I. ZÁKLADY AFINNÍ ALGEBRAICKÉ GEOMETRIE

<u>Značení:</u> K těleso

$\mathbb{A}^n(K)$ = afinní prostor nad K dimenze n

… $A \in \mathbb{A}^n(K)$ … souřadnice $A = (a_1, \dots, a_n) \in K^n$

$\mathbb{P}^n(K)$ = projektivní prostor nad K dimenze n

… $P \in \mathbb{P}^n(K)$ … homogenní souřadnice $P = (a_0 : \dots : a_n) \in K^{n+1}/\sim$

$\left.\begin{array}{l} f \in K[x_1, \dots, x_n] \\ A \in \mathbb{A}^n(K) \end{array}\right\}$ A je nula pro f $\equiv$ $f(A) = 0$ $\equiv$ $f(a_1, \dots, a_n) = 0$

Galoisova korespondence body $\leftrightarrow$ polynomy

$$\text{podmnožiny } \mathbb{A}^n(K) \underset{V}{\overset{I}{\rightleftarrows}} \text{podmnožiny } K[x_1, \dots, x_n]$$

$$X \longmapsto I(X) := \{ f : f(A) = 0 \ \forall A \in X \}$$

$$\underbrace{\{ A : f(A) = 0 \ \forall f \in S \}}_{\text{"řešení té soustavy"}} =: V(S) \longleftarrow \underbrace{S}_{\text{"soustava polynomiálních rovnic"}}$$

<u>Tvrzení:</u> Je to Galoisova korespondence, tj.

- $X \subseteq Y \Rightarrow I(X) \supseteq I(Y)$, $S \subseteq R \Rightarrow V(S) \supseteq V(R)$
- $I(V(I(X))) = I(X)$, $V(I(V(S))) = V(S)$
- $X \subseteq V(I(X))$, $S \subseteq I(V(S)) = \sqrt{(S)}$

pro K alg. uzavřené … Hilbertova věta o nulách

<u>Co jsou obrazy I, V?</u>

def: množiny tvaru $V(S)$ se nazývají algebraické

— " — $V(\{f\})$ — " — algebraické nadplochy

(v $\mathbb{A}^2(K)$ … alg. křivky; $\mathbb{A}^3$ … plochy)

☺ množiny tvaru $I(X)$ jsou radikálové ideály

☺ (HVN) K alg. uz. $\Rightarrow$ radikálové ideály jsou $I(X)$ pro nějaké X

$$\ldots \quad \underset{\text{radikálový}}{I = \sqrt{I}} \underset{\text{HVN}}{=} I(V(I)) \quad \rightsquigarrow \quad X := V(I)$$

Množinové operace s alg. množinami:

☺ $V(IJ) = V(I) \cup V(J)$

$V\left(\bigcup_{j\in J} I_j\right) = \bigcap_{j\in J} V(I_j)$

$\Big\}$ alg. mny uzavřené na $\Big\langle$ koneč. $\cup$, libo. $\cap$

$\rightsquigarrow$ tvoří topologii (otevřené mny)

= Zariského topologie na $\mathbb{A}^n(K)$

Hilbertova věta o bázi: $\forall I \ \exists n \ \exists f_1,\ldots,f_n \quad I = (f_1,\ldots,f_n)$

tj. geometricky: $V(I) = \bigcap_{i=1}^{n} V(f_i)$ ... průnik konečně mnoha nadploch

Ireducibilní rozklady

def: X ireducibilní $\equiv$ $X = Y \cup Z$ (obě alg.) $\Rightarrow$ $X = Y$ nebo $X = Z$

Tvrzení: X ireducibilní $\Leftrightarrow$ $I(X)$ prvoideál

Pozor: I prvoideál $\not\Leftrightarrow$ $V(I)$ ireducibilní

$\not\Leftarrow$ $\quad I = (x^2)$

$\not\Rightarrow$ $\quad f$ ireduc., $V(f)$ konečná, $|V(f)| \geq 2$

např. $f = y^2 + x^2(x-1)^2$ nad $\mathbb{R}$

Tvrzení: $\forall X$ alg. $\exists!\, X_1,\ldots,X_n$ ired. alg. t.ž. $X = X_1 \cup \ldots \cup X_n$ & $X_i \not\subseteq X_j \ \forall i \neq j$

☺ $\{A\}$ je alg. mna ... $I(\{A\}) = (x_1 - a_1, \ldots, x_n - a_n)$ ... je to max. ideál

& K alg. uz. $\Rightarrow$ jiné max. ideály nejsou (HVN)

Pozor! komponenty ve smyslu klasické geometrie (Eukleidovská metrika)

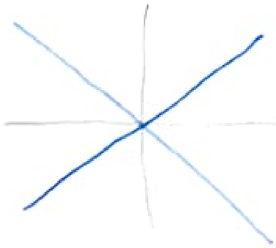
$\not\equiv$

komponenty ve smyslu algebraické geometrie (Zariského topologie)

Př.: $V(x^2-y^2) = V(x-y) \cup V(x+y)$

... 1 komponenta eukleidovsky

... 2 komponenty algebraicky

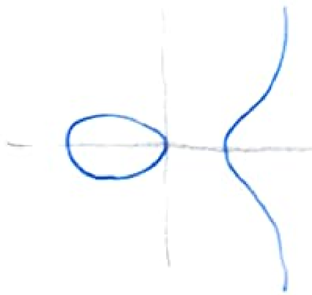


Př.: $V(y^2 - x(x^2-1))$

... 2 komponenty eukl.

... 1 komponenta alg.

(tj. je to ired. alg. křivka)



Shrnutí pro K alg. uzavřené:

$$\text{body} \underset{V}{\overset{I}{\rightleftarrows}} \text{polynomy}$$

jednobodovky $\longleftrightarrow$ maximální ideály

ireducibilní mny $\longleftrightarrow$ prvoideály

alg. množiny $\longleftrightarrow$ radikálové ideály

bijekce

Potíže s $\mathbb{R}$:

- $I = (x^2+1)$ ... $V(I) = \emptyset$, $I(V(I)) = K[x] \neq \sqrt{I}$
- každá alg. mna je nadplocha (→ s dimenzí to bude složité...)

... $\underbrace{V(f_1, \dots, f_n)}_{\text{kon. mnoho (HVB)}} = \underbrace{V(f_1^2 + \dots + f_n^2)}_{\text{jeden}}$

Soustavy s konečně mnoha řešeními

Věta: I ideál v $K[x_1,\dots,x_n]$ $\Rightarrow$

(1) $|V(I)| \leq \dim_K K[x_1,\dots,x_n]/I$

(2) K alg. uz. $\Rightarrow$ $\boxed{V(I) \text{ konečná} \Leftrightarrow \dim_K K[\bar{x}]/I \text{ koneč.}}$

Pozn.: v jakém smyslu $\dim_K \underbrace{K[\bar{x}]/I}$?

vektorový prostor nad K

... prvky: $[f]_I = f + I$ $\quad (f \in K[\bar{x}])$

... dobře def. $+$, $r\cdot$ $\quad (r \in K)$

Pozn.: v jakém smyslu $|V(I)| \leq \dim$?

... všechna nekonečna považuju za stejná

(může být $V(I)$ nespočetná, ale dimenze nejvýše spočetná)

Pozn.: znáte pro $n=1$: $\quad I = (f)$ ideál v $K[x]$

$\Rightarrow |V(I)| = \#\text{kořenů } f \leq \deg f = \dim K[x]/I$

Př.: $I = (x^2+y)$ ... $\mathbb{R}/\mathbb{C}$: $|V(I)| = \infty$, $\dim = \infty$

$\hookrightarrow$ báze $[1], [x], [x^2], \dots$

$I = (x^2+y^2+1)$ ... $\mathbb{R}$: $V(I) = \emptyset$, $\dim = \infty$

$\mathbb{C}$: $|V(I)| = \infty$

$\hookrightarrow$ báze $[1], [x], [x^2], \dots$
$[y], [xy], [x^2y], \dots$

$I = (x^2-y, y^3-1)$ ... $\mathbb{R}$: $V(I) = \{(\pm 1, 1)\}$

$\mathbb{C}$: $|V(I)| = 6$

$\dim = 6$ ... báze $[1], [y], [y^2]$,
$[x], [xy], [xy^2]$

$I = (x^2-y, (y-1)^3)$ ... $\mathbb{R}/\mathbb{C}$: $V(I) = \{(\pm 1, 1)\}$

$\dim = 6$ ... báze stejná

K čemu je to dobré ? Bézout je o křížení křivek

tj. o soustavách dvou rovnic dvou neznámých v $\mathbb{A}^2(\mathbb{C})$

Chci: nesdílejí komponentu

tj. průnik konečný

👁 X alg. mna, $B \notin X \Rightarrow \exists f \in K[\bar{x}]$ t.ž. $\begin{cases} f(A) = 0 & \forall A \in X \\ f(B) \neq 0 \end{cases}$

... kdyby ne, tj. kdyby $\forall f \left[\underbrace{f(A) = 0 \ \ \forall A \in X} \Rightarrow f(B) = 0 \right]$,

tak to znamená, že $B \in V(I(X)) = X$

protože X alg. $\square$

Důkaz Věty, část (1):

CHCI: aspoň tolik lineárně nezávislých prvků, kolik je $|V(I)|$

uvažuj $A_1, \dots, A_k \in V(I)$

zvol $f_1, \dots, f_k \in K[\bar{x}]$ t.ž. $f_i(A_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$

... aplikuj 👁 na $X = \{A_1, \dots, A_{i-1}, A_{i+1}, \dots, A_k\}$

& normalizuj, tj. $f_i = \frac{1}{f(A_i)} \cdot f$

dokážeme, že $[f_1]_I, \dots, [f_k]_I$ jsou lin. nezávislé v $K[\bar{x}]/_I$:

... nechť $\sum_{i=1}^{k} \lambda_i [f_i]_I = [0]_I$ pro nějaká $\lambda_i \in K$

$\Rightarrow \sum \lambda_i f_i \in I$

$\Rightarrow \forall j \ \ \underbrace{\left(\sum \lambda_i f_i\right)}_{\in I} \underbrace{(A_j)}_{\in V(I)} = 0$

//

$\sum \lambda_i f_i(A_j) = 0 + \dots + 0 + \lambda_j + 0 + \dots + 0 = \lambda_j$ $\square$

Důkaz Věty, část (2): $(K \text{ alg. uz.})$

$\Leftarrow$ plyne z části (1)

$\Rightarrow$ označ $V(I) = \{A_1, \dots, A_k\}$

$$A_i = (a_{i1}, \dots, a_{in})$$

definujeme $f_j := \underbrace{(x_j - a_{1j}) \cdot \ldots \cdot (x_j - a_{kj})}_{\in K[x_j]}, \quad j = 1..n$

$\forall j$: $\overset{\text{!!!}}{\odot}$ $f_j \in I(V(I))$, protože nuluje každý A_i

$$I(V(I)) \overset{\text{HVN}}{=} \sqrt{I}$$

$\Longrightarrow \exists N_j$ t.ž. $f_j^{N_j} \in I$

tj. $\underbrace{[f_j^{N_j}]_I}_{} = [0]_I$ v $K[\bar{x}]/_I$

polynom stupně $k \cdot N_j$ v proměnné x_j

$\rightsquigarrow$ můžeme to přepsat jako

$$[x_j^{N_j \cdot k}] = \sum_{i=0}^{N_j k - 1} \lambda_{ji} [x_j]^i \quad \text{pro něj. } \lambda_{ij} \in K$$

tj. $[x_j^{\geq N_j k}]$ lze napsat jako lineární kombinaci prvků $[x_j^{< N_j k}]$

$\rightsquigarrow$ obecný člen $[x_1^{\dots} \cdots x_n^{\dots}]$ lze napsat jako lin. komb. členů, kde ty exponenty jsou malé (v j-té složce $< N_j \cdot k$)

$\Longrightarrow$ členy $[x_1^{i_1} \cdots x_n^{i_n}]$, kde $i_j < N_j \cdot k$ generují vektorový prostor $K[\bar{x}]/_I$

$\Longrightarrow$ dimenze je $\leq k^n \cdot \prod N_j$, tedy konečná

$\square$

Algebraické množiny v rovině $\mathbb{A}^2(K)$

... stačí popsat ty ireducibilní, ostatní jsou jejich konečné $\cup$

KROK 1: "více rovnic $\Rightarrow$ nic zajímavého"

$\odot$ $NSD(f,g) = h \Rightarrow V(f,g) = V(h) \cup V(\underbrace{\tfrac{f}{h}, \tfrac{g}{h}}_{\text{nesoudělné}})$

... $\left.\begin{array}{l} f = h\cdot\tilde{f} \\ g = h\cdot\tilde{g} \end{array}\right\}$ $(f,g) = (h)\cdot(\tilde{f},\tilde{g})$

$$\Downarrow$$

$$V(f,g) = V(h) \cup V(\tilde{f},\tilde{g}) \qquad \square$$

Tvrzení: $NSD(f,g) = 1 \Rightarrow V(f,g)$ je konečná

! Pozor! Zde je nutné $\mathbb{A}^2(K)$, tj. $f,g \in K[x,y]$

(Proč důkaz selže pro $K[x,y,z]$?)

racionální funkce

Dk: $NSD(f,g) = 1$ v $K[x,y]$ $\xrightarrow[\text{Gaussova věta}]{}$ tady v $\underbrace{K(x)[y]}_{\text{obor hlavních ideálů}}$

$\underset{\text{Bézout}}{\Longrightarrow}$ $\exists r,s \in K(x)[y]$ t.ž.

$1 = r\cdot f + s\cdot g$ (počítáme v $K(x)[y]$) ($\Rightarrow$ Bézout!)

$\Longrightarrow$ $\exists h \in K[x]$ $\exists \tilde{r},\tilde{s} \in K[x,y]$ t.ž.

• (společný jmenovatel pro všechny koef. r,s) $h = \tilde{r}\cdot f + \tilde{s}\cdot g$ (počítáme v $K[x,y]$)

$\Longrightarrow$ $\exists h \in K[x]$ t.ž. $h \in (f,g)$ v $K[x,y]$

Teď to celé zopakuj pro $K(y)[x]$: ....

$\Longrightarrow$ $\exists k \in K[y]$ t.ž. $k \in (f,g)$ v $K[x,y]$

$\Longrightarrow$ $\dim K[x,y]/(f,g) \leq \deg h \cdot \deg k$, tedy konečná

h přepisuje $[x^{\deg h}]$ na menší členy

k — " — $[y^{\deg k}]$ — " —

$\underset{}{\xRightarrow{\text{Věta}}}$ $V(f,g)$ konečná $\square$

KROK 2: "jedna ireducibilní rovnice je zajímavá"

Tvrzení: $f \in K[x,y]$, $V(f)$ nekonečná, f ireducibilní

$\Rightarrow$ $I(V(f)) = (f)$ & $V(f)$ je ireducibilní

Dk: $\supseteq$ vždy

$\subseteq$ $g \in I(V(f))$ $\Rightarrow$ $V(f,g) = V(f)$ ... nekonečná

$\xRightarrow{\text{KROK 1}}$ f, g soudělné

$\xRightarrow{f \text{ ired.}}$ $f \mid g$ $\Rightarrow$ $g \in (f)$

? $V(f)$ ired. ? ... stačí: ? $I(V(f))$ prvoideál ?

$I(V(f)) = (f)$, f ired. ... je prvoid. $\square$

Věta: K nekonečné $\Rightarrow$ ireducibilní alg. množiny v $\mathbb{A}^2(K)$ jsou

- $\emptyset$, jednobodové, $\mathbb{A}^2(K)$
- $\underbrace{V(f) \text{ t.ž. } f \text{ ired.}}_{\text{křivky dané ired. polynomem}}$ & $V(f)$ nekonečná

Dk: Buď X alg. mna $\neq \emptyset, \{A\}, \mathbb{A}^2(K)$, tj. nutně nekonečná.
ired.

čili $I(X)$ je prvoideál, $\neq 0$

... vezmi $f \in I(X)$, $f \neq 0$

... $f = \prod p_i^{k_i}$, $I(X)$ prvoideál $\rightsquigarrow$ $\exists p$ ired. t.ž. $p \mid f$ & $p \in I(X)$

dokážeme, že $I(X) = p$

čili, že $X = V(I(X)) = V(p)$

kdyby $h \in I(X) \setminus (p)$, tak $X \subseteq \underbrace{V(p,h)}_{\text{konečná dle KROK 1}}$ $\lightning$

(tj. $p \nmid h$) $\square$