Bodá!

Algebraické variety

21.3.2006 Ut.

E^n nad poľom k - algebraicky uzavreté
$\downarrow$ $\forall$ polynóm má koreň ($\Leftrightarrow$ 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.: $\forall$ lin. varieta v E^n je alg. varieta
- rovina v E^3 : $x-y+z-1=0$
- priamka v E^3 : $x+y-1=0$, $x+z+2=0$

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

$$I=\{g_1f_1+\dots+g_sf_s;\ g_i\in k[x_1;\dots;x_n]\}=:\underbrace{(f_1;\dots;f_s)}_{\text{generátory}}\cdot \underbrace{k[x_1;\dots;x_n]}_{\text{ideál}}$$

Def. 1.2.: Ideálom v okruhu R (komutatívny, noetherovský) nazveme neprázdnu podmnožinu $I\subseteq R$, ktorá spĺňa:
1. $\forall a,b\in I$: $a-b\in I$ ($\Leftrightarrow$ I je podgrupa)
2. $\forall a\in I$: $\forall r\in R$: $r.a\in I$

(Ideál $\subseteq$ podokruh)

- $(Z;+;\cdot)\supseteq(n.Z)$ $\rightarrow$ 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:

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

$\Updownarrow$ $\uparrow$ množina nulových bodov ideálu I

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

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

Pozn: $\forall$ ideál má konečnú bázu (= noetherovský)

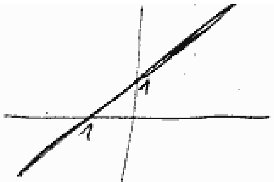
$$k[x_1;\dots;x_n]\rightsquigarrow E^n\rightsquigarrow k[x_1;\dots;x_n]$$

$$I\rightsquigarrow V(I)\rightsquigarrow \overbrace{I(V)}^{\text{ideál asociovaný s varietou } V}:=\{f\in k[x_1;\dots;x_n]:\ f(x_1;\dots;x_n)=0\ \forall(x_1;\dots;x_n)\in V\}$$

$V(I)=V$

$I\subseteq I(V)$, rovnosť nemusí nastať

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



(priamka, 2-krát)

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

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

$\mathbb{I}\subseteq rad(\mathbb{I})$

Platí: $I(V(\mathbb{I}))=rad(\mathbb{I})$

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

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

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

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

① $\mathbb{I}\subseteq\mathbb{J}\Rightarrow V(\mathbb{I})\supseteq V(\mathbb{J})$ $\longrightarrow$ Dôk: $x\in V(\mathbb{J})$ - x sa anuluje v $\mathbb{J}$, $\Rightarrow$ tým sa anuluje v $\mathbb{I}$

② $V\subseteq W\Rightarrow I(V)\supseteq I(W)$ $\longrightarrow$ podobne: $g\in I(W)\dots$

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

④ $V(\mathbb{I}\cap\mathbb{J})=V(\mathbb{I})\cup V(\mathbb{J})$

Dôkaz: ①, ② triv.

③ „$\subseteq$": $\mathbb{I}\subseteq\mathbb{I}+\mathbb{J}\overset{①}{\Rightarrow}\left.\begin{array}{l}V(\mathbb{I}+\mathbb{J})\subseteq V(\mathbb{I})\\ \subseteq V(\mathbb{J})\end{array}\right\}\subseteq V(\mathbb{I})\cap V(\mathbb{J})$

$\mathbb{J}\in\mathbb{I}+\mathbb{J}\Rightarrow\dots$

„$\supseteq$": $X\in V(\mathbb{I})\cap V(\mathbb{J})\Rightarrow \begin{array}{l}f(X)=0\ \forall f\in\mathbb{I}\\ g(X)=0\ \forall g\in\mathbb{J}\end{array}\Rightarrow (f+g)(X)=0\ \forall (f+g)\in\mathbb{I}+\mathbb{J}$

④ „$\supseteq$": triv.: $\mathbb{I}\cap\mathbb{J}\subseteq\mathbb{I}\Rightarrow V(\mathbb{I})\subseteq V(\mathbb{I}\cap\mathbb{J})\Rightarrow V(\mathbb{I}\cap\mathbb{J})\supseteq V(\mathbb{I})\cup V(\mathbb{J})$

$V(\mathbb{J})\subseteq V(\mathbb{I}\cap\mathbb{J})\nearrow$

„$\subseteq$":

$\mathbb{I}.\mathbb{J}=\{a.b,\ a\in\mathbb{I}, b\in\mathbb{J}\}$

$\mathbb{I}.\mathbb{J}\subseteq\mathbb{I}\cap\mathbb{J}\subseteq\begin{array}{c}\mathbb{I}\\ \mathbb{J}\end{array}$

$a.b$

$V(\mathbb{I}.\mathbb{J})=V(\mathbb{I})\cup V(\mathbb{J})$

„$\supseteq$" jasné

$X\in V(\mathbb{I}.\mathbb{J})$ $\quad X\notin V(\mathbb{I})$ $\quad X\in V(\mathbb{J})$

$(f\cdot g)(X)=0\ \forall f\in\mathbb{I}\ \ g\in\mathbb{J}$ $\quad\Uparrow$

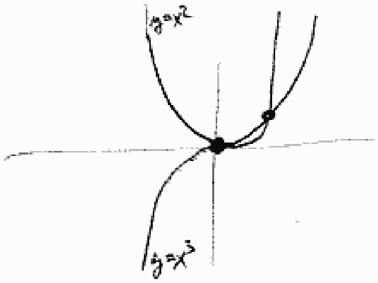
$f(X)\neq 0\Rightarrow$ $\quad g(X)=0$

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

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

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

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



$y = x^2$
$y = x^3$

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

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.

$$\begin{tikzcd} k[x_1;\dots;x_n] & E^n & k[x_1;\dots;x_n] \\ I \arrow[r, squiggly] & V(I) = \{(x)\in E^n; f(x)=0\ \forall f\in I\} & \\ & V \arrow[r, squiggly] & J(V) = \{f\in k[x_1;\dots;x_n]; f(x)=0\ \forall (x)\in V\} \end{tikzcd}$$

$I \subseteq k[x_1;\dots;x_n]$, $V(I) \subseteq E^n$, $V(I) = V$, $J(V) \subseteq k[x_1;\dots;x_n]$

$J(V)$ || 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, ireducibilné rozklady variet

Def.: $X \subseteq E^n$ sa nazýva ireducibilná, ak spĺňa

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

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

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

Veta: $X \subsetneq E^n$ je ireducibilná $\Leftrightarrow J(X)$ je prvoideál.

Dôkaz: „$\Rightarrow$": X je ired. a $f.g \in J(X)$

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

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

„$\supseteq$" jasné

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

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

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

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

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

$$\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2 . \quad \mathcal{X}_1 \subsetneq \mathcal{X} \quad \mathcal{X}_2 \subsetneq \mathcal{X}$$
$$\mathcal{I}(\mathcal{X}) = \mathcal{I}(\mathcal{X}_1) \cap \mathcal{I}(\mathcal{X}_2) \Rightarrow \mathcal{I}(\mathcal{X}) \subsetneq \mathcal{I}(\mathcal{X}_1) \quad \mathcal{I}(\mathcal{X}) \subsetneq \mathcal{I}(\mathcal{X}_2)$$
$$\Rightarrow \exists f \in \mathcal{I}(\mathcal{X}_1)\big|_{\mathcal{I}(\mathcal{X})}$$
$$\exists g \in \mathcal{I}(\mathcal{X}_2)\big|_{\mathcal{I}(\mathcal{X})} \quad \Rightarrow \underline{f \cdot g} \in \mathcal{I}(\mathcal{X}_1) \cap \mathcal{I}(\mathcal{X}_2) = \mathcal{I}(\mathcal{X})$$

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.

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

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

<u>Veta:</u> Radikál primárneho ideálu je prvoideál.

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

$a \quad b \quad q \quad p$

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

<u>Dôkaz</u>

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

$$(f \cdot g)^{\rho} = f^{\rho} \cdot g^{\rho} \in \mathfrak{q},\ f^{\rho} \notin \mathfrak{q} \Rightarrow$$
$$\Rightarrow (g^{\rho})^{\sigma} \in \mathfrak{q} \Rightarrow g \in \operatorname{rad}(\mathfrak{q}) \qquad \boxed{\mathfrak{q} \text{ je } \mathfrak{p}\text{-primárny}}$$
$$\operatorname{rad}(p^{\rho}\mathbb{Z}) = (p)\mathbb{Z}$$

<u>Df.:</u> 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.

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

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 je prienikom konečného počtu ireducibilných.

R ← noetherovský

Dôkaz?: $\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \ldots$

$\overset{\shortparallel}{\mathfrak{a}_{11}} \cap \ \mathfrak{a}_{12}$

$\vdots$

$\mathfrak{a} \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_{11} \subsetneq \ldots$

jedna z definícií noetherovských okruhov

Veta: Každý ireducibilný ideál je primárny.

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

$$\underset{\{r \in R;\, r \cdot g \in \mathfrak{a}\}}{\overset{}{(\mathfrak{a} : g)}} \subseteq (\mathfrak{a} : g^2) \subseteq (\mathfrak{a} : g^3) \subseteq \ldots \subseteq (\mathfrak{a} : g^r) \underset{\uparrow}{=} (\mathfrak{a} : g^{r+1})$$

„noetherovskosť"

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

„$\supseteq$" jasné

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

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

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

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

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

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

| $\operatorname{rad}(\mathfrak{a} \cap \mathfrak{b}) = \operatorname{rad}(\mathfrak{a}) \cap \operatorname{rad}(\mathfrak{b})$

„$\subseteq$" jasné

„$\supseteq$": $f \in \operatorname{rad}(\mathfrak{a}) \cap \operatorname{rad}(\mathfrak{b}) \Rightarrow$

$f^{\varrho} \in \mathfrak{a} \quad f^{\nu} \in \mathfrak{b} \Rightarrow f^{\max\{\varrho;\nu\}} \in \mathfrak{a} \cap \mathfrak{b}$

$\Rightarrow f \in \operatorname{rad}(\mathfrak{a} \cap \mathfrak{b})$

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

$\overset{\shortparallel}{(x^2 + y^2 - 1; x)} \cap (x^2 + y^2 - 1; y) = (y^2 - 1; x) \cap (x^2 - 1; y) =$

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

$\cap \underset{[1;0]}{(x-1; y)} \cap \underset{[-1;0]}{(x+1; y)}$ priamky

$x \cdot y = 0$ - = osi

$x^2 + y^2 - 1 = 0$ - kružnica

} prienik ↗ 4 body

Rozmer alg. variety, Rozmer ideálu

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

$X = X_s \supsetneq X_{s1} \supsetneq X_{s2} \supsetneq \dots \underset{\hookrightarrow \text{krivka}}{X_1} \supsetneq \overset{\rightarrow \text{bod}}{X_0} \supsetneq \emptyset$ - ireducibilné alg. variety

- maximálny reťazec

Def.: $s := \dim X$ - s-rozmer variety X

$X = X_s \supsetneq X_{s-1} \supsetneq \dots \supsetneq X_1 \supsetneq X_0 \supsetneq \emptyset$

$\Updownarrow$

$I(X_s) \subseteq I(X_{s-1}) \subsetneq \dots \subsetneq I(X_1) \subsetneq I(X_0) \subseteq k[x_1, \dots, x_n]$

asociovaný prvoideál

→ asociovaný prvoideál bodu so súr. $a_1, \dots, a_n$

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

Veta: $\dim X = \dim I(X)$, X - ired.

Nech $X = X_1 \cup X_2 \cup \dots \cup X_n$ $\forall$ ireducibilné!

Def.: $\dim X := \max\{\dim X_i\}$

Platí $\dim I(X) = \max\{\dim I(X_i)\}$

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

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

$\mathfrak{a} = {}^{d}\mathfrak{q} \cap \dots \cap {}^{d}\mathfrak{q}_r \cap {}^{d-1}\mathfrak{q}_{+} \cap \dots \cap {}^{d-1}\mathfrak{q}_s \cap \dots$

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

$\mathfrak{a} \in k[x_1; \dots; x_n]$

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

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

$\mathbb{X}: F=0$, $\mathbb{Y}: G=0$ } krivky, $\deg F = m$, $\deg G = n$ | $\# \mathbb{X} \cap \mathbb{Y} = m.n$, 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.: $\mathfrak{a} = (x^2-y^2-4; x^2y^2) = \overset{\overset{(x-2;y)}{\cup}}{(x-2; y^2)} \cap \overset{\overset{(x+2;y)}{\cup}}{(x+2; y^2)} \cap \overset{\overset{(y-2;x)}{\cup}}{(y-2; x^2)} \cap \overset{(y+2;x)}{(y+2; x^2)}$

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

Usporiadania v okruhu polynómov

$k[x_1; \dots; x_n] =: R$ $\mathbb{X}^\alpha := X_1^{\alpha_1} X_2^{\alpha_2} \dots X_n^{\alpha_n}$ – 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 $X^\alpha > X^\beta, X^\beta > X^\alpha \Rightarrow X^\alpha > X^\gamma$ - 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 - ~~tot.~~, refl., antisym.; tranz.

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

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

- budeme brať $x_1 > x_2 > \dots > x_n$

$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

prvých niekoľko prvkov je nulových

$; \alpha - \beta = (0;\dots;0;\underset{\substack{\neq \\ 0}}{\alpha_r - \beta_r};\dots;\underset{\substack{\neq \\ 0}}{\alpha_s - \beta_s};0;\dots;0)$ prvé nenul.

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

lexikografické

- toto usp. je monomiálne

↳ 3.): Nech $x_i < 1 \quad / \cdot x_i$

$x_i^2 < x_i$ SPOR

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

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

$x^\alpha \underset{glex}{>} x^\beta \Leftrightarrow |\alpha| > |\beta| \vee (|\alpha| = |\beta| \wedge \alpha_r - \beta_r > 0)$

; je tiež monomiálne

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

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

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

$\| $

$\sum c_\alpha x^\alpha$ 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 člen ideálu I

$\cup|$

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

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

nsd $(Lt(f_1); Lt(f_2)) = (x^2; x) = (x)$

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

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

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

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

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

$g = x^2 + x$

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

$-x^2 - 2x + 1$

$-x + 1$

$\Rightarrow f = g\underbrace{(x-1)}_{\text{podiel}} + \underbrace{(-x+1)}_{\text{zvyšok}}$

zachovanie usp.

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

$$(x^4 - x^3y + xy - 1) : (\underline{x}^2 - y) = x^2 - xy + y$$
$$-(x^4 - x^2y)$$
$$-x^3y + x^2y + xy - 1$$
$$-(-x^3y + xy^2)$$
$$x^2y - xy^2 + xy - 1$$
$$-(x^2y - y^2)$$
$$-xy^2 + xy + y^2 - 1$$

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

$$(-xy^2 + xy + y^2 - 1) : (\underline{x} - y^2) = -y^2 + y$$
$$-(-xy^2 + y^4)$$
$$xy - y^4 + y^2 - 1$$
$$-(xy - y^3)$$
$$-y^4 + y^3 + y^2 - 1$$

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

$$(x^2y - xy^2 + xz - z^2) : (\underline{x}^2 - y) = y$$
$$-(x^2y - y^2)$$
$$(-xy^2 + xz + y^2 - z^2) : (\underline{x} - z) = -y^2 + z$$
$$-(-xy^2 + y^2z)$$
$$xz - y^2z + y^2 - z^2$$
$$-(xz - z^2)$$
$$(-y^2z + y^2) : (\underline{y} - z^2) = -yz + y - z^3 + z^2$$
$$-(-y^2z + yz^3)$$
$$y^2 - yz^3$$
$$-(y^2 - yz^2)$$
$$-yz^3 + yz^2$$
$$-(-yz^3 + z^5)$$
$$(yz^2 - z^5$$
$$-(yz^2 - z^4)$$
$$-z^5 + z^4$$

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

---

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:

$$f = g_1F_1 + g_2F_1 + \dots + g_sF_s + r$$, 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
$$S(f;g) = \frac{x^\gamma}{Lt(f)}\cdot f - \frac{x^\gamma}{Lt(g)}\,g$$
, pričom x^γ je najmenší spol. násobok x^α, x^β

$x^\beta \to$ vedúci monóm g

$x^\alpha \to$ vedúci monóm f

O- sa vykrátia vedúce

Pr.: $f = \underline{x^2y}-y^3$ lex.;

$g = \underline{xy^2}-xy$

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

(Buchbergerovo kritérium)

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

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

Pr.: $I = (\overbrace{\underline{x}-y^2}^{F};\overbrace{\underline{y^3}-y}^{G})$ lex.

$Lt(I)=(x;y^3)$

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

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

$-(y^5+y^3)$

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

$-(xy-y^3)$

0

$(-y^3+xy) : (y^3-y) = -1$

$-(-y^3+y)$

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

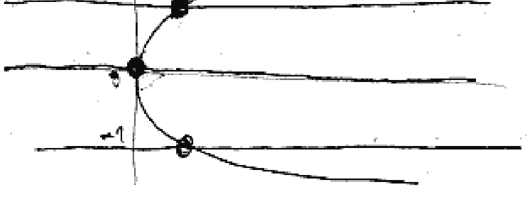
$-(xy-y^3)$

$(y^3-y) : (y^3-y) = 1.$

0

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

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



25.4.2006 Ut.

Buchbergerov algoritmus

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

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

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

pridali 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 označíme $h_1;\dots;h_r$

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

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

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

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

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

0

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

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

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

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

$-(xy^3-y^6)$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lema: $\{f;g\}=\Gamma$; $\mathrm{nsd}(Lt(f);Lt(g))=1 \Rightarrow$

$\Rightarrow \overline{S(f;g)}^{\Gamma}=0$

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

$\overline{S(f,h)}^{\Gamma_2} = 0$ (z lemy)

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

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

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

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

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

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

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

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

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

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

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

0

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

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

$\nearrow$ 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 (Jana)

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

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

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

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

0

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

~~Dôkaz~~

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

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

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

$Lt(r_1) \vee Lt(r_2) \Rightarrow Lt(r_1) \vee Lt(r_2)$ 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 $I = (f_1, \dots, f_s) \Rightarrow$

$\Rightarrow$ $\underset{\overline{f}^{\Gamma}}{\overset{\shortparallel}{r}}$ je určený jednoznačne

---

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

$0 + (3)\mathbb{Z} = \bar{0}$
$1 + (3)\mathbb{Z} = \bar{1}$
$2 + (3)\mathbb{Z} = \bar{2}$

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

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

$I = (f_1; \dots; f_s)$ 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. $f = a_1 f_1 + \dots + a_s f_s + \boxed{\overline{f}^{\Gamma}}^{=0} \in I$

„$\Rightarrow$": 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. $f \in k[x_1;\dots;x_n] \xrightarrow{\varphi} k[x_1;\dots;x_n]/Lt(I)$

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

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

$\wr\wr$

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

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
$1, x, x^2, y, y^2$

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

$x = y^3 = 0 \Rightarrow (0,0)$ 3-krát $\quad I \subset k[x_1;\dots;x_n]$ $\quad I = \overset{0}{\mathcal{Y}}_1$

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

9.5.2006. Ut.

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

Použitie

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

$(F_1;\dots;F_s) = I = \overset{0}{\mathcal{Y}}_{c_1} \cap \overset{0}{\mathcal{Y}}_{c_2} \cap \dots \cap \overset{0}{\mathcal{Y}}_{c_s}$

$\downarrow$ $\quad (a_{21};\dots;a_{2n})$ $\quad (a_{s1};\dots;a_{sn})$

$0 = (0;0;\dots;0)$
$(x_1-a_1;\dots;x_n-a_n)$
$\updownarrow$
$c_1 = (a_{11};\dots;a_{1n})$

$I = (F_1;\dots;F_s)$ - štandardná
$\Downarrow$
$\dim_k (k[x_1;\dots;x_n]/Lt(I)) = \dots$

$I = (F_1;\dots;F_s)$ - Gröbnerova
$\Downarrow$
$\dim (k[x_1;\dots;x_n]/Lt(I)) = \# V(I)$

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

$k[x_1;\dots;x_n]/I \xrightarrow{\sim} k[x_1;\dots;x_n]/\overset{0}{\mathcal{Y}}_1 \oplus k[x_1;\dots;x_n]/\overset{0}{\mathcal{Y}}_2 \oplus \dots \oplus k[x_1;\dots;x_n]/\overset{0}{\mathcal{Y}}_s$

$f \to (f+\overset{0}{\mathcal{Y}}_1;\dots;f+\overset{0}{\mathcal{Y}}_s)$; $f \in Ker\,\varphi \Leftrightarrow f \in \overset{0}{\mathcal{Y}}_1 \cap \dots \cap \overset{0}{\mathcal{Y}}_s$

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

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

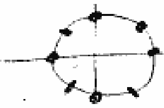
$V(I)$ $\quad x^3-y^5=0$

$\quad x-y^4=0$

$y^{12}-y^5=0$

$y^5(y^7-1)=0 \begin{cases} y=0 & 5x \\ y^7=1 \end{cases}$

$x=0 \Rightarrow [0;0]$ $5x$



komplexné čísla, 12 koreňov (1,1) . . .

$\# V(I)=12$

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

$\Rightarrow Lt(I)=(x; y^{12})$

x^3 nemusíme písať, lebo je tam automaticky

$\wedge x$

$$S(f;g)=-y^5+x^2y^4 : x-y^4 = xy^4+y^8$$
$$\underline{+xy^8-x^2y^4}$$
$$xy^8-y^5$$
$$\underline{-xy^8+y^{12}}$$
$$y^{12}-y^5$$

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

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

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

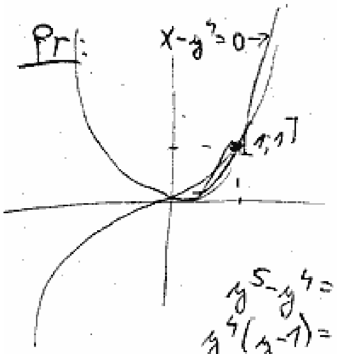
$$S(f;g)=\frac{y^5x}{y^5}(y^5-x^3)+\frac{y^5x}{y^4}(y^4-x) \quad -x^3+xy$$

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

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

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

Pr:



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

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

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

$k[x;y]/(x;y^5)$

$\# V(I)=5$

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

$y^5-y^4=0$

$y^4(y-1)=0 \to [1;1]$ $1x$

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

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

v glex $(y^3x^2; x^3-y^2; z^3-y^2)$

$Lt(I): (x^3, y^3, z^3)$ $\hookrightarrow$ Gröbnerova bá (nesúdeliteľné!)

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

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

$$S(f;n)=-y^6+xz^3 : y^2-z^3=-y^4$$
$$\underline{+y^6-y^4z^3}$$
$$xz^3-y^4z^3 : y^2-z^3=-y^2z^3$$
$$\underline{-y^2z^6+y^4z^3}$$
$$xz^3-y^2z^6 : y^2-z^3=-z^6$$
$$\underline{-z^9+y^2z^6}$$
$$xz^3-z^9$$

$$S(g;n)=-y^5+x^2z^3 : xz^3-z^9=x$$
$$\underline{xz^9-x^2z^3}$$
$$xz^9-y^5 : y^2-z^3=-y^3$$
$$\underline{-y^3z^3+y^5}$$
$$xz^9-y^3z^3 : xz^3-z^9=z^6$$
$$\underline{-xz^9+z^{15}}$$
$$-y^3z^3+z^{15} : y^2-z^3=-yz^3$$
$$\underline{+y^3z^3-z^6y}$$
$$-yz^6+z^{15}$$

$(F;G) = I$ — ak nsd$(Lt(F);Lt(G)) = 1$ – nesúdeliteľné, tak (F,G) – gröbnerova báza

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

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

vedúce ↑ ostatné

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

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

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

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

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

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: $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, $x^\beta = x_1^{\beta_1} \dots x_n^{\beta_n}$ $\quad \alpha - \beta = (0, 0, \dots; 0; \underset{\ne 0}{\alpha_r - \beta_r}; \dots; \underset{\ne 0}{\alpha_s - \beta_s}; 0; \dots; 0)$

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

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

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

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

∀ antigradované usp. je lokálne.

antigradované lex. usp. ↳ antigradované + …

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

- s týmto usp. zistíme, koľko je tam 0

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

∀ platí ako pri Gröbner~~[illegible]~~ových bázach, ak vymením $<$ … za lokálne, Gröbner. za štandardnú bázu

Využitie:

$$I = \underset{\downarrow\ (0;0;\dots;0)}{\mathring{\mathcal{Y}}_1} \cap \underset{\downarrow\ (a_{21};\dots;a_{2n})}{\mathring{\mathcal{Y}}_2} \cap \dots \underset{\downarrow\ (a_{s1};\dots;a_{sn})}{\mathring{\mathcal{Y}}_s}$$

$I = (F_1; \dots; F_s)$ štandardná

$Lt(I)$ $\quad \dim_k \left(k[x_1; \dots; x_n] / Lt(I)\right) = \mu(0)$ | $I = (F_1; \dots; F_s)$ – Gröbnerova $\quad \dim \left(k[x_1; \dots; x_n] / Lt(I)\right) = \# V(I)$

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:

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

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

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

$-y^6 + y^5$

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

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

0

s h máme ∀ kombinácie 0, ešte sm

$S(f;n) = 0$
$S(g;n) = 0$ (Lema 7 (vedúce nesúdeliteľné))

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

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

$xy^5 - y^6 \; : xy^3 - y^4 = y^2$

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

0

$I = (f;g;h;n)$ je Gröbnerova báza

teda:

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

$\#V(I) = 9$ · počet bodov variety I_g: $2.3 + 6 - 3 = 9$

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

teraz v glex:

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

$S(f;g) = 0$
$S(f;h) = 0$
$S(g;h) = 0$
$S(f;n) = 0$
$S(g;n) = 0$

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

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

$-y^6 + y^7 \; : y^5 - y^6 = -y$

0

⇒ máme štandardnú bázu

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

$r(0) = 8 : 1, x, y, y^2, y^3, y^4, xy, xy^2$ ⇒ $[0;0]$ je 8-krát

$[1;1]$ je 1-krát

9-krát

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

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

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

$f \overset{?}{\in} I$

delíme v akomkoľvek poradí:

(treba brať Gröbnerovu bázu)

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

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

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

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

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

0