Matematika IV – 8. týden
Systémy polynomiálních rovnic

Jan Slovák

Masarykova univerzita
Fakulta informatiky

8. 4. – 12. 4. 2013

Obsah přednášky

Plán přednášky

Připomeňme induktivní definici polynomů r proměnných. Budeme v dalším pracovat nad tělesem $\mathbb{K}$.

$$\mathbb{K}[x_1, \ldots, x_r] := \mathbb{K}[x_1, \ldots, x_{r-1}][x_r].$$

Např. $\mathbb{K}[x, y] = \mathbb{K}[x][y]$, tzn. že uvažujeme polynomy v proměnné y nad okruhem $\mathbb{K}[x]$.

Připomeňme induktivní definici polynomů r proměnných. Budeme v dalším pracovat nad tělesem $\mathbb{K}$.

$$\mathbb{K}[x_1, \ldots, x_r] := \mathbb{K}[x_1, \ldots, x_{r-1}][x_r].$$

Např. $\mathbb{K}[x, y] = \mathbb{K}[x][y]$, tzn. že uvažujeme polynomy v proměnné y nad okruhem $\mathbb{K}[x]$.
Zavedli jsem také tzv. podílová tělesa okruhů polynomů $\mathbb{K}[x_1, \ldots, x_r]$, kterým říkáme **těleso racionálních funkcí** a značíme je $\mathbb{K}(x_1, \ldots, x_r)$.
Všechny algebraické operace s polynomy v softwarových systémech jako je Maple nebo Mathematica jsou prováděny ve skutečnosti nad podílovými tělesy, tj. v tělesech raciolnálních funkcí, zpravidla s použitím $\mathbb{K} = \mathbb{Q}$.

Polynomy v proměnných $x_1, \ldots, x_r$ lze i při této definici chápat jako výrazy vzniklé z písmen $x_1, \ldots, x_n$ a prvků okruhu $\mathbb{K}$ konečným počtem (formálního) sčítání a násobení v komutativním okruhu. Například prvky v $\mathbb{K}[x, y]$ jsou tvaru

$$\begin{aligned} f &= a_n(x)y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \\ &= (a_{mn}x^m + \cdots + a_{0n})y^n + \cdots + (b_{p0}x^p + \cdots + b_{00}) \\ &= c_{00} + c_{10}x + c_{01}y + c_{20}x^2 + c_{11}xy + c_{02}y^2 + \ldots \end{aligned}$$

Pro zjednodušení zápisu si zavedeme 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.

Okamžitě se také nabízejí analogické vzorce pro sčítání a násobení polynomů

$$f + g = \sum_{|\alpha| \leq \max(m,n)} (a_\alpha + b_\alpha) x^\alpha$$

$$fg = \sum_{|\gamma|=0}^{m+n} \left(\sum_{\alpha+\beta=\gamma} (a_\alpha b_\beta) x^\gamma \right)$$

kde multiindexy se sčítají po složkách a formálně neexistující koeficienty považujeme za nulové.

Okamžitě se také nabízejí analogické vzorce pro sčítání a násobení polynomů

$$f + g = \sum_{|\alpha| \leq \max(m,n)} (a_\alpha + b_\alpha) x^\alpha$$

$$fg = \sum_{|\gamma|=0}^{m+n} \left(\sum_{\alpha+\beta=\gamma} (a_\alpha b_\beta) x^\gamma \right)$$

kde multiindexy se sčítají po složkách a formálně neexistující koeficienty považujeme za nulové.

Lemma

Tyto vzorce opravdu popisují sčítání a násobení v induktivně definovaném okruhu polynomů v r proměnných.

Důkaz.

Tvrzení lze snadno dokázat indukcí přes počet proměnných. Předpokládejme, že vztahy platí v $\mathbb{K}[x_1, \ldots, x_{r-1}]$ a počítejme součet

$$\begin{aligned} f &= a_k(x_1, \ldots, x_{r-1})x_r^k + \cdots + a_0(x_1, \ldots, x_{r-1}) \\ &= \left(\sum_\alpha a_{k,\alpha} x^\alpha \right) x_r^k + \ldots \\ g &= b_l(x_1, \ldots, x_{r-1})x_r^l + \cdots + b_0(x_1, \ldots, x_{r-1}) \\ &= \left(\sum_\beta b_{l,\beta} x^\beta \right) x_r^k + \ldots \end{aligned}$$

Pokračování.

$$
\begin{aligned}
f+g &= \big(a_0(x_1,\dots,x_{r-1}) + b_0(x_1,\dots,x_{r-1})\big) + \\
&+ \big(a_1(x_1,\dots,x_{r-1}) + b_1(x_1,\dots,x_{r-1})\big)x_r + \dots \\
&= \Big(\sum_{\gamma}(a_{k,\gamma}+b_{k,\gamma})(x_1,\dots,x_{r-1})^{\gamma}\Big)x_r^k + \dots \\
&\quad + \Big(\sum_{\gamma}(a_{0,\gamma}+b_{0,\gamma})(x_1,\dots,x_{r-1})^{\gamma}\Big) \\
&= \sum_{(\gamma,j)}(a_{j,\gamma}+b_{j,\gamma})(x_1,\dots,x_{r-1})^{\gamma}x_r^j.
\end{aligned}
$$

Podobně lze vést důkaz pro součin (proveďte si samostatně!). □

Pro jednoduchost (existence kořenů), budeme pracovat zejména nad polem komplexních čísel, nicméně úvahy některé uvedeme pro obecné pole $\mathbb{K}$.

Afinním n-rozměrným prostorem nad polem $\mathbb{K}$ rozumíme $\mathbb{K}^n = \underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{n}$ se standardní afinní strukturou, viz ??.

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

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

Pro jednoduchost (existence kořenů), budeme pracovat zejména nad polem komplexních čísel, nicméně úvahy některé uvedeme pro obecné pole $\mathbb{K}$.

Afinním n-rozměrným prostorem nad polem $\mathbb{K}$ rozumíme $\mathbb{K}^n = \underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{n}$ se standardní afinní strukturou, viz ??.

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 $\{x = 0, y = 0\}$.

Definition

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.

Theorem

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*

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

Plán přednášky

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 pole), pro čísla reálná je to komplikovanější a velmi zlé to je pro obecná pole, tj. například racionální čísla.
Takové rozhodnutí, zda $\mathfrak{V}(x^n + y^n - z^n) = \emptyset$ nad racionálními čísly vede na velkou Fermatovu větu.

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:

Definition

Množinu $I \subseteq \mathbb{K}$, kde $\mathbb{K}$ 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

$$I = \{\sum_i a_i b_i, \ b_i \in \mathbb{K}\}.$$

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

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

Theorem

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 $V = \mathfrak{V}(f_1, \ldots, f_s)$.*

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 pole $\mathbb{K}$

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 $V, W \subseteq k^n$ 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 $\mathfrak{I}\big(\mathfrak{V}(f_1, \ldots, f_s)\big)$?

Plán přednášky

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

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

Jde ve skutečnosti o algoritmický postup, podíl q a zbytek r počítá následující algoritmus.

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

Corollary

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

Definition

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

1. $h := f$, $s := g$
2. `while` $s \neq 0$
   1. $r :=$ zbytek po dělení h/s
   2. $h := s$
   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. Definujme největšího společného dělitele více než dvou polynomů. Je-li $s > 2$, potom

$$GCD(f_1, \ldots, f_s) := GCD\big(f_1, GCD(f_2, \ldots, f_s)\big)$$

Theorem

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

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.

Plán přednášky

Zadat varietu v prostoru pomocí dvou polynomů znamená zadat průnik obecně i dost komplikovaných útvarů.
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.
Dělením se zbytkem polynomu $f \in \mathbb{K}[x_1, \ldots, x_n]$ polynomy $g_1, \ldots, g_s$ budeme rozumět vyjádření

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

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

Například $f = x^2y + xy^2 + y^2$, $g_1 = xy - 1$ a $g_2 = y^2 - 1$. 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?

Definition

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 se na polynomy rozšíříme „lexikograficky“, tedy větší je ten polynom, který má větší první monom, pokud tak nelze rozhodnou, bere se v potaz druhý monom atd.

Definition

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 se na polynomy rozšíříme „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 $x_1 > x_2 > \cdots$.

Definition

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

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

Definition

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

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

Definition

Lexikografické uspořádání je takové $<_{\text{lex}}$, 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 je takové $<_{\text{grlex}}$, 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 je takové $<_{\text{grevlex}}$, 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.

Definition

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

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

Theorem (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` $LT\, f_i | LT\, p$
         $a_i := a_i + LT\, p / LT\, f_i$
         $p := p - (LT\, p / LT\, f_i) \cdot f_i$
         $d := \mathit{true}$
      2. `else` $i := i + 1$
   4. `if` not d
      1. $r := r + LT\, p$
      2. $p := p - LT\, p$

Diskuse správnosti algoritmu

Při každém průchodu vnějším cyklem se právě jednou provede právě jeden z příkazů 1, 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.

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

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

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

Plán přednášky

Definition

Ideál $I \subseteq k[x_1, \ldots, x_n]$ 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 $h_\alpha \in k[x_1, \ldots, x_n]$. Potom píšeme $I = \langle x^\alpha,\ \alpha \in A \rangle$.

Zřejmě pro monomiální ideál I platí

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

Lemma

Nechť $I \subseteq k[x_1, \ldots, x_n]$ je monomiální ideál, $f \in k[x_1, \ldots, x_n]$ 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.*

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 $h_\beta \in k[x_1, \ldots, x_n]$. Každý člen $a_\alpha x^\alpha$ se musí rovnat některému členu z druhé rovnosti, tedy existují taková $d \in k, \delta \in \mathbb{N}^n$ tak, že $a_\alpha x^\alpha = d x^{\beta+\delta}$. Proto $x^\alpha \in I$, a tedy platí (3). □

Corollary

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

Theorem (Dicksonovo lemma)

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

Plán přednášky

Je-li $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ nenulový, 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 $g_1, \ldots, g_s \in I$.

Theorem (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 $g_1, \ldots, g_s$. □

Definition

Konečná báze $g_1, \ldots, g_s$ ideálu $I \subseteq k[x_1, \ldots, x_n]$ 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.