[Boďa !] Algebraické variety 21.3.2006 Ut.

E^n nad poľom k - algebraicky uzavreté

↓ ∀ polynóm má koreň (⟺ polyn. st. n má práve n koreňov)

$k[x_1, \dots, x_n]$ - okruh polynómov n-neurčitých

Def. 1.1: Alg. varietou (AV) v E^n nazveme množinu V definovanú nasledovne

$$V = \{x = (x_1, \dots, x_n) \in E^n;\ f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0\}$$

$f_i \in k[x_1, \dots, x_n]$ pevné, $s \in N$

Pr.: ∀ lin. varieta v E^n je alg. varieta

- rovina v E^3 : $x - y + z - 1 = 0$
- priamka v E^3 : $x + y - 1 = 0$, $x + z + 2 = 0$

generátory ideál

Nech V je AV daná rovnicami $f_1 = \dots = f_s = 0$. Definujme $I \subseteq k[x_1, \dots, x_n]$:

$$I = \{g_1 f_1 + \dots + g_s f_s;\ g_i \in k[x_1, \dots, x_n]\} =: (f_1, \dots, f_s) \cdot k[x_1, \dots, x_n]$$

Def. 1.2.: Ideálom v okruhu R (komutatívny, noetherovský) nazveme neprázdnu podmnožinu $I \subseteq R$, ktorá spĺňa:

1. $\forall a, b \in I:\ a - b \in I$ (⟺ I je podgrupa)
2. $\forall a \in I:\ \forall r \in R:\ r.a \in I$

(Ideál ⊆ podokruh)

- $(Z; +; \cdot) \supseteq (n.Z)$ ideály v $(Z; +; \cdot)$

Tvrdenie: $(f_1, \dots, f_s) \cdot k[x_1, \dots, x_n]$ je ideál v $k[x_1, \dots, x_n]$.

Def. 1.3.: Nech $I = (f_1, \dots, f_r) \cdot k[x_1, \dots, x_n]$ je ideál v $k[x_1, \dots, x_n]$. Definujme:

$$E^n \supseteq V(I) = \{x = (x_1, \dots, x_n) \in E^n:\ f(x_1, \dots, x_n) = 0\ \forall f \in I\}$$

↑ množina nulových bodov ideálu I

$x \in X$: $f_1 = \dots = f_s = 0$

Záver: algebraická varieta v E^n je teda množinou nulových bodov ideálu I v $k[x_1, \dots, x_n]$. Teda ∀ varieta je tvaru $V(I)$

Pozn: ∀ ideál má konečnú bázu (= noetherovský)

$k[x_1, \dots, x_n] \rightsquigarrow E^n \rightsquigarrow k[x_1, \dots, x_n]$ ideál asociovaný s varietou V

$I \rightsquigarrow V(I) \rightsquigarrow \mathcal{I}(V) := \{f \in k[x_1, \dots, x_n]:\ f(x_1, \dots, x_n) = 0\ \forall (x_1, \dots, x_n) \in V\}$

$\| \quad V$

$I \subseteq \mathcal{I}(V)$, rovnosť nemusí nastať

Pr.: $I = ((x-y+1)^2)\cdot k[x,y] \rightsquigarrow V(I)$

$\rightsquigarrow J(V(I)) = (x-y+1)\cdot k[x,y]$

(priamka, 2-krát)

Def 1.4.: Nech $I \subseteq R$ je ideál. $rad(I) = \{r \in R;\ r^s \in I$ pre určité $s \in \mathbb{N}\}$ radikál

$I \subseteq rad(I)$

Platí: $J(V(I)) = rad(I)$

Def 1.5.: Nech $I, J \subseteq R$ sú ideály.

$I+J := \{a+b;\ a \in I, b \in J\}$ - súčet ideálov

$I \cap J := \{a \in R;\ a \in I, a \in J\}$ - prienik

Veta 1.6.: $I, J \subseteq k[x_1, \dots, x_n]$, $V, W \subseteq E^n$.

(1) $I \subseteq J \Rightarrow V(I) \supseteq V(J)$ → Dôk: $x \in V(J)$ - x sa anuluje v J, ⇒ tým skôr sa anuluje v I

(2) $V \subseteq W \Rightarrow J(V) \supseteq J(W)$ → podobne: $g \in J(W)$...

(3) $V(I+J) = V(I) \cap V(J)$ → $I = (f_1, \dots, f_s)$, $J = (f_{s+1}, \dots, f_r)$ | $I+J = (\underbrace{f_1, \dots, f_s}_{V(I)}, \underbrace{f_{s+1}, \dots, f_r}_{V(J)})$ $V(I) \cap V(J)$

(4) $V(I \cap J) = V(I) \cup V(J)$

Dôkaz: (1), (2) triv.

(3) "⊆": $I \subseteq I+J \overset{(1)}{\Rightarrow} V(I+J) \subseteq V(I)$, $\subseteq V(J)$ $\} \subseteq V(I) \cap V(J)$

$J \in I+J \Rightarrow \dots$

"⊇": $X \in V(I) \cap V(J) \Rightarrow f(X) = 0\ \forall f \in I$, $g(X) = 0\ \forall g \in J$ $\Rightarrow (f+g)(X) = 0\ \forall (f+g) \in I+J$

(4) "⊇": triv.: $I \cap J \subseteq I \Rightarrow V(I) \subseteq V(I \cap J) \Rightarrow V(I \cap J) \supseteq V(I) \cup V(J)$

$V(J) \subseteq V(I \cap J)$

"⊆":

$I \cdot J = \{a \cdot b,\ a \in I, b \in J\}$

$\underset{a \cdot b}{I \cdot J} \subseteq I \cap J \subseteq I, J$

$V(I \cdot J) \supseteq V(I) \cup V(J)$ "⊇" jasné

$X \in V(I \cdot J)$ $X \notin V(I)$ $X \in V(J)$

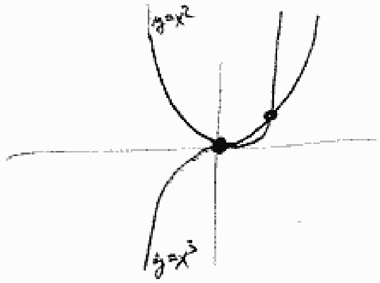
$(f \cdot g)(X) = 0\ \forall f \in I\ g \in J$

$f(X) \neq 0 \Rightarrow (f \cdot g)(X) = f(X) \cdot g(X) = 0$ $g(X) = 0$

$k[x;y] \longleftrightarrow E^2$

$I = (y-x^2; y-x^3)\cdot k[x;y] = \underbrace{(y-x^2)\cdot k[x;y]}_{I_1} + \underbrace{(y-x^3)\cdot k[x;y]}_{I_2}$

$V(I) = V(I_1) \cap V(I_2)$



$y = x^2$ $\quad x^3 - x^2 = 0$
$y = x^3$ $\quad x(x-1) = 0$
$(0;0)$
$(1;1)$

v bode $[0;0]$ - majú spol. dotyčnicu (x)
$[1;1]$ - nemajú

- musia mať 6 spol. bodov (2.3)
$[1;1]$ - 1x
$[0;0]$ - 2x
$[\infty;\infty]$ - 3x

---

28. 3. 2006. Ut.

$$\begin{array}{ccc} k[x_1;\dots;x_n] & E^n & \\ \cup\!\!\mid & \cup\!\!\mid & \\ I & \rightsquigarrow V(I) = \{(x)\in E^n;\ f(x)=0\ \forall f\in I\} & \\ & \| & \\ & V & \end{array}$$

$k[x_1;\dots;x_n]$
$\cup\!\!\mid$
$V \rightsquigarrow J(V) = \{f\in k[x_1;\dots;x_n];\ f(x)=0\ \forall (x)\in V\}$
$\|$ platí
$rad(I) = \{f\in k[x_1;\dots;x_n] : \exists \rho\in N: f^{\rho}\in I\}$

$V(I) = V(rad(I))$

$V(I) = V(J) \Leftrightarrow rad(I) = rad(J)$

Primárne rozklady ideálov, iredukcibilné rozklady variet

<u>Def.</u>: $X \subseteq E^n$ sa nazýva iredukcibilná, ak spĺňa:

ideál $X = X_1 \cup X_2$, X_1, X_2 - alg. var. $\Rightarrow X = X_1 \vee X = X_2$

<u>Def.</u>: $I \subseteq R$ nazveme prvoideálom, ak platí ~~spĺňa~~: $a\cdot b\in I$, $a\notin I \Rightarrow b\in I$

$\mathbb{Z} \supseteq (n)\mathbb{Z}$ - prvoideál
$\Updownarrow$
n je prvočíslo

<u>Veta</u>: $X \subsetneq E^n$ je iredukcibilná $\Leftrightarrow J(X)$ je prvoideál.

<u>Dôkaz</u>: „$\Rightarrow$": $\quad X$ je ired. a $f\cdot g\in J(X)$

$\quad ? \quad X = (X\cap V(f)) \cup (X\cap V(g))$

$V(f) = \{(x)\in E^n;\ f(x)=0\}$ ~~...~~ - plocha

„$\supseteq$" jasné

„$\subseteq$": $x\in X \Rightarrow (f\cdot g)(x) = 0 \Rightarrow f(x)=0 \ \vee\ g(x)=0$
$\qquad\qquad\qquad\qquad \| $
$\qquad\qquad\qquad f(x)\cdot g(x)$

$(x)\in V(f) \vee (x)\in V(g) \Rightarrow (x)\in X\cap V(f) \vee (x)\in X\cap V(g)$

$\Rightarrow \mathcal{X} = \mathcal{X} \cap V(f) \vee \mathcal{X} = \mathcal{X} \cap V(g) \Rightarrow \mathcal{X} \subseteq V(f) \vee \mathcal{X} \in V(g) \Rightarrow$
$f \in \mathcal{I}(\mathcal{X}) \vee g \in \mathcal{I}(\mathcal{X})$

$\Rightarrow \mathcal{X}$ je ired. a $f \cdot g \in \mathcal{I}(\mathcal{X})$

"$\Leftarrow$" Nech $\mathcal{I}(\mathcal{X})$ je prvoideál a $\mathcal{X}$ je redukovaná

$$\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 \quad \mathcal{X}_1 \subsetneq \mathcal{X} \quad \mathcal{X}_2 \subsetneq \mathcal{X}$$

$$\mathcal{I}(\mathcal{X}) = \mathcal{I}(\mathcal{X}_1) \cap \mathcal{I}(\mathcal{X}_2) \Rightarrow \mathcal{I}(\mathcal{X}) \subsetneq \mathcal{I}(\mathcal{X}_1) \qquad \mathcal{I}(\mathcal{X}) \subsetneq \mathcal{I}(\mathcal{X}_2)$$

$\Rightarrow \exists f \in \mathcal{I}(\mathcal{X}_1) / \mathcal{I}(\mathcal{X})$

$\exists g \in \mathcal{I}(\mathcal{X}_2) / \mathcal{I}(\mathcal{X})$ $\Rightarrow \underline{f \cdot g} \in \mathcal{I}(\mathcal{X}_1) \cap \mathcal{I}(\mathcal{X}_2) = \mathcal{I}(\mathcal{X})$ ale $\left.\begin{matrix} f \notin \mathcal{I}(\mathcal{X}) \\ g \notin \mathcal{I}(\mathcal{X}) \end{matrix}\right\} \Rightarrow \mathcal{I}(\mathcal{X})$ nie je prvoid.

Df.: $I \subseteq R$ nazveme primárny, ak spĺňa: $f \cdot g \in I$, $f \notin I \Rightarrow g^{\varrho} \in I$ pre nejaké $\varrho \in \mathbb{N}$

$\mathbb{Z} \supseteq (p^{\varrho})\mathbb{Z}$ sú prim. ideály na $\mathbb{Z}$

Veta: Radikál primárneho ideálu je prvoideál.

Písmená švabachu: $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{q}$, $\mathfrak{p}$
a b q p

primárny $\quad \mathrm{rad}(\mathfrak{q}) = \mathfrak{p}$

Dôkaz
$\mathfrak{q}$ - primárny. Nech $f \cdot g \in \mathrm{rad}(\mathfrak{q})$, $f \notin \mathrm{rad}(\mathfrak{q}) \Rightarrow (f \cdot g)^{\varrho} \in \mathfrak{q}$

$$\overset{\parallel}{f^{\varrho} \cdot g^{\varrho}} \in \mathfrak{q},\ f^{\varrho} \notin \mathfrak{q} \Rightarrow$$

$\Rightarrow (g^{\varrho})^{f} \in \mathfrak{q} \Rightarrow g \in \mathrm{rad}(\mathfrak{q})$ $\quad \boxed{\mathfrak{q} \text{ je } \mathfrak{p}\text{-primárny}}$

$\mathrm{rad}(p^{\varrho}\mathbb{Z}) = (p)\mathbb{Z}$

Df.: Ideál $\mathfrak{a} \in R$ nazveme ireducibilný, ak spĺňa

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \Rightarrow \mathfrak{a} = \mathfrak{a}_1 \vee \mathfrak{a} = \mathfrak{a}_2$$

Uvedomíme si, že každá algebraická varieta je zjednotením kon. počtu ireducibilných alg. variet.

$$\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$$
$$\parallel$$
$$\mathcal{X}_{11} \cup \mathcal{X}_{12}$$
$$\parallel$$
$$\mathcal{X}_{111} \cup \mathcal{X}_{112}$$
$$\vdots$$

prečo to musí niekedy skončiť?

$\ldots \subsetneq \mathcal{X}_{11} \subsetneq \mathcal{X}_1 \subsetneq \mathcal{X}$ - najmenšia varieta je bod - musí to skončiť

Veta: Každý ideál v R (noetherovský) je prienikom konečného počtu ireducibilných.

Dôkaz?: $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2$
$\mathfrak{a}_1 = \mathfrak{a}_{11} \cap \mathfrak{a}_{12}$
$\vdots$

$\mathfrak{a} \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_{11} \subsetneq \dots$ jedna z definícií noetherovských okruhov

Veta: Každý ireducibilný ideál je primárny.

Dôkaz: $\mathfrak{a}$ - ired., $f \cdot g \in \mathfrak{a}$, $f \notin \mathfrak{a}$

$$(\mathfrak{a} : g) \subseteq (\mathfrak{a} : g^2) \subseteq (\mathfrak{a} : g^3) \subseteq \dots \subseteq (\mathfrak{a} : g^r) \overset{\text{noetherovskosť}}{=} (\mathfrak{a} : g^{r+1})$$

$(\mathfrak{a} : g) = \{r \in R ; r \cdot g \in \mathfrak{a}\}$

tvrdíme: $(\mathfrak{a} + (g^r)) \cap (\mathfrak{a} + (f)) = \mathfrak{a}$ "$\supseteq$" jasné

"$\subseteq$": $x \in L' \Rightarrow x = \underset{\in \mathfrak{a}}{a} + u \cdot g^r = \underset{\in \mathfrak{a}}{a'} + v \cdot f$ $\quad / \cdot g$

$$g \cdot x = \underbrace{g \cdot a}_{\in \mathfrak{a}} + u \cdot g^{r+1} = \underbrace{a' \cdot g}_{\in \mathfrak{a}} + v \cdot \underbrace{f \cdot g}_{\in \mathfrak{a}}$$

$u \cdot g^{r+1} \in \mathfrak{a} \Rightarrow u \cdot g^r \in \mathfrak{a}$ č.b.t.d.

$\Rightarrow \mathfrak{a} = \mathfrak{a} + g^r \Rightarrow g^r \in \mathfrak{a}$

Veta: Každý ideál v R je prienikom konečného počtu primárnych ideálov.

$\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \dots \cap \mathfrak{q}_s$

| $rad(\mathfrak{a} \cap \mathfrak{b}) = rad(\mathfrak{a}) \cap rad(\mathfrak{b})$
"$\subseteq$" jasné
"$\supseteq$": $f \in rad(\mathfrak{a}) \cap rad(\mathfrak{b}) \Rightarrow$
$f^{\rho} \in \mathfrak{a}$ $\quad f^{\nu} \in \mathfrak{b} \Rightarrow f^{\max\{\rho;\nu\}} \in \mathfrak{a} \cap \mathfrak{b}$
$\Rightarrow f \in rad(\mathfrak{a} \cap \mathfrak{b})$

$rad(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \dots \cap \mathfrak{p}_s$

$$V(\mathfrak{a}) = V(rad(\mathfrak{a})) = \underbrace{\overset{V(\mathfrak{q}_1)}{V(\mathfrak{p}_1)} \cup \overset{V(\mathfrak{q}_2)}{V(\mathfrak{p}_2)} \cup \dots \cup \overset{V(\mathfrak{q}_s)}{V(\mathfrak{p}_s)}}_{\text{ireducibilné}}$$

Pr.: $k[x;y]$ (rovina) $\ni \mathfrak{a} := (x^2+y^2-1; xy)$ - vyjadrime ako prienik primárnych

$(x^2+y^2-1; x) \cap (x^2+y^2-1; y) = (y^2-1; x) \cap (x^2-1; y) =$
$= ((y-1)(y+1); x) \cap ((x-1)(x+1); y) = \underset{[0;1]}{(y-1; x)} \cap \underset{[0;-1]}{(y+1; x)} \cap$
$\cap \underset{[1;0]}{(x-1; y)} \cap \underset{[-1;0]}{(x+1; y)}$ prvoideály

$x \cdot y = 0$ - = osi

$x^2+y^2-1 = 0$ - kružnica

} prienik 4 body

Rozmer alg. variety, Rozmer ideálu

Nech $\mathbb{X} \subseteq E^n$ je ireducibilná alg. varieta.

$\mathbb{X} = \mathbb{X}_s \supsetneq \mathbb{X}_{s-1} \supsetneq \mathbb{X}_{s-2} \supsetneq \ldots \mathbb{X}_1 \supsetneq \mathbb{X}_0 \supsetneq \emptyset$ — ireducibilné alg. variety — maximálny reťazec

$\mathbb{X}_1$ → krivka, $\mathbb{X}_0$ → bod

Def.: $s := \dim \mathbb{X}$ – s-rozmer variety $\mathbb{X}$

$\mathbb{X} = \mathbb{X}_s \supsetneq \mathbb{X}_{s-1} \supsetneq \ldots \supsetneq \mathbb{X}_1 \supsetneq \mathbb{X}_0 \supsetneq \emptyset$

$\Updownarrow$

$\mathcal{I}(\mathbb{X}_s) \subseteq \mathcal{I}(\mathbb{X}_{s-1}) \subsetneq \ldots \subsetneq \mathcal{I}(\mathbb{X}_1) \subsetneq \mathcal{I}(\mathbb{X}_0) \subseteq k[x_1, \ldots, x_n]$

asociovaný prvoideál; $\mathcal{I}(\mathbb{X}_0)$ → asociovaný prvoideál bodu so súr. $a_1, \ldots, a_n$

Def.: Nech $p \subseteq k[x_1, \ldots, x_n]$ je prvoideál a $p = p_s \subsetneq p_{s-1} \subsetneq \ldots \subsetneq p_0 \subsetneq m$ – max. ideál je maximálny reťazec prvoideálov. $s := \dim p$ s-rozmer prvoideálu p

Veta: $\dim \mathbb{X} = \dim \mathcal{I}(\mathbb{X})$, $\mathbb{X}$ – ired.

Nech $\mathbb{X} = \mathbb{X}_1 \cup \mathbb{X}_2 \cup \ldots \cup \mathbb{X}_n$ $\forall$ ireducibilné!

Def.: $\dim \mathbb{X} := \max \{\dim \mathbb{X}_i\}$

Platí $\dim \mathcal{I}(\mathbb{X}) = \max \{\dim \mathcal{I}(\mathbb{X}_i)\}$

Nech $\dim \mathbb{X} = d \Rightarrow \mathbb{X} = \overset{d}{\mathbb{X}_1} \cup \ldots \cup \overset{d}{\mathbb{X}_k} \cup \overset{d-1}{\mathbb{X}_1} \cup \ldots \cup \overset{d-1}{\mathbb{X}_l} \cup \overset{0}{\mathbb{X}_1} \cup \ldots \cup \overset{0}{\mathbb{X}_s}$

$I(\mathbb{X}) = I({}^d\mathbb{X}_1) \cap \ldots$

$\mathfrak{a} = {}^d\mathfrak{q} \cap \ldots \cap {}^d\mathfrak{q}_r \cap {}^{d-1}\mathfrak{q}_1 \cap \ldots \cap {}^{d-1}\mathfrak{q}_s \cap \ldots$

$V(\mathfrak{a}) = V({}^d\mathfrak{q}) \cup \ldots \cup V({}^{d-1}\mathfrak{q}_s) \cup \ldots$

$\mathfrak{a} \subseteq k[x_1; \ldots; x_n]$

$\dim \mathfrak{a} = 0 \Rightarrow \mathfrak{a} = {}^0\mathfrak{q} \cap \ldots \cap {}^0\mathfrak{q}_s$ | $V(\mathfrak{a}) = c_1 \cup \ldots \cup c_s$ – c_i – body

Veta (Bezoutova): v $E^2 \Leftrightarrow k[x;y]$ algebr. uzavreté

$\mathbb{X}: F = 0$, $\mathbb{Y}: G = 0$ } krivky $\deg F = m$, $\deg G = n$ | $\# \mathbb{X} \cap \mathbb{Y} = m \cdot n$, pričom každý bod sa počíta s príslušnou násobnosťou (medzi spoločné body spočítame aj spol. asymptotické smery)

Pr.: $x^2 + y^2 = 1$, $y = x^2$ ...

Pr.: $\mathfrak{a} = (x^2 - y^2 - 4; x^2y^2) = \overset{(x-2;y)}{(x-2; y^2)} \cap \overset{(x+2;y)}{(x+2; y^2)} \cap \overset{(y-2;x)}{(y-2; x^2)} \cap \overset{(y+2;x)}{(y+2; x^2)}$

$V(\mathfrak{a}) = \underset{2x}{[2;0]} \cup \underset{2x}{[-2;0]} \cup \underset{2x}{[0;2]} \cup \underset{2x}{[0;-2]}$ $\quad \# 8$

Usporiadania v okruhu polynómov

$k[x_1; \ldots; x_n] =: R \qquad \mathbb{X}^\alpha := X_1^{\alpha_1} X_2^{\alpha_2} \ldots X_n^{\alpha_n}$ – monóm – polynóm, kde nie sú súčty, iba súčiny

Def.: Usporiadaním na monómoch R nazveme reláciu $>$, ktorá spĺňa:

1. $X^\alpha > X^\beta \Rightarrow X^\beta \not> X^\alpha$ – antisymetria
2. $X^\alpha > X^\beta$, $X^\beta > X^\gamma \Rightarrow X^\alpha > X^\gamma$ – tranzitívnosť
3. z výrazov $X^\alpha > X^\beta$, $X^\beta > X^\alpha$, $X^\alpha = X^\beta$ platí práve 1 – trichotómia

} $>$ – lineárne usporiadanie

4. $X^\alpha > X^\beta \Rightarrow X^\alpha \cdot X^\gamma > X^\beta \cdot X^\gamma$ – kompatibilnosť s násobením

11.4.2006. Ut.

- monomiálne usporiadanie v $k[x_1;\dots;x_n]$:

① lineárne - refl., antisym., tranz.

② kompatibilné s násobením $\longrightarrow \forall\, x^\alpha > x^\beta \Rightarrow x^\alpha x^\gamma > x^\beta x^\gamma$

③ $x_i > 1 \quad \forall i = 1,\dots,n$

- budeme brať $x_1 > x_2 > \dots > x_n$ — prvých niekoľko prvkov je nulových

$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2}\dots x_n^{\alpha_n}$; $\alpha - \beta = (0;\dots;0;\underset{\text{prvé nenul.}}{\alpha_r-\beta_r};\dots;\alpha_s-\beta_s;0;\dots;0)$

Def.: $x^\alpha \overset{lex}{>} x^\beta \overset{def}{\iff} \alpha_r - \beta_r > 0$

lexikografické — toto usp. je monomiálne

Pr.: $x^3y > xy^2z > xyz^2 > y^3 > z^4$

↳ ③: Keby $x_i < 1 \quad /\cdot x_i$

$x_i^2 < x_i$ SPOR

Def.: Gradované lexikografické usp.: Ozn. $|\alpha| = \sum \alpha_i$ (stupeň monómu)

$x^\alpha \underset{glex}{>} x^\beta \iff |\alpha|>|\beta| \vee (|\alpha|=|\beta| \wedge \alpha_r-\beta_r>0)$; je tiež monomiálne

Pr.: $x^3y > xy^2z > xyz^2 > z^4 > y^3$

- všade v ďalšom predpokladáme $>$ monomiálne na $k[x_1;\dots;x_n]$

$f \in k[x_1;\dots;x_n]$

$\quad = \sum c_\alpha x^\alpha$ nech x^{α_0} je vedúci monóm v f.

Def.: $\boxed{Lt(f) = c_{\alpha_0} x^{\alpha_0}}$ — vedúci člen

- nech I je ideál $I=(f_1;\dots;f_s)\subseteq k[x_1;\dots;x_n]$

Def.: $Lt(I) := \{Lt(f);\ f\in I\}$ - vedúci členy ideálu I

$\cup|$

mnd $(Lt(f_1);\dots;Lt(f_s))$

Pr.: $I=(x^2-y;\ x-y^3)$, berme lex. usp.

mnd $(Lt(f_1);\ Lt(f_2)) = (x^2;\ x) = (x)$

x^2-y ; x^2-xy^3 /- ... $\to xy^3-y$; xy^3-y^6

$\hookrightarrow y^6-y \notin (x)$

$y^6-y \in Lt(I)$

Deliaci algoritmus v $k[x_1;\dots;x_n]$

Pr.: $f = x^3-2x+1$, $g = x^2+x$

$f:g = (x^3-2x+1):(x^2+x) = x-1$

$\quad -x^2-2x+1$

$\quad -x+1$

$\Rightarrow f = g\underset{\text{podiel}}{(x-1)} + \underset{\text{zvyšok}}{(-x+1)}$ [illegible]

Pr.: $k[x,y]$, lex; $\Gamma = \{\overbrace{x^2-y}^{F_1};\ \overbrace{x-y^2}^{F_2}\}$ $\qquad f = x^4 - x^3y + xy - 1$

$$
\begin{array}{l}
(x^4 - x^3y + xy - 1) : (x^2 - y) = x^2 - xy + y \\
-(x^4 - x^2y) \\
\hline
-x^3y + x^2y + xy - 1 \\
-(-x^3y + xy^2) \\
\hline
x^2y - xy^2 + xy - 1 \\
-(x^2y - y^2) \\
\hline
-xy^2 + xy + y^2 - 1
\end{array}
$$

počas výpočtu treba stále usporadúvať (v danom usp.)

$$f = (x^2 - xy + y)F_1 + (-xy^2 + xy + y^2 - 1)$$

už sa nedá deliť F_1, ale ešte existuje monóm deliteľný F_2

$$
\begin{array}{l}
(-xy^2 + xy + y^2 - 1) : (x - y^2) = -y^2 + y \\
-(-xy^2 + y^4) \\
\hline
xy - y^4 + y^2 - 1 \\
-(xy - y^3) \\
\hline
-y^4 + y^3 + y^2 - 1
\end{array}
$$

- nezáleží na poradí polynómov z Γ, v akom ich používame pri delení!

$$f = (x^2 - xy + y)F_1 + (-y^2 + y)F_2 + (-y^4 + y^3 + y^2 - 1)$$

- delenie vždy musí skončiť, lebo znižujeme stupeň

$k[x,y,z]$, lex; $\Gamma = \{\underbrace{\boxed{x^2}-y}_{F_1},\ \underbrace{\boxed{x}-z}_{F_2},\ \underbrace{\boxed{y}-z^2}_{F_3}\}$ $\quad ; f = x^2y - xy^2 + xz - z^2$

$$
\begin{array}{l}
(x^2y - xy^2 + xz - z^2) : (x^2 - y) = y \\
-(x^2y - y^2) \\
\hline
(-xy^2 + xz + y^2 - z^2) : (x - z) = -y^2 + z \\
-(-xy^2 + y^2z) \\
\hline
xz - y^2z + y^2 - z^2 \\
-(xz - z^2) \\
\hline
(-y^2z + y^2) : (y - z^2) = -yz + y - z^3 + z^2 \\
-(-y^2z + yz^3) \\
\hline
y^2 - yz^3 \\
-(y^2 - yz^2) \\
\hline
-yz^3 + yz^2 \\
-(-yz^3 + z^5) \\
\hline
yz^2 - z^5 \\
-(yz^2 - z^4) \\
\hline
-z^5 + z^4
\end{array}
$$

$$f = yF_1 + (-y^2 + z)F_2 + (-yz + y - z^3 + z^2)F_3 + (-z^5 + z^4)$$

Veta (deliaci algoritmus v $k[x_1, \dots, x_n]$): Nech $F_1, \dots, F_s \in k[x_1, \dots, x_n]$, $f \in k[x_1, \dots, x_n]$. Potom $\exists\, g_1, \dots, g_s, r \in k[x_1, \dots, x_n]$ také, že:

$$f = g_1F_1 + g_2F_2 + \dots + g_sF_s + r$$

pričom monómy z r nie sú deliteľné monómami $Lt(F_1), \dots, Lt(F_s)$

$\Gamma = \{F_1, \dots, F_s\}$; r - zvyšok po delení polynómu f množinou Γ

ozn.: $r := \overline{f}^{\Gamma}$

Gröbnerove bázy

- pri ideáloch každá mn. generujúca ideál sa naz. báza (nemusí byť minimálna)

Pr.: $(x^2-y; x-y^3)$ je báza, ale aj $(x^2-y; x-y^3; y^6-y)$ je báza

Def.: Bázu $F_1;\dots;F_s$ ideálu I nazývame Gröbnerovou bázou, ak

$$Lt(I) = (Lt(F_1);\dots;Lt(F_s))$$

Def.: Nech $f,g \in k[x_1;\dots;x_n]$, S-polynómom polynómov f,g nazveme polynóm

$$S(f;g) = \frac{x^\gamma}{Lt(f)} f - \frac{x^\gamma}{Lt(g)} g,$$ pričom x^γ je najmenší spol. násobok x^α, x^β — vedúci monóm g, vedúci monóm f

○ - sa vykrátia vedúce

Pr.: $f = x^2y - y^3$, $g = xy^2 - xy$ lex.;

$$S(f;g) = \frac{x^2y^2}{x^2y}(x^2y - y^3) - \frac{x^2y^2}{xy^2}(xy^2 - xy) =$$
$$= -y^4 + x^2y = x^2y - y^4$$

(Buchbergerovo kritérium)

Veta: Báza $I=(F_1;\dots;F_s)$ je Gröbnerova $\iff \overline{S(F_i;F_j)}^{\Gamma} = 0$ (zvyšok)

$\Gamma = \{F_1;\dots;F_s\}$

Pr.: $I = (\underbrace{x - y^2}_{F}; \underbrace{y^3 - y}_{G})$ lex. $\qquad Lt(I) = (x; y^3)$

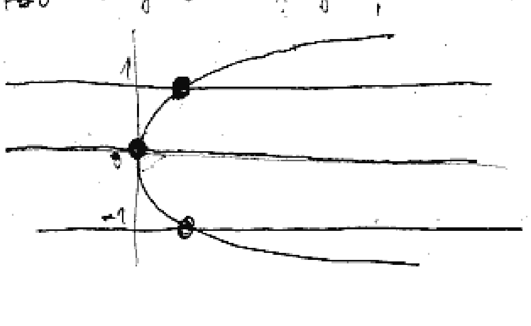
$$S(F;G) = \frac{xy^3}{x}\cdot F - \frac{xy^3}{y^3}\cdot G = -y^5 - xy$$

$(-y^5 - xy) : (y^3 - y) = -y^2$
$-(y^5 + y^3)$
$(xy - y^3) : (x - y^2) = y$
$-(xy - y^3)$
0

$(-y^3 + xy) : (y^3 - y) = -1$
$-(-y^3 + y)$
$(xy - y) : (x - y^2) = y$
$-(xy - y^3)$
$(y^3 - y) : (y^3 - y) = 1.$
0

$\overline{S(F,G)}^{\Gamma} = 0 \Rightarrow$ je to Gröbnerova báza

F=0: $x - y^2 = 0 \Rightarrow x = y^2$; G=0: $y^3 - y = 0 \iff y(y^2 - 1) = 0 \iff y = 0 \vee y = \pm 1$



Buchbergerov algoritmus

25.4.2006 Ut.

$I=(f_1;\dots;f_s)$ $\quad \Gamma=\{f_1,\dots,f_s\}$ $\quad \Gamma$ je Gröbnerova báza $I \Leftrightarrow \forall i,j$ $\overline{S(f_i;f_j)}=0$

① $I=(f_1;\dots;f_s)$ $\quad \Gamma_1=\{f_1;\dots;f_s\}$ $\quad \overline{S(f_i;f_j)}^{\Gamma_1}$ – zvyšky po delení Γ_1; označme $\forall$ nenulové zvyšky ako $g_1;\dots;g_t$

② $I=(f_1;\dots;f_s;g_1;\dots;g_t)$ $\quad \Gamma_2=\{f_1;\dots;f_s;g_1;\dots;g_t\}$

patria do I a nemenia ho, ale pre Gröbnerovu bázu nie sú potrebné

spravíme $\overline{S(f_i;f_j)}^{\Gamma_2}=0$ – určite sú nula (dajú sa deliť niečím z $g_1;\dots;g_t$)

$\overline{S(f_i;g_j)}^{\Gamma_2}$, $\overline{S(g_i;g_j)}^{\Gamma_2}$ → všetky nenulové označme $h_1;\dots;h_r$

po niekoľkých krokoch sú všetky bez zvyšku ($\forall\ \overline{S}=0$)

lex; $I=\overbrace{(\underbrace{x^2-y^3}_{f};\underbrace{xy-y^2}_{g})}^{\Gamma_1}=\overbrace{(\underbrace{x^2-y^3}_{f};\underbrace{xy-y^2}_{g};\underbrace{y^4-y^3}_{h})}^{\Gamma_2}$

$S(f;g)=\frac{x^2y}{x^2}f-\frac{x^2y}{xy}g=-y^4+xy^2 \quad : xy-y^2=y$

$-(-y^3+xy^2)$

$-y^4+y^3 \quad : y^4-y^3=-1$

0

$\overline{S(f,g)}^{\Gamma_2}=0$

$S(f;h)=\frac{x^2y^4}{x^2}f-\frac{x^2y^4}{y^4}h=-y^7+x^2y^3 \quad : y^4-y^3=-y^3$

$-(y^7+y^6)$

$x^2y^3-y^6 \quad : x^2-y^3=y^3$

$-(x^2y^3-y^6)$

0

$S(g;h)=\frac{xy^4}{xy}g-\frac{xy^4}{y^3}h=-y^5+xy^3 \quad : y^4-y^3=-y$

$-(-y^5+y^4)$

$xy^3-y^4 \quad : xy-y^2=y^2$

$-(xy^3-y^4)$

0

$\overline{S(g;h)}^{\Gamma_2}=0$

$Lt(I)=(x^2;xy;y^4) \to 5$

$I=(x^2-y^3, xy-y^2, y^4-y^3)$ – Gröbnerova báza

glex.: $I=(\underbrace{y^3-x^2}_{f};\underbrace{xy-y^2}_{g})=(y^3-x^2;\ xy-y^2;\ \overbrace{x^3-x^2}^{h})$

$S(f;g)=-x^3+y^4 \quad : y^3-x^2=y$

$-(y^4-x^2y)$

$-x^3+x^2y \quad : xy-y^2=x$

$-(x^2y-xy^2)$

$-x^3+xy^2 \quad : xy-y^2=y$

$-(xy^2-y^3)$

$-x^3+y^3 \quad : y^3-x^2=1$

$-(-x^2+y^3)$

$(-x^3+x^2)$

Lema: $\{f;g\}=\Gamma$; $\quad nsd(Lt(f);Lt(g))=1 \Rightarrow \overline{S(f;g)}^{\Gamma}=0$

Dôkaz: stačí deliť oboma (v ľub. poradí) a vyjde zvyšok 0

$\overline{S(f,h)}^{\Gamma} = 0$ (s lemy)

$S(g,h) = -x^2y^2 + xy^3 \quad : xy - y^2 = -xy$

$-(-x^2y^2 + xy^3)$

$x^2y - xy^3 \quad : y^3 - x^2 = -x$

$-(-xy^3 + x^3)$

$x^2y - x^3 \quad : xy - y^2 = x$

$-(x^2y - y^2x)$

$-x^3 + y^2x \quad : xy - y^2 = y$

$-(xy^2 - y^3)$

$-x^3 + y^3 \quad : y^3 - x^2 = -1$

$-(-x^3 + y^2)$

$y^3 - x^2 \quad : y^3 - x^2 = 1$

0

$Lt(I) = (x^3; xy; y^3) \longrightarrow 5 = 3+3-1$

$Lt(I) = (x^2; xy; y^4) \longrightarrow 5 = 2+4-1$

minulý pr.

Pr.: lex $I = (\underbrace{x^2 - y^3}_{f}; \underbrace{x^3 - y^2}_{g}) = (x^2 - y^3; x^3 - y^2; \overbrace{xy^3 - y^2}^{h})$

$S(f,g) = -xy^3 + y^2$ nie je čím deliť

$S(f,h) = -y^6 + xy^2$ nie je čím deliť

$I = (x^2 - y^3; x^3 - y^2; xy^3 - y^2; -y^6 + xy^2)$.

v glex: $I = (\underbrace{y^3 - x^2}_{f}; \underbrace{x^3 - y^2}_{g})$ už je Gröbnerova báza (lema)

$S(f,g) = -x^5 + y^5 \quad : x^3 - y^2 = -x^2$

$-(-x^5 + x^2y^2)$

$y^5 - x^2y^2 \quad : y^3 - x^2 = y^2$

$-(y^5 - x^2y^2)$

0

$Lt(y^3; x^3) \leadsto 6$

$R = k[x_1, \dots, x_n]$

$\Gamma = \{f_1, \dots, f_s\}$

$f \in R: \quad f = a_1f_1 + \dots + a_sf_s + r_1 = b_1f_1 + \dots + b_sf_s + r_2 \Big\} \Rightarrow r_1 - r_2 \in I \quad Lt(r_1 - r_2) \in Lt(I) = (Lt(f_1), \dots, Lt(f_s))$

$Lt(r_1) \vee Lt(r_2) \Rightarrow Lt(r_1)$ podeliteľný niektorým $Lt(f_i)$ $\Rightarrow r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

Veta 4: ak $\Gamma = \{f_1, \dots, f_s\}$ je Gröbnerova báza ideálu $I = (f_1, \dots, f_s) \Rightarrow$

$\Rightarrow r$ je určený jednoznačne

$r = \overline{f}^{\Gamma}$

$\mathbb{Z}/(3)\mathbb{Z} \longrightarrow$

$0 + (3)\mathbb{Z} = \bar{0}$

$1 + (3)\mathbb{Z} = \bar{1}$

$2 + (3)\mathbb{Z} = \bar{2}$

$\bar{a} + \bar{b} = \overline{a+b} \qquad \bar{a}.\bar{b} = \overline{a.b}$

$k[x_1, \dots, x_n]/I \cong k[x_1, \dots, x_n]/Lt(I)$

$I = (f_1, \dots, f_s)$ G-báza

$f \in k[x_1, \dots, x_n] \twoheadrightarrow k[x_1, \dots, x_n]/Lt(I)$ surjektívny homomorfizmus = epimorfizmus

$f = a_1f_1 + \dots + a_sf_s + \overline{f}^{\Gamma} \twoheadrightarrow \overline{f}^{\Gamma} + Lt(I)$

nech $f \in Ker\varphi \Rightarrow \overline{f}^{\Gamma} + Lt(I) = 0 + Lt(I) \Leftrightarrow \overline{f}^{\Gamma} \in Lt(I) \Leftrightarrow \overline{f}^{\Gamma} = 0 \Leftrightarrow f \in I$

Veta 2: ak $\Gamma = \{f_1; \dots; f_s\}$ je Gröbnerova báza : $f \in I \Leftrightarrow \overline{f}^{\Gamma} = 0$

Dôkaz: „$\Leftarrow$": triv. $f = a_1 f_1 + \dots + a_s f_s + \overline{f}^{\Gamma} \in I$, $\overline{f}^{\Gamma} = 0$

„$\Rightarrow$": sporom: nech $f \in I$ a $\overline{f}^{\Gamma} \neq 0 \Rightarrow \overline{f}^{\Gamma} \in I \Rightarrow Lt(\overline{f}^{\Gamma}) \in (Lt(f_1); \dots; Lt(f_s))$

$\Rightarrow Lt(f_i) \,/\, Lt(\overline{f}^{\Gamma})$ SPOR

Veta 3: $I = (f_1; \dots; f_s)$ - G-báza. $f \in k[x_1; \dots; x_n] \xrightarrow{\varphi} k[x_1; \dots; x_n] / Lt(I)$

$f = a_1 f_1 + \dots + a_s f_s + \overline{f}^{\Gamma} \longrightarrow \overline{f}^{\Gamma} + Lt(I)$

Potom $k[x_1; \dots; x_n]/I \cong k[x_1; \dots; x_n]/Lt(I)$

Dôkaz (konštruktívny):
nech $f \in Ker(\varphi) \Leftrightarrow (\overline{f}^{\Gamma} + Lt(I) = 0 + Lt(I)) \Leftrightarrow (\overline{f}^{\Gamma} \in Lt(I)) \Leftrightarrow (\overline{f}^{\Gamma} = 0) \Leftrightarrow (f \in I)$ veta

Pr.: $k[x;y]/(x^2-y^3; xy-y^4) \cong k[x;y]/(x^2; xy; y^4)$

$\cong k[x;y]/(x^3; xy; y^3)$

izomorfné aj ako vektorové priestory nad k

$1, x, y, y^2, x^3$ tam nie sú $\Rightarrow$

$\Rightarrow$ toto je báza, jej rozmer je 5 $\quad 1, x, x^2, y, y^2$

$x^2 = y^3 = xy^2 \qquad x(x-y^4) = 0$

$x = y^3 = 0 \Rightarrow (0;0)$ 3. rád $\quad I \subset k[x_1; \dots; x_n]$ $I = \mathcal{U}_1 \cap \dots$

$y = 1 \Rightarrow (1;1)$

9.5.2006 Ut.

$I = (x^2 - y^3; x^3 - y^4)$

Použitie

$I \subseteq k[x_1; \dots; x_n]$ $\dim I = 0$

$(F_1; \dots; F_s) = I = \overset{o}{\mathcal{U}}_1 \cap \overset{o}{\mathcal{U}}_2 \cap \dots \cap \overset{o}{\mathcal{U}}_s$

$O = (0; 0; \dots; 0) \quad (a_{21}; \dots; a_{2n}) \quad (a_{s1}; \dots; a_{sn})$

$(x_1 - a_1; \dots; x_n - a_n)$

$c_1 = (a_{11}; \dots; a_{1n})$

$V(I) = \{c_1; \dots; c_s\}$

$k[x_1; \dots; x_n]/I \xrightarrow{\sim} k[x_1; \dots; x_n]/\overset{o}{\mathcal{U}}_1 \oplus k[x_1; \dots; x_n]/\overset{o}{\mathcal{U}}_2 \oplus \dots \oplus k[x_1; \dots; x_n]/\overset{o}{\mathcal{U}}_s$

$f \to (f + \overset{o}{\mathcal{U}}_1; \dots; f + \overset{o}{\mathcal{U}}_s)$; $f \in Ker\,\varphi \Leftrightarrow f \in \overset{o}{\mathcal{U}}_1 \cap \dots \cap \overset{o}{\mathcal{U}}_s$

$\Rightarrow \dim_k k[x_1, \dots; x_n]/I = \sum_{i=1}^{s} \dim_k k[x_1; \dots; x_n]/\mathcal{U}_i$ = # bodov variety $V(I)$ počítaných s príslušnou násobnosťou

$I = (F_1; \dots; F_s)$ - štandardná

$\Downarrow$

$\dim_k (k[x_1; \dots; x_n]/Lt(I)) = \sum \mu(c_i)$

$I = (F_1; \dots; F_s)$ - Gröbnerova

$\Downarrow$

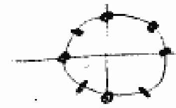
$\dim (k[x_1; \dots; x_n]/Lt(I)) = \# V(I)$

Pr.: $(x^3-y^5;\ x-y^4)=I$

$V(I)$ $\quad x^3-y^5=0$ $\quad y^{12}-y^5=0$

$x-y^4=0$ $\quad y^5(y^7-1)=0$ $\quad y=0$ $\quad 5x$ $\quad x=0 \Rightarrow [0;0]$ $5x$

$y^7=1$



komplexné čísla, 12 koreňov $(1,1)\dots$

$\# V(I)=12$

lex $\quad (\underbrace{x^3-y^5}_{f};\ \underbrace{x-y^4}_{g};\ \underbrace{y^{12}-y^5}_{h})$ – Gröbnerova báza

$\Rightarrow Lt(I)=(x;y^{12})$ $\quad x^3$ nemusíme písať, lebo je tam automaticky x

$S(f;g)=-y^5+x^2y^4 : x-y^4 = xy^4+y^8$

$+xy^8-x^2y^4$

xy^8-y^5

$-xy^8+y^{12}$

$y^{12}-y^5$

$k[x;y]/(x;y^{12})$ hľadáme $\forall$ monómy, ktoré nie sú v ideáli:

$1, y, y^2, \dots, y^{11} \rightarrow 12$

glex: $I=(y^5-x^3,y^4-x);\ x^3-xy)$ $\quad Lt(I)=(x^3,y^4)$

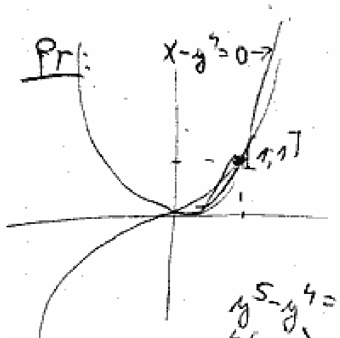
$S(f;g)=\frac{y^5x}{y^5}(y^5-x^3)+\frac{y^5x}{y^4}(y^4-x)$ $\quad -x^3+xy$

$k[x;y]/(x^3,y^4)$

$1, x, x^2, y, y^2, y^3, xy, xy^2, xy^3$

x^2y, x^2y^2, x^2y^3 $\rightarrow 12$

Pr.:



$I=(x-y^4;\ x-y^5;\ y^5-y^4)$

$S(f;g)=-y^4+y^5$

$Lt(I)=(x;y^5)$ $\quad 1.5=5$

$k[x;y]/(x;y^5)$ $\quad \#V(I)=5$

$1, y, y^2, y^3, y^4 \rightarrow 5$

$y^5-y^4=0$

$y^4(y-1)=0$

$\rightarrow [1;1]$ $1x$

$\rightarrow [0;0]$ $4x$

Pr.: $I=(\underbrace{x^2-y^3}_{f};\ \underbrace{x^3-y^2}_{g};\ \underbrace{y^2-z^3}_{h});\ \underbrace{xy^3-z^3}_{n};\ \underbrace{xz^3-z^9}_{r})$ $\quad$ v glex $(y^3x^2;\ x^3-y^2;\ z^3-y^2)$

$Lt(I):(x^3,y^3,z^3)$ $\rightarrow$ Gröbnerova báza (neredukovateľná)

$S(f;g)=-xy^3+y^2 : y^2-z^3=1$

z^3-y^2

$-xy^3+z^3$

$S(f;h)\rightarrow 0$; $S(g;h)\rightarrow 0$

$S(f;n)=-y^6+xz^3 : y^2-z^3=-y^4$

$+y^6-y^4z^3$

$xz^3-y^4z^3 : y^2-z^3=-y^2z^3$

$-y^2z^6+y^4z^3$

$xz^3-y^2z^6 : y^2-z^3=-z^6$

$-z^9+y^2z^6$

xz^3-z^9

$S(g;n)=-y^5+x^2z^3 : xz^3-z^9=x$

$xz^9-x^2z^3$

$xz^9-y^5 : y^2-z^3=-y^3$

$-y^3z^3+y^5$

$xz^9-y^3z^3 : xz^3-z^9=z^6$

$-xz^9+z^{15}$

$-y^3z^3+z^{15} : y^2-z^3=-yz^3$

$+y^3z^3-z^6y$

$-yz^6+z^{15}$

$(F;G)=I$ — ak $\gcd(Lt(F);Lt(G))=1$ – nesúdeliteľné, tak (F,G) – Gröbnerova bása

$a\,Lt(F)+\bar F=F$

$b\,Lt(G)+\bar G=G$

redukce — lokálne

$$S(F;G)=\frac{Lt(F)\cdot Lt(G)}{a\,Lt(F)}\cdot F-\frac{Lt(F)\cdot Lt(G)}{b\cdot Lt(G)}\cdot G=\frac{Lt(G)}{a}F-\frac{Lt(F)}{b}G=\frac{Lt(G)}{a}(a\,Lt(F)+\bar F)-\frac{Lt(F)}{b}(b\,Lt(G)+\bar G)=\frac{Lt(G)}{a}\cdot\bar F-\frac{Lt(F)}{b}\bar G$$

$$\frac{Lt(G)}{a}\bar F-\frac{Lt(F)}{b}\bar G : b\,Lt(G)+\bar G=\frac{1}{ab}\bar F$$

$$-\frac{1}{a}Lt(G)\bar F\mp\frac{1}{ab}\bar F\cdot\bar G$$

$$\frac{-Lt(F)}{b}\bar G-\frac{1}{ab}\bar F\bar G \quad : a\,Lt(F)+\bar F=-\frac{1}{ab}\cdot\bar G$$

$$+\frac{Lt(F)}{b}\bar G+\frac{1}{ab}\bar F\bar G$$

$$0$$

$\# V(x^a-y^b;x^c-y^d)=\max\{ad;bc\}$

$\# V(x^a-y^b;x^c-z^d;y^e-z^f)=\max\{ade,bcf\}$

Pr.: lex: $\# V(\underset{f}{x^3-y^4},\underset{g}{x^4-y^3})=\max\{9;16\}=16$

v glex: $(\underline{y^4}-x^3;x^4-y^3)$ $\quad Lt(I)=(x^4;y^4)\quad 4.4=16$

$S(f;g)=-xy^4+y^3$

$S(f;h)=-y^8+x^2y^3$

$V(\underset{f}{x^3-y^4};\underset{g}{x^4-y^3};\underset{h}{xy^4-y^3});x^2y^3-y^8)$

Lokálne usporiadania. Štandardné bázy

$R=k[x_1;\dots;x_n]$

monomiálne usp.: lin., komp. s nás., $x_i>1$

lokálne usp.:

Df: Usporiadanie $>$ v R nazveme lokálnym, ak platí:

1. $>$ je lineárne
2. $>$ je kompatibilné s násobením
3. $1>x_i \quad \forall i=1,\dots;n$

Df: lex: $x^\alpha=x_1^{\alpha_1}\dots x_n^{\alpha_n}$ $\quad \alpha-\beta=(0,0,\dots;0;\alpha_r-\beta_r;\dots;\alpha_s-\beta_s;0;\dots;0)$

$x^\beta=x_1^{\beta_1}\dots x_n^{\beta_n}$ $\quad \alpha_r-\beta_r\neq 0,\ \alpha_s-\beta_s\neq 0$

Df: Usporiadanie nazveme reverzné lexikografické, ak $\alpha_s-\beta_s<0$

Keby $x_1>1 \Rightarrow x_1^2>x_1$ $\quad \alpha=(0,\dots;0;2;\dots 0)\quad \beta=(0;\dots;1;\dots 0)$

$\alpha-\beta=(0,\dots;0;1;0;\dots;0)$

Každé gradované$^{\text{lex, glex, reverse lex}}$... usporiadanie je monomiálne

$\forall$ antigradované usp. je lokálne.

antigradované lex. usp. ($\hookrightarrow$ antigradované + ...)

Df.: Usp. $>$ nazveme $\ldots$ ak platí $x^\alpha > x^\beta \overset{\text{df.}}{\Leftrightarrow} |\alpha| < |\beta|$ alebo ak $|\alpha| = |\beta|$, potom $\alpha_n - \beta_n > 0$

- s týmto usp. zistíme, koľko je tam 0

Df.: Bázu $\{F_1; \ldots; F_s\}$ ideálu $I = (F_1; \ldots; F_s)$ nazveme štandardnou, ak $Lt(I) = (Lt(F_1); \ldots; Lt(F_s))$ v určitom lokálnom usporiadaní.

$\forall$ platí ako pri Gröbnerovej báze, ak vymením $<$ ... za lokálne, Gröbner. za štandardnú bázu

Použitie:

$$I = \mathring{\mathcal{Y}}_1 \cap \mathring{\mathcal{Y}}_2 \cap \ldots \mathring{\mathcal{Y}}_s$$

$\mathcal{Y}_1 \to (0; 0; \ldots; 0)$, $\mathcal{Y}_2 \to (a_{21}; \ldots; a_{2n})$, $\mathcal{Y}_s \to (a_{s1}; \ldots; a_{sn})$

$I = (F_1; \ldots; F_s)$ štandardná

$Lt(I)$

$$\dim_k \left(k[x_1; \ldots; x_n] / Lt(I) \right) = \mu(0)$$

$I = (F_1; \ldots; F_s)$ - Gröbnerova

$$\dim \left(k[x_1; \ldots; x_n] / Lt(I) \right) = \# V(I)$$

Pr.: $I = (x^2 - y^3; x^3 - y^4)$

lex. monomiálne

antigradované = alex

$$I = (\underset{f}{x^2 - y^3} \,;\, \underset{g}{x^3 - y^4} \,;\, \underset{h}{xy^3 - y^4} \,;\, \underset{n}{y^6 - y^5})$$

lex:

$S(f;g) = -xy^3 + y^4$

$S(f;h) = -y^6 + xy^4 \;:\; xy^3 - y^4 = y$

$\quad -(y^5 + xy^4)$

$\quad \overline{\;-y^6 + y^5\;}$

$S(g;h) = -y^7 + x^2y^4 \;:\; x^2 - y^3 = y^4$

$\quad -(-y^7 + x^2y^4)$

$\quad \overline{\quad 0 \quad}$

ak máme ∀ kombinácie 0, ešte m...

$S(f;n) = 0$ (lema?) (vedúce nesúdeliteľné)

$S(g;n) = 0$

$S(h;n) = -y^7 + xy^5 \;:\; y^6 - y^5 = -y$

$\quad -(-y^7 + y^6)$

$\quad \overline{\;xy^5 - y^6\;} \;:\; xy^3 - y^4 = y^2$

$\quad -(xy^5 - y^6)$

$\quad \overline{\quad 0 \quad}$

$I = (f;g;h;n)$ je Gröbnerova báza

teda:

$Lt(I) = (x^2; xy^3; y^6)$

$\#V(I) = 9$ počet bodov variety I je: $2 \cdot 3 + 6 - 3 = 9$

báza je: $1, x, y, y^2, y^3, y^4, y^5, xy, xy^2$

teraz v alex:

$$I = (\underset{f}{x^2 - y^3} \,;\, \overset{g}{x^3 - y^4} \,;\, \overset{h}{xy^3 - y^4} \,;\, \overset{n}{y^5 - y^6})$$

$S(f;g) = 0$

$S(f;h) = 0$

$S(g;h) = 0$

$S(f;n) = 0$

$S(g;n) = 0$

$S(h;n) = -y^6 + xy^6 \;:\; xy^3 - y^4 = y^3$

$\quad -(-y^7 + xy^6)$

$\quad \overline{\;-y^6 + y^7\;} \;:\; y^5 - y^6 = -y$

$\quad 0$

$\Rightarrow$ máme štandardnú bázu

$Lt(x^2; xy^3; y^5)$

$\mu(0) = 8 : 1, x, y, y^2, y^3, y^4, xy, xy^2 \Rightarrow [0;0]$ je 8-násobný

$[1;1]$ je 1-násobný

$\overline{\quad 9\text{-násob.}}$

Veta: $I = (\overbrace{F_1, \dots, F_s}^{F})$ je Gröbnerova (štandardná) báza, potom $f \in I \Leftrightarrow \overline{f}^{F} = 0$

$f = x^2y - y^4 + x^3y - y^5$ } lex $\quad f \overset{?}{\in} I$

$f = x^3y + x^2y - y^5 - y^4$

delíme v akomkoľvek poradí:

(treba brať Gröbnerovu bázu)

$x^3y + x^2y - y^5 - y^4 \;:\; x^2 - y^3 = xy$

$\quad -(x^3y - xy^4)$

$\quad \overline{\;x^2y + xy^4 - y^5 - y^4\;} \;:\; x^2 - y^3 = y$

$\quad -(x^2y - y^4)$

$\quad \overline{\;xy^4 - y^5\;} \;:\; xy^3 - y^4 = y$

$\quad 0$