho **podílové těleso** (Field of fractions) definujeme jako třídy ekvivalence dvojic $(a, b) \in R \times R$, $b \neq 0$, které zapisujeme $\frac{a}{b}$, a ekvivalence je dána vztahem

$$\frac{a}{b} = \frac{a'}{b'} \quad \Leftrightarrow \quad ab' = a'b.$$

Sčítání a násobení definujeme prostřednictvím reprezentantů tříd

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Snadno se ověří korektnost této definice a všechny axiomy tělesa. Zejména je $\frac{0}{1}$ neutrální prvek vzhledem ke sčítání, $\frac{1}{1}$ je neutrální prvek vzhledem k násobení a pro $a \neq 0$, $b \neq 0$ je $\frac{a}{b}\frac{b}{a} = \frac{1}{1}$.

Touto konstrukcí „přidáme“ k okruhu R minimální množství prvků tak, abychom již mohli dělit libovolnými nenulovými prvky.

Příklad

Podílové těleso okruhu $R[x_1, \ldots, x_r]$ nazýváme **těleso racionálních funkcí** a značíme je $R(x_1, \ldots, x_r)$.

Všechny algebraické operace s polynomy v softwarových systémech jako je Maple nebo Mathematica jsou prováděny ve skutečnosti nad podílovými tělesy, tj. v tělesech racionálních funkcí, zpravidla s použitím $R = \mathbb{Q}$.

Multiindex

Připomeňme tzv. multiidexovou symboliku.

Multiindexy

Multiindex α délky r je r-tice nezáporných celých čísel $(\alpha_1, \ldots, \alpha_r)$. Celé číslo $|\alpha| = \alpha_1 + \cdots + \alpha_r$ nazýváme **velikost** multiindexu α.
Stručně zapisujeme monomy x^α místo $x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_r^{\alpha_r}$.
Pro polynomy v r proměnných pak máme symbolické vyjádření velice podobné obvyklému značení pro polynomy v jedné proměnné:

$$f = \sum_{|\alpha| \leq n} a_\alpha x^\alpha, \; g = \sum_{|\beta| \leq m} a_\beta x^\beta \in \mathbb{K}[x_1, \ldots, x_r].$$

Říkáme, že f má celkový stupeň n, je-li alespoň jeden z koeficientů s multiindexem α velikosti n nenulový.

Afinní variety

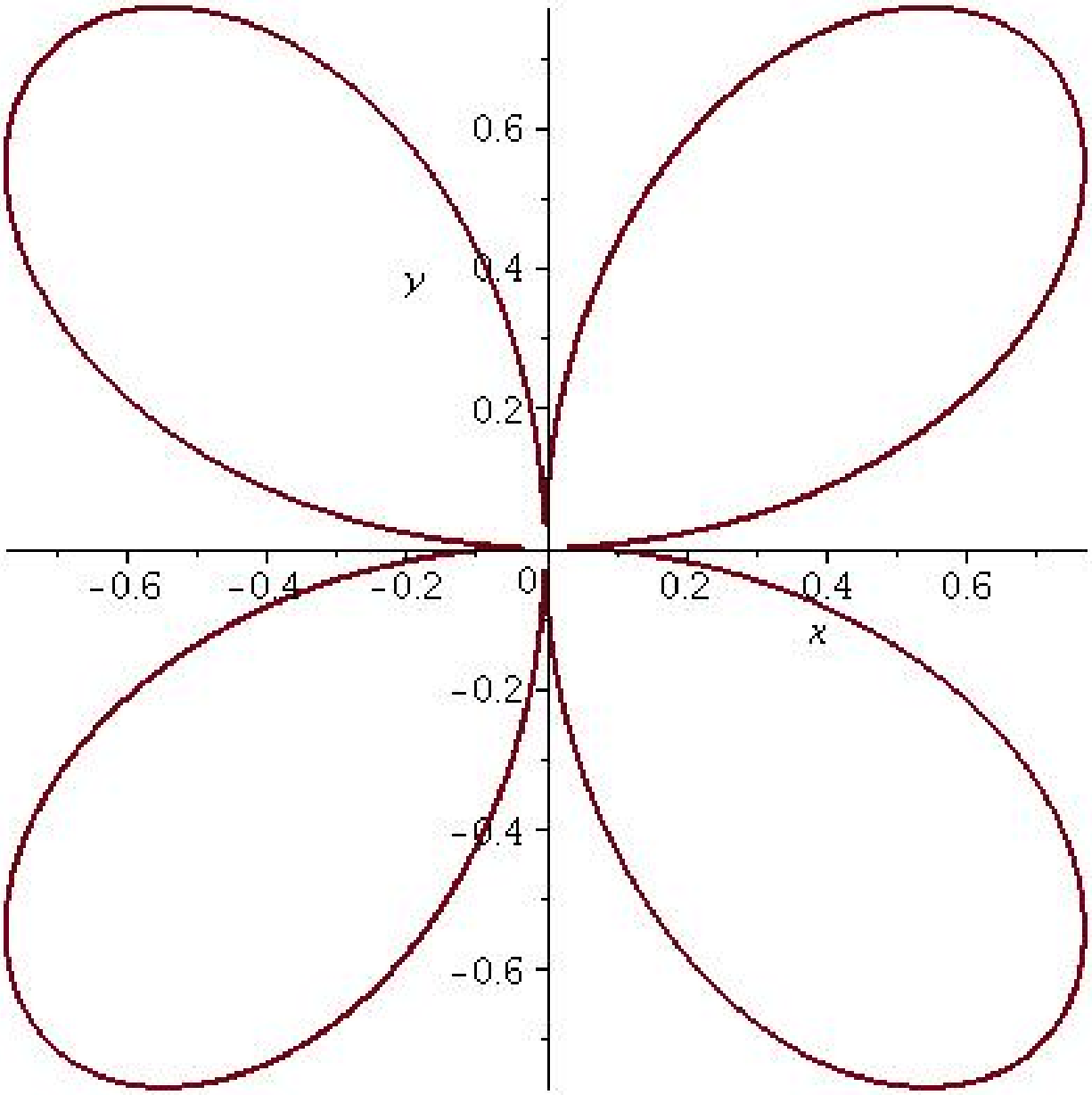
Pro jednoduchost (existence kořenů) budeme pracovat zejména nad $\mathbb{C}$, nicméně některé úvahy provedeme pro obecné těleso $\mathbb{K}$. Afinním n-rozměrným prostorem nad tělesem $\mathbb{K}$ rozumíme $\mathbb{K}^n = \underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{n}$ se standardní afinní strukturou.

Jak jsme již viděli, polynom $f = \sum_\alpha a_\alpha x^\alpha \in \mathbb{K}[x_1 \ldots, x_n]$ lze přirozeným způsobem chápat jako zobrazení $f : \mathbb{K}^n \to \mathbb{K}^n$ definované

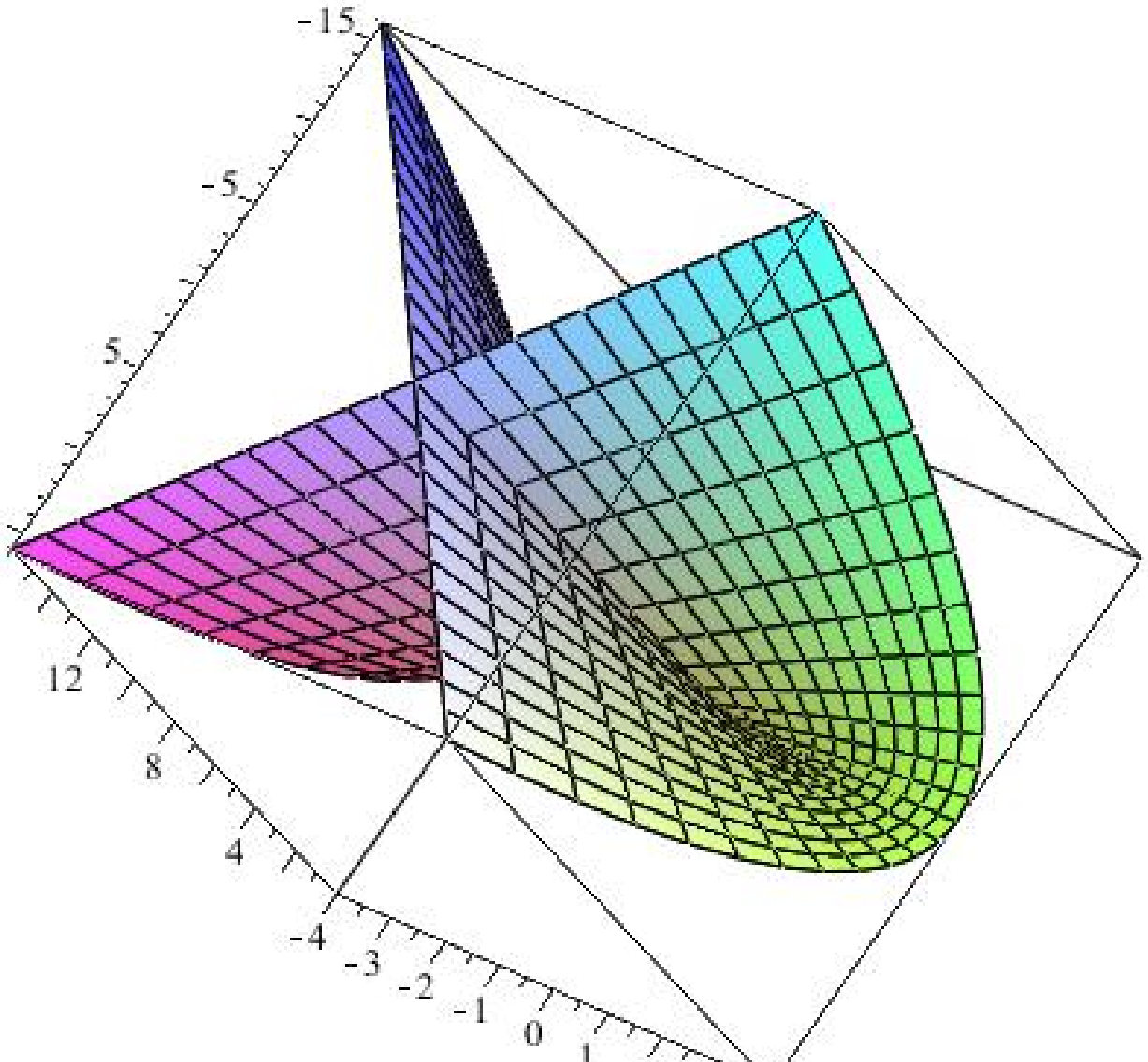
$$f(u_1, \ldots, u_n) := \sum_\alpha a_\alpha u^\alpha \quad \text{kde } u^\alpha = u_1^{\alpha_1} \cdots u_n^{\alpha_n}$$

V dimenzi $n = 1$ popisuje rovnost $f(x) = 0$ jen nejvýše konečně mnoho bodů v $\mathbb{K}$. Ve vyšší dimenzi bude rovnost $f(x_1, \ldots, x_n)$ popisovat podmnožiny podobné, jako jsou křivky v rovině nebo plochy v trojrozměrném prostoru, mohou ale mít docela složité a samoprotínající se tvary.

Např. množina zadaná rovnicí $(x^2 + y^2)^3 - 4x^2y^2 = 0$ vypadá jako čtyřlístek.



Pěkný obrázek dává také tzv. Whitneyho detník $x^2z - y^2 = 0$, který kromě znázorněné části na obrázku obsahuje také celou přímku $\{x = 0, y = 0\}$.



Definice

Nechť $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$. **Afinní varietou** v $\mathbb{K}^n$ určenou polynomy $f_1, \ldots, f_n$ nazveme množinu

$$\mathfrak{V}(f_1, \ldots, f_s) = \big\{(a_1, \ldots, a_n) \in \mathbb{K}^n, \\ f_i(a_1, \ldots, a_n) = 0;\ i = 1, \ldots, s\big\}$$

Afinní variety jsou například všechny kuželosečky, kvadriky a nadkvadriky singulární i regulární. Mnoho pěkných křivek či ploch můžeme snadno popsat jako afinní variety.

Věta

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

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

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?

Tyto problémy lze „rozumně“ řešit pro variety v oboru komplexních čísel (resp. pro všechna algebraicky uzavřená tělesa), pro reálná čísla je to komplikovanější a velmi obtížné to je pro obecná tělesa, tj. například racionální čísla.

Příklad

Např. rozhodnutí, zda $\mathfrak{V}(x^n + y^n - z^n) = \emptyset$ nad racionálními čísly vede na velkou Fermatovu větu.

Motivační příklad

Polynomiální rovnice mají celou řadu aplikací v mnoha oblastech – např. v softwarovém inženýrství, robotice (viz [MDS]) nebo třeba v teorii grafů.

Příklad

Graf $G = (V, E)$ nazveme 3-colourable, pokud je možné jeho vrcholy obarvit třemi barvami tak, aby sousední vrcholy neměly stejnou barvu. Pro „obarvení“ použijeme komplexní číslo

$$\zeta = e^{\frac{2\pi}{3}} = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}$$

a jeho mocniny. Snadno se uváží, že obarvení všech vrcholů $j \in V$ splňuje $x_j^3 = 1$ a pro sousední vrcholy j, k musí navíc platit, že $x_j \neq x_k$. Odtud se snadno odvodí, že požadovaný systém rovností je $x_j^2 + x_j x_k + x_k^2$ pro každou dvojici sousedních vrcholů a požadovaná vlastnost grafu je ekvivalentní s neprázdností příslušné variety.

Různé systémy polynomiálních rovnic mohou snadno zadávat stejnou varietu. Budeme proto spolu s daným systémem rovnic chtít uvažovat i všechny důsledky rovnic. To vede na pojem ideálu:

Definice

Množinu $I \subseteq R$, kde R je komutativní okruh, nazveme *ideálem*, platí-li $0 \in I$ a zároveň

$$f, g \in I \implies f + g \in I$$
$$f \in I, h \in \mathbb{K} \implies f \cdot h \in I$$

Ideály můžeme *generovat* podmnožinami, budeme používat značení $I = \langle a_1, \ldots, a_n \rangle$. Tím máme na mysli

$$I = \Big\{ \sum_i a_i b_i, \;\; b_i \in R \Big\}.$$

Množina generátorů může být také nekonečná, je-li generátorů jen konečný počet, říkame, že ideál je *konečně generovaný.*

Pro varietu $V = \mathfrak{V}(f_1, \ldots, f_s)$ klademe

$$\mathfrak{I}(V) := \left\{ f \in \mathbb{K}[x_1, \ldots, x_n],\ f(a_1, \ldots, a_n) = 0,\ \forall\, (a_1, \ldots, a_n) \in V \right\}$$

Věta

Nechť $f_1, \ldots, f_s, g_1, \ldots, g_t \in \mathbb{K}[x_1, \ldots, x_n]$ 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. *$\mathfrak{I}(\mathfrak{V}(f_1, \ldots, f_s))$ je ideál a platí $\langle f_1, \ldots, f_s \rangle \subseteq \mathfrak{I}(\mathfrak{V}(f_1, \ldots, f_s))$.*

Příklad

Jednoduché příklady:

$\mathfrak{I}\big(\{(0,0,\ldots,0)\}\big) = \langle x_1, \ldots, x_n \rangle$

$\mathfrak{I}(\mathbb{K}^n) = \{\,0\}$ pro libovolné nekonečné těleso $\mathbb{K}$

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 $V, W \subseteq \mathbb{K}^n$ 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.

Můžeme formulovat další přirozené problémy

1. Je každý ideál $I \in \mathbb{K}[x_1, \ldots, x_n]$ konečně generovaný?
2. Lze algoritmicky zjistit, zda $f \in \langle f_1, \ldots, f_s \rangle$?
3. Jaký je přesný vztah mezi $\langle f_1, \ldots, f_s \rangle$ a $\mathfrak{I}\big(\mathfrak{V}(f_1, \ldots, f_s)\big)$?

Dimenze 1

Podívejme se na polynomy v jedné proměnné x:

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

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

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

Nechť $\mathbb{K}$ je těleso a g nenulový polynom. Již jsme viděli, že každé $f \in \mathbb{K}[x]$ lze jednoznačně psát jako

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

Důsledek

Nechť $\mathbb{K}$ je těleso. Pak každý ideál v $\mathbb{K}[x]$ je tvaru $\langle f \rangle$.

Položili jsme několik otázek. Tady jsou odpovědi pro dimenzi 1:

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

Zadat varietu v prostoru pomocí dvou polynomů znamená zadat průnik obecně i dost komplikovaných útvarů.

Příklad

Např.

$$\mathfrak{V}(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z)$$

je kružnice ležící v rovině $z = \frac{1}{2} - \frac{1}{2}\sqrt{5}$. Jistě proto tutéž varietu zadáme 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.

Bude proto lepší varietu reprezentovat generujícím ideálem a pro ten nalézt vyjádření nezávislé na volbě generátorů. To skutečně budeme umět a navíc algoritmicky!

Nejprve najdeme pořádný ekvivalent pojmu stupeň polynomu pro případ více proměnných, tak abychom vůbec mohli mluvit o vedoucím členu polynomu.

Definice

Dělením se zbytkem polynomu $f \in \mathbb{K}[x_1, \ldots, x_n]$ polynomy $g_1, \ldots, g_s$ pak budeme rozumět vyjádření

$$f = a_1 g_1 + \cdots + a_s g_s + r,$$

kde žádný člen zbytku r nebude dělitelný některým z vedoucích členů $LT\, g_i$.

Příklad

Například $f = x^2y + xy^2 + y^2$, $g_1 = xy - 1$ a $g_2 = y^2 - 1$ (předpokládejme na chvíli, že členy polynomů máme uspořádány). Prvním dělením získáme

$$f = (x + y) \cdot g_1 + (x + y^2 + y)$$

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

$$f = (x + y) \cdot g_1 + g_2 + (x + y + 1)$$

Zde již žádný člen zbytku není dělitelný žádným z $LT(g_1)$, $LT(g_2)$.

Jak jsme ale vlastně určovali vedoucí členy?

Uspořádání na monomech

Definice

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

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

nazveme *monomiálním uspořádáním* na $\mathbb{K}[x_1, \ldots, x_n]$.

Uspořádání na $\mathbb{N}^n$ indukuje uspořádání na monomech.
Každý polynom lze však přeskládat jako klesající posloupnost monomů (na koeficienty teď nehledíme). Uspořádání na polynomy rozšíříme „lexikograficky“, tedy větší je ten polynom, který má větší první monom, pokud tak nelze rozhodnout, 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 $x_1 > x_2 > \cdots$.

Definice

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

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

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

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

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

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

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 $x^2yz^2 <_{\text{grevlex}} xy^3z$.

Lemma

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

Definice

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

- Stupeň multideg $f := \max\{\alpha \in \mathbb{N}^n,\ a_\alpha \neq 0\}$
- Vedoucí koeficient $LC\, f := a_{\text{multideg } f}$
- Vedoucí monom $LM\, f := x^{\text{multideg } f}$
- Vedoucí člen $LT\, f := LC\, f \cdot LM\, f$

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

Lemma

Nechť $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ *a* $<$ *je monomiální. Pak*

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

Věta (Dělení se zbytkem)

Nechť $<$ je monomiální a $F = (f_1, \ldots, f_s)$ s-tice polynomů v $\mathbb{K}[x_1, \ldots, x_n]$. Pak každý $f \in \mathbb{K}[x_1, \ldots, x_n]$ lze vyjádřit jako

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

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 multideg $f \geq$ multideg $a_i f_i$ *pro každé i.*
Polynom r nazýváme zbytkem po dělení f/F.

Věta neříká nic o jednoznačnosti výsledku. Následující algoritmus dává jedno možné řešení. Nadále budeme výsledkem dělení se zbytkem chápat právě tento výstup pevně zvoleného algoritmu.

1. $a_1 := 0, \ldots, a_s := 0, r := 0, p := f$
2. `while` $p \neq 0$
   1. $i := 1$
   2. $d := \mathit{false}$
   3. `while` $i \leq s \wedge \text{not } d$
      1. `if` $LT\, f_i | LT\, p$
         $a_i := a_i + LT\, p / LT\, f_i$
         $p := p - (LT\, p / LT\, f_i) \cdot f_i \quad (1)$
         $d := \mathit{true}$
      2. `else` $i := i + 1$
   4. `if` not d
      1. $r := r + LT\, p$
      2. $p := p - LT\, p \quad (2)$

Diskuse správnosti algoritmu

Při každém průchodu vnějším cyklem se právě jednou provede právě jeden z příkazů (1), (2), a stupeň p tedy 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.

V $\mathbb{K}[x_1, \ldots, x_n]$ obecně platí pouze implikace

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

Příklad

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 $f \in \langle f_1, f_2 \rangle$.

Naší snahou bude tento deficit napravit – zavedeme tzv. Gröbnerovy báze.

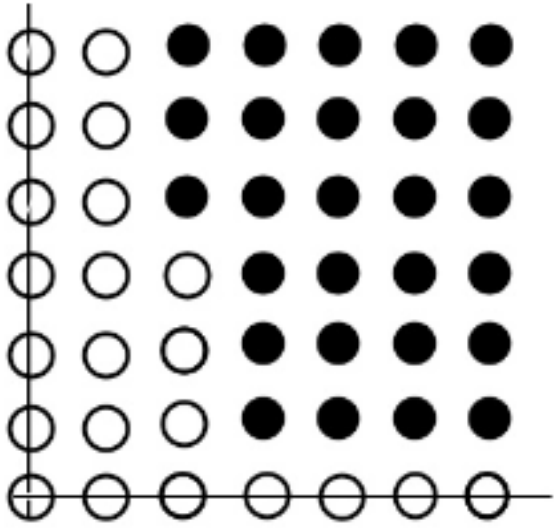
Definice

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

Zřejmě pro monomiální ideál I platí

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

Příklad monomiálního ideálu $I = \langle x^3 y, x^2 y^4 \rangle$:



Lemma

Nechť $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ je monomiální ideál, $f \in \mathbb{K}[x_1, \ldots, x_n]$ 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.*

Důsledek

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

Věta (Dicksonovo lemma)

Každý monomiální ideál $I = \langle x^\alpha,\ \alpha \in A \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$ má konečně mnoho generátorů, tj. lze jej psát ve tvaru $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, kde $\alpha_1, \ldots, \alpha_s \in A$.

Je-li $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ nenulový ideál, označme

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

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 $g_1, \ldots, g_s \in I$.
Následující věta je příkladem toho, že poměrně snadná tvrzení o monomiálních ideálech lze občas rozšířit na libovolné ideály.

Věta (Hilbertova věta)

Každý ideál $I \in \mathbb{K}[x_1, \ldots, x_n]$ 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

$$f = a_1 g_1 + \cdots + a_s g_s + r$$

kde žádný člen r 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 $g_1, \ldots, g_s$. □

Definice

Konečná báze $g_1, \ldots, g_s$ ideálu $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ se nazývá *Gröbnerova*, jestliže platí $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$.

Báze použitá v důkazu Hilbertovy věty byla Gröbnerova.

Důsledek

Každý ideál $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ má Gröbnerovu bázi. Naopak každá množina polynomů $g_1, \ldots, g_s \in I$ splňující $\langle LT\, I \rangle = \langle LT\, g_1, \ldots, LT\, g_s \rangle$ je Gröbnerovou bází ideálu I.

Věta

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

1. *Žádný člen* r *není dělitelný žádným z* $LT\, g_1, \ldots, LT\, g_t$, *tj.* $\forall \alpha \forall i \colon LT\, g_i \not| \, a_\alpha x^\alpha$.
2. $\exists g \in I \colon f = g + r$

Důsledek

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

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

Definice

Pro $\alpha = \text{multideg}\, f$ a $\beta = \text{multideg}\, g$ uvažme

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

Monom x^γ nazýváme *nejmenším společným násobkem (least common multiple)* monomů $LM\, f$ a $LM\, g$ a zavádíme 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** (nebo také *syzygy*, neboli spřežení) polynomů f, g.

Jedná se o nástroj k 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.

Věta

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

Věta poskytuje účinný prostředek pro zjištění, zda nějaká báze je Gröbnerova.

Příklad

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.

Naivní algoritmus pro Gröbnerovy báze

Gröbnerovy báze zavedl v roce 1965 Bruno Buchberger ve své Ph.D. disertaci, po němž je rovněž pojmenován algoritmus na jejich výpočet. Dnes existují další algoritmy, mezi nejznámější patří Faugèreho algoritmy známé pod názvem F4 a F5.

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

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.

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 plyne tvrzení. □

Definice

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

Příklad

Například mějme $\mathbb{C}[x, y]$ 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 zbytečné.
Všimněme si: pro každé a je $\{x^2 + axy, xy, y^2 - 1/2x\}$ minimální Gröbnerovou bází uvedeného ideálu.

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.

Zjevně každá redukovaná Gröbnerova báze je minimální a navíc platí:

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. □

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.

Eliminační věta

Na závěr si uveďme alespoň jednu aplikaci.
Budeme považovat okruh $\mathbb{K}[x_{p+1}, \ldots, x_n]$ za podokruh $\mathbb{K}[x_1, \ldots, x_n]$. Jedná se o polynomy, v nichž se nevyskytují proměnné $x_1, \ldots, x_p$. Je to skutečně podokruh, ale už ne ideál.

Definice

Nechť $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{K}[x_1, \ldots, x_n]$. Pro $p = 0, \ldots, n$ definujeme

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

Tuto množinu nazveme *p-tým eliminačním ideálem.*

Samozřejmě I_p je ideálem pouze v $\mathbb{K}[x_{p+1}, \ldots, x_n]$.

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 $x_{p+1}, \ldots, x_n$.

Věta (Eliminační věta)

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