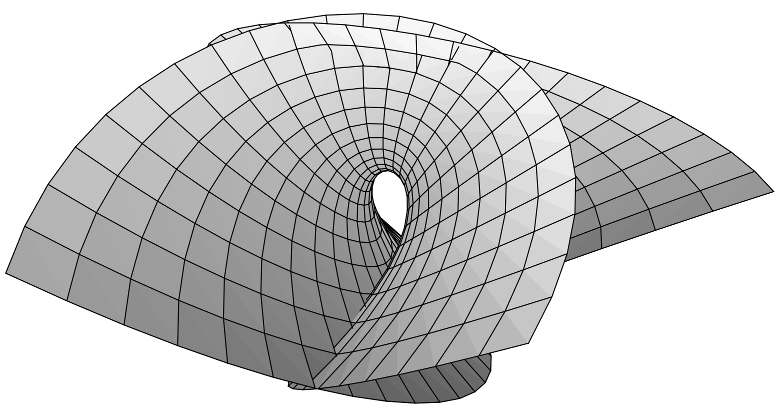
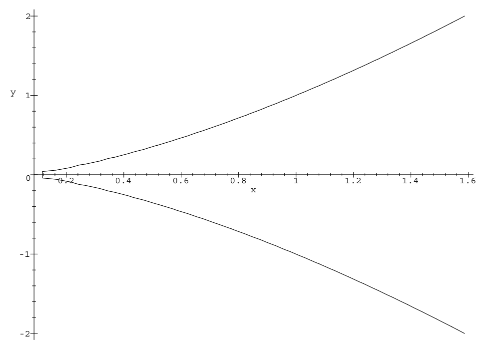
Jan Slovák

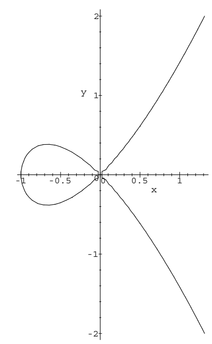
Algebraická geometrie



říjen 1995 – květen 1996

Obsah





Obr. 1: Křivky zadané $f(x,y) = x^3 - y^2$ a $f(x,y) = x^3 + x^2 - y^2$

1 Příklady a motivace

Předmětem (klasické) algebraické geometrie je studium objektů zadaných algebraickými rovnicemi nebo parametrizacemi, zejména jejich geometrických vlastností.

V této úvodní části si uvedeme několik motivujících příkladů a pokusíme se diskutovat problémy související s vhodným vymezením třídy objektů, které budou předmětem našeho zájmu.

1.1 Křivky v afinní rovině $\mathbb{R}^2$. Každý nenulový polynom $f(x,y)$ ve dvou proměnných zadává „křivku“ v $\mathbb{R}^2$ rovnicí $f(x,y) = 0$. Jde tedy o množinu nulových bodů jednoho polynomu f, budeme ji značit $K = \mathcal{V}(f)$. Odvoďte si, že je-li $f = f_1 \dots f_k$, pak $\mathcal{V}(f) = \mathcal{V}(f_1) \cup \dots \cup \mathcal{V}(f_k)$.

Příklady takto zadaných křivek jsou ovedeny na obrázcích 1 – 2.

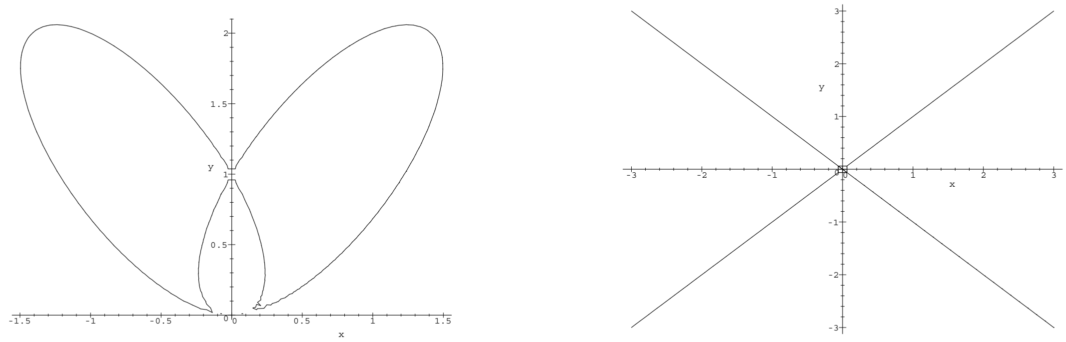
1.2 Parametrizace křivek. Křivky se můžeme pokusit zadat rovnicemi $x = f(t)$, $y = g(t)$, kde $f, g \in \mathbb{R}[t]$. Křivka je pak zadaná jako „polynomiální vložení“ reálné přímky do roviny.

Například rovnice $x = -1 + t$, $y = t(1 - t^2)$ dává křivku $\mathcal{V}(x^3 + x^2 - y^2)$, viz. obrázek 1. (Tuto parametrizaci snadno odvodíte výpočtem průniků přímek $y = tx$ s naší křivkou, tj. parametrizujeme směrnicí těchto přímek.)

O něco více křivek obdržíme, když budeme v parametrizaci uvažovat podíly polynomů $f = \frac{f_1}{f_2}$, $g = \frac{g_1}{g_2}$. Hovoříme pak o racionální parametrizaci. Příkladem může být parametrizace kružnice

$$x = \frac{2t}{1+t^2},\ y = \frac{-1+t^2}{1+t^2}$$

kterou obdržíme tzv. stereografickou projekcí, viz. obrázek 3. (Spočtěte si sami!) Všimněme si, že tentokrát vložení reálné přímky dá pouze „skoro všechny body“ parametrizované variety, jeden z nich (tj. bod z kterého promítáme) totiž není dosažitelný pro žádnou hodnotu parametru t. To není způsobeno naší nešikovností, z rozdílných topologických vlastností přímky a kružnice totiž vyplývá, že globální parametrizace existovat



Obr. 2: Křivky zadané $f(x,y) = 2x^4 - 3x^2y + y^2 - 2y^3 + y^4$ a $f(x,y) = x^2 - y^2$

nemůže.

1.3 Problémy s $\mathbb{R}^2$.

- Protože $\mathbb{R}$ není algebraicky uzavřené pole, máme problémy s existencí kořenů polynomů. V důsledku toho se při malé změně koeficientů zadávající rovnice může drasticky změnit výsledná varieta. Nabízí se pracovat s komplexními polynomy v $\mathbb{C}[x,y]$ a jimi zadanými podmnožinami c $\mathbb{C}^2$. To nás nemusí nijak děsit, naopak naše původně reálné křivky jsou obsaženy ve svých „komplexifikacích" (reálné polynomy prostě chápeme jako komplexní, které mají náhodou reálné koeficienty) a pouze získáváme bohatější nástroje pro popis jejich vlastností (imaginární tečny apod.).
- Chybí nám „nevlastní body". Např. při parametrizaci kružnice můžeme chybějící bod popsat jako obraz jediného nevlastního bodu reálné přímky, tj. bodu v „nekonečnu". Těchto problémů se nejlépe zbavíme tím, že budeme pracovat v tzv. projektivním rozšíření (reálné nebo komplexní) roviny.

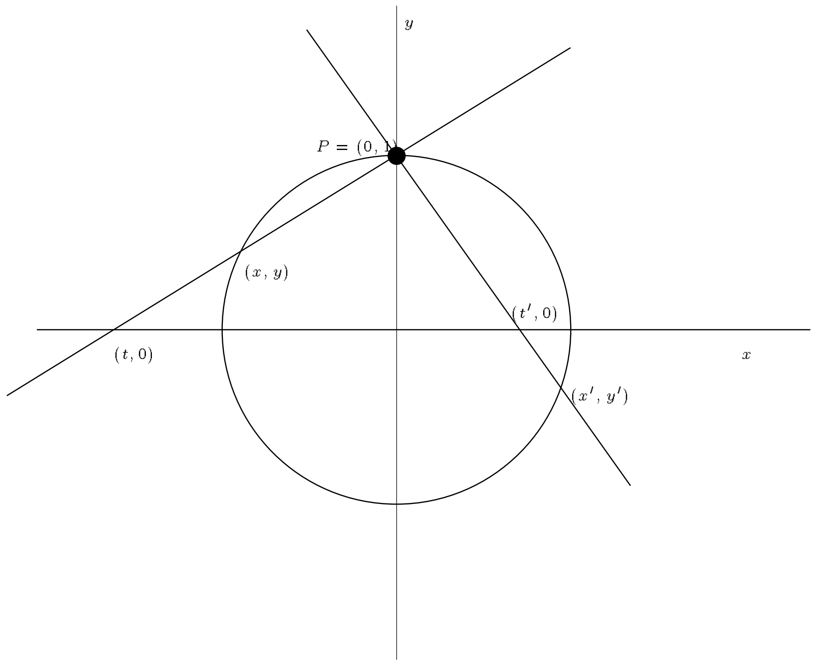
Naznačený technický postup sice s sebou nese poněkud složitější algebraický aparát, vede ale k daleko bohatější, přehlednější a symetričtější teorii.

1.4 Příklad (Komplexní kružnice). Uvažme množiny bodů $X^\varepsilon = \mathcal{V}(z_1^2 + z_2^2 - \varepsilon) \subset \mathbb{C}^2$ pro libovolné $\varepsilon \in \mathbb{R} \setminus \{0\}$. Příslušné reálné křivky jsou

$$X^\varepsilon_{\mathbb{R}} = X^\varepsilon \cap \mathbb{R}^2 = \begin{cases} \text{kružnice s poloměrem } \sqrt{\varepsilon} & \varepsilon > 0 \\ \emptyset & \varepsilon < 0 \end{cases}$$

Budeme psát $z_j = x_j + iy_j = x_j + \sqrt{-1}y_j$, je tedy X^ε zadáno jako podmnožina v $\mathbb{R}^4$ systémem dvou reálných rovnic

$$\begin{aligned} \mathrm{Re}(z_1^2 + z_2^2 - \varepsilon) &= x_1^2 + x_2^2 - y_1^2 - y_2^2 - \varepsilon = 0 \\ \mathrm{Im}(z_1^2 + z_2^2 - \varepsilon) &= 2(x_1y_1 + x_2y_2) = 0 \end{aligned}$$



Obr. 3: Stereografická projekce kružnice

Lze proto očekávat, že X^ε bude „dvourozměrná plocha" v $\mathbb{R}^4$, zkusíme si ji představit jako plochu v $\mathbb{R}^3$ ve vhodném průmětu $\mathbb{R}^4 \to \mathbb{R}^3$. Zvolme si za tím účelem zobrazení

$$\varphi_+ : (x_1, x_2, y_1, y_2) \mapsto (x_1, x_2, \frac{x_1 y_2 - x_2 y_1}{\sqrt{(x_1^2 + x_2^2)}})$$

Označme ještě V podmnožinu v $\mathbb{R}^4$ zadanou druhou naší rovnicí, tj.

$$V = \{(x_1, x_2, y_1, y_2);\ x_1 y_1 + x_2 y_2 = 0, (x_1, x_2) \neq (0, 0)\}.$$

Zúžení zobrazení φ_+ na V je invertibilní a jeho inverze ψ_+ je dána

$$\psi_+ : (u, v, w) \mapsto (u, v, \frac{-vw}{\sqrt{u^2 + v^2}}, \frac{uw}{\sqrt{u^2 + v^2}}).$$

Všimněme si nyní, že

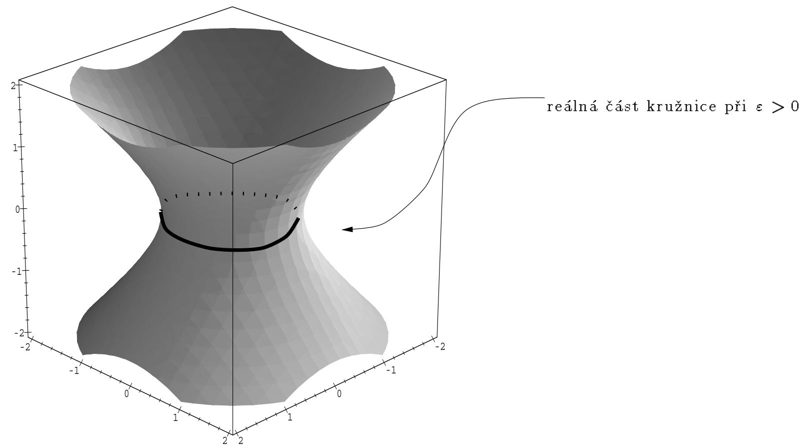
$$\left(\frac{x_1 y_2 - x_2 y_1}{\sqrt{x_1^2 + x_2^2}} \right)^2 = y_1^2 + y_2^2$$

a odtud vyplývá

$$\varphi_+(V \cap X^\varepsilon) = H^\varepsilon = \{(u, v, w);\ u^2 + v^2 - w^2 - |\varepsilon| = 0\}.$$

Nyní můžeme složit zkonstruovaná zobrazení

$$\varphi_\varepsilon : X^\varepsilon \to V \xrightarrow{\varphi_+} \mathbb{R}^3 \setminus \{(0, 0, 0)\} \supset H^\varepsilon$$



Obr. 4: Zobrazení komplexní kružnice do $\mathbb{R}^3$

a pro každé $\varepsilon > 0$ získáme bijekci $\varphi_\varepsilon : X^\varepsilon \to H^\varepsilon$. Reálná část této variety je „nejužší kružnice“ na jednodílném rotačním hyperboloidu H^ε, viz. obrázek 4.

Pro $\varepsilon < 0$ můžeme zopakovat předchozí úvahy, pouze v definici φ_+ přehodíme proměnné x a y a znaménka:

$$\varphi_- : (x_1, x_2, y_1, y_2) \mapsto (-y_1, -y_2, \frac{-y_1 x_2 + y_2 x_1}{\sqrt{(y_1^2 + y_2^2)}})$$

což přivodí změnu inverze ψ_-

$$\psi_+ : (u, v, w) \mapsto (\frac{-vw}{\sqrt{u^2+v^2}}, \frac{uw}{\sqrt{u^2+v^2}}, -u, -v).$$

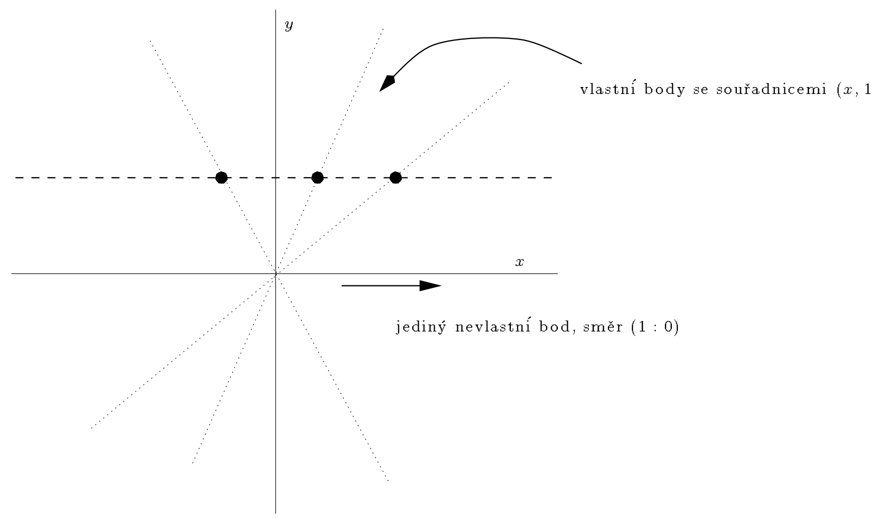
Nyní je opět H^ε jednodílý rotační hyperboloid, ovšem jeho reálná část je $X^\varepsilon_\mathbb{R} = \emptyset$.

V komplexním případě můžeme pozorovat, že při spojité změně koeficientů se výsledná varieta většinou v podstatě nemění, až na jisté „kastastrofické“ body, kdy může dojít ke kvalitativnímu skoku. Říká se tomu *princip permanence*. V reálném případě tento princip vůbec neplatí.

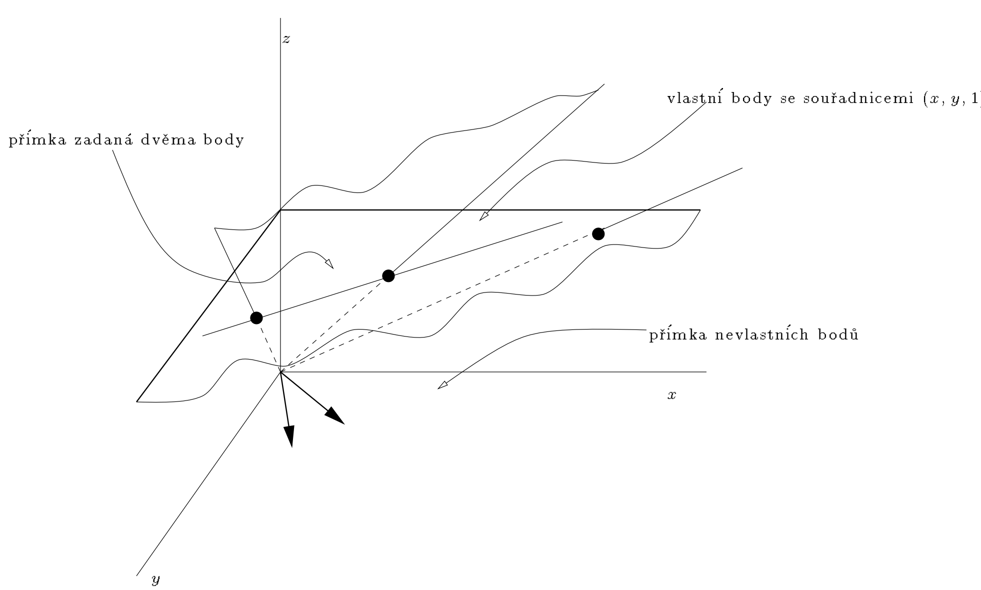
1.5 Projektivní rozšíření přímky a roviny. Reálný prostor $\mathbb{P}_1(\mathbb{R})$ je definován jako množina všech směrů v $\mathbb{R}^2$, tj. jeho body jsou jednorozměrné podprostory vektorového prostoru $\mathbb{R}^2$.

Komplexní projektivní prostor $\mathbb{P}_1(\mathbb{C})$ je definován jako množina všech směrů v $\mathbb{C}^2$, jeho body jsou tedy jednorozměrné podprostory komplexního vektorového prostoru $\mathbb{C}^2$.

Analogicky, body reálných, resp. komplexních, dvourozměrných projektivních prostorů jsou definovány jako směry v $\mathbb{R}^3$, resp. $\mathbb{C}^3$, viz. obrázky 5, 6.



Obr. 5: Ilustrace definice projektivních rošíření



Obr. 6: Projektivní rošíření afinní roviny

Zkusme si nyní rozšířit definici stereografické projekce tak, aby kružnice byla parametrizována body $\mathbb{P}_1(\mathbb{R})$. Podívejme se tedy, jak bude vypadat odpovídající zobrazení $\mathbb{P}_1(\mathbb{R}) \to \mathbb{P}_2(\mathbb{R}^2)$. Body v projektivních rozšířeních budeme zadávat tzv. *homogenními souřadnicemi*, které jsou dány až na společný násobek. Např. body v $\mathbb{P}_2(\mathbb{R})$ budou $(x : y : z)$.

Kružnice v rovině $z = 1$ je dána jako průnik kužele směrů zadaných rovnicí $x^2 + y^2 - z^2 = 0$ s touto rovinou. Inverzi k sterografické projekci (tj. naší parametrizaci kružnice) můžeme nyní zapsat takto:

$$(t : 1) \mapsto (\frac{2t}{1+t^2} : \frac{t^2-1}{t^2+1} : 1) = (2t : t^2 - 1 : t^2 + 1).$$

Přitom je pro $t \neq 0$ $(t : 1) = (2t^2 : 2t)$ a původní stereografickou projekci (tj. inverzi předchozí zobrazení) můžeme také zapsat pomocí lineárního předpisu

$$(x : y : z) \mapsto (y + z : x)$$

který rozšiřuje naší parametrizaci i na nevlastní bod $(0 : 1) \mapsto (0 : 1 : 1)$. Zobrazní celého $\mathbb{P}_1(\mathbb{R})$ na kružnici má pak „lineární“ zápis

$$\mathbb{P}_1(\mathbb{R}) \ni (x : y) \mapsto (2x : x - y : x + y) \in \mathbb{P}_2(\mathbb{R}).$$

Podívejme se ještě, jak jednoduché je spočíst přímo vzorec pro stereografickou projekci v projektivních rozšířeních: Vložíme si $\mathbb{P}_1(\mathbb{R})$ jako body s homogenními souřadnicemi $(t : 0 : 1)$ a mezi lineárními kombinacemi bodů $(0 : 1 : -1)$ (tj. pól ze kterého promítáme) a $(x : y : z)$ (obecný bod kružnice) musíme najít ten, který má souřadnice $(u : 0 : v)$. Jediná možnost je bod $(x : 0 : z + y)$, což je náš předchozí vztah.

1.6 Problémy. Můžeme si nyní vytyčit problémy, kterými se budeme zabývat.

- Jak vhodně definovat obecné objekty podobné křivkám, zejména ve vyšších dimenzích?
- Jaké algebraické nástroje máme k dispozici pro studium takových objektů?
- Jaká jsou vhodná zobrazení zachovávající podstatné vlastnosti našich objektů?
- Jak poznat, že geometrické vlastnosti dvou objektů naší třídy jsou stejné?
- Jak nalézt body našich objektů, v nichž se výrazně projevují jejich vlastnosti, a jak studovat chování objektu v okolí takových bodů?
- Jak studovat globální vlastnosti našich objektů?

Zdaleka se nám nepodaří uspokojivě vypracovat odpovědi na všechny naznačené otázky, na konci přednášek by však posluchač měl mít alespoň jistou představu, jaké techniky by k uspokojivé teorii vést mohly.

1.7 Singularity křivek. Zatím budeme úplně ignorovat zásadní problém, jak budou naše úvahy týkající se křivky $K = \mathcal{V}(f)$ záviset na volbě definujícího polynomu f. Z technických důvodů však budeme předpokládat, že neexistují polynomy g, h takové, že $f = gh$. Rovnici $f = 0$ budeme říkat *redukovaná rovnice nerozložitelné křivky* K a stupeň polynomu f je *stupeň křivky* K.

Každá přímka L v afinním prostoru $\mathbb{R}^2$ je zadána parametricky rovnicemi $(x, y) = (a, b) + t(u, v)$. Dosazením do polynomu f dostaneme polynom $g(t) = f(a + tu, b + tv)$ v jedné proměnné t. Body průniku $L \cap K$ jsou dány kořeny tohoto polynomu. Násobné kořeny t_0 vypovídají o dotyku vyššího řádu a zadávají *tečny křivky* K v bodech $(a + t_0u, b + t_0v)$. Zvolíme-li pevně bod $(a, b) \in K$, a hledáme (u, v) takové, aby $t = 0$ byl násobný kořen, dostaneme vztah

$$\frac{dg}{dt} = \frac{\partial f}{\partial x}(a, b) \cdot u + \frac{\partial f}{\partial y}(a, b) \cdot v) = 0.$$

Tato rovnice má prostor řešení dimenze 1 právě, když alespoň jedna z parciálních derivací f v (a, b) je nenulová. Takové body nazýváme *regulární body křivky* K. Ostatní jsou *singulární body* křivky K.

1.8 Tečny v singulárních bodech. Právě studium chování křivky v okolí singulárních bodů nám podá dobrou informaci o celé křivce. Všechny přímky procházející takovým bodem sice mají dotyk vyššího řádu, jistě je ale všechny nechceme považovat za tečny. Podle Taylorovy věty (snad dobře známé z matematické analýzy) má polynom f rozvoj v singulárním bodě (a, b)

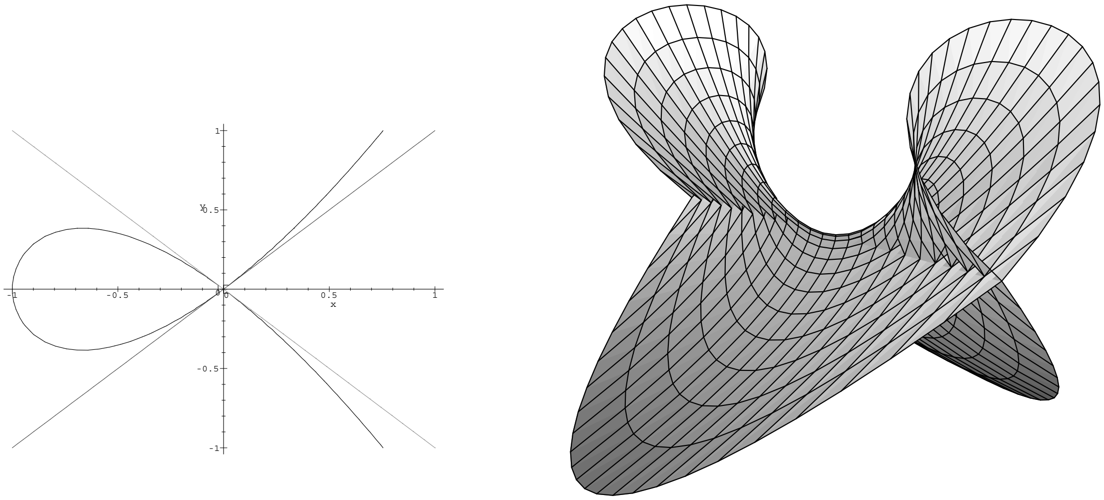
$$\begin{aligned} f(x, y) = & \underbrace{f(a, b)}_{=0 \text{ protože } (a, b \in K)} + \underbrace{\frac{\partial f}{\partial x}(a, b)(x - a) + \frac{\partial f}{\partial y}(y - b)}_{=0 \text{ protože je } (a, b) \text{ singulární}} + \\ & + \frac{\partial^2 f}{\partial x^2}(a, b)(x - a)^2 + \frac{\partial^2 f}{\partial x \partial y}(a, b)(x - a)(y - b) + \frac{\partial^2 f}{\partial y^2}(a, b)(y - a)^2 + \dots \end{aligned}$$

Předpokládejme, že $f_r(x - a, y - b) = \sum_{i=1}^{r} \frac{\partial^r f}{\partial x^i \partial y^{r-i}}(a, b)(x - a)^i (y - a)^{r-i}$ je první nenulová homogenní část. Pak množina všech řešení $(u : v)$ rovnice $f_r(u, v) = 0$ dává směrové vektory *tečen v singulárním bodě* (a, b). Množinu všech těchto tečen nazýváme *tečný kužel křivky* K v singulárním bodě (a, b).

1.9 Příklad. Pro nám již známou kubickou křivku $K = \mathcal{V}(x^3 + x^2 - y^2)$ snadno spočteme, že její jediný singulární bod je $(0, 0)$, první nenulová homogenní část polynomu je $x^2 - y^2$, tečný kužel je tedy tvořen dvěma přímkami $x \pm y = 0$, viz. obrázek 7.

1.10 Objekty ve vyšších dimenzích. Přímou analogií křivek v $\mathbb{C}^2$ jsou plochy v $\mathbb{C}^3$, které jsou opět zadány jediným polynomem. Pokud chceme obdržet křivky v $\mathbb{C}^3$, musíme použít polynomy alespoň dva, tj. křivku zadáme jako průnik dvou ploch.

Pro plochy můžeme počítat tečny v regulárních bodech a tečné kužely v singulárních bodech velmi podobně jako tomu bylo u křivek v rovině. Např. v regulárních bodech je alespoň jedna parciální derivace nenulová a získaná rovnice pro směrové vektory přímek majících protínání vyššího stupně bude mít prostor řešení kodimenze jedna, tj. pro plochy v $\mathbb{R}^3$ dostaneme právě tečné roviny. V singulárních bodech dostaneme opravdové analogie kuželů (které ovšem mohou zdegenerovat např. na dvojici rovin).



Obr. 7: Tečný kužel křivky $\mathcal{V}(x^3+x^2-y^2)$ v singulárním bodě a plocha $\mathcal{V}(x^2-y^2z^2+z^3)\subset\mathbb{R}^3$

Jako příklad křivek nám může sloužit tzv. tvistovaná kubika $\mathcal{V}(y-x^2, z-x^3)$ v $\mathbb{R}^3$ znázorněná (včetně odpovídajících ploch z definujících polynomů) na obrázku 8. Uvědomme si, že u křivek už definice tečných prostorů není zdaleka tak jednoduchá. Uvidíme, že ve skutečnosti není ani tak složité tečné prostory v regulárních bodech definovat, jako je spolehlivě spočíst z generujících polynomů.

1.11 Deformace singularit. Jednoduchý postup jak zjistit chování křivky v okolí regulárního bodu je spočíst její tečnu v tomto bodě. Pro singulární body je to s tečnami složitější, často však stačí libovolně málo pozměnit vhodný parametr (tj. koeficient) definujícího polynomu a singularita vymizí. Díky principu permanence pak z chování tečen pro blízké hodnoty parametru můžeme usuzovat na typ původní singularity. Již jsme se potkali se singularitou v počátku u křivek $\mathcal{V}(x^3-y^2)$ a $\mathcal{V}(x^3+x^2-y^2)$. Uvažme polynomy

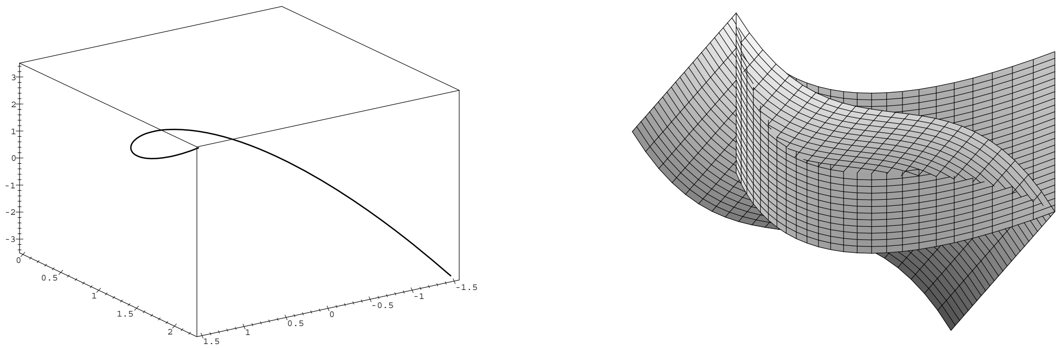
$$f_\varepsilon = x^3-y^2-\varepsilon,\ g_\delta = x^3+\delta x^2-y^2,\ h_{\varepsilon,\delta} = x^3+\delta x^2-y^2-\varepsilon.$$

Polynomy f_0 a g_0 dávají první z našich křivek, g_1 dá druhou.

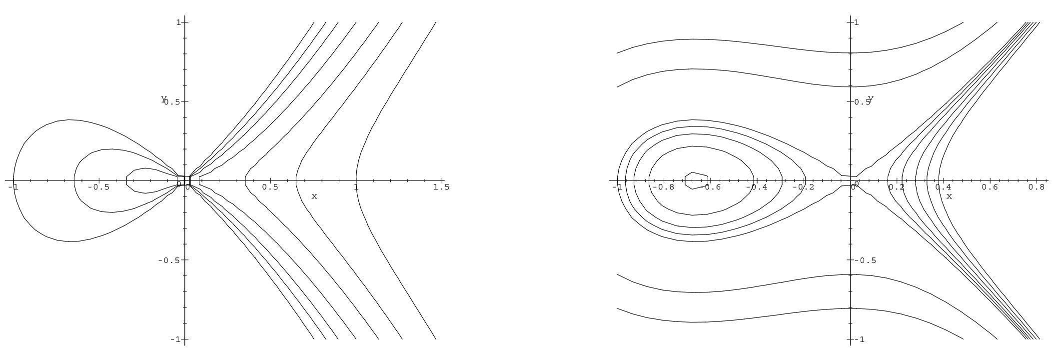
Podívejme se nejprve na chování křivek $\mathcal{V}(g_\delta)$. Snadno spočteme, že vždy mají pouze jeden singulární bod $(0,0)$, jeho typ je ovšem zcela odlišný pro $\delta<0$ a $\delta>0$. Je-li δ kladné, pak nám vyjdou dvě reálné tečny ve směrech $(1:\pm\sqrt{\delta})$, zatímco pro $\delta<0$ vyjdou obě tečny imaginární, je proto počátek izolovaným bodem křivky, viz. levý obrázek na 9.

Při deformacích f_ε je situace ještě daleko jednodušší. Pro nenulové ε totiž budou všechny body křivky regulární, viz. pravý obrázek na 9.

V obou případech získáváme jasnou představu o typu singularity Neilovy paraboly $\mathcal{V}(x^3-y^2)$. Diskuzí současných deformací $h_{\varepsilon,\delta}$ dospějeme ke křivce hodnot parametrů $\mathcal{V}(\varepsilon)\cup\mathcal{V}(\varepsilon-\frac{4\delta^3}{27})$, pro které křivky obsahují nějaký singulární bod, pro všechny hodnoty vně této křivky jsou všechny body regulární. Tvar křivky se přitom podstatně mění



Obr. 8: Tvistovaná kubika v $\mathbb{R}^3$



Obr. 9: Deformace singularit křivek

pouze při přechodech mezi uvedenými čtyřmi oblastmi. Hodnoty odpovídající Neilově parabole jsou právě jediným bodem společným všem čtyřem oblastem.

2 Projektivní rozšíření afinního prostoru

2.1 Definice. *n–rozměrný projektivní prostor* nad polem $\mathbb{K}$ je množina jednorozměrných podprostorů v $\mathbb{K}^{n+1}$, značíme jej $\mathbb{P}_n(\mathbb{K})$. Je-li $p \in \mathbb{P}_n(\mathbb{K})$, nazýváme libovolný nenulový vektor $x = (x_0, \dots, x_n) \in p \subset \mathbb{R}^n$ *homogenní souřadnice* bodu p. Píšeme $p = (x_0 : \dots : x_n)$.

2.2 Věta. *Podmnožiny $U_i = \{(x_0 : \dots : x_n) \in \mathbb{P}_n(\mathbb{K});\ x_i \neq 0\}$ jsou afinní prostory se zaměřením $\mathbb{K}^n$. Přitom $\mathbb{P}^n(\mathbb{K}) \setminus U_i \cong \mathbb{P}_{n-1}(\mathbb{K})$.*

Důkaz: Homogenní souřadnice jsou určeny jednoznačně, až na násobek skalárem z $\mathbb{K}$. Protože $\mathbb{K}$ je pole a $x_i \neq 0$, lze vždy najít právě jeden skalár $\lambda \in \mathbb{K}$ tak, že $(\lambda x_0, \dots, \lambda x_n)$ mají na i–tém místě 1. Touto volbou už jsou zbylé hodnoty $\lambda x_0, \dots, \lambda x_n$ dány jednoznačně. Tím tedy máme zkonstruováno zobrazení

$$\varphi : \mathbb{K}^n \to U_i, \quad (y_1, \dots, y_n) \to (y_1, \dots, y_i, 1, y_{i+1}, \dots, y_n)$$

a zřejmě jde o bijekci. Naopak, zobrazení

$$\psi : U_i \to \mathbb{K}_n, \quad (x_0, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) \to \frac{1}{x_i}(x_0, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$$

je dobře definováno a platí $\varphi \circ \psi = id_{U_i}$, $\psi \circ \varphi = id_{\mathbb{K}^n}$.

Zřejmě platí $\mathbb{P}_n(\mathbb{K}) \setminus U_i = \{(x_0 : x_1 : \dots : x_n) \in \mathbb{P}_n(\mathbb{K});\ x_i = 0\}$. Přitom zbylé skaláry $x_0, \dots, x_n$ jsou opět určeny až na násobek a zobrazení

$$\eta : \mathbb{P}_n(\mathbb{K}) \setminus U_i \to \mathbb{P}_{n-1}(\mathbb{K})$$
$$(x_0 : x_1 : \dots : x_{i-1} : 0 : x_{i+1} : \dots : x_n) \to (x_0 : \dots : x_{i-1} : x_{i+1} : \dots : x_n)$$

je dobře definovaná bijekce. □

2.3 Poznámka. Množina $H_i = \mathbb{P}_n(\mathbb{K}) \setminus U_i$ se nazývá *projektivní nadrovina bodů v nekonečnu.* Celý projektivní prostor $\mathbb{P}_n(\mathbb{K})$ lze také zkonstruovat tak, že začneme s afinní rovinou U_0 a vytvoříme její „projektivní rozšíření“ přidáním $H_0 = \mathbb{P}_{n-1}(\mathbb{K})$, kde H_0 lze chápat jako množinu směrů v U_0 (definovaných jako třída ekvivalence rovnoběžných přímek v $\mathbb{K}^n$).

Souřadně pak vzniklý prostor popisujeme tak, že pro „konečné body“ $(x_1, \dots, x_n) \in U_0$ užíváme souřadnice $(1, x_1, \dots, x_n)$, zatímco pro „body v nekonečnu“ užíváme souřadnice $(0, y_1, \dots, y_n) \in H_0$, a všechny souřadnice jsou určeny až na násobek jednoznačně.

2.4 Příklad. V afinním prostoru $\mathbb{R}^2$ uvažujme dvě přímky $L_1 : y - x - 1 = 0$ a $L_2 : y - x + 1 = 0$.
Jestliže budeme body přímek L_1 a L_2 chápat jako konečné body (tj. body v U_2) v

projektivním prostoru $\mathbb{P}_2(\mathbb{R}^2)$, budou zjevně jejich homogenní souřadnice $(x : y : z)$ splňovat rovnice

$$L_1 : y - x - z = 0, \quad L_2 : y - x + z = 0.$$

Podívejme se, jak budou rovnice těchto přímek vypadat v souřadnicích v U_1. Za tím účelem stačí dosadit $y = 1$ do předchozích rovnic:

$$L_1' : 1 - x - z = 0, \quad L_2' : 1 - x + z = 0$$

Nyní jsou „nekonečné" body naší původní afinní roviny U_2 dány vztahem $z = 0$ a vidíme, že naše přímky L_1' a L_2' se protínají v bodě $(1, 1, 0) \in U_1$. To odpovídá geometrické představě, že rovnoběžné přímky $L_1, L_2 \subset U_2$ v afinní rovině se protínají v nekonečnu (a to v bodě $(1 : 1 : 0)$).

2.5 Definice. *Projektivní přímka* v projektivním prostoru $\mathbb{P}_n(\mathbb{K})$ je množina bodů $p \in \mathbb{P}_n(\mathbb{K})$ taková, že jejich homogenní souřadnice $p = (x_0 : \cdots : x_n)$ zaplní právě všechny nenulové vektory 2–rozměrného podprostoru v $\mathbb{K}_{n+1}$.

Obecně, *podprostor v* $\mathbb{P}_n(\mathbb{K})$ *dimenze* k je množina bodů, jejichž homogenní souřadnice vyplní $(k+1)$–rozměrný podprostor v $\mathbb{K}^{n+1}$. Ekvivalentně, k–rozměrný podprostor v $\mathbb{P}_n(\mathbb{K})$ je podmnožina v $\mathbb{K}^{n+1}$, zadaná v homogenních souřadnicích systémem $(n-k)$ nezávislých lineárních homogenních rovnic.

2.6 Příklad.

1. Každé dvě různé přímky v $\mathbb{P}_2(\mathbb{R})$ se protínají v jednom bodě. (Je-li $L_1 : ax + by + cz = 0$, $L_2 = dx + ey + fz = 0$ a $(a : b : c) \neq (d : e : f)$, pak homogenní souřadnice bodů průniku jsou všechna řešení systému těchto dvou nezávislých homogenních rovnic. Jde tedy o právě jeden bod v $\mathbb{P}_2(\mathbb{K})$.)

2. Každé dva různé body v $\mathbb{P}_2(R)$ určují jedinou přímku je obsahující. (Dosazením homogenních souřadnic dvou různých bodů do obecné rovnice $ax + by + cz = 0$ přímky v $\mathbb{P}_2(\mathbb{K})$ získáme systém dvou nezávislých rovnic pro koeficienty a, b, c, proto dostaneme právě jedno řešení až na násobek.)

3. Každé dvě různé roviny v $\mathbb{P}_3(\mathbb{R})$ se protínají v jediné projektivní přímce. (Roviny jsou dány rovnicemi $\sigma_1 : a_1x + b_1y + c_1z + d_1w = 0$, $\sigma_2 : a_2x + b_2y + c_2z + d_2w = 0$, které jsou nezávislé, protože $\sigma_1 \neq \sigma_2$. Prostor všech řešení systému těchto dvou rovnic je tedy dvourozměrný, proto zadává projektivní přímku. Spočtěte si, že pro rovnoběžné roviny v afinní rovině U_3 dostaneme přímku, jejíž všechny body leží v H_3, tzv. projektivní přímku bodů v nekonečnu!)

2.7 Projektivní souřadné systémy. Podle naší definice je $\mathbb{P}_n(\mathbb{K})$ množina všech jednorozměrných podprostorů v $\mathbb{K}^{n+1}$ a pomocí standardních souřadnic (tj. standardní báze) v $\mathbb{K}^{n+1}$ jsme definovali homogenní souřadnice. Zcela stejným způsobem lze ovšem použít libovolnou bázi v $\mathbb{K}^{n+1}$. Opět bude každý jednorozměrný podprostor zadán souřadnicemi libovolného svého nenulového vektoru ve vybrané bázi. Hovoříme o *projektivním souřadném systému* určeném bazí $e_1, \ldots, e_n$ prostoru $\mathbb{K}^{n+1}$. Podobně jako pro homogenní souřadnice jsou projektivní souřadnice $(x_0, \ldots, x_n)$ bodu $p \in \mathbb{P}^n(\mathbb{K})$ (v příslušné projektivní souřadné soustavě) dány vektorem $v \in p$, $v = x_0e_0 + \ldots + x_ne_n$.

Z lineární algebry známe, jak se mění souřadnice vektorů při změnách bazí, vždy se jedná o násobení vhodnou invertibilní maticí (zleva). Nechť tedy jsou v $\mathbb{K}^n$ zvoleny báze $e_0, \dots, e_n$ a $e'_0, \dots, e'_n$ a příslušná matice přechodu A nechť má prvky a_{ij}. Tzn., že souřadnice $x = (x_0, \dots, x_n)$ odpovídají souřadnicím $x' = (x'_0, \dots, x'_n) = A \cdot x^T$. (Musí tedy platit $e_i = a_{0i}e'_0 + \dots + a_{ni}e'_n$.)

Naopak, kdykoliv zvolíme invertibilní matici A s $n+1$ řádky a sloupci, dostaneme zobrazení $\mathbb{P}_n(\mathbb{K}) \to \mathbb{P}_n(\mathbb{K})$, které homogenní souřadnice x^T zobrazí na $A \cdot x^T$. Taková zobrazení nazýváme *kolineace* a je zřejmé, že matice kolineace je určena až na násobek skalárem. Podívejme se nyní, jak takové kolineace mohou vypadat. V afinních podprostorech U_0, $U_1 \subset \mathbb{P}_n(\mathbb{K})$ získáme zejména speciální volbou matic tvaru

$$A = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ a_{10} & a_{11} & a_{12} & \dots & a_{1n} \\ \vdots & & & & \vdots \\ a_{n0} & a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{00} & b_{01} & b_{02} & \dots & b_{0n} \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & & & & \vdots \\ b_{n0} & b_{n1} & b_{n2} & \dots & b_{nn} \end{pmatrix}$$

všechny afinní transformace $U_0 \to U_0$ a všechny afinní transformace $U_1 \to U_1$. Všimněme si, že pevnou volbou $a_{00} = 1$, resp. $b_{11} = 1$, jsme již jednoznačně vybrali matici A, resp. B, zadávající danou kolineaci. Součiny matic těchto dvou typů již snadno získáme všechny invertibilní matice. Vidíme, že kolineace jsou přesně zobrazení, která získáme „rozšířením“ afinních zobrazení na celá projektivní rozšíření afinních prostorů.

2.8 Poznámka. Obecněji, projektivní prostor $\mathbb{P}(V)$ je definován jako množina jednorozměrných podprostorů ve vektorovém prostoru V a kolineace jsou taková zobrazení $\varphi : \mathbb{P}(V) \to \mathbb{P}(W)$, pro která existují invertibilní lineární zobrazení $\psi : V \in W$, tak že $\varphi(\langle v \rangle) = \langle \psi(v) \rangle$.

2.9 Projektivní nadroviny. Projektivní podprostory v $\mathbb{P}_n(\mathbb{K})$ dimenze $n-1$ se nazývají *projektivní nadroviny*. Vznikají řešením jediné nenulové rovnice $a_0x_0 + \dots + a_nx_n = 0$ pro homogenní souřadnice. Protože koeficienty této rovnice jsou určeny až na násobek, lze nadrovinu ztotožnit s bodem $(a_0 : a_1 : \dots : a_n) \in \mathbb{P}_n(\mathbb{K})$. Proto se množině všech nadrovin v $\mathbb{P}_n(\mathbb{K})$ říká *duální projektivní prostor* k prostoru $\mathbb{P}_n(\mathbb{K})$. Tento prostor označujeme $\mathbb{P}_n(\mathbb{K}^*)$.

2.10 Definice. Jsou-li $M \subset \mathbb{P}_n(\mathbb{K})$ a $M' \subset \mathbb{P}_n(\mathbb{K})$ dvě množiny bodů takové, že existuje kolineace $\varphi : \mathbb{P}_n(\mathbb{K}) \to \mathbb{P}_n(\mathbb{K})$ splňující $\varphi(M) = M'$, pak říkáme, že množiny M a M' jsou *projektivně ekvivalentní.*

2.11 Body v obecné poloze. Je evidentní, že výběrem souřadnic, tj. popisem nějakého objektu v homogenních nebo jiných projektivních souřadnicích nemohou být ovlivněny geometrické vlastnosti studovaného objektu. Zejména musí být všechny geometrické vlastnostnosti invariantní vzhledem k působení kolineací. Všimněme si nyní nejjednodušších objektů, konečných podmnožin bodů projektivních prostorů.

O $(n+1)$ bodech $p_1, \dots, p_{n+1} \in \mathbb{P}_n(\mathbb{K})$ řekneme, že jsou v *obecné poloze*, jestliže neexistuje projektivní nadrovina $\sigma \subset \mathbb{P}_n(\mathbb{K})$ obsahující všechny p_i, $i = 1, \dots, n+1$. O množině bodů $M \subset \mathbb{P}_n(\mathbb{K})$ mohutnosti větší než $n+1$ řekneme, že je v obecné poloze, je-li každá její podmnožina $n+1$ bodů v obecné poloze. Je zřejmé, že všechny množiny $M = p_1, \dots, p_{n+1}$ bodů v obecné poloze jsou projektivně ekvivalentní.

(Zvolíme-li nenulové vektory $v_1 \in p_1, \dots, v_{n+1} \in p_{n+1}$, jsou tyto jistě lineárně nezávislé a proto máme bázi na $\mathbb{K}^{n+1}$, tj. projektivní souřadnice na $\mathbb{P}_n(\mathbb{K})$, ve které je $p_1 = (1:0:0:\dots:0), p_2 = (0:1:0:\dots:0), \dots, p_{n+1} = (0:\dots:0:1)$.)

2.12 Věta. *Buďte $p_1, \dots, p_{n+2}$ a $q_1, \dots, q_{n+2}$ dvě skupiny bodů v $\mathbb{P}^n(\mathbb{K})$ v obecné poloze. Pak existuje kolineace $\varphi : \mathbb{P}^n(\mathbb{K}) \to \mathbb{P}^n(\mathbb{K})$ taková, že $\varphi(p_i) = q_i$.*

Důkaz: Protože body $p_1, \dots, p_{n+1}$ jsou v obecné poloze, definují jejich libovolně zvolené homogenní souřadnice v $\mathbb{K}^{n+1}$ projektivní souřadnice na $\mathbb{P}_n(\mathbb{K})$. Homogenní souřadnice bodu p_{n+2} pak můžeme vyjádřit jako

$$(x_0^{n+2} : \dots : x_n^{n+2}) = \lambda_1(x_0^1 : \dots : x_n^1) + \dots + \lambda_{n+1}(x_0^{n+1} : \dots : x_n^{n+1}).$$

Přitom všechny koeficienty $\lambda_1, \dots, \lambda_{n+1}$ musí být nenulové, protože jinak by některých $n+1$ bodů leželo v jedné nadrovině. Totéž platí pro body $q_1, \dots, q_{n+2}$, nechť tedy bod q_{n+2} má souřadné vyjádření

$$(y_0^{n+2} : \dots : y_n^{n+2}) = \tilde{\lambda}_1(y_0^1 : \dots : y_n^1) + \dots + \tilde{\lambda}_{n+1}(y_0^{n+1} : \dots : y_n^{n+1}).$$

Zvolíme (jednoznačně určené a invertibilní) lineární zobrazení $\psi : \mathbb{K}^{n+1} \to \mathbb{K}^{n+1}$ zobrazující $(\lambda_i(x_0^i, \dots, x_n^i)$ na $\tilde{\lambda}_i(y_0^i, \dots, y_n^i)$, $i = 1, \dots, n+1$. Příslušná kolineace φ zobrazí p_i na q_i a

$$(x_0^{n+2} : \dots : x_n^{n+2}) \mapsto \tilde{\lambda}_1(y_0^1 : \dots : y_n^1) + \dots + \tilde{\lambda}_{n+1}(y_0^{n+1} : \dots : y_n^{n+1}) = (y_0^{n+2} : \dots : y_n^{n+2})$$

$\square$

3 Polynomy

3.1 Definice. Nechť $\mathbb{K}$ je komutativní okruh.[1] *Polynom* f nad okruhem koeficientů $\mathbb{K}$ je výraz $f = a_n x^n + \dots + a_1 x + a_0$, kde $a_n, \dots, a_0 \in \mathbb{K}$, $a_n \neq 0$. Říkáme, že f má *stupeň* n, značíme $\deg f = n$. Množinu všech polynomů nad okruhem koeficientů $\mathbb{K}$ (v proměnné x) značíme $\mathbb{K}[x]$.

Polynom lze vždy chápat jako zobrazení[2] $f : \mathbb{K} \to \mathbb{K}$, $b \mapsto f(b) = a_n b^n + \dots + a_1 b + a_0$.

Součet polynomů $f = a_n x^n + \dots + a_0$ a $g = b_m x^m + \dots + b_0$ je dán formálním sečtením koeficientů

$$f + g = a_n x^n + \dots + a_0 + b_m x^m + \dots + b_0 = (a_0 + b_0) + (a_1 + b_1)x + \dots$$

a součin polynomů f a g je dán formálním součinem

$$f \cdot g = (a_0 + \dots + a_n x^n)(b_0 + \dots + b_m x^m) = \sum_{j=0}^{n+m} (\sum_{i=0}^{j} a_i b_{j-i}) x^j.$$

Takto definované sčítání a násobení zadává na $\mathbb{K}[x]$ strukturu komutativního okruhu s jedničkou.

[1] Uvidíme v dalším, že budeme uvažovat výhradně okruhy bez dělitelů nuly.

[2] Pro rozumné okruhy $\mathbb{K}$ jsou si dva polynomy f a g rovny (jako formální výrazy) právě, když určují stejné zobrazení.

Sčítání a násobení polynomů je kompatibilní se sčítáním a násobením zobrazení, tj. $(f+g)(a) = f(a)+g(a)$ a $(f\cdot g)(a) = f(a)g(a)$. Všimněme si, že znak $\cdot$ značí násobení v okruhu $\mathbb{K}[x]$ zatímco násobení v $\mathbb{K}$ značíme prostým zřetězením výrazů.

3.2 Polynomy více proměnných. Okruhy polynomů v proměnných $x_1, \dots, x_r$ definujeme induktivně vztahem

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

Např. $\mathbb{K}[x,y] = \mathbb{K}[x][y]$, tzn. že uvažujeme polynomy v proměnné y nad okruhem $\mathbb{K}[x]$. Snadno si každý ověří (proveďte si to!), že polynomy v proměnných $x_1, \dots, x_r$ lze chápat jako výrazy vzniklé z písmen $x_1, \dots, x_n$ a prvků okruhu $\mathbb{K}$ konečným počtem (formálního) sčítání a násobení v komutativním okruhu. Například prvky v $\mathbb{K}[x,y]$ jsou tvaru

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

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

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

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

$$\begin{aligned} f + g &= \sum_{|\alpha|\le max(m,n)} (a_\alpha + b_\alpha)x^\alpha \\ fg &= \sum_{|\gamma|=0}^{m+n} \left(\sum_{\alpha+\beta=\gamma} (a_\alpha b_\beta) x^\gamma \right) \end{aligned}$$

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

Samozřejmě musíme ověřit, že tyto vzorce opravdu popisují sčítání a násobení v induktivně definovaném okruhu polynomů v r proměnných. Dokážeme to indukcí přes počet proměnných. Předpokládejme, že vztahy platí v $\mathbb{K}[x_1, \dots, x_{r-1}]$ a počítejme součet

$$
\begin{aligned}
f &= a_k(x_1,\dots,x_{r-1})x_r^k + \dots + a_0(x_1,\dots,x_{r-1}) = \left(\sum_\alpha a_{k,\alpha}x^\alpha\right) x_r^k + \dots \\
g &= b_l(x_1,\dots,x_{r-1})x_r^l + \dots + b_0(x_1,\dots,x_{r-1}) = \left(\sum_\beta b_{l,\beta}x^\beta\right) x_r^k + \dots \\
f+g &= \Big(a_0(x_1,\dots,x_{r-1}) + b_0(x_1,\dots,x_{r-1})\Big) + \\
&\qquad + \Big(a_1(x_1,\dots,x_{r-1}) + b_1(x_1,\dots,x_{r-1})\Big)x_r + \dots \\
&= \Big(\sum_\gamma (a_{k,\gamma}+b_{k,\gamma})(x_1,\dots,x_{r-1})^\gamma\Big)x_r^k + \dots + \Big(\sum_\gamma (a_{0,\gamma}+b_{0,\gamma})(x_1,\dots,x_{r-1})^\gamma\Big) \\
&= \sum_{(\gamma,j)} (a_{j,\gamma}+b_{j,\gamma})(x_1,\dots,x_{r-1})^\gamma x_r^j.
\end{aligned}
$$

Podobně se provede důkaz pro součin (proveďte!).

3.3 Lemma. *Jestliže v okruhu $\mathbb{K}$ nejsou dělitelé nuly, pak také v okruhu polynomů $\mathbb{K}[x_1,\dots,x_r]$ nejsou dělitelé nuly.*

Důkaz: Budeme postupovat indukcí přes počet proměnných r. [3] Pro $r = 1$ uvažujme polynomy $f = a_n x_1^n + \dots + a_1x_1 + a_0$ a $g = b_m x^m + \dots + b_0$, přičemž $b_m \neq 0$ a $a_n \neq 0$. Vedoucí člen součinu fg je $a_nb_mx^{n+m}$, protože $a_nb_m \neq 0$, zejména tedy je součin nenulových polynomů opět nenulový.

Pokud tvrzení platí pro $r-1$ proměnných, pak použijeme předchozí úvahu pro okruh polynomů v jedné proměnné x_r s koeficienty v $\mathbb{K}[x_1,\dots,x_{r-1}]$. $\square$

3.4 Podílové těleso. Nechť $\mathbb{K}$ je komutativní okruh (s jedničkou) bez dělitelů nuly. Jeho *podílové těleso* definujeme jako třídy ekvivalence dvojic $(a,b) \in \mathbb{K}\times\mathbb{K}$, $b \neq 0$, které zapisujeme $\frac{a}{b}$, a ekvivalence je dána

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

Sčítání a násobení definujeme prostřednictvím reprezentantů tříd

$$
\begin{aligned}
\frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd} \\
\frac{a}{b}\frac{c}{d} &= \frac{ac}{bd}
\end{aligned}
$$

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

Podílové těleso okruhu $\mathbb{K}[x_1,\dots,x_r]$ nazýváme *těleso racionálních funkcí* a značíme je $\mathbb{K}(x_1,\dots,x_r)$.

[3] Důkaz lze vést také přímo s použitím multiindexových formulí pro součin, ale museli bychom si nadefinovat určité vhodné uspořádání monomů, abychom mohli pracovat s vedoucím koeficientem. Zkuste si to!)

3.5 Dělitelnost a nerozložitelnost. Nechť R je komutativní okruh bez dělitelů nuly. Řekneme, že b je dělitelné a a píšeme $a|b$, jestliže existuje $c \in R$ takové, že $b = ac$. Platí

1. je-li $a|b$ a zároveň $b|c$ pak také $a|c$
2. $a|b$ a zároveň $a|c$ pak také $a|(\alpha b + \beta c)$ pro všechny $\alpha, \beta \in R$
3. $a|0$ pro všechny $a \in R$
4. je-li $b = ac$ a $b \neq 0$ pak c je jednoznačně dáno volbou a, b (pro $b = ac = ac'$ totiž $0 = a(c - c')$ a $a \neq 0$)
5. invertibilní prvky v R (nazýváme je *jednotky*) tvoří komutativní podgrupu vzhledem k operaci násobení
6. každý prvek $a \in R$ je dělitelný všemi jednotkami $e \in R$ a jejich násobky ae (plyne z existence e^{-1})

Řekneme, že prvek $a \in R$ je *nerozložitelný*, jestliže je dělitelný pouze jednotkami $e \in R$ a jejich násobky ae. Řekneme, že okruh R je *obor integrity s jednoznačným rozkladem*, jestliže platí

7. pro každý nenulový prvek $a \in R$ existují nerozložitelné $a_1, \dots, a_r \in R$ takové že $a = a_1 a_2 \dots a_r$
8. jsou-li prvky $a_1, \dots, a_r$ a $b_1, \dots, b_s$ nerozložitelné, nejsou mezi nimi žádné jednotky a $a = a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$ pak je $r = s$ a ve vhodném přeuspořádání platí $a_j = e_j b_j$ pro vhodné jednotky e_j.

3.6 Příklad.

1. $\mathbb{Z}$ je obor integrity s jednoznačným rozkladem.

2. Každé pole (komutativní těleso) je obor integrity s jednoznačným rozkladem (a každý nenulový prvek je jednotka).

3. Nechť R má prvky tvaru $a_0 + \sum_{i=1}^{k} a_i \left(\sqrt[2^{n_i}]{x^{m_i}} \right)$ kde $a_0, \dots, a_k \in \mathbb{Z}$, $m_i, n \in \mathbb{Z}_{>0}$. Pak jednotky jsou pouze prvky ± 1, všechny prvky s $a_0 = 0$ jsou rozložitelné, ale např. výraz x nelze vyjádřit jako součin nerozložitelných. (Nerozložitelných je zde příliš málo.)

3.7 Věta. *Je-li R obor integrity s jednoznačným rozkladem, pak také okruh polynomů $R[x_1, \dots, x_r]$ je obor integrity s jednoznačným rozkladem.*

Důkaz: Myšlenka důkazu je velice jednoduchá. Stačí totiž provést důkaz pro polynomy v jedné proměnné nad oborem integrity s jednoznačným rozkladem R a zbytek plyne přímo z induktivní definice polynomů více proměnných. Uvažujme tedy $f \in R[x]$. Je-li f rozložitelný, pak je $f = f_1 f_2$, kde žádný z polynomů $f_1, f_2 \in R[x]$ není jednotka. Předpokládejme na chvíli navíc, že je-li f dělitelný nerozložitelným polynomem h, pak jistě h dělí f_1 nebo f_2.

Pokud tomu tak vždy bude, docílíme postupnou aplikací předchozí úvahy jednoznačný rozklad. Pokud je totiž f_1 dále rozložitelné, opět $f_1 = g_1 g_2$, kde g_1, g_2 nejsou jednotky, a přitom vždy buď oba polynomy g_1 a g_2 mají menší stupeň než f, nebo se sníží počet nerozložitelných faktorů ve vedoucích členech g_1 a g_2 (např. nad celými čísly $\mathbb{Z}$ je $2x^2 + 2x + 2 = 2(x^2 + x + 1)$). Proto po konečném počtu kroků dojdeme k rozkladu $f = f_1 \dots f_r$ na nerozložitelné polynomy $f_1, \dots, f_r$. Z našeho dodatečného předpokladu také plyne, že každý nerozložitelný polynom h dělící f, dělí některý z $f_1, \dots, f_r$. Proto pro každý další rozklad $f = f_1' f_2' \dots f_s'$ nutně každý z faktorů f_i dělí některý z f_j' a v takovém případě musí být $f_j' = e f_i$ pro vhodnou jednotku e. Postupným krácením takových dvojic odvodíme, že $r = s$ a jednotlivé faktory se liší pouze o násobky jednotek.

Zbývá tedy dokázat, že je-li $f = f_1 f_2$ dělitelný nerozložitelným polynomem h, pak jistě h dělí f_1 nebo f_2. To bude cílem následující série technických lemmat.[4] □

3.8 Lemma. *Nechť R je obor integrity s jednoznačným rozkladem. Pak platí*

1. *jsou-li $a, b, c \in R$, a je nerozložitelné a $a|bc$, pak buď $a|b$ nebo $a|c$*
2. *jestliže konstantní polynom $a \in R[x]$ dělí $f \in R[x]$ pak a dělí všechny koeficienty polynomu f*
3. *je-li a nerozložitelný konstantní polynom v $R[x]$ a $a|fg$, $f, g \in R[x]$, pak $a|f$ nebo $a|g$.*

Důkaz: 1. Podle předpokladu $bc = ad$ pro vhodné $d \in R$ a nechť $d = d_1 \dots d_r$, $b = b_1 \dots b_s$, $c = c_1 \dots c_q$ jsou rozklady na nerozložitelné faktory. Tzn. $ad_1 \dots d_r = b_1 \dots b_s c_1 \dots c_q$. Z jednoznačnosti rozkladu ad plyne $a = eb_j$ nebo $a = ec_i$ pro vhodnou jednotku e.

2. Nechť $f = b_0 + b_1 x + \dots + b_n x^n$. Protože $a|f$, jistě existuje polynom $g = c_0 + c_1 x + \dots c_k x^k$ takový, že $f = ag$. Odtud okamžitě plyne $k = n$, $ac_0 = b_0, \dots, ac_n = b_n$.

3. Uvažujme $f, g \in R[x]$ jako výše a předpokládejme, že a nedělí ani f ani g. Pak podle předchozího bodu existuje nějaké i tak, že a nedělí b_i a nějaké j tak, že a nedělí c_j. Zvolme taková i, j nejmenší možná. Koeficient u x^{i+j} v polynomu fg je $b_0 c_{i+j} + b_1 c_{i+j-1} + \dots + b_{i+j} c_0$. Podle naší volby a dělí všechny $b_0 c_{i+j}, \dots, b_{i-1} c_{j+1}, b_{i+1} c_{j-1}, \dots, b_{i+j} c_0$. A zároveň nedělí $b_i c_j$. Proto nemůže dělit celý koeficient. □

3.9 Lemma. *Nechť K je podílové těleso oboru integrity R s jednoznačným rozkladem. Je-li polynom f nerozložitelný v $R[x]$ je nerozložitelný také v $K[x]$.*

Důkaz: Uvažme libovolný nenulový polynom $f \in R[x] \subset K[x]$ (každý koeficient $a \in R$ můžeme považovat za prvek $\frac{a}{1} \in K$). Předpokládejme, že $f = g'h'$ pro vhodné $g', h' \in K[x]$, kde polynomy g', h' nejsou jednotky v $K[x]$ (tzn. nejsou to konstantní polynomy, neboť K je pole). Nechť a je společný násobek jmenovatelů koeficientů v g' a b je společný násobek jmenovatelů koeficientů v h'. Pak $bh', ag' \in R[x]$ a platí $abf = (bh')(ag')$. Nechť c je nerozložitelný faktor v rozkladu ab. Pak c dělí $(bh')(ag')$ a proto c dělí polynom bh' nebo polynom ag' (podle předchozího lemmatu). To ale znamená, že c můžeme vykrátit. Po konečném počtu takových krácení zjistíme, že $f = gh$ pro polynomy $g, h \in R[x]$. Přitom stupeň polynomů se neměnil, proto i g a h nejsou konstantní. Tím jsme dokázali negaci požadované implikace. □

3.10 Lemma (Algoritmus pro dělení se zbytkem). *Nechť R je komutativní okruh bez dělitelů nuly a $f, g \in R[x]$, $g \neq 0$. Pak existuje $a \in R$, $a \neq 0$, a polynomy q a r splňující $af = qg + r$, kde $r = 0$ nebo $\deg r < \deg g$. Je-li navíc R pole, nebo je*

[4] A při prvním čtení bude možná vhodné tuto pasáž vynechat a vrátit se k ní později.

aspoň vedoucí koeficient polynomu g roven jedné, potom lze volit $a = 1$ a polynomy q, r jsou v tomto případě určeny jednoznačně.

Důkaz: Tvrzení dokážeme indukcí vzhledem ke stupni f. Je-li $\deg f < \deg g$ nebo $f = 0$, pak volíme $a = 1$, $q = 0$, $r = f$, což vyhovuje všem našim podmínkám. Pro konstantní polynom g klademe $a = g$, $q = f$, $r = 0$.

Předpokládejme tedy, že $\deg f \geq \deg g > 0$ a pišme $f = a_0 + \cdots + a_n x^n$, $g = b_0 + \cdots + b_m x^m$. Buď platí $b_m f - a_n x^{n-m} g = 0$ a nebo je $\deg(b_m f - a_n x^{n-m} g) < \deg f$. V prvém případě jsme hotovi, ve druhém pak, podle indukčního předpokladu, existují a', q', r' splňující $a'(b_m f - a_n x^{n-m} g) = q'g + r'$ a buď $r' = 0$ nebo $\deg r' < \deg g$. Tzn.

$$a' b_m f = (g' + a' a_n x^{n-m}) g + r'.$$

Přitom je-li $b_m = 1$ nebo R je pole, pak podle indukčního předpokladu lze volit $a' = 1$ a q', r' jsou tak určeny jednoznačně. V takovém případě ovšem získáme $b_m f = (g' + a_n x^{n-m}) g + r'$ a je-li R pole, můžeme rovnost vynásobit b^{-1}. Předpokládejme, že $f = q_1 g + r_1$ je jiné řešení. Pak $0 = f - f = (q - q_1) g + (r - r_1)$ a buď je $r = r_1$, nebo $\deg(r - r_1) < \deg g$. V prvém případě odtud ovšem plyne i $q = q_1$, protože $R[x]$ neobsahuje dělitele nuly. Nechť ax^s je člen nejvyššího stupně v $q - q_1 \neq 0$ (určitě existuje). Potom jeho součin se členem nejvyššího stupňe v g musí být nulový (protože nejvyšší stupeň dostaneme tak , že vynásobíme nejvyšší stupně). To ovšem znamená, že $a = 0$. Protože ax^s byl největší nenulový stupeň, nutně dostáváme, že $q - q_1$ žádné nenulové monomy neobsahuje, je tedy určitě nulové. Pak ovšem i $r = r_1$. $\square$

3.11 Lemma (Bezoutova rovnost). *Nechť K je pole a nechť $f, g \in K[x]$. Pak existuje největší společný dělitel[5] h polynomů f a g. Polynom h je určený jednoznačně, až na násobek nenulovým skalárem. Přitom existují polynomy $A, B \in K[x]$ takové, že $h = Af + Bg$.*

Důkaz: Přímá konstrukce polynomů h, A a B se provede tzv. Euklidovým algoritmem. Provádíme postupně dělení se zbytkem (K je pole, takže to vždy umíme jednoznačně, viz. předchozí lemma):

$$\begin{aligned} f &= q_1 g + r_1 \\ g &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{p-1} &= q_{p+1} r_p + 0. \end{aligned}$$

V tomto postupu neustále klesají stupně r_i, proto jistě nastane rovnost z posledního řádku (pro vhodné p) a ta říká že $r_p | r_{p-1}$. Z předposledního řádku pak ale plyne $r_p | r_{p-2}$ a postupně dojdeme až nazpět k prvnímu a druhému řádku, které dají $r_p | g$ a $r_p | f$. Pokud $h | f$ a $h | g$, pak ze stejných rovností postupně plyne, že h dělí všechny r_i, zejména tedy r_p, tzn. získali jsme největšího společného dělitele $h = r_p$ polynomů f a g.

[5]Tzn. (i) $h|f \wedge h|g$ (ii) $k|f \wedge k|g \quad \Rightarrow \quad k|h$.

Nyní můžeme postupně dosazovat z poslední do předchozích rovnic.

$$\begin{aligned}
h = r_p &= r_{p-2} - q_p r_{p-1} \\
&= r_{p-2} - q_p(r_{p-3} - q_{p-1} r_{p-2}) \\
&= -q_p r_{p-3} + (1 + q_{p-1}) r_{p-2} \\
&= -q_p r_{p-3} + (1 + q_{p-1} q_p) r_{p-2} \\
&= -q_p r_{p-3} + (1 + q_p q_{p-1})(r_{p-4} - q_{p-2} r_{p-3}) \\
&\vdots \\
&= Af + Bg.
\end{aligned}$$

□

3.12 Lemma. *Nechť R je obor integrity s jednoznačným rozkladem a $f, g, h \in R[x]$. Předpokládejme, že f je nerozložitelné a $f|gh$. Pak buď $f|g$ nebo $f|h$.*

Důkaz: Je-li f konstantní polynom (tj. prvek v R), pak jsme tvrzení již dokázali, viz. jedno z předchozích lemmat.

Předpokládejme, že $\deg f > 0$. Již víme, že f je nerozložitelný také v $K[x]$, kde K je podílové těleso okruhu R. Předpokladejme tedy nejdříve, že R je pole (a je tedy rovno svému podílovému tělesu). Předpokládejme dále, že $f|gh$ a zároveň f nedělí g. Ukážeme, že pak jistě $f|h$. Největší společný dělitel polynomů g a f musí být konstantní polynom v K, proto existují $A, B \in K[x]$ takové, že $1 = Af + Bg$. Odtud $h = Afh + Bgh$ a protože $f|gh$ musí platit i $f|h$.

Vraťme se nyní k obecnému případu. Podle předchozího vyplývá z našich předpokladů, že $f|g$ nebo $f|h$ v okruhu polynomů $K[x]$ nad podílovým tělesem K okruhu R. Nechť např. $h = kf$ v $K[x]$ a zvolme $a \in R$ tak, aby $ak \in R[x]$. Pak $ah = akf$ a pro každý nerozložitelný faktor $e \in a$ musí platit $e|ak$, protože f je nerozložitelný a nekonstantní. Můžeme proto e krátit. Po konečném počtu takových krácení je z a jednotka, tzn. $h = k'f$ pro vhodné $k' \in R[x]$. □

Důkaz tohoto lemmatu ukončil celý důkaz věty 3.7.

3.13 Kořeny polynomu. *Hodnotou polynomu* $f \in R[x]$ v bodě $a \in R$ rozumíme prvek $f(a) = a_0 + a_1 a + \cdots + a_n a^n \in R$. *Kořen* polynomu f je takový prvek $a \in R$, pro který je $f(a) = 0$. Dělením polynomem $x - b$, $b \in R$, (všimněme si, že vedoucí koeficient je jednička, tedy algoritmus pro dělení vždy funguje jednoznačně) dostaneme jednoznačně zadané polynomy q, r splňující $f = q(x-b) + r$, kde $r = 0$ nebo $\deg r = 0$, tj. $r \in R$. Tzn., že hodnota polynomu f v $b \in R$ je rovna právě $f(b) = r$. Z toho plyne, že prvek $b \in R$ je kořen polynomu f právě, když $(x-b)|f$. Tím jsme dokázali následující tvrzení:

3.14 Lemma. *Každý polynom $f \in R[x]$ má nejvýše $\deg f$ kořenů.*

3.15 Důsledek. *Nechť $f \in R[x_1, \ldots, x_r]$. Je-li $f(a_1, \ldots, a_r) = 0$ pro libovolnou volbu prvků $a_1, \ldots, a_r$ z nekonečné množiny $D \subset R$, pak $f = 0$.*

Důkaz: Provedeme indukcí přes počet proměnných. Pro polynomy v jedné proměnné tvrzení plyne okamžitě z předchozího lemmatu.

Nechť $f \in R[x_1, \ldots, x_{r-1}][x_r]$ a předpokládejme, že pro menší počet proměnných tvrzení platí. Máme $f = f_0 + f_1 x_r + \cdots + f_n x_r^n$ a $f_n \neq 0$. Proto podle předpokladu existují prvky $a_1, \ldots, a_{r-1}$ z D takové, že $f_n(a_1, \ldots, a_{r-1}) \neq 0$. Z toho ale plyne, že pouze pro konečně mnoho a_r z D může být $f(a_1, \ldots, a_r) = 0$. □

Pokud má každý nekonstantní polynom $f \in R[x]$ kořen, pak je R pole (všimněte si, že polynom $ax - 1$, $a \neq 0$, má mít kořen, tj. vždy existuje $a^{-1} \in R$). Pro každé pole to ale samozřejmě neplatí, např. polynom $x^2 + 1 \in \mathbb{R}[x]$ kořen nemá. Pole R se nazývá *algebraicky uzavřené*, jestliže má každý nekonstantní polynom kořen.

3.16 Věta (ZÁKLADNÍ VĚTA ALGEBRY). *Pole $\mathbb{C}$ je algebraicky uzavřené.*

Důkaz: Předpokládejme, že $f \in \mathbb{C}[z]$ je nenulový polynom, který nemá kořen, tj. $f(z) \neq 0$ pro všechny $z \in \mathbb{C}$. Definujme zobrazení

$$\varphi : \mathbb{C} \to \mathbb{C}, \quad z \mapsto \frac{f(z)}{|f(z)|}$$

tj. φ zobrazí celé $\mathbb{C}$ do jednotkové kružnice $K_1 = \{e^{it}, t \in \mathbb{R}\} \subset \mathbb{R}^2 = \mathbb{C}$. Díky našemu předpokladu o nenulovosti $f(z)$ je to skutečně dobře definované zobrazení. Dále definujme zobrazení s hodnotami v kružnici $K_r \subset \mathbb{C}$ se středem v nule a poloměrem $r \geq 0$

$$\psi_r : \mathbb{R} \to K_r, \quad t \mapsto \psi(t) = re^{it}.$$

Pro každé $r \in \langle 0, \infty)$ máme definováno spojité zobrazení $\kappa_r = \varphi \circ \psi_r : \mathbb{R} \to K_1$. Ze spojité závislosti κ na parametru r navíc vyplývá existence zobrazení $\alpha_r : \mathbb{R} \to \mathbb{R}$ jednoznačně zadaných podmínkami $0 \leq \alpha_r(0) < 2\pi$ a $\kappa_r(t) = e^{i\alpha_r(t)}$. Získané zobrazení α_r opět spojitě závisí na r. Celkem tedy máme spojité zobrazení

$$\alpha : \mathbb{R} \times \langle 0, \infty) \to \mathbb{R}, \quad (t, r) \mapsto \alpha_r(t)$$

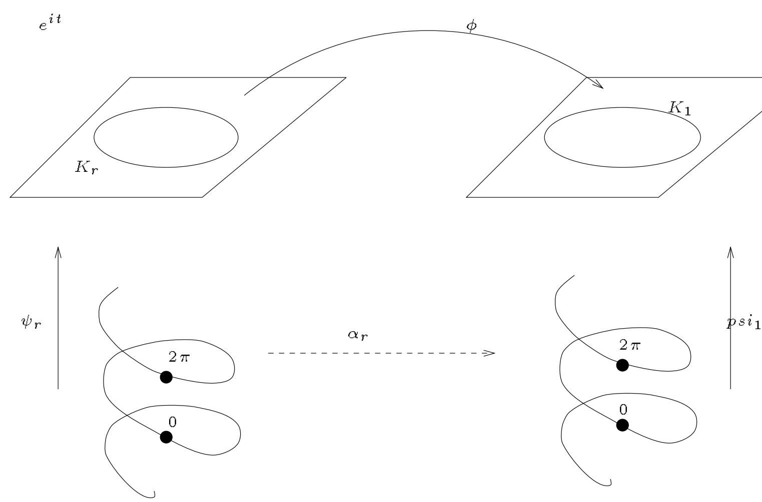
a z jeho konstrukce plyne že pro všechna r je $\frac{1}{2\pi}(\alpha_r(2\pi) - \alpha_r(0)) = n_r \in \mathbb{Z}$, viz. 10. Protože je α spojité, znamená to, že n_r je celočíselná konstanta nezávislá na r!

Pro dokončení důkazu si stačí uvědomit, že pokud $f = a_0 + \cdots + a_d z^d$ a $a_d \neq 0$, pak pro malá r se bude α_r chovat podobně jako konstantní zobrazení, zatímco pro velká r to vyjde stejně, jako kdyby $f = z^d$. Nejprve si spočtěme, jak tedy n_r dopadne při $f = z^d$, pak toto tvrzení upřesníme a důkaz tím bude ukončen.

Funkce $\mathbb{C} \to \mathbb{C}$, $z \mapsto z^d$, $z \mapsto \frac{z^d}{|z^d|}$ se snadno vyjádří pomocí goniometrického tvaru komplexních čísel $z = r(\cos\alpha + i \sin\alpha)$.

$$z^d = r^d(\cos d\alpha + i \sin d\alpha) = r^d e^{id\alpha}$$
$$\frac{z^d}{|z^d|} = 1(\cos d\alpha + i \sin d\alpha) = e^{id\alpha}$$

zobrazení φ je tedy v tomto případě pouze „zatočení“ na jednotkové kružnici. Pak tedy $\kappa_r(t) = e^{idt}$ a proto $\alpha_r(t) = dt$, nezávisle na r. Odtud pro naši volbu $f = z^d$ vyplývá $n_r = d$. Pokud zvolíme $f = az^d$, $a \neq 0$, nebude to mít na předchozí výsledek žádný vliv (přesvědčte se!).



Obr. 10: Konstrukce zobrazení α

Zvolme nyní obecný polynom $f = a_0 + \cdots + a_d z^d$, který nemá kořen. Víme tedy, že $a_0 \neq 0$ (pokud by bylo $a = 0$, existoval by kořen). Pro $z \neq 0$ platí

$$\frac{f(z)}{a_d z^d} = 1 + \frac{1}{a_d}(a_0 z^{-d} + \cdots + a_{d-1} z^{-1})$$

a proto $\lim_{|z|\to\infty} \frac{f(z)}{a_d z^d} = 1$. Když tohle víme, můžeme spočítat

$$\lim_{|z|\to\infty} \left| \frac{f(z)}{|f(z)|} - \frac{a_d z^d}{|a_d z^d|} \right| = \lim_{|z|\to\infty} \left| \frac{f(z)}{a_d z^d} \frac{a_d z^d}{|a_d z^d|} \frac{|a_d z^d|}{|f_(z)|} - \frac{a_d z^d}{|a_d z^d|} \right| = 0.$$

Proto $n_r = d$ pro velká r.

Podobnou úvahu uděláme i pro malá r. Připomeňme si, že $a_0 \neq 0$.

$$\frac{f(z)}{a_0} = 1 + \frac{1}{a_0}(a_1 z + \cdots + a_d z^d)$$

proto $\lim_{|z|\to 0} \frac{f(z)}{a_0} = 1$. Přitom opět platí $\frac{f(z)}{|f(z)|} = \frac{f(z)}{a_0} \frac{a_0}{|a_0|} \frac{|a_0|}{|f(z)|}$. Odtud $\lim_{|z|\to 0} \frac{f(z)}{|f(z)|} = \lim_{|z|\to 0} \frac{a_0}{|a_0|}$, tj. $n_r = 0$ pro malá r. Celkem vidíme, že stupeň našeho polynomu je $d = 0$.

□

3.17 Definice (Algebraická definice derivace). Nechť R je obor integrity s jednoznačným rozkladem, $f = a_0 + a_1 x \cdots + a_n x^n \in R[x]$. *Derivaci f' polynomu f* definujeme vztahem

$$f' = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

Derivace f' polynomu $f \in R[x_1, \ldots, x_r]$ podle proměnné x_i se definuje jako derivace polynomu $f \in R[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_r][x_i]$. Hovoříme o *parciální derivaci* polynomu f a značíme ji $\frac{\partial}{\partial x_i} f$. Zřejmě je opět $\frac{\partial}{\partial x_i} f \in R[x_1, \ldots, x_r]$. Derivace vyšších řádů definujeme indukcí, tj. $\frac{\partial^k}{\partial x_{i_1} \ldots \partial x_{i_k}} f = \frac{\partial}{\partial x_{i_k}} (\frac{\partial^{k-1}}{\partial x_{i_1} \ldots \partial x_{i_{k-1}}} f)$.

3.18 Lemma. *Nechť R je obor integrity s jednoznačným rozkladem a $f, g \in R[x]$.*

1. $(f+g)' = f' + g'$
2. *je-li $a \in R$, pak $a' = 0$ a $(af)' = af'$*
3. $(fg)' = f'g + g'f$, $(f^k)' = k(f^{k-1})f'$
4. *pro $f \in R[x_1, \dots, x_r]$ a $g_1, \dots, g_r \in R[x]$ je derivace složené funkce $g(x) = f(g_1(x), \dots, g_r(x)) \in R[x]$ rovna*

$$g'(x) = \sum_{i=1}^{r} \left(\frac{\partial}{\partial x_i} f\right) \Big(g_1(x), \dots, g_r(x)\Big) g_i'(x).$$

Důkaz: Tvrzení 1. a 2. jsou zřejmá přímo z definice derivace.

3. Zvolme dva polynomy $f = a_0 + \dots + a_n x^n$, $g = b_0 + \dots + b_m x^m$ v $R[x]$ a počítejme

$$\begin{aligned}
(fg) &= \sum_{j=0}^{n+m} \left(\sum_{i=0}^{j} (a_i b_{j-1}) \right) x^j \\
(fg)' &= \sum_{j=0}^{n+m} j \left(\sum_{i=0}^{j} a_i b_{j-1} \right) x^{j-1} = \sum_{j=0}^{n+m-1} (j+1) \left(\sum_{i=0}^{j+1} a_i b_{j-i+1} \right) x^j \\
f'g + g'f &= \sum_{j=0}^{m+n-1} \left(\sum_{i=0}^{j} (i+1) a_{i+1} b_{j-i} \right) x^j + \sum_{j=0}^{m+n-1} \left(\sum_{i=0}^{j} (j-i+1) a_i b_{j-i+1} \right) x^j \\
&= \sum_{j=0}^{m+n-1} \left(\sum_{i=0}^{j} (i+1) a_{i+1} b_{j-i} + (j-i+1) a_i b_{j-i+1} \right) x^j
\end{aligned}$$

a přímým srovnáním se ověří, že výsledné sumy dávají tentýž výsledek.[6] Zbytek tvrzení se odvodí snadno indukcí.

4. Víme, že derivace součtu je součet derivací, proto nám stačí dokázat tvrzení pro polynomy tvaru $x^\alpha = x_1^{\alpha_1} \dots x_r^{\alpha_r}$ (obecný případ pak plyne z 1. a 2.). To znamená, že $g(x) = (g_1(x))^{\alpha_1} \dots (g_r(x))^{\alpha_r}$, ale pak 3. poskytuje právě požadované tvrzení. □

3.19 Věta. *Nechť R je obor integrity s jednoznačným rozkladem a s charakteristikou*[7] *větší než 2. Nechť $g \in R[x]$ je nerozložitelný a nekonstantní. Pak $g^2 | f$ právě, když $g | f$ a zároveň $g | f'$.*

Důkaz: Předpokládejme $g|f$, tj. $f = gh$ (definice dělitelnosti). Pak $f' = g'h + gh'$. Pokud navíc $g|f'$, pak také $g|g'h$. Protože je g nerozložitelný, dělí buď h nebo g', ale g' má menší stupeň než g, takže $g|h$. Proto platí $g^2|f$.

Naopak, je-li $g^2|f$, tj. $f = g^2 h$, je $f' = 2gg'h + g^2 h'$. Odtud plyne, že $g|f'$. □

---

[6] Důkaz lze vést také např. matematickou indukcí přes stupeň polynomů, nebo pomocí distributivity a úvah o monomech.

[7] Např. $R = \mathbb{R}[x_1, \dots, x_r]$, $R = \mathbb{C}[x_1, \dots, x_r]$ apod.

3.20 Důsledek. *Za předpokladů předchozí věty, prvek $a \in R$ je vícenásobný kořen polynomu f právě, když polynom $(x-a)$ dělí f i f'.*

3.21 Věta (Taylorova věta pro polynomy jedné proměnné). *Pro každý polynom $f \in R[x]$ stupně n a každé prvky $a, b \in R$ platí*

$$f(b) = f(a) + f'(a)(b-a) + \cdots + \frac{1}{n!} f^{(n)}(a)(b-a)^n.$$

Důkaz: Po dosazení prvku $x+a$ do polynomu f dostaneme roznásobením polynomiální výraz $g(x) = f(x+a) = a_0 + a_1 x + \cdots + a_n x^n$. Iterované derivování nyní dá

$$\begin{aligned} g^{'}(x) &= a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \\ g^{''}(x) &= 2a_2 + 2.3 a_3 x + \cdots + n(n-1) a_n x_{n-2} \\ &\vdots \\ g^{(n)} &= n! a_n \end{aligned}$$

a další derivace je již nulová. Dosazením $x = 0$ dostaneme

$$f(a) = a_0, f'(a) = a_1, \ldots, f^{(n)}(a) = n! a_n.$$

Vyčíslením $g(b-a)$ získáme právě požadovaný vztah. □

3.22 Věta (Taylorova věta pro polynomy více proměnných). *Pro každý polynom $f \in R[x_1, \ldots, x_r]$ s celkovým stupněm n a pro libovolné prvky $a_1, \ldots, a_r, b_1, \ldots, b_r \in R$ platí*

$$\begin{aligned} f(b_1, \ldots, b_r) = f(a_1, \ldots, a_r) &+ \sum_{i=1}^{r} \frac{\partial}{\partial x_i} f(a_1, \ldots, a_r)(b_i - a_i) + \ldots \\ &+ \frac{1}{n!} \sum_{|\alpha|=n} \left(\frac{\partial^{\alpha_1}}{\partial x_1^{\alpha_1}} \cdots \frac{\partial^{\alpha_r}}{\partial x_r^{\alpha_r}} f \right) (a_1, \ldots, a_r)(b_1 - a_1)^{\alpha_1} \ldots (b_r - a_r)^{\alpha_r}. \end{aligned}$$

Důkaz: Uvažme polynom $F(t) = f(a_1 + (b_1 - a_1)t, \ldots, a_r + (b_r - a_r)t)$ pro $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_r)$ pevné, tj. $F \in R[t]$. Podle již dokázané Taylorovy věty platí

$$\begin{aligned} F(t) &= F(0) + F'(0)t + \cdots + F^n(0)t^n \\ &= f(a_1, \ldots, a_r) + (\sum_{i=1}^{r} (a_1, \ldots, a_r)(b_i - a_i))t + \ldots \\ &\quad + \frac{1}{n!} \sum_{|\alpha|=n} \frac{\partial^\alpha}{\partial x^\alpha} f(a_1, \ldots, a_n)(b-a)^\alpha t^n. \end{aligned}$$

Pro $t = 1$ dostáváme právě tvrzení věty. □

4 Afinní variety

4.1 Definice. *Afinní varieta* $V \subset \mathbb{K}^n$ zadaná množinou polynomů $S = \{f_1, \dots, f_s\} \subset \mathbb{K}[x_1, \dots, x_n]$ je množina všech bodů $x \in \mathbb{K}^n$ takových, že $f(x) = 0$. Píšeme $V = \mathcal{V}(f_1, \dots, f_s) = \mathcal{V}(S)$. Množinu všech polynomů $g \in \mathbb{K}[x_1, \dots, x_n]$ splňujících $g(x) = 0$ pro všechny $x \in V$, nazýváme *ideál variety* V, značíme $\mathcal{I}(V)$.

Varieta $V \subset \mathbb{K}^n$ se nazývá *nerozložitelná* (ireducibilní) jestliže neexistují dvě vlastní podvariety V_1, V_2, $V_1 \neq V, V_2 \neq V$, takové, že $V = V_1 \cup V_2$. V opačném případě říkáme, že varieta V je *rozložitelná*.

4.2 Věta. *Pro afinní variety* $V, W \subset \mathbb{K}^n$, $V = \mathcal{V}(f_1, \dots, f_k), W = \mathcal{V}(g_1, \dots, g_l)$ *platí*

1. $\mathcal{I}(V)$ *je ideál v* $\mathbb{K}[x_1, \dots, x_n]$.
2. $\mathcal{I}((\mathcal{V}(S)) \supseteq \langle S \rangle$, *kde* $\langle S \rangle$ *označuje ideál generovaný množinou* S, *tj. nejmenší ideál obsahující* S.
3. $V \subseteq W$ *právě, když* $\mathcal{I}(V) \supseteq \mathcal{I}(W)$
4. $V \cup W = \mathcal{V}(\{f_i g_j; i = 1, \dots, k; j = 1, \dots, l\})$
5. $V \cap W = \mathcal{V}(f_1, \dots, f_k, g_1, \dots, g_l)$.

Důkaz: (1): $\mathcal{I}(V)$ je ideál, jestliže je tato množina uzavřena vzhledem ke sčítání plynomů a pro všechny $g \in \mathbb{K}[x_1, \dots, x_n]$ a pro všechny $f \in \mathcal{I}(V)$ je také $gf \in \mathcal{I}(V)$. Skutečně $f(x) = 0$ zaručuje $(gf)(x) = g(x)f(x) = 0$ a také uzavřenost vůči sčítání je zřejmá.

(2): prvky $\langle f_1, \dots, f_n \rangle$ jsou tvaru $h = h_1 f_1 + \dots + h_s f_s$, kde $h_i \in \mathbb{K}[x_1, \dots, x_n]$, proto se jistě nulují ve všech bodech variety $\mathcal{V}(S)$.

(3): „$\Rightarrow$“ Vezmeme $x \in V$, $f \in \mathcal{I}(W)$. Protože $V \subseteq W$ a tudíž $x \in W$, je $f(x) = 0$ a tedy $f \in \mathcal{I}(V)$.

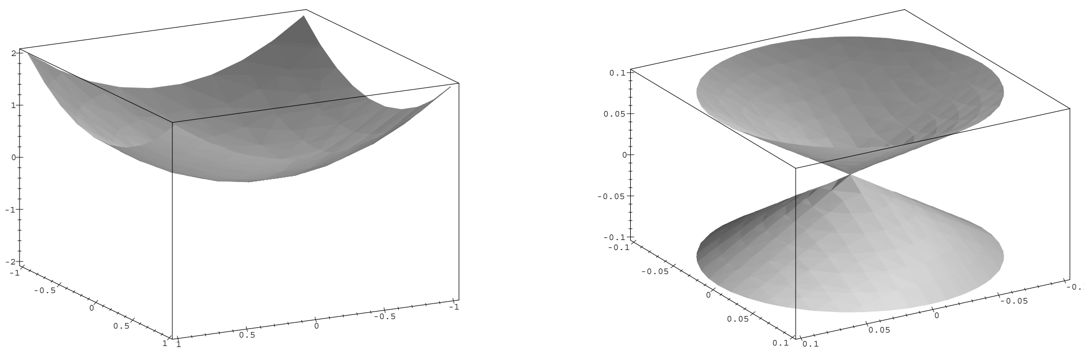
„$\Leftarrow$“ Nechť $x \in V$ (a chceme dokázat $x \in W$). Nechť $W = \mathcal{V}(f_1, \dots, f_n)$ (takové f_i jistě existují podle definice), pak také $f_i \in \mathcal{I}(W) \subseteq \mathcal{I}(V)$ a tudíž $f_i(x) = 0$, tj. $x \in W$.

(4): „$\subseteq$“ Zvolme si $x \in V$, tzn. $f_i(x) = 0$ pro všechny i. Tedy pro všechny i, j je $f_i g_j(x) = 0$. Stejně pro $x \in W$.

„$\supseteq$“ Předpokládejme, že $x \notin V \cup W$. Pak existuje i_0 takové, že $f_i(x) \neq 0$ a zároveň existuje j_0 tak že $g_{j_0}(x) \neq 0$. Proto $f_{i_0} g_{j_0}(x) \neq 0$ a tedy $x \notin \mathcal{V}(f_i g_j)$.

(5): $x \in V \cap W$ právě, když všechny f_i i g_j se v x nulují a to je právě, když $x \in \mathcal{V}(f_1, \dots, f_k, g_1, \dots, g_l)$. $\square$

4.3 Nadplochy v $\mathbb{K}^n$. *Nadplochou* v $\mathbb{K}^n$ rozumíme varietu $V = \mathcal{V}(f)$ zadanou jedním polynomem $f \in \mathbb{K}[x_1, \dots, x_n]$. Tzn. ideál $\langle f \rangle$ generující V je hlavní ideál. Sjednocení nadploch $V = \mathcal{V}(f_1) \cup \dots \cup \mathcal{V}(f_k)$ je opět nadplocha, $V = \mathcal{V}(f_1 \dots f_k)$. Podle věty 3.7 lze naopak každý polynom $f \in \mathbb{K}[x_1, \dots, x_n]$ rozložit na součin $f = a f_1^{l_1} \dots f_k^{l_k}$ nerozložitelných polynomů $f_1, \dots, f_k \in \mathbb{K}[x_1, \dots, x_n]$, $a \in \mathbb{K}$, a podle předchozí věty je $\mathcal{V}(f)$ sjednocením nerozložitelných nadploch $\mathcal{V}(f_i)$. Přitom původní varieta je také dána $V = \mathcal{V}(f_1 \dots f_k)$ pro polynom $g = f_1 \dots f_k$ obecně nižšího stupně, v jehož rozkladu se již nevyskytují exponenty různé od jedničky. Říkáme, že nadplocha $\mathcal{V}(f_1 \dots f_k)$ je dána *redukovanou rovnicí* $g = 0$.



Obr. 11: paraboloid s (redukovanou) rovnicí $f = x^2 + y^2 - z$ a kuželová plocha daná $f = x^2 + y^2 - z^2$ se singulárním bodem v počátku

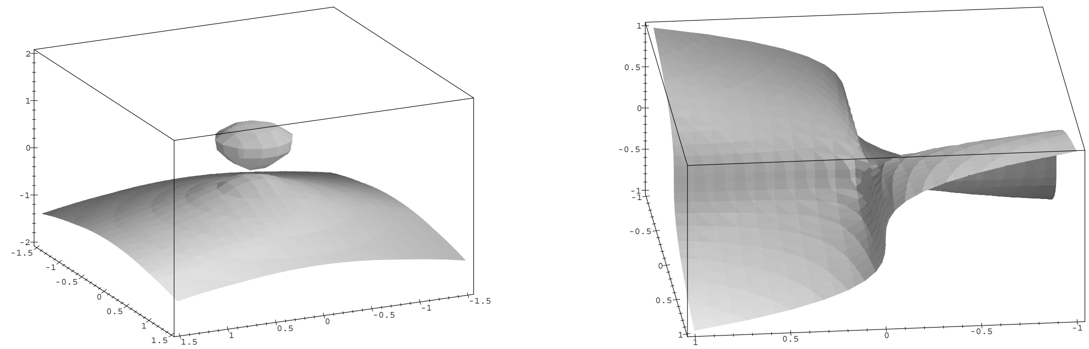
4.4 Příklady nadploch. Řadu příkladů nadploch v $\mathbb{R}^2$, tj. algebraických křivek v rovině, jsme již diskutovali v úvodní motivační kapitole. Na serii obrázků 11 – 13 můžeme shlédnout několik příkladů nadploch v $\mathbb{R}^3$, tj. obvyklých algebraických ploch.

Všimněme si, že paraboloid nemá žádné singulární body, zatímco kuželová plocha jeden singulární bod má. Velmi zajímavá je singularita variety zadané polynomem $xy + z^3$, prozkoumejte její řezy různými rovinami. Poslední dvě variety dávají nahlédnout další možnosti singularit, první je analogie bodu vratu u křivek, v druhé máme celou přímku singulárních bodů. Ve všech uvedených příkladech tvoří množiny singulárních bodů opět variety, které působí dojmem menší dimenze. To není náhoda, uvidíme, že je tomu tak vždy.

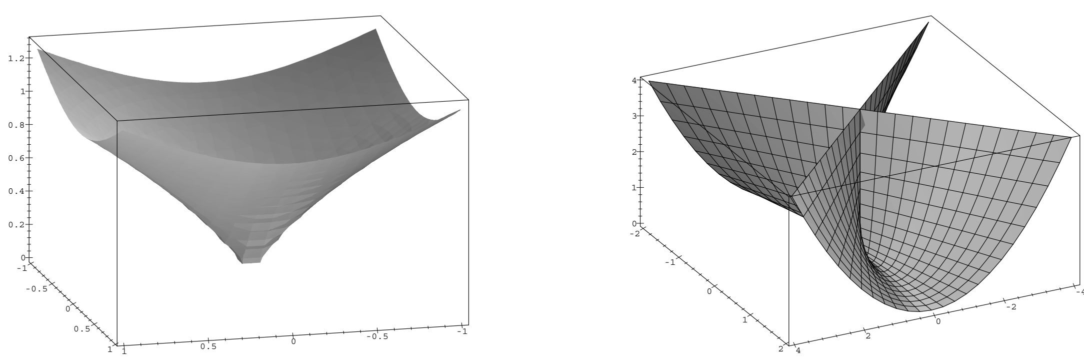
Ve všech našich příkladech jsou také variety zadány redukovanými rovnicemi. To je vidět např. z toho, že singularity můžeme opravdu spočíst jako společné nulové body všech parciálních derivací. Kdyby totiž některý z faktorů vystupoval ve vyšší mocnině, tj. mohli bychom psát $f = g^2 h$, pak by všechny parciální derivace ve všech bodech komponenty příslušné faktoru g byly nulové. Je tedy vidět, že i u nadploch nemůžeme vybírat generující polynomy jakkoliv. Z teorie kuželoseček a kvadrik patrně víte, že technicky se (pro potřeby klasifikací) může hodit také počítat komponenty variety s násobnostmi danými právě exponenty v příslušném rozkladu. Např. možnost jediné přímky odpovídá dvojnásobné komponentě kuželosečky.

Pro ideál generovaný obecnou varietou $\mathcal{I}(\mathcal{V}(f_1, \dots, f_s)) \supseteq \langle f_1, \dots, f_s \rangle$, a to i v případě nadplochy, tzn. při $s = 1$, může tedy být inkluze ostrá. Nejjednodušší příklad je $\langle x^2 \rangle \neq \langle x \rangle$, přičemž ideál generovaný $\mathcal{V}(x^2)$ je právě $\langle x \rangle$. Pro obecnější variety budeme proto potřebovat další vhodné algebraické pojmy.

4.5 Definice. Nechť R je libovolný okruh a $I \subset R$ je ideál. Říkáme, že ideál I je
vlastní , jestliže $I \neq R$ a $I \neq \{0\}$
maximální, jestliže neexistuje vlastní ideál I' takový, že $I \neq I'$ a $I \subset I' \subset R$.
konečně generovaný, jestliže existují $f_1, \dots, f_s \in R$ takové, že $I = \langle f_1, \dots, f_s \rangle$.



Obr. 12: variety zadané polynomy $f = x^2 + y^2 - z^2 + z^3$ a $f = xy + z^3$, první má singularitu v nule, řezy druhé rovinami $x = \pm y$ dávají Neilovu parabolu



Obr. 13: první zadaná $f = x^2 + y^2 - z^3$ a tzv. Whitneyho deštník $f = x^2 - y^2 z$

hlavní ideál , je-li $I = \langle f \rangle$.
prvoideál , jestliže z $f \notin I$ a $g \notin I$ vyplývá $fg \notin I$.
radikálový , jestliže z $f^k \in I$ pro jisté $k \geq 1$ plyne $f \in I$.
okruh R nazýváme *noetherovský*, je-li každý jeho ideál konečně generovaný.

4.6 Poznámka. Každý okruh s jedničkou je konečně generovaný. Pole nemá nevlastní ideály, zejména je tedy každé pole je noetherovské. Pojem prvoideálu zobecňuje vlastnosti prvočísel v $\mathbb{Z}$, radikálové ideály jsou takové, které obsahují i všechny odmocniny svých prvků (odtud název).

4.7 Věta (HILBERTOVA VĚTA O BÁZI). *Je-li R noetherovský okruh, pak také okruh polynomů $R[x]$ je noetherovský.*

Tuto větu nebudeme nyní dokazovat.[8]

4.8 Důsledek. *Je-li R noetherovský, pak*

1. *$R[x_1, \dots, x_n]$ je také noetherovský.*
2. *Okruhy R je noetherovský právě, když každá neklesající posloupnost $I_1 \subset I_2 \subset I_3 \subset \dots$ ideálů v R se stabilizuje (tj. pro jisté $N \in \mathbb{N}$ platí $I_N = I_{N+1} = I_{N+2} = \dots$.)*
3. *Variety $V \subset \mathbb{K}^n$ jsou právě množiny všech bodů v $\mathbb{K}^n$, ve kterých se nulují všechny polynomy některého ideálu $I \subset R[x_1, \dots, x_n]$, tj. $V = \mathcal{V}(I)$.*

Důkaz: 1. Plyne okamžitě indukcí přes počet proměnných z Hilbertovy věty.

2. Sjednocení všech ideálů I_k je opět ideál a ten musí být konečně generovaný podle Hilbertovy věty. Všechny generátory pak ovšem leží v některém I_N, tj. každá taková posloupnost ideálů se zastaví. Naopak, pro každý ideál $I \subset \mathbb{K}[x_1, \dots, x_n]$ je možné vytvořit posloupnost $I_1 \subset I_2 \subset \dots \subset I$ generovanou postupně více a více generátory z I. Předpokládáme-li platnost podmínky „neklesajících řetězců", pak jistě dojde při vhodné volbě k rovnosti $I = I_N$, tj. dostáváme Hilbertovu větu.

3. Naše definice variety používala jen prvky konečně generovaných ideálů, takové jsou však všechny. □

4.9 Poznámka. Přiřazení, které varietě V přiřadí $\mathcal{I}(V)$, tj. ideál asociovaný s V, je mimořádně důležité, protože tento ideál nejen zadává varietu V, ale zároveň nijak nezáleží na našich volbách generátorů. Proto vše co spočteme pomocí algebraických manipulací s tímto ideálem opravdu popisuje geometrické vlastnosti variety V. Zejména tedy $V = \mathcal{V}(\mathcal{I}(V))$ a z 4.2 plyne, že $V = W$ právě, když $\mathcal{I}(V) = \mathcal{I}(W)$.

Další podstatný pokrok v algoritmizaci studia variet spočívá v zavedení jistých kanonických bazí pro ideály $\mathcal{I}(V)$. Takové objekty nejenže existují, ale dokonce jsou k dispozici efektivní algoritmy na jejich konstrukci. Jedná se tzv. Gr̋obnerovy báze polynomiálních ideálů. Touto problematikou se zde nebudeme podrobněji zabývat, budeme však tyto báze používat, aniž bychom se o to zasloužili, při výpočtech v softwarových systémech pro algebraické manipulace, zejména v systému Maple V. Zájemce odkazuji na moje přednášky Geometrické algoritmy, II, jejichž texty jsou dostupné v lokální síti.

[8] Elementární důkaz založený na dělení polynomů se zbytkem lze nalézt v mých přednáškách "Geometrické algoritmy, II", na stejném WWW-serveru jako tyto přednášky.

4.10 Lemma (Slabá věta o nulách). *Nechť pole $\mathbb{K}$ je algebraicky uzavřené, $I \subset \mathbb{K}[x_1, \dots, x_n]$ je ideál. Pak $\mathcal{V}(I) = \emptyset$ právě, když $I = \mathbb{K}[x_1, \dots, x_n]$.*

Všimněme si, že ve speciálním případě polynomů v jedné proměnné, $I \subset \mathbb{K}[x]$, $I = \langle f \rangle$, lemma říká, že pokud f není invertibilní prvek okruhu polynomů, pak f má kořen. V polynomech o jedné proměnné je každý ideál hlavní ideál, tj. všechny ideály jsou tohoto tvaru. Můžeme tedy Slabou větu o nulách považovat za velmi silné zobecnění Základní věty algebry. *Důkaz:* Jeden směr implikace je triviální: Je-li $I = \mathbb{K}[x_1, \dots, x_n]$ pak $1 \in I$, tj. $\mathcal{V}(I) = \emptyset$ (podle definice – v žádném bodě není nulový konstantní polynom 1). Opačný směr vyžaduje další technické úvahy, opět odkazuji na svoje texty Geometrické algoritmy, II. □

4.11 Věta (Hilbertova věta o nulách). *Nechť $\mathbb{K}$ je algebraicky uzavřené pole, $S \subset \mathbb{K}[x_1, \dots, x_n]$ je libovolný ideál. Pak $\mathcal{I}(\mathcal{V}(S))$ je radikálový ideál $\sqrt{S}$ ideálu S. Tzn. polynom f splňuje $f(a) = 0$ pro všechny $a \in \mathcal{V}(S)$ právě, když $f^m \in S$ pro vhodné m. Je-li $S = \langle f_1, \dots, f_s \rangle$, pak to znamená, že $f^m = h_1 f_1 + \cdots + h_s f_s$ pro vhodné polynomy h.*

Důkaz: Ve skutečnosti se jedná o tvrzení ekvivalentní předchozímu lemmatu. Uvažme $g \in \mathcal{I}(\mathcal{V}(S))$, tj. g se nuluje ve všech bodech variety $\mathcal{V}(S)$, a předpokládejme $S = \langle f_1, \dots, f_s \rangle$. Definujeme

$$\tilde{S} = \langle f_1, \dots, f_s, 1 - yg \rangle \subset \mathbb{K}[x_1, \dots, x_n, y].$$

Z předpokladů plyne $\mathcal{V}(\tilde{S}) = \emptyset$. Skutečně, pro bod $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$ píšme $a := (a_1, \dots, a_n)$ a je buď $f_1(a) = \cdots = f_s(a) = 0$, a tedy i $g(a) = 0$, a proto $1 - a_{n+1} g(a) = 1 \neq 0$, nebo je $1 - a_{n+1} g(a) = 0$. Pak ale není $a \in \mathcal{V}(S)$, nutně je proto nějaký z polynomů $f_1, \dots, f_s$ v a nenulový. Podle Slabé věty o nulách je nyní $\tilde{S} = \mathbb{K}[x_1, \dots, x_n, y]$, což znamená, že $1 \in \tilde{S}$. Odtud

$$1 = h_1 f - 1 + \cdots + h_s f_s + h_{s+1}(1 - yg).$$

Nyní v podílovém tělese $\mathbb{K}(x_1, \dots, x_n, y)$ můžeme dosadit $y = \frac{1}{g}$, tj.

$$1 = h_1(x_1, \dots, x_n, \frac{1}{g}) f_1(x_1, \dots, x_n) + \cdots + h_s(x_1, \dots, x_n, \frac{1}{g}) f_s(x_1, \dots, x_n) + 0.$$

Vynásobením vhodnou mocninou g získáme rovnost v $\mathbb{K}[x_1, \dots, x_m]$ tvaru

$$g^m = h'_1 f_1 + \cdots + h'_s f_s.$$

□

4.12 Důsledek. *Pro algebraicky uzavřená pole je korespondence $V \leftrightarrow \mathcal{I}(V)$ bijekce mezi varietami a radikálovými ideály.*

Důkaz: Víme že $\mathcal{I}(\mathcal{V}(S))$ je vždy radikálový ideál a podle Hilbertovy věty o nulách je to ten nejmenší, který obsahuje S. Navíc $V = W$ právě, když $\mathcal{I}(V) = \mathcal{I}(W)$. □

4.13 Důsledek. *Polynom $f \in \mathbb{C}[x_1, \dots, x_n]$ nemá ve svém rozkladu na nerozložitelné polynomy faktory s mocninou vyšší než 1 právě, když $\langle f \rangle$ je radikálový. Zejména pak pro $g \in \mathcal{I}(\mathcal{V}(f))$ je $g = fh$ pro vhodné h.*

Důkaz: Předpokládejme $f = g^2h$ a g je nerozložitelné. Pak $g^2h^2 = fh \in \langle f \rangle$, tj. i $(gh)^2 \in \langle f \rangle$. Polynom gh do tohoto idálu jistě nepatří, protože gh nelze napsat jako násobek f. Proto $\langle f \rangle$ není radikálový ideál. Tím jsme dokázali, že pokud $\langle f \rangle$ je radikálový, pak f neobsahuje kvadráty.

Předpokládejme naopak, že $f = f_1 \dots f_r$ je rozklad na nerozložitelné a všechny f_i, $i = 1, \dots, r$, jsou různé polynomy stupně alespoň 1. Nechť $g^m \in \langle f \rangle$, tj. $g^m = fh$ pro vhodné h. Nechť $g = g_1 \dots g_k$, $h = h_1, \dots, h_s$ jsou rozklady na nerozložitelné faktory. Tedy $g^m = g_1^m g_2^m \dots g_k^m = f_1 \dots f_r h_1 \dots h_s$. Všechny $f_1, \dots, f_r$ jsou různé, proto musí být i mezi $g_1, \dots, g_k$. Nechť jsou to $g_1, \dots, g_r$, tzn.

$$g^m = f^m g_{r+1}^m \dots g_k^m = fh_1 \dots h_s.$$

Zejména $f^{m-1} g_{r+1}^m \dots g_k^m = h_1 \dots h_s$. Potom $g_{r+1}, \dots, g_k$ jsou mezi $h_1, \dots, h_s$ a odtud (nechť jsou to opět ty první)

$$g = g_1 \dots g_r g_{r+1} \dots g_k = f_1 \dots f_r h_1 \dots h_{k-r} = fh'.$$

Tím jsme dokázali, že radikálový ideál $\sqrt{\langle f \rangle} = \langle f \rangle$. Druhá polovina tvrzení plyne z Hilbertovi věty o nulách. □

4.14 Věta. *Varieta $V = \mathcal{V}(S)$ je nerozložitelná právě, když $\mathcal{I}(V)$ je prvoideál.*

Důkaz: „$\Rightarrow$“ Předpokládejme, že $f, g \notin \mathcal{I}(V)$ a $fg \in \mathcal{I}(V)$ pro dva nekonstantní polynomy f, g. Množiny $W_1 = \mathcal{V}(f) \cap V$ a $W_2 = \mathcal{V}(g) \cap V$ jsou opět variety. Ukážeme, že tyto variety jsou vlastní podvariety. Existuje $b \in V$ s vlastností $f(b) \neq 0$, odtud $b \notin \mathcal{V}(f)$ a proto $W_1 \neq V$. Je to tedy vlastní podvarieta. Podobně $W_2 \neq V$. Přitom ale pro $a \in V$ je $f(a)g(a) = 0$, tj. buď $a \in W_1$, nebo $a \in W_2$. Odtud plyne, že $V = W_1 \cup W_2$ je rozložitelná varieta.

„$\Leftarrow$“ Předpokládejme, že V je rozložitelná, tj. $V = W_1 \cup W_2$, kde $W_1 \subseteq V$, $W_2 \subseteq V$, $W_1 \neq V$, $W_2 \neq V$ jsou vlastní podvariety. Odtud plyne, že $\mathcal{I}(W_1) \supset \mathcal{I}(V)$ a $\mathcal{I}(W_2) \supset \mathcal{I}(V)$ jsou ostře větší ideály. Proto existují polynomy f, g takové, že $f \notin \mathcal{I}(V)$, $f \in \mathcal{I}(W_1)$ a $g \notin \mathcal{I}(V)$, $g \in \mathcal{I}(W_2)$. Přitom platí $fg \in \mathcal{I}(W_1 \cup W_2) = \mathcal{I}(V)$, tzn. $\mathcal{I}(V)$ není prvoideál. □

4.15 Věta. *Každá varieta $V \subseteq \mathbb{K}^n$ je sjednocením takových nerozložitelných variet $V_1, \dots, V_k$, že neplatí $V_i \subset V_j$ pro jakákoliv různá i, j a variety $V_1, \dots, V_k$ jsou určeny jednoznačně, až na pořadí.*

Důkaz: Nejprve sporem ukážeme, že existuje nějaký rozklad. Předpokládejme tedy, že pro danou varietu V neexistuje žádný rozklad požadovaných vlastností. Pak nutně $V = V_1 \cup V_2$ pro dvě vlastní podvariety (jinak by se jednalo o rozklad s jediným objektem). Dále alespoň jedna z nich se dá opět rozložit, píšeme $V_1 = V_{11} \cup V_{12}$ nebo $V_2 = V_{21} \cup V_{22}$. Induktivně můžeme pokračovat dále a tento proces se nikdy nezastaví (jinak bychom měli požadovaný rozklad). Tzn., že jsme získali posloupnost

$$V = W_0 \supseteq W_1 \supseteq W_2 \supseteq \dots \supseteq W_k \supseteq \dots$$

kde všechny inkluze jsou ostré. Pro příslušné asociované ideály tím dostaneme neklesající posloupnost

$$\mathcal{I}(V) = \mathcal{I}(W_0) \subset \mathcal{I}(W_1) \subset \dots \subset \mathcal{I}(W_k) \subset \dots$$

která se nikdy nestabilizuje, ale to je spor s tvrzením Hilbertovy věty o bázi. Proto při předchozí konstrukci postupných rozkladů nutně dojdeme do stavu, kdy všechny variety V_{ij} budou nerozložitelné a pokud je některá z nich obsažena v jiné, prostě ji vynecháme.

Nyní jednoznačnost. Předpokládejme, že $V = W_1 \cup \dots \cup W_l = V_1 \cup \dots \cup V_k$ jsou dva takové rozklady. Chceme dokázat, že jsou až na pořadí stejné. Platí $W_1 = (W_1 \cap V_1) \cup (W_1 \cap \cup_{i=2}^k V_i)$. Proto, pokud W_1 není pod V_1, je $W_1 \subset \cup_{i=2}^k V_i$, protože je W_1 nerozložitelné. Podobně, pokud W_1 není obsaženo v $V_1 \cup \dots \cup V_s$, pak $W_1 \subset \cup_{i=s+1}^k V_i$. Celkem tedy vidíme, že vždy existuje nějaké j takové, že $W_1 \subset V_j$. Podobně pro všechny ostatní $W_2, \dots, W_k$ a také naopak pro inkluze $V_i \subset W_j$. Celkem jsme tedy ověřili, že $V_i \subset W_{k_i} \subset V_{j_i}$. To je ale možné jen pro $V_{j_i} = V_i$, tj. $V_i \subset W_{k_i} \subset V_i$, a všude musí nastat rovnost, tedy $V_i = W_{k_i} = V_i$. Stejně pro komponenty W_j. □

4.16 Poznámka. Každý prvoideál I je radikálový ideál. Je-li totiž $g^m \in I$, pak buď g^{m-1} nebo g je v I, tj. po konečně mnoha krocích ověříme $g \in I$. Proto je $\mathcal{V}(S)$ nerozložitelná varieta, kdykoliv je S prvoideál v algebraicky uzavřeném $\mathbb{K}$.

4.17 Příklad.

1. $V = \mathcal{V}(y - x^2, z - x^3) \subset \mathbb{C}^3$ je tzv. tvistovaná kubika. Ukážeme, že ideál $S = \langle y - x^2, z - x^3 \rangle$ je prvoideál. Definujme homomorfismus okruhů φ předpisem

$$\varphi : \mathbb{C}[x, y, z] \to \mathbb{C}[t], x \mapsto t, y \mapsto t^2, z \mapsto t^3.$$

Nyní, je-li $\varphi(fg) = \varphi(f)\varphi(g) = 0$, pak buď $\varphi(f)$, nebo $\varphi(g)$ je nulový polynom. Stačí tedy ukázat, že S je jádro homomorfismu φ. Pak totiž bude platit, že při $fg \in S$ je $\varphi(fg) = 0$ a proto buď $\varphi(f)$ nebo $\varphi(g)$ je 0 v $\mathbb{C}[t]$, tzn. buď f nebo g patří do S. Každé $f \in S$ lze vyjádřit jako $f = h_1(y - x^2) + h_2(z - x^3)$, proto $\varphi(f) = 0$. Odtud $S \subset \ker \varphi$. Z tvaru generátorů S plyne, že každý polynom $h \in \mathbb{C}[x, y, x]$ lze vyjádřit ve tvaru

$$h = h_1(y - x^2) + h_2(z - x^3) + r, \ r \in \mathbb{C}[x].$$

Odtud již vyplývá, že $\ker \varphi = S$ a je tedy S prvoideál. Zejména je tvistovaná kubika nerozložitelná.

2. Pro plochy v $\mathbb{C}^3$ a křivky v $\mathbb{C}^2$ je situace jednodušší. Jsou zadané polynomem $f = f_1^{k_1} \dots f_r^{k_r} = 0$ a $\langle f \rangle$ je prvoideál právě, když rozklad má jen jeden faktor v první mocnině. Přitom jsme již dokázali, že $\langle f \rangle = \sqrt{\langle f \rangle}$ právě, když f je redukovaná rovnice nadplochy.

3. Uvažme další křivku v $\mathbb{C}^3$ zadanou ideálem $S = \langle y^2 - xz, z^2 - y^3 \rangle$. Zdá se, že stejná varieta by měla být zadaná také ideálem $\langle y^2 - xz, z^2 - xyz \rangle$. Snadný výpočet ukazuje, že dokonce i tyto ideály jsou si rovny:

$$\begin{aligned} z^2 - xyz &= (z^2 - y^3) + y(y^2 - xz) \\ z^2 - y^3 &= (z^2 - xyz) - y(y^2 - xz) \end{aligned}$$

Je tedy $\mathcal{V}(S) = \mathcal{V}(y^2 - x^2, z(z - xy)$. Snadná úvaha nyní dává, že ve skutečnosti je $\mathcal{V}(S) = \mathcal{V}(y^2 - xz, z) \cup \mathcal{V}(y^2 - xz, z - xy)$.

První z komponent, $V_1 = \mathcal{V}(y^2 - xz, z) = \mathcal{V}(y^2, z) = \mathcal{V}(y, z)$, je nerozložitelná varieta, protože $\langle y, z\rangle$ obsahuje právě polynomy v $\mathbb{C}[x][y, z]$ bez absolutních členů a v součinu fg bez absolutních členů musí jistě mít tuto vlastnost buď f nebo g, je to tedy jistě prvoideál. Je vidět, že jde o všechny body na ose x.

Druhá komponenta je $V_2 = \mathcal{V}(y^2 - xz, z - xy)$. Všimněme si, že $y^2 - xz = (y^2 - x^2y) - x(z - xy)$, tzn. $V_2 = \mathcal{V}(y(y - x^2), z - xy) = \mathcal{V}(y, z - xy) \cup \mathcal{V}(y - x^2, z - xy)$. První z těchto komponent už nemusíme znovu uvažovat, zbývá $V_2' = \mathcal{V}(y - x^2, z - xy)$ což je varieta z prvního příkladu. (Je totiž $z - x^3 = (z - xy) + x(y - x^2)$.) Celkem jsme získali rozklad uvažované variety na dvě komponenty, tvistovanou kubiku V' a body na ose x. Všimněme si, že osa x se přitom v našem rozkladu vyskytuje „dvakrát“.

4.18 Definice. Pro libovolný polynom $f \in \mathbb{K}[x_1, \dots, x_n]$ definujeme jeho *lineární část* v bodě $p = (p_1, \dots, p_n) \in \mathbb{K}^n$ jako polynom

$$D_p^1 f = \frac{\partial f}{\partial x^1}(p)(x_1 - p_1) + \dots + \frac{\partial f}{\partial x^n}(p)(x_n - p_n).$$

Tečný prostor k varietě V v bodě $p \in V$ je varieta $T_pV = \mathcal{V}(\langle D_p^1 f; f \in \mathcal{I}(V)\rangle)$.

4.19 Věta.

1. *Tečný prostor k varietě V v libovolném bodě $p \in V \subset \mathbb{K}^n$ je afinní podprostor v $\mathbb{K}^n$.*
2. *Je-li $\mathcal{I}(V) = \langle f_1, \dots, f_s\rangle$, pak $T_pV = \mathcal{V}(D_p^1 f_1, \dots, D_p^1 f_s)$.*

Důkaz: Stačí dokázat pouze druhé tvrzení, protože pak je vidět, že T_pV je množina všech řešení systému lineárních rovnic.

Spočtěme $D_p^1(hf)$ pro součin. Podle definice to je

$$\frac{\partial (hf)}{\partial x_1}(p)(x_1 - p_1) + \dots = (\frac{\partial h}{\partial x_1}(p)f(p) + h(p)\frac{\partial f}{\partial x_1}(p))(x_1 - p_1) + \dots$$

Protože p je bod variety, pro každý polynom $h = h_1 f_1 + \dots + h_s f_s \in \mathcal{I}(V)$ dostaneme $D_p^1 h = h_1(p) D_p^1 f_1 + \dots + h_s(p) D_p^1 f_s$. Pro libovolný polynom h v asociovaném ideálu je tedy $D_p^1(h)$ lineární kombinací $D_p^1(f_1), \dots D_p^1(f_s)$. Proto $D_p^1 h \in \langle D_p^1 f_1, \dots, D_p^1 f_s\rangle$ a věta je dokázaná. □

4.20 Věta. *Nechť L je přímka v $\mathbb{K}^n$ zadaná parametricky, $L : p + tv$, a $V \subset \mathbb{K}^n$ varieta. Pak $L \subset T_pV$, $p \in V$, právě, když pro každé $f \in \mathcal{I}(V)$ je hodnota $t = 0$ kořenem polynomu $f(p + tv) \in \mathbb{K}[t]$ s násobností alespoň 2.*

Důkaz: Označme $g(t) = f(p + tv) \in \mathbb{K}[t]$. Skalár $t = 0$ je kořen s násobností alespoň 2 právě, když je i kořenem derivace $g'(t)$. Spočteme

$$g'(0) = \frac{\partial f}{\partial x^1}(p)v_1 + \frac{\partial f}{\partial x^2}(p)v_2 + \dots + \frac{\partial}{\partial x^n}(p)v_n = D_p^1 f(p + v)$$

kde $v = (v_1, \dots, v_n)$. Odtud plyne, že $g'(0) = 0$ právě, když $v \in T_pV$. To nastane právě, když $L \subset T_pV$. □

4.21 Důsledek. *Pro nadplochu $V \subset \mathbb{K}^n$ s redukovanou rovnicí $V = \mathcal{V}(f)$ je $T_pV = \mathcal{V}(D_p^1 f)$. Přitom, je-li $f = f_1 \dots f_r$ rozklad na nerozložitelné faktory a $V_i = \mathcal{V}(f_i)$ jsou příslušné komponenty, pak pro $v \in V_i$ je $\dim T_pV = n - 1$ právě, když $D_p^1 f_i \neq 0$ a $\dim T_pV_i = n$ v opačném případě. Dále, $\dim T_pV = \dim T_pV_i$ právě, když $p \notin V_i \cap V_j$ pro nějaká $i \neq j$.*

4.22 Příklad. Uvažme polynom $f = (x^2 + y^2 - 1)(x - 1)$, tj. $\mathcal{V}(f)$ je sjednocení jednotkové kružnice a její tečny v bodě $p = (1, 0)$. Ideál $I = \langle f \rangle$ je radikálový, protože f je redukované. Platí

$$D_p^1 f = (2x^2 - 2x + x^2 + y^2 - 1) \mid_{(1,0)} (x - 1) + (2y(x - 1) \mid_{(1,0)} (y) = 0 + 0.$$

V tomto bodě tedy bude každá jím procházející přímka v T_pV. Ve všech ostatní budou tečné prostory jednorozměrné (tečny k příslušným křivkám).

4.23 Definice. Pro nerozložitelnou varietu V definujeme její *dimenzi* vztahem

$$\dim V = \min\{\dim T_pV, p \in V\}.$$

Obecně, pro varietu V a bod $p \in V$ definujeme *dimenzi V v bodě p*,

$$\dim_p V = \max\{\text{dimenze komponent do nichž } p \text{ patří}\}.$$

Dimenze variety V je pak maximum dimenzí v bodech $p \in V$. Body ve kterých je $\dim V = \dim T_pV$ jsou *regulární* , ostatní nazýváme *singulární*.

Zaveďme nyní přesně pojem parametricky zadané variety.

4.24 Definice. *Racionální parametrickou reprezentací* variety $\mathcal{V}(f_1, \dots, f_r) \subseteq \mathbb{K}^n$ rozumíme racionální funkce $r_1, \dots, r_n \in k(t_1, \dots, t_s)$ splňující následující podmínky

- Je-li $x_i = r_i(t_1, \dots, t_n)$ pro $i = 1, 2, \dots, n$, pak $(x_1, \dots, x_n) \in \mathcal{V}(f_1, \dots, f_r)$ pro libovolná $t_1, \dots, t_s$.
- $\mathcal{V}(f_1, \dots, f_r)$ je minimální afinní varieta obsahující takto dané body $(x_1, \dots, x_n)$.

Pokud jsou všechny r_i polynomy v $\mathbb{K}[t_1, \dots, t_s]$, pak hovoříme o *polynomiální parametrizaci.*

4.25 Věta. *Nechť $V \subseteq \mathbb{K}^n$ je afinní varieta zadaná parametricky ve tvaru $x_1 = g_1(t_1, \dots, t_m), \dots, x_n = g_n(t_1, \dots, t_m)$, kde $g_i \in \mathbb{K}(t_1, \dots, t_m)$. Pak V je nerozložitelná.*

Důkaz: Provedeme nejprve důkaz pro polynomiální parametrizace, tj. $g_i \in \mathbb{K}[t_1, \dots, t_m]$, kdy je celkem snadný.

Uvažme zobrazení $\varphi : \mathbb{K}^m \to \mathbb{K}^n$, $(t_1, \dots, t_m) \mapsto (g_1(t_1, \dots, t_m), \dots, g_n(t_1, \dots, t_m))$. Pak $\mathcal{I}(V) = \mathcal{I}(\varphi(\mathbb{K}^n))$. Je tedy $f \in \mathcal{I}(V)$ právě, když $f \circ \varphi = 0$ jako polynom v $\mathbb{K}[t_1, \dots, t_m]$. Chceme ukázat, že asociovaný ideál je prvoideál, předpokládejme tedy, že $fh \in \mathcal{I}(V)$. Pak $(fh) \circ \varphi = (f \circ \varphi) \cdot (h \circ \varphi) = 0$, jako polynom v $\mathbb{K}[t_1, \dots, t_m]$. Proto buď $f \circ \varphi$ nebo $h \circ \varphi$ je nula.

Obecný případ vyžaduje o trochu složitější postup. Nechť $h_1, \dots, h_n$ jsou jmenovatelé racionálních funkcí z parametrizace a předpokládejme, že nejsou všechny konstantní.

Označme $W = \mathcal{V}(h_1, \dots, h_n)$ varietu nulových bodů alespoň jednoho polynomu h_i. Nyní můžeme definovat $\varphi : \mathbb{K}^m \setminus W \to \mathbb{K}^n$, $\varphi(t_1, \dots, t_m) = (g_1(t_1, \dots, t_m), \dots)$ a opět platí $\mathcal{I}(V) = \mathcal{I}(\varphi(\mathbb{K}^m \setminus W))$. Uvažme $fh \in \mathcal{I}(V)$, tj. $(f \circ \varphi) \cdot (h \circ \varphi) = 0$, kde poslední rovnost chápeme v podílovém tělese. Jeden z nich musí tedy být nulový prvek podílového tělesa.

Nechť $f \circ \varphi = 0$, tj. $f(\frac{r_1}{h_1}, \dots, \frac{r_n}{h_n}) = 0$ na $\mathbb{K}^m \setminus W$. Tzn. do obyčejného polynomu dosazujeme podíly nějakých polynomů. Existuje přitom k takové, že součin $(h_1 \dots h_n)^k (f \circ \varphi)$ je již obyčejný polynom v $\mathbb{K}[t_1, \dots, t_m]$. Pak ovšem také $(h_1 \dots h_n)^k (f \circ \varphi) = 0$ v $\mathbb{K}[t_1, \dots, t_n]$ a hodnoty tohoto polynomu na $\mathbb{K}^m \setminus W$, což je otevřená podmnožina, jsou nulové. Proto je tento polynom identicky nulový všude, je proto identicky nulové i $f \circ \varphi$ a to jsme potřebovali ukázat. $\square$

4.26 Příklad.

1. Uvažme varietu zadanou parametricky

$$x = t(u^2 - t^2), \quad y = u, \quad z = u^2 - t^2$$

Jde o varietu vyobrazenou na titulní straně textů. Přesvědčit se o tom můžeme eliminací proměnných t, u z rovnic.

$$x = tz, z = y^2 - t^2$$
$$x^2 = t^2 z^2 = (y^2 - z) z^2 = y^2 z^2 - z^3$$

Dostali jsme tedy skutečně varietu $\mathcal{V}(x^2 - y^2 z^2 + z^3)$. Podle předchozí věty je nerozložitelná. Tečné prostory k této varietě jsme počítali již v úvodní kapitole.

2. Tvistovaná kubika je dána $\mathcal{V}(y - x^2, z - x^2)$ a její parametrizace je vidět okamžitě: $x = t$, $y = t^2$, $z = t^3$. Znovu jsme tedy ukázali, že $\langle y - x^2, z - x^3 \rangle$ je pvoideál, tentokrát daleko jednodušeji. Každý prvoidál je radikálový, proto pro tečné prostory dostáváme

$$T_p V = \mathcal{V}(D_p^1(y - x^2), D_p^1(z - x^3)).$$

Označíme-li $p = (p_x, p_y, p_z)$, dostaneme

$$T_p V = \mathcal{V}(-2p_x(x - p_x) + (y - p_y), -3p_x^2(x - p_x) + (z - p_z)).$$

Např. pro $p = (1, 1, 1)$ je tečný prostor přímka $\mathcal{V}(-2(x-1) + (y-1), -3(x-1) + (z-1))$.

3. Varieta $\mathcal{V}(x^2 - y^2 z)$ je zadána parametricky

$$x = uv, \quad y = v, \quad z = u^2$$

je tedy nerozložitelná. Pro libovolný bod tvaru $p = (0, 0, \alpha)$ je tečný prostor $T_p V = \mathcal{V}(0) = \mathbb{K}^3$. Jsou tedy všechny body na ose z singulární.

Bez důkazu uvedeme obecnou větu o rozkladu variet na komponenty. Pro speciální případ nadploch je ale důkaz již snadný, zkuste si sami!

4.27 Věta. *Nechť $V \subset \mathbb{K}^n$ je afinní varieta a označme $\Sigma = \{p \in V;\ p \text{ je singulární bod}\}$*

1. Σ je afinní varieta obsažená ve V.

2. *Pro $p \in \Sigma$ je $\dim(T_pV) > \dim_p V$.*
3. *Σ neobsahuje žádnou nerozložitelnou komponentu V.*
4. *Jsou-li V_i, V_j různé nerozložitelné komponenty V, pak $V_i \cap V_j \subseteq \Sigma$.*

4.28 Poznámka. Každou s-tici polynomů $(f_1, \ldots, f_s)$ můžeme chápat jako zobrazení $\varphi = (f_1, \ldots, f_s) : \mathbb{K}^n \to \mathbb{K}^s$. Vlastnosti tohoto zobrazení ve společném nulovém bodě $p \in \mathbb{K}^n$ jistě budou vypovídat i něco o chování variety $\mathcal{V}(f_1, \ldots, f_s)$ v okolí bodu p. Z analýzy je známo, že „lineární část chování“ je zachycena tzv. Jacobiho maticí

$$J(f_1, \ldots, f_s)(p) = \begin{pmatrix} \frac{\partial}{\partial x_1} f_1 & \cdots & \frac{\partial}{\partial x_n} f_1 \\ \vdots & \vdots & \vdots \\ \frac{\partial}{\partial x_1} f_s & \cdots & \frac{\partial}{\partial x_n} f_s \end{pmatrix} (p)$$

Determinant této matice se nazývá Jacobián příslušného zobrazení v bodě p. Hodnost $J(f_1, \ldots, f_s)(p) \leq \min(n, s)$. Předpokládejme, že hodnost je rovna s, zejména je tedy $s \leq n$. Pak (jak je známo z analýzy) je varieta $\mathcal{V}(f_1, \ldots, f_s) = \varphi^{-1}(0)$ lokálně grafem jistého zobrazení $\mathbb{K}^{n-s} \to \mathbb{K}^n$ (tzv. věta o implicitní funkci). Zejména tedy v tomto případě jistě bude bod p regulárním bodem variety.

Samozřejmě, naopak tvrzení neplatí. Např. $f = (x^2 - y)^2$ zadává parabolu, všechny body jsou regulární, Jacobiho matice ale bude pro všechny bdy na parabole nulová.

4.29 Definice. Uvažme polynom $f \in \mathbb{K}[x_1, \ldots, x_n]$ stupně d a bod $p \in \mathbb{K}^n$. Taylorův rozvoj f v bodě p dává

$$f(x) = f(p) + D_p^1 f(x-p) + \cdots + \frac{1}{k!} D_p^k f(x-p) + \cdots + \frac{1}{d!} D_p^d f(x-p)$$

kde $D_p^k f = \sum_{|\alpha|=k} \frac{\partial^{|\alpha|} f}{\partial x^\alpha}(p)(x-p)^\alpha$, viz. tzv. multiindexovou symboliku zavedenou v 3.2. Homogenní polynom $D_p^k f$, který je buď stupně k nebo nulový, nazýváme k-lineární část f v bodě p. Definujeme $D_p^{min} f$ jako první nenulovou homomgenní část f v p. Pro každý nenulový polynom f je jeho první nenulová část dobře definovaná v každém bodě $p \in \mathbb{K}^n$, pro body mimo $\mathcal{V}(f)$ je to konstanta $f(p)$.

Tečný kužel variety $V = \mathcal{V}(f_1, \ldots, f_s)$ v bodě $p \in V$ definujeme vztahem

$$C_p(V) = \mathcal{V}(D_p^{min} f; f \in \mathcal{I}(V)).$$

Tečný kužel je podle definice průnik variet $\cap_{f \in \mathcal{I}(V)} \mathcal{V}(D_p^{min} f)$.

4.30 Věta. *Nechť $V = \mathcal{V}(f)$ je nadplocha a $\mathcal{I}(V) = \langle g \rangle$. Pak $C_p(V) = \mathcal{V}(D_p^{min} g)$. Je-li $\mathbb{K} = \mathbb{C}$, pak navíc také $C_p(V) = \mathcal{V}(D_p^{min} f)$.*

Důkaz: Polynomy z $\mathcal{I}(V) = \langle g \rangle$ jsou násobky g. Spočítáme pro libovolný polynom h minimální nenulovou část $D_p^{min}(hg)$. Dostaneme

$$\begin{aligned} D_p^k(hg) &= \sum_{|\alpha|=k} \frac{\partial^{|\alpha|}}{\partial x^\alpha}(hg)(p)(x-p)^\alpha \\ &= \sum_{|\alpha|=k} \Big(\sum_{\beta+\gamma=\alpha} (\frac{\partial^{|\beta|}}{\partial x^\beta} h)(\frac{\partial^{|\gamma|}}{\partial x^\gamma} g)(p) \Big)(x-p)^\alpha \end{aligned}$$

Označme minimální stupně k' pro g, k'' pro g. Je-li $k < k' + k''$, pak buď $\frac{\partial^{|\beta|}}{\partial x^\beta}h$ nebo $\frac{\partial^{|\gamma|}}{\partial x^\gamma}g$ je nulové. Proto dostaneme minimální nenulovou část pro $k = k' + k''$, tzn.

$$\begin{aligned} D_p^{min}(hg) &= (\sum_{|\beta|=k'}(\frac{\partial^{|\beta|}}{\partial x^\beta}h)(p)(x-p)^\beta)\cdot(\sum_{|\gamma|=k''}(\frac{\partial^{|\gamma|}}{\partial x^\gamma}g)(p)(x-p)^\gamma) \\ &= (D_p^{min}h)(D_p^{min}g) \end{aligned}$$

Odtud plyne, že pro $hg \in \mathcal{I}(V)$ je $\mathcal{V}(D_p^{min}(hg)) \supseteq \mathcal{V}(D_p^{min}g)$.

Předpokládejme navíc, že $\mathbb{K} = \mathbb{C}$. Spočteme, že ideály $\langle f\rangle$ a $\mathcal{I}(V)$ budou dávat tentýž kužel (ale s násobností). Máme $h \in \mathcal{I}(V)$ právě, když $h^m \in \langle f\rangle$ pro vhodné m. Podle předchozího výpočtu je $D_p^{min}(h^m) = (D_p^{min}h)^m$ a proto $\mathcal{V}(D_p^{min}h) = \mathcal{V}(D_p^{min}h^m) \supseteq \mathcal{V}(D_p f)$ plyne z předchozí části důkazu. □

4.31 Příklad. Pro variety větších kodimenzí je bohužel situace daleko složitější. Vezměme křivku $V = \mathcal{V}(xy, xz + z(y^2 - z^2)) \subseteq \mathbb{C}^3$. Lze spočítat, že $\langle xy, xz + z(y^2 - z^2)\rangle$ je radikálový ideál. Mohli bychom doufat, že $C_0(V) = \mathcal{V}(xz, xz)$, uvidíme však, že to není pravda. Uvažme $f = y(xz + z(y^2 - z^2)) - z(xy) = zy(y^2 - z^2) \in \mathcal{I}(V)$. Polynom $D_f^{min} = zy(y^2 - z^2)$ není nulový v bodech roviny $x = 0$, která je celá obsažena v $\mathcal{V}(xz, xz)$! Tečný kužel proto musí ve skutečnosti být daleko menší.

Následující věta říká, že tečný kužel v libovolném bodě je vyplněn právě všemi limitními stavy sečen tímto bodem procházejících. O sečnách L_k procházejících bodem p přitom řekneme, že konvergují k přímce $L : p + tv$, jestliže existují směrové vektory v_k, $v_k \to v$, takové, že $L_k = p + tv_k$).

4.32 Věta. *Nechť V je afinní varieta v $\mathbb{C}^n$. Přímka $L : p+tv$ leží celá v C_pV právě když existuje posloupnost bodů $q_k \in V, q_k \neq p$ konvergujících k p takových, že $L_k : p+t(q_kp)$ konverguje k L.*

Důkaz: Napřed ukážeme, že pro body $q_k \in V$, $q_k \to p$, konvergují sečny k přímce v C_pV. Zvolíme $p = 0$ (bez újmy na obecnosti můžeme provést posunutí do počátku). Předpokládejme, že $L_k : p + t(q_k - p) = tq_k$ konverguje k přímce $L : p + tv = tv$. Tzn. existuje $v_k \to v, q_k = t_kv_k$. Zjevně $t_k \to 0$. Nechť $f \in \mathcal{I}(V)$, tj. $f \equiv 0$ na V. Dále nechť k je minimální číslo takové, že $D_0^k f \neq 0$. Tzn. $f = D_0^k f + \cdots + D_0^d f$, kde d je stupeň f. Nyní

$$\begin{aligned} 0 &= f(t_lv_l) = t_l^k D_0^k f(v_l) + t_l^{k+1} D_0^{k+1} f(v_l) + \cdots + t_l^d D_0^d f(v_l) \\ 0 &= D_0^k f(v_l) + t_l D_0^{k+1} f(v_l) + \ldots \end{aligned}$$

Limitním přechodem $l \to \infty$, tj. $t_l \to 0$, dostaneme $D_0^k f(v) = 0$. To ale znamená, že přímka L je obsažena v tečném kuželi C_0V, což jsme chtěli dokázat.

Opačný směr je nepříjemnější. V podstatě se jedná o diskuzi, jaká je nejmenší varieta obsahující všechny limity sečen. Provádí se v $\mathbb{C}[t, x_1, \ldots, x_n]$. Detaily vynecháme. □

4.33 Věta. *Nechť $p \in V \subset \mathbb{C}^n$. Pak $\dim_p V = \dim C_pV$.*

Důkaz: Pro nadplochy plyne z definice, obecný důkaz vynecháme □

4.34 Důsledek. *Nechť $p \in V \subset \mathbb{C}^n$. Následující podmínky jsou ekvivalentní.*

1. *p je regulární bod*
2. *$\dim \mathbb{C}_p(V) = \dim T_pV$*
3. *$C_pV = T_pV$*

5 Projektivní variety

Připomeňme, že projektivní prostor $\mathbb{P}_n(\mathbb{K})$ je množina jednorozměrných podprostorů $(a_0 : a_1 : \cdots : a_n)$ v $\mathbb{K}^{n+1}$.

5.1 Definice. *Homogenní polynom stupně k* v $\mathbb{K}[x_0, \ldots, x_n]$ je takový polynom, jehož všechny monomy mají stupeň k. Tj. $f = \sum_{|\alpha|=k} c_\alpha x^\alpha$. Každý $f \in \mathbb{K}[x_0, \ldots, x_n]$ je jednoznačně vyjádřen jako součet homogenních komponent $f = \sum_{i=1}^k f_{(i)}$, kde $f_{(i)}$ je homogenní polynom stupně i, $i = 0, \ldots, k$.

Ideál $I \subset \mathbb{K}[x_0, \ldots, x_n]$ je *homogenní*, jestliže pro každý polynom $f \in I$ jsou i všechny jeho homogenní komponenty v I.

5.2 Lemma. *Nechť $f \in \mathbb{K}[x_0, \ldots, x_n]$ je libovolný polynom a $f(x) = 0$ pro všechny homogenní souřadnice $x = (x_0 : x_1 : \cdots : x_n)$ jistého bodu $p \in \mathbb{P}_n(\mathbb{K})$. Pak všechny homogenní komponenty polynomu f splňují $f_{(i)}(x) = 0$.*

Důkaz: Nechť je $f = \sum_{i=0}^k f_{(i)}$. Platí $f_{(i)}(\lambda x) = \lambda^i f(x)$. Je-li $f(\lambda x) = 0$ pro všechny hodnoty λ, pak $0 = f(\lambda x) = \sum_{i=0}^k f_{(i)}(x)\lambda^i$ je identicky nulový polynom, musí tedy mít nulové všechny koeficienty. Právě to jsme měli dokázat. □

5.3 Poznámka. Pro množinu $S \subset \mathbb{P}_n(\mathbb{K})$ definujeme

$$\mathcal{I}(S) = \{f \in \mathbb{K}[x_0, \ldots, x_n], f(x) = 0 \text{ pro všechny homogenní souřadnice bodů v } S\}$$

Zjevně je $\mathcal{I}(S)$ ideál a z předchozího lemmatu plyne, že $\mathcal{I}(S)$ je homogenní ideál. Nabízí se definovat „nejmenší varietu“ obsahující S jako množinu všech bodů v $\mathbb{P}_n(\mathbb{K})$, jejichž homogenní souřadnice jsou nenulovými body všech $f \in \mathcal{I}(S)$. Následující věta ukazuje, že homogenní ideály jsou generovány konečně mnoha homgenními polynomy. To nám umožní použít explicitnější definici.

5.4 Věta. *Ideál $I \subset \mathbb{K}[x_0, \ldots, x_n]$ je homogenní ideál, právě když existují homogenní polynomy $f_1, \ldots, f_s \in \mathbb{K}[x_0, \ldots, x_n]$ takové, že $I = \langle f_1, \ldots, f_s \rangle$.*

Důkaz: Uvažme dva polynomy $f = \sum_{i=0}^k f_{(i)}$, $g = \sum_{j=0}^l g_{(j)}$. Pak

$$(f+g) = \sum_{q=0}^{\max(k,l)} (f_{(q)} + g_{(q)})$$

$$(fg) = \sum_{q=0}^{k+l} (\sum_{i+j=q} f_{(i)} g_{(i)})$$

Z Hilbertovy věty o bázi plyne, že $I = \langle f_1, \ldots, f_s \rangle$ pro vhodné generátory $f_i = \sum_j f_{i(j)}$. Protože I je homogenní ideál, jsou $f_{i(j)} \in I$ (z definice). Dále f_i leží v ideálu generovaném $f_{i(j)}$, tzn. $I = \langle f_{i(j)} \rangle$.

Předpokládejme naopak, že $I = \langle f_1, \dots, f_s \rangle$ s homogenními polynomy $f_i \in I$. Nechť $f = h_1 f_1 + \dots + h_s f_s$ a nechť $f = \sum_{j=0}^{k} f_{(j)}$. Pak $f_{(k)}$ se vyjádří jako součet (některých) nejvyšších homogenních komponent $h_i f_i$. Ty jsou ale součiny f_i s nejvyššími komponentami h_i. Odtud $f_{(k)} \in I$. Nyní $f - f_{(k)} \in I$ a nejvyšší homogenní komponenta $f - f_{(k)}$ opět leží v I. Po konečném počtu kroků všechny $f_{(j)} \in I$. $\square$

5.5 Definice. *Projektivní varieta* $V \subset \mathbb{P}_n(\mathbb{K})$ je množina zadaná homogenními polynomy $f_1, \dots, f_s \in \mathbb{K}[x_0, \dots, x_n]$,

$$V = \mathcal{V}(f_1. \dots, f_s) = \{(a_0 : \dots : a_n) \in \mathbb{P}_n(\mathbb{K}) \ ; \ f_i(a_0, \dots, a_n) = 0 \ ; \ i = 1, \dots, s)\}$$

Projektivní varieta se nazývá *nerozložitelná* , jestliže ji nelze vyjádřit jako sjednocení $V = V_1 \cup V_2$ dvou projektivních variet takových , že $V_i \not\subseteq V_j$, $i \neq j$.

5.6 Věta. *Pro každé nekonečné pole* $\mathbb{K}$ *zadávají přiřazení* $V \mapsto \mathcal{I}(V)$, $I \mapsto \mathcal{V}(I)$ *korespondence*

$$\{ \text{ projektivní variety } \} \rightleftharpoons \{ \text{ homogenní ideály } \}$$

a platí $\mathcal{V}(\mathcal{I}(V)) = V$. *Zejména* $V = W$ *právě, když* $\mathcal{I}(V) = \mathcal{I}(W)$.

Důkaz: Úplně stejný jako v afinním případě. $\square$

5.7 Věta. *Každou projektivní varietu lze jednoznačně (až na pořadí) vyjádřit jako sjednocení nerozložitelných variet* $V = V_1 \cup \dots \cup V_k$, $V_i \not\subseteq V_j$ *pro všechny* $i \neq j$.

Důkaz: Stejně jako v afinním případě, získáme pro V klesající řetězec $V = V_0 \supseteq V_1 \supseteq V_2 \supseteq \dots$ projektivních variet. Odtud $\mathcal{I}(V_0) \subseteq \mathcal{I}(V_1) \subseteq \dots$ je rostoucí řetězec homogenních ideálů. Proto existuje N takové, že $\mathcal{I}(V_N) = I(V_{N+1}) = \dots$. Pro získaný rozklad se pak analogicky k afinnímu případu odvodí jednoznačnost. $\square$

5.8 Poznámka. Projektivní prostor jsme vyjádřili jako $\mathbb{P}_n(\mathbb{K}) \cong U_0 \cup \mathbb{P}_{n-1}(\mathbb{K})$, kde U_0 je afinní rovina $\mathbb{K}^n$ a o jednu dimenzi menší projektivní prostor $\mathbb{P}_{n-1}(\mathbb{K})$ hraje roli bodů v nekonečnu. Přesněji, $U_0 = \{p = (x_0 : \dots : x_n); x_0 \neq 0\}$, $p \cong (1, x_1, \dots, x_n) \cong (x_1, \dots, x_n)$, a podobně můžeme do $\mathbb{P}_n(\mathbb{K})$ vložit afinní roviny $U_i = \{p = (x_0 : \dots : x_n); x_i \neq 0\}$. Pro varietu $V \subset \mathbb{P}_n(\mathbb{K})$, $V = \mathcal{V}(f_1, \dots f_s)$, definujeme její „afinní část v U_i“ jako $V_{af} = V \cap U_i$. Rádi bychom také naopak uměli k varietě $V_{af} \subset U_0$ najít odpovídající projektivní varietu V.

5.9 Věta. *Nechť* $V = \mathcal{V}(f_1, \dots, f_s) \subset \mathbb{P}_n(\mathbb{K})$ *je projektivní varieta. Definujeme* $g_i \in \mathbb{K}[x_1, \dots, x_n]$, $g_i(x_1, \dots, x_n) = f_i(1, x_1, \dots, x_n)$, $i = 1, \dots, s$. *Pak* $V_{af} = V \cup U_0 = \mathcal{V}(g_1, \dots, g_s) \subset \mathbb{K}_n$.

Důkaz: Je-li $(1 : a_1 : \dots : a_n) \in V \cap U_0$, pak $f_i(1, a_1, \dots, a_n) = g_i(a_1, \dots, a_n) = 0$. Tím je dokázáno, že $V_{af} \subset \mathcal{V}(g_1, \dots, g_s)$. Naopak, je-li $g_i(a_1, \dots, a_n) = 0$, $i = 1, \dots, s$, pak $f_i(1, a_1, \dots, a_n) = g_i(a_1, \dots, a_n) = 0$, tj. $(1 : a_1 : \dots : a_n) \in V \cap U_0$. $\square$

5.10 Definice. Nechť $I \subset \mathbb{K}[x_1, \dots, x_n]$ je ideál. *Homogenizací ideálu* I je ideál

$$I^h = \langle f^h; f \in I \rangle \subset \mathbb{K}[x_0, \dots, x_n]$$

kde f^h je tzv. *homogenizace polynomu* $f = \sum_{i=0}^{k} f_{(i)}$, daná vztahem

$$f^h(x_0, \dots, x_h) = \sum_{i=0}^{k} f_{(i)}(x_0, \dots, x_n) x_0^{k-i} = x_0^k f(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}).$$

Projektivní rozšíření afinní variety $V = \mathcal{V}(f_1, \ldots, f_s) \subset \mathbb{K}^n \cong U_0 \subset \mathbb{P}_n(\mathbb{K})$ definujeme jako projektivní varietu $\mathcal{V}((\mathcal{I}(V))^h)$.

5.11 Věta. *Nechť V je nadplocha v $\mathbb{K}^n$ zadaná redukovanou rovnicí $f = 0$. Potom projektivním rozšířením variety V je $\mathcal{V}(f^h)$.*

Důkaz: Nadplocha V je zadána hlavním ideálem $\langle f \rangle$, který je radikálový, proto je také asociovaný ideál $I = \mathcal{I}(V) = \langle f \rangle$. Z formule pro homogenizaci polynomu ihned plyne, že homogenizace součinu dvou polynomů je součin jejich homogenizací. Pak ovšem libovolný prvek g homogenizovaného ideálu I^h je nutně opět násobkem f^h. Odtud vyplývá dokazované tvrzení. □

5.12 Příklad. Tvistovaná kubika $W = \mathcal{V}(x_2 - x_1^2, x_3 - x_1^3)$ (parametricky je zadaná $x_1 = t,\ x_2 = t^2,\ x_3 = t^3$). Homogenizací generátorů $f = x_2 - x_1^2$, $g = x_3 - x_1^2$, získáme polynomy $f^h = x_0x_2 - x_1^2$, $g^h = x_0^2x_3 - x_1^3$.

Uvažme varietu $V = \mathcal{V}(x_0x_2 - x_1^2,\ x_0^2x_3 - x_1^3)$. Její průnik s projektivní rovinou bodů v nekonečnu je $V \cap H = \mathcal{V}(x_0x_2 - x_1^2, x_0^2x_3 - x_1^3, x_0) = \mathcal{V}(x_1, x_0)$, což je celá projektivní přímka. Dá se proto tušit, že varieta V je zbytečně příliš veliká.

Skutečně, má také $V' = \mathcal{V}(x_2x_0 - x_1^2, x_0^2x_3 - x_1^3, x_1x_3 - x_2^2)$ afinní část v U_0 rovnu W. Přitom $V' \cap H = \mathcal{V}(x_2x_0 - x_1^2, x_0^2x_3 - x_1^3, x_1x_3 - x_2^2, x_0) = \mathcal{V}(x_1, x_0, x_2)$, tzn. v „nekonečnu“ přibyl jediný bod $(0 : 0 : 0 : 1)$. To odpovídá daleko lépe intuitivní představě o rozšíření křivky o body v nekonečnu.

Přitom si všimněme, že $I = \langle x_2 - x_1^2, x_3 - x_1^3 \rangle$ je prvoideál, tedy zejména radikálový ideál, stačí proto uvažovat homogenizovaný ideál I^h. To však neznamená, že stačí zhomogenizovat libovolné generátory. V našem případě jsme museli přidat polynom, který je v I, je homogenní, ale není v $\langle f^h, g^h \rangle$.

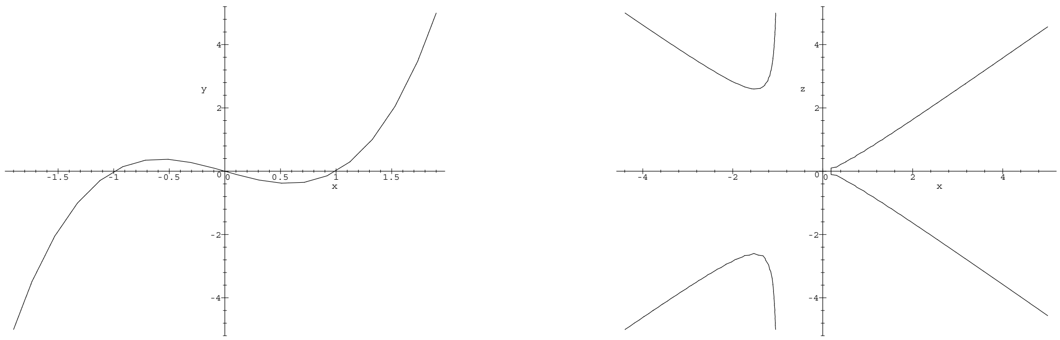
5.13 Příklad. Graf reálné funkce $y = x^3 - x$ je varieta $W = \mathcal{V}(y - x^3 + x)$ jejíž projektivní rozříšení je podle předchozí věty $V = \mathcal{V}(z^2y - x^3 + z^2x) \subset \mathbb{R}^3$. Její body v projektivní rovině H bodů v nekonečnu spočteme přidáním rovnice $z = 0$, tj. vyjde jediný bod $(0 : 1 : 0) \in H \cap V$.

Pro polynom $g = z^2y - x^3 + z^2x$ řešme soustavu rovnic

$$g = 0,\ \frac{\partial g}{\partial x} = 0,\ \frac{\partial g}{\partial y} = 0,\ \frac{\partial g}{\partial z} = 0$$

Řešením je jediný bod $(0 : 1 : 0) \in \mathbb{P}_2(\mathbb{R})$, což znamená, že nevlastní bod je jediným singulárním bodem křivky. Podívejme se jak se chová naše křivka v okolí svého jediného singulárního bodu. Stačí zvolit jiné vložení afinní roviny do projektivní roviny, např. uvažujme body s nenulovou y-ovou souřadnicí. Tzn. dosadíme $y = 1$ do g, označme nově vzniklý polynom $h = z^2 - x^3 + xz$. Původně nekonečný bod nyní přejde na bod $(0, 0)$ a snadno přepočítáme, že první derivace h jsou v tomto bodě nulové. Nemá proto smysl počítat tečnu, můžeme se ale zajímat o tečný kužel v singulárním bodě $(0, 0)$. Spočteme $D^2_{(0,0)}h = z^2$, je tedy tečným kuželem dvojnásobná tečna $z = 0$. Prohlédněte si situaci na obrázku 15.

Bez důkazu uvedu obecnou větu popisující vztah mezi původní afinní varietou a jejím projektivním rozšířením.



Obr. 14: Graf funkce $y = x^3 - x$ a chování v okolí nevlastního singulárního bodu $(0:1:0)$. Všimněte si, že tři nulové hodnoty původní funkce se ocitají na projektivní přímce nevlastních bodů, proto se křivka vpravo zdá na první pohled nesouvislá.

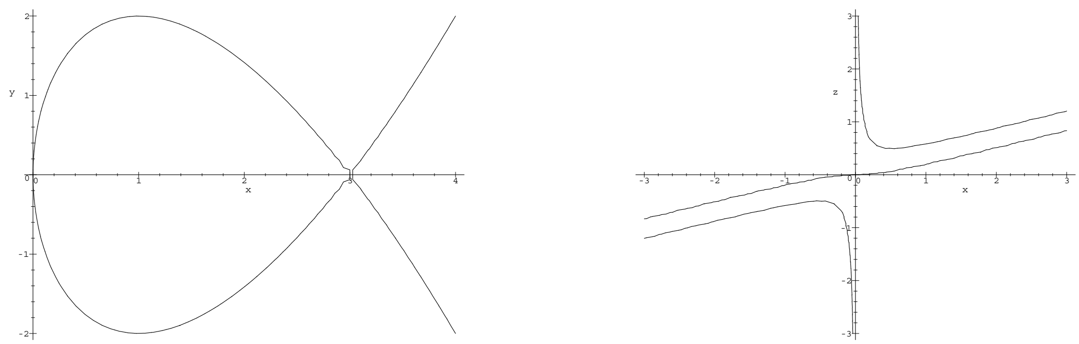
5.14 Věta. *Nechť $W \subset \mathbb{K}^n$ je afinní varieta a nechť $V = \mathcal{V}((\mathcal{I}(V))^h)$ je její projektivní rozšíření. Potom*

1. *$V_{af} = V \cap U_0 = W$*
2. *V je nejmenší afinní varieta v $\mathbb{P}_n(\mathbb{K})$ taková, že její afinní část $V_{af} = W$*
3. *Žádná komponenta projektivního rozšíření V neleží celá v projektivní nadrovině nevlastních bodů $H = \mathcal{V}(x_0)$*
4. *Je-li W nerozložitelná, potom je i V nerozložitelná.*

5.15 Poznámka. Je-li $\mathbb{K} = \mathbb{C}$ (a stejně pro libovolné algebraicky uzavřené pole), pak není třeba znát asociovaný ideál $\mathcal{I}(W)$ pro nalezení projektivního rozšíření. Je-li totiž $W = \mathcal{V}(I)$, pak přímo platí $V = \mathcal{V}(I^h)$. Důvodem je platnost Hilbertovy věty o nulách a skutečnost, že homogenizace součinu polynomů je součin jejich homogenizací.

Bohužel, pro obecná pole to neplatí. Např. $I = \langle x^2 + y^4 \rangle \subset \mathbb{R}^2$ dává $\mathcal{V}(I) = \{(0,0)\}$, ale $I^h = \langle z^2x^2 + y^4 \rangle$ zadává varietu $\{(0:0:1), (1:0:0)\}$. Přitom samozřejmě je nejmenší varieta v $\mathbb{P}_2(\mathbb{R})$ obsahující jediný bod $\{(0:0:1)\}$ zase tento jediný bod. Když přitom vezmeme celý asociovaný ideál $\langle x, y \rangle$, dostaneme správný výsledek.

5.16 Příklad. Zkoumejme křivku zadanou polynomem $f = y^2 - x^3 + 6x^2 - 9x$. Jeho homogenizace je $g = zy^2 - x^3 + 6zx^2 - 9z^2x$. Snadno spočteme, že jediný singulární bod projektivního rozšíření je bod $(3:0:1)$ s tečným kuželem $y \pm \sqrt{3}(x - \sqrt{3}z) = 0$. Dehomogenizací dosazením $y = 1$ dostaneme polynom $h = z - x^3 + 6zx^2 - 9z^2x$ a jím zadaná afinní varieta je bez singulárních bodů. všimněme si ještě, že jediný nekonečný bod projektivního rozšíření naší křivky má homogenní souřadnice $(0:1:0)$, tj. přechází na bod $(0,0) \in \mathcal{V}(h)$. Tento bod je sice regulární, tečna v něm je ale přímka $y = 0$, je to tedy právě přímka nevlastních bodů původní afinní roviny. Proto naše původní křivka $\mathcal{V}(f)$ nemá asymptoty.



Obr. 15: Ilustrace příkladu 5.16, vlevo $\mathcal{V}(y^2 - x^3 + 6x^2 - 9x)$, vpravo $\mathcal{V}(z - x^3 + 6zx^2 - 9z^2x)$

Nyní se podívejme podrobněji na nejjednodušší nadplochy. Po projektivních nadrovinách (zadaných jedním lineárním homogenním polynomem), jsou nejjednodušší tzv. kvadriky, zadané homomogenním polynomem stupně 2. Připomeňme, že dvě podmnožiny $S_1, S_2 \subset \mathbb{P}_n(\mathbb{K})$ jsou projektivně ekvivalentní, jestliže existuje kolineace φ zobrazující bijektivně S_1 na S_2.

5.17 Lemma. *Nechť $A \in \mathbb{G}L(n+1, \mathbb{K})$ je matice kolineace φ na $\mathbb{P}_n(\mathbb{K})$. Pak pro každou varietu $V = \mathcal{V}(f_1, \dots, f_s) \subset \mathbb{P}_n(\mathbb{K})$ je $\varphi(V)$ projektivně ekvivalentní varieta $\mathcal{V}(g_1, \dots, g_s)$ zadaná polynomy*

$$g_i(x_0, \dots, x_n) = f_i(b_{00}x_0 + b_{01}x_1 + \dots + b_{0n}x_n, \dots, b_{n0}x_0 + \dots + b_{nn}x_n)$$

kde $B = (b_{ij}) = A^{-1}$. Všechny g_i jsou homogenní polynomy stejných stupňů jako f_i.

Důkaz: Stačí si uvědomit, že kolineace φ působí prostřednictvím násobení homogenních souřadnic maticí A. Pro $y = \varphi(x)$ získáme hodnoty $g_i(y)$ tak, že vezmeme f_i a vyčíslíme je v $B(Ax)$, tzn. $f_i(B(Ax)) = f_i(x)$, ale to je právě když $x \in V$. $\square$

5.18 Lemma. *Všechny projektivní podprostory stejné dimenze k v $\mathbb{P}_n(\mathbb{K})$ jsou projektivně ekvivalentní.*

Důkaz: V libovolných projektivních souřadnicích je takový prostor dán $n-k$ nezávislými lineárními rovnicemi. Proto ve vhodných souřadnicích je každý k-rozměrný podprostor zadán rovnicemi $x_1 = \dots = x_{n-k} = 0$. $\square$

5.19 Definice. Nadplochy $V = \mathcal{V}(f) \subset \mathbb{P}_n(\mathbb{K})$ zadané kvadratickým homogenním polynomem se nazývají *(hyper-) kvadriky* . Kvadriky bez singulárních bodů se nazývají *regulární* , ostatní jsou *singulární* .

Každý homogenní kvadratický polynom je v homogenních souřadnicích zadán výrazem $f(x) = \sum_{i,j=0}^{n} a_{ij}x_ix_j = x^TAx$ kde $A = (a_{ij})$ je symetrická matice stupně $n+1$.

5.20 Kanonické formy. Z elementární lineární algebry víme, že ve vhodné bázi má kvadratická forma (tj. náš homogenní polynom) f diagonální matici, tj.

$$f(x) = c_0x_0^2 + c_1x_1^2 + \cdots + c_kx_k^2,\ c_i \neq 0,$$

kde číslo $k+1 \leq n+1$ se nazývá *hodnost formy* f.

Navíc při $\mathbb{K} = \mathbb{C}$ lze dosáhnout, aby všechny nenulové c_i byly rovny jedné, tj. $f(x) = x_0^2 + \cdots + x_k^2$ kde $k+1$ je hodnost formy. Je-li $\mathbb{K} = \mathbb{R}$, pak dosáhneme pouze $f(x) = x_0^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_k^2$ a číslo $0 \leq r+1 \leq k+1$ se nazývá *signatura* formy f.

Např. formy $x_2^2 - x_1x_0$ a $x_2^2 - x_1x_2 - x_0^2$, které vzniknou homogenizací rovnic pro parabolu a hyperbolu, vyjádříme postupnou změnou souřadnic takto

$$\begin{aligned} x_2^2 - x_1x_0 &= -(y_1 - y_0)(y_1 + y_0) + y_2^2 \\ &= -y_1^2 + y_0^2 + y_2^2 \\ x_2^2 - x_1x_2 - x_0^2 &= (x_2 - \frac{1}{2}x_1)^2 - \frac{1}{4}x_1^2 - x_0^2 \\ &= z_1^2 - z_2^2 - z_0^2 \end{aligned}$$

a je vidět že obě křivky jsou jistě projektivně ekvivalentní.

Hodnost a signatura zřejmě nezávisí na volbě homogenních souřadnic, můžeme proto hovořit o hodnosti a signatuře kvadrik. Protože f a $-f$ zadávají stejnou varietu, budeme pro kvadriky vždy předpokládat $k - r \leq r$.

5.21 Věta. *Kvadriky $\mathcal{V}(f)$, $\mathcal{V}(g)$ v $\mathbb{P}_n(\mathbb{K})$ jsou projektivně ekvivalentní právě, když*

- $\mathbb{K} = \mathbb{C}$ *a mají stejnou hodnost*
- $\mathbb{K} = \mathbb{R}$ *a mají stejnou hodnost i signaturu.*

Důkaz: Elementární lineární algebra □

5.22 Důsledek. *Regulární kvadriky jsou právě kvadriky hodnosti n+1 .*

5.23 Důsledek. *Všechny komplexní regulární kvadriky jsou projektivně ekvivalentní.*

5.24 Segreho zobrazení. Definujme zobrazení $\sigma : \mathbb{P}_n(\mathbb{K}) \times \mathbb{P}_m(\mathbb{K}) \to \mathbb{P}_{n+m+nm}(\mathbb{K})$ předpisem

$$((x_0, \ldots, x_n), (y_0, \ldots, y_m)) \mapsto (x_0y_0, x_0y_1, \ldots, x_0y_m, x_1y_0, \ldots, x_1y_m, \ldots, x_ny_m)$$

Použijeme-li jiné homogenní souřadnice týchž bodů, obraz se změní jen o násobek, je tedy naše zobrazení skutečně dobře definované. Ukážeme, že je prosté.

Předpokládejme $\sigma(p,q) = \sigma(p',q')$. Pak jistě existují homogenní souřadnice, pro které už definiční předpis pro σ má stejné hodnoty. Zejména je $x_0(y_0, \ldots, y_m) = x_0'(y_0', \ldots, y_m')$, tj . buď $q = q'$ nebo $x_0 = x_0' = 0$. Pokud $q \neq q'$, pak stejný argument dá postupně $x_0 = x_1 = \cdots = x_n = 0$, to je ale ve sporu s naším předpokladem, že $(x_0 : \ldots, x_n)$ jsou homogenní souřadnice bodu v $\mathbb{P}_n(\mathbb{K})$. Analogicky se dokáže i $p = p'$.

Zúžením na vnořené afinní roviny $x_0 = 0$, $y_0 = 0$ dostaneme zobrazení $\mathbb{K}^n \times \mathbb{K}^m \to \mathbb{K}^{n+m+nm}$,

$$\begin{aligned}((1 : x_1 : \dots : x_n), (1 : y_1 : \dots : y_m)) \mapsto& \\ &\mapsto ((1 : y_1 : \dots : y_m : x_1 : x_1y_1 : \dots : x_1y_m : x_2 : \dots : x_ny_m) \\ &\cong (x_1, \dots, x_n, y_1, \dots, y_m, x_1y_1, \dots, x_1y_m, \dots, x_ny_m)\end{aligned}$$

Nejjednodušší případ je $\sigma_{1,1} : \mathbb{P}_1(\mathbb{K}) \times \mathbb{P}_1(\mathbb{K}) \to \mathbb{P}_3(\mathbb{K})$.

5.25 Lemma. *Obrazem* $\operatorname{Im}\sigma_{1,1}$ *je varieta* $\mathcal{V}(z_0z_3 - z_1z_2)$.

Důkaz: Zobrazení σ je dáno vztahem $((x_0 : x_1), (y_0 : y_1)) \mapsto (x_0y_0 : x_0y_1 : x_1y_0 : x_1y_1)$, pro body $(z_0 : z_1 : z_2 : z_3)$ obrazu máme tedy rovnice

$$z_0 = x_0y_0,\ z_1 = x_0y_1,\ z_2 = x_1y_0,\ z_3 = x_1y_1$$

Jistě proto $\operatorname{Im}\sigma \subset \mathcal{V}(z_0z_3 - z_1z_2)$. Předpokládejme $(w_0 : w_1 : w_2 : w_3) \in V$. Pro určitost předpokládejme, že třeba $w_0 \neq 0$ (jinak můžeme proměnné přečíslovat). Pak $(w_0 : w_2) \in \mathbb{P}_1(K)$ a $(w_0 : w_1) \in \mathbb{P}_1(\mathbb{K})$. Nyní

$$\begin{aligned}\sigma(w_0 : w_2 : w_0 : w_1) &= (w_0^2 : w_0w_1 : w_2w_0 : w_2w_1) \\ &= (w_0^2 : w_0w_1 : w_0w_2 : w_0w_3) = (w_0 : w_1 : w_2 : w_3)\end{aligned}$$

$\square$

V závěru této kapitoly se zmíníme o speciálních konstrukcích variet vyšších dimenzí, které jsou „poskládány“ z projektivních podprostorů v jistém smyslu podobným způsobem, jako je jednodílný rotační hyperboloid vyplněn přímkami.

5.26 Přímkové plochy. Dosazením pevného bodu $p \in \mathbb{P}_1(\mathbb{K})$ dostaneme $\sigma(p, \ ) : \mathbb{P}_1(\mathbb{K}) \to \mathbb{P}_3(\mathbb{K})$, případně $\sigma(\ , p) : \mathbb{P}_1(\mathbb{K}) \to \mathbb{P}_3(\mathbb{K})$. Pro pevné $p = (a : b)$ je v prvém případě obrazem projektivní přímka procházející body $(a : 0 : b : 0)$ a $(0 : a : 0 : b)$, ve druhém případě přímka procházející $(a : b : 0 : 0)$ a $(0 : 0 : a : b)$. Obrazem σ je tedy plocha získaná sjednocením sítě přímek. Takovým plochám se říká přímkové plochy.

Celkem jsme zjistili, že regulání kvadrika $\mathcal{V}(z_0z_3 - z_1z_2)$ v $\mathbb{P}_3(\mathbb{C})$ je prostřednictvím Segreho zobrazení ztotožněna s $\mathbb{P}_1(\mathbb{K}) \times \mathbb{P}_1(\mathbb{K})$ a toto zobrazení je dáno sítí přímek. Všimněme si, že tato varieta také obsahuje body tvistované kubiky $(1 : t : t^2 : t^3)$.

Další speciální případ je $\sigma_{2,1} : \mathbb{P}_2(\mathbb{K}) \times \mathbb{P}_1(\mathbb{K}) \to \mathbb{P}_5(\mathbb{K})$. Obraz tohoto zobrazení opět vyplňuje projektivní varietu. Označme $(z_{00}, z_{01}, z_{10}, z_{11}, z_{20}, z_{21})$ souřadnice v $\mathbb{P}_5(\mathbb{K})$, tj. Segreho zobrazení má rovnice $z_{ij} = x_iy_j$. Obraz σ je varieta zadaná všemi minory stupně 2 v matici

$$\begin{pmatrix} z_{00} & z_{01} \\ z_{10} & z_{11} \\ z_{02} & z_{21} \end{pmatrix}$$

tj. $\operatorname{Im}\sigma = \mathcal{V}(z_{00}z_{11} - z_{10}z_{01}, z_{00}z_{21} - z_{20}z_{01}, z_{10}z_{21} - z_{20}z_{11})$.

Dosadíme-li $z_{00} = 1$, dostáváme afinní část této variety $\mathcal{V}(z_{11} - z_{10}z_{01}, z_{21} - z_{20}z_{01})$, protože zbylá rovnice $z_{10}z_{21} - z_{20}z_{11}$ je důsledkem předchozích. Afinní varieta zadaná rovnicemi $z_{11} = z_{10}z_{01}$, $z_{21} = z_{20}z_{21}$ je vyplněna „ sítí přímek a rovin“.

Podobně lze získat popis v obecných dimenzích.

5.27 Plűckerovy souřadnice. Z technických důvodů je vhodné, aby co nejvíce běžných objektů v algebraické geometrii mělo strukturu variety. Množina všech bodů $\mathbb{P}_n(K)$ je varieta $\mathcal{V}(0)$, nadroviny odpovídají bodům duálního projektivního prostoru. V $\mathbb{P}_3(\mathbb{K})$ tedy mezi lineárními podprostory zbývá popsat množinu všech projektivních přímek v $\mathbb{P}_3(\mathbb{K})$ jako algebraickou varietu. Každá přímka je dána dvojicí různých bodů $p = (a_0 : a_1 : a_2 : a_3)$, $q = (b_0 : b_1 : b_2 : b_3)$ v $\mathbb{P}_3(\mathbb{K})$, tj. jejich všechny homogenní souřadnice vyplňují rovinu v $\mathbb{K}^4$. Dvě volby takových bodů (p, q) a (p', q') jsou svázány lineárními závislostmi. V každém případě ale na takové volbě nebudou záviset hodnoty minorů stupně 2 v matici

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}$$

Proto daným bodům p a q přiřaďme všechny determinanty submatic řádu 2. Označme si tyto souřadnice postupně $w_{01}, w_{02}, w_{03}, w_{12}, w_{13}, w_{23}$ (tj. např $w_{01} = a_0b_1 - a_1b_0$). Získané hodnoty jsou dány libovolnými homogenními souřadnicemi bodů p, q až na násobek, máme proto dobře definovaný bod

$$w = (w_{01} : w_{02} : w_{03} : w_{12} : w_{13} : w_{23}) \in \mathbb{P}_5(\mathbb{K}).$$

5.28 Věta. *Výše popsané zobrazení $(p, q) \mapsto w$ je bijekce*

$$\{\textit{přímky v } \mathbb{P}_3(\mathbb{K})\} \to \mathcal{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12})$$

Důkaz: Uvažujme body $p = (a_0 : a_1 : a_2 : a_3)$ a $q = (b_0 : b_1 : b_2 : b_3)$ a označme $L(p, q)$ přímku jimi určenou.

$$\begin{aligned}
z_{01}z_{23} &= (a_0b_1 - b_0a_1)(a_2b_3 - b_2a_3) \\
&= a_0b_1a_2b_3 - a_0b_1b_2a_3 - b_0a_1a_2b_3 + b_0a_1b_2a_3 \\
-z_{02}z_{13} &= -(a_0b_2 - b_0a_2)(a_1b_3 - b_1a_3) \\
&= -a_0b_2a_1b_3 + a_0b_2b_1a_3 + b_0a_2a_1b_3 - b_0a_2b_1a_3 \\
z_{03}z_{12} &= (a_0b_3 - b_0a_3)(a_1b_2 - b_1a_2) \\
&= a_0b_3a_1b_2 - a_0b_3b_1a_2 - b_0a_3a_1b_2 + b_0a_3b_1a_2
\end{aligned}$$

Pro $w = w(L(p, q)) = (w_{01} : w_{02} : w_{03} : w_{12} : w_{13} : w_{23})$ spočteme

$$\begin{aligned}
b_0p - a_0q &= (0, -w_{01}, -w_{02}, -w_{03}) \in L(p, q) \\
b_1p - a_1q &= (w_{01}, 0, -w_{12}, -w_{13}) \in L(p, q) \\
b_2p - a_2q &= (w_{02}, w_{12}, 0, -w_{23}) \in L(p, q) \\
b_3p - a_3q &= (w_{03}, w_{13}, w_{23}, 0) \in L(p, q)
\end{aligned}$$

vše za předpokladu, že jsou příslušné body nenulové. Dokážeme nyní, že w je prosté. Nechť tedy body (p', q') zadávají stejný bod w' s homogenními souřadnicemi w'_{ij}, tzn. $w_{ij} = \lambda w'_{ij}$ pro jistý nenulový skalár λ. Pro určitost předpokládejme, že $w_{01} \neq 0$. Potom $(0 : -w_{01} : -w_{02} : -w_{03})$ a $(w_{01} : 0 : -w_{12} : -w_{13})$ patří do obou přímek, jsou tedy obě přímky totožné.

Nechť dále $w = (w_{01} : w_{02} : w_{03} : w_{12} : w_{13} : w_{23}) \in \mathcal{V}(z_{01}z_{23} - z_{02}z_{13} + z_{03}z_{12})$. Předpokládejme opět $w_{01} \neq 0$ a uvažme $p = (0 : -w_{01} : -w_{02} : -w_{03})$, $q = (w_{01} : 0 : -w_{12} : -w_{13})$. Potom $w(L(p,q)) = (w_{01}^2 : w_{01}w_{02} : w_{01}w_{03} : w_{01}w_{12} : w_{01}w_{13} : w_{02}w_{13} - w_{12}w_{03} = w_{01}w_{23})$, což je původně zadaný bod. Je tedy naše zobrazení také surjektivní. $\square$

5.29 Definice. *Plückerovy souřadnice* projektivních přímek jsou souřadnice obrazu těchto přímek v $\mathbb{P}_5(\mathbb{K})$ v právě zavedeném zobrazení.

6 Homogenní polynomy

V této části je R vždy obor integrity s jednoznačným rozkladem.

6.1 Věta. *Je-li R obor integrity s jednoznačným rozkladem a $f \in \mathbb{R}[x_1, \dots, x_n]$ je homogenní polynom, pak i každý člen f_i (jednoznačného) rozkladu $f = f_1 \dots f_s$ na (nerozložitelné) faktory je homogenní.*

Důkaz: Předpokládejme, že $f = gh$ a $g = g^{(i)} + g^{(i+1)} + \dots + g^{(l)}$, $h = h^{(j)} + h^{(j+1)} + \dots + h^{(k)}$, jsou rozklady na homogenní komponenty, $g^{(i)} \neq 0$, $g^{(l)} \neq 0$, $h^{(j)} \neq 0$, $h^{(k)} \neq= 0$. Rozklad součinu na homogenní části je $f = g^{(i)}h^{(j)} + \dots + g^{(l)}h^{(k)}$. Je-li f homogenní, je $i + j = l + k$, a z nerovností $l \geq i$, $k \geq j$ proto plyne $i = l$, $j = k$. Tedy g a h jsou homogenní. $\square$

6.2 Věta. *Nechť $f \in \mathbb{R}[x_1, \dots, x_n]$ a $g \in \mathbb{R}[x_1, \dots, x_m]$ je jeho homogenizace.*

1. *Jsou-li $f = f_1 \dots f_s$ a $g = g_1 \dots g_r$ rozklady na nerozložitelné faktory, pak $s = r$ a všechny g_i jsou homogenizací faktorů f_i (po případné permutaci indexů).*
2. *f je nerozložitelný právě, když je jeho homogenizace g nerozložitelná.*

Důkaz: Dokážeme napřed druhé tvrzení. Předpokládejme, že f je rozložitelný, tzn. $f = f_1 f_2 \dots$. Protože ze vztahu pro homogenizaci ihned plyne, že homogenizace součinu je součinem homogenizací činitelů, je samozřejmě $g = f^h = f_1^h f_2^h \dots$. Je-li naopak $g = g_1 g_2 \dots$ a

$$f = g(1, x_1, \dots, x_n) = g_1(1, x_1, \dots, x_n) g_2(1, x_1, \dots, x_n)$$

přičemž komponenty g_i jsou nenulového stupně v proměnných $x_1, \dots, x_n$, pak zjevně je f rozložitelné. Složením předchozích dvou úvah dostáváme požadovanou ekvivalenci.

Nyní již víme, že

$$f(x_1, \dots, x_n) = g(1, x_1, \dots, x_n) = g_1(1, x_1, \dots, x_n) g_2(1, x_1, \dots, x_n) \dots g_r(1, x_1, \dots, x_n)$$

a z jednoznačnosti rozkladu plyne (po případném přečíslování faktorů)

$$f_1(x_1, \dots, x_n) = g_1(1, x_1, \dots, x_n), \dots, f_r(x_1, \dots, x_n) = g_r(1, x_1, \dots, x_n).$$

Proto jsou g_i homogenizací f_i. Přitom je g_i nerozložitelný právě, když je $g_i(1, x_1, \dots, x_n)$ rovněž nerozložitelný. $\square$

6.3 Věta (Eulerova). *Homogenní polynom $f \in \mathbb{R}[x_1, \dots, x_n]$ stupně k splňuje pro všechny $1 \le s \le k$*

$$\sum_{|\alpha|=s} x^\alpha \frac{\partial^{|\alpha|} f}{\partial x^\alpha} = k(k-1)\dots(k-s+1)f$$

Důkaz: Pro homogení polynony stupně k platí $f(tx_1, tx_2, \dots, tx_n) = t^k f(x_1, x_2, \dots, x_n)$. Obě strany derivujme s-krát podle t.

$$\begin{aligned}
L(s) &= \frac{\partial^s}{\partial t^s} f(tx_1, \dots, tx_n) \\
P(s) &= \frac{\partial^s}{\partial t^s} t^k f(x_1, \dots, x_n) \\
&= k(k-1)\dots(k-s+1)t^{k-s} f(x_1, \dots, x_n) \\
L(1) &= \sum \frac{\partial f}{\partial x_i}(tx_1, \dots, tx_n)x_i \\
L(2) &= \sum_{i,j} \frac{\partial^2 f}{\partial x_i x_j}(tx_1, \dots, tx_n)x_i x_j \\
&\vdots
\end{aligned}$$

Provedeme-li derivaci levé strany s-krát, pak po dosazení $t = 1$ dostaneme požadovanou rovnost. $\square$

6.4 Definice. Nechť $f, g \in R[x]$, $f = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$, $a_n \neq 0$, $g = b_m x^m + \dots, b_0$, $b_m \neq 0$. Následující matice s $m+n$ řádky a sloupci se nazývá *Sylvestrova matice*, označujeme ji $\mathrm{Syl}(f, g)$.

$$\begin{pmatrix}
a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & \dots & \dots & 0 \\
0 & a_n & a_{n-1} & \dots & a_1 & a_0 & \dots & \dots & 0 \\
\vdots & \vdots & \vdots & & & & & & \\
0 & 0 & \dots & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_0 \\
b_m & b_{m-1} & b_{m-2} & \dots & b_0 & \dots & \dots & \dots & 0 \\
0 & b_m & b_{m-1} & \dots & b_1 & b_0 & \dots & \dots & \dots \\
\vdots & \vdots & \vdots & & & & & & \\
0 & \dots & \dots & \dots & 0 & b_m & \dots & \dots & b_0
\end{pmatrix}$$

Determinant této matice se nazývá *resultant* f a g, označujeme ho jako $\mathrm{Res}(f, g)$.

6.5 Poznámka. Přímo z definice plyne $\mathrm{Res}(f, g) = (-1)^{nm} \mathrm{Res}(g, f)$

6.6 Lemma. *Nechť $\mathbb{K}$ je pole, $f, g \in \mathbb{K}[x]$ polynomy stupňů m a n, $n, m > 0$. Polynomy f, g mají společný faktor (tj. $f = hf_1$, $g = hg_1$, kde $h \in \mathbb{K}[x]$ je nekonstantní polynom) právě, když existují polynomy $A, B \in \mathbb{K}[x]$ takové, že platí*

1. $Af + Bg = 0$
2. $A \neq 0$, $B \neq 0$
3. $\deg A < m = \deg g$, $\deg B < n = \deg f$ *(zde $\deg A$ je stupeň polynomu A).*

Důkaz: Napřed směr „$\Rightarrow$“. Nechť $f = hf_1$, $g = hg_1$. Je-li $\deg h \geq 1$, pak lze volit $A = g_1$, $B = -f_1$. Potom $Af + Bg = g_1 h f_1 + (-f_1) g_1 h = 0$, přičemž $\deg A = \deg_1 < \deg g$, $\deg B = \deg f_1 1 < \deg f$ a součastně $g_1 \neq 0$, $f_1 \neq 0$.

Směr „$\Leftarrow$“ dokážeme sporem. Nechť polynomy A, B daných vlastností existují, ale f a g nemají společný faktor. Největší společný dělitel f, g je tedy konstantní polynom 1. Podle Bezoutovy rovnosti (Lemma 3.11) pak existují polynomy $\tilde{A}, \tilde{B}$ takové, že $\tilde{A}f + \tilde{B}g = 1$. Protože $Af = -Bg$, platí

$$A = A\tilde{A}f + A\tilde{B}g = (A\tilde{B} - \tilde{A}B)g.$$

Přitom polynom v závorce je nenulový, což je ve sporu s předpokladem $\deg A < \deg g$.
$\square$

6.7 Věta. *Nekonstantní polynomy $f, g \in \mathbb{K}[x]$ mají společný faktor právě, když*

$$\mathrm{Res}(f, g) = 0.$$

Důkaz: Podle předchozího lemmatu mají f, g společný faktor právě, když existují A, B splňující 6.6.(1)-(3). Pišme

$$f = a_n x^n + \cdots + a_0,\ g = b_m x^m + \cdots + b_0.$$

Hledáme tedy polynomy A, B ve tvaru

$$A = c_{m-1} x^{m-1} + \cdots + c_0,\ B = d_{n-1} x^{n-1} + \cdots + d_0$$

kde alespoň jedno c_i a d_j jsou nenulové. V rovnosti $Af + Bg = 0$ porovnáme koeficienty u jednotlivých mocnin x. Tím dostaneme soustavu rovnic pro neznámé $c_{m-1}, c_{m-2}, \ldots, c_0$, $d_{n-1}, \ldots, d_0$.

$$\begin{aligned}
x^{n+m-1} &: a_n c_{m-1} + b_m d_{n-1} = 0 \\
x^{n+m-2} &: a_n c_{m-2} + a_{n-1} c_{m-1} + b_m d_{n-2} + b_{m-1} d_{n-1} = 0 \\
&\ \vdots \\
x^0 &: a_0 c_0 + b_0 d_0 = 0
\end{aligned}$$

Přepišme soustavu v maticovém tvaru $K \cdot L = M$ (všimněme si, že rovnic je $m + n$), kde

$$K = \begin{pmatrix}
a_n & 0 & 0 & \ldots & \ldots & 0 & b_m & 0 & 0 & \ldots & \ldots & 0 \\
a_{n-1} & a_n & 0 & \ldots & \ldots & 0 & b_{m-1} & b_m & 0 & \ldots & \ldots & 0 \\
a_{n-2} & a_{n-1} & a_n & 0 & \ldots & 0 & b_{m-2} & b_{m-1} & b_m & 0 & \ldots & 0 \\
\vdots & \vdots & & & & & & & & & & \\
\vdots & \vdots & & & & & & & & & & \\
0 & \ldots & \ldots & \ldots & 0 & a_0 & \ldots & \ldots & \ldots & \ldots & 0 & b_0
\end{pmatrix}$$

$$L^T = (c_{m-1}, c_{m-2}, \ldots, c_0, d_{n-1}, d_{n-2}, \ldots, d_0)$$

$$M^T = (0, 0, 0, \ldots, 0)$$

Matice K této soustavy je právě transponovaná Sylvestrova matice $\mathrm{Syl}(f, g)^T$. Proto má tato homogenní soustava lineárních rovnic netriviální řešení právě, když $\mathrm{Res}(f, g) = \det(\mathrm{Syl}(f, g))^T = 0$. $\square$

6.8 Lemma. *Nechť $f, g \in \mathbb{K}[x_1, \dots, x_r]$ a nechť mají kladný stupeň v x_r. Pak f a g mají společný faktor s kladným stupněm v proměnné x_r právě, když mají společný faktor v $\mathbb{K}(x_1, \dots, x_{r-1})[x_r]$.*

Důkaz: Jeden směr implikace je zřejmý: jestliže mají f a g společný faktor v $\mathbb{K}[x_1, \dots, x_r]$, pak jej mají i v $\mathbb{K}(x_1, \dots, x_{r-1})[x_r]$.

Naopak předpokládejme, že $f = \tilde{h}\tilde{f}_1$, $g = \tilde{h}\tilde{g}_1$, kde $\tilde{h}, \tilde{g}_1, \tilde{f}_1 \in \mathbb{K}(x_1, \dots, x_{r-1}[x_r]$, a pišme $\tilde{h} = \frac{h}{d}$, $\tilde{f}_1 = \frac{f_1}{e}$, $\tilde{g}_1 = \frac{g}{c}$, kde $h, f_1, g_1 \in \mathbb{K}[x_1, \dots, x_r]$ a $c, e, d \in \mathbb{K}[x_1, \dots, x_{r-1}]$. (Pro ilustraci

$$\tilde{h} = \frac{a_n}{b_n}x_r^n + \frac{a_{n-1}}{b_{n-1}}x_r^{n-1} + \cdots = \frac{A_n x^r + A_{n-1}x^{r-1} + \cdots + A_0}{b_n b_{n-1} \dots b_0}$$

kde $a_n, b_n \in \mathbb{K}[x_1, \dots, x_{r-1}]$.) Vynásobením dostáváme

$$def = hf_1, \quad dcg = hd_1$$

přičemž h má kladný stupeň v x_r. Proto má h nějaký nerozložitelný faktor h_1 s kladným stupněm v x_r. Nyní tedy $def = h_1 h_2 f_1$, tj. h_1 dělí některého z činitelů def. Přitom de nezávisí na x_r, proto h_1 dělí f. Obdobně z druhé rovnosti $dlg = h_1 h_2 g_1$ získáme, že h_1 dělí g. Tudíž h_1 je společný faktor f a g s kladným stupněm v x_r. □

6.9 Definice. Nechť $f, g \in \mathbb{K}[x_1, \dots, x_r]$. Potom můžeme f a g chápat jako prvky $\mathbb{K}(x_1, \dots, x_{r-1})[x_r]$ a definovat jejich *resultant* vzhledem k proměnné x_r

$$\operatorname{Res}(f, g, x_r) = \operatorname{Res}(f, g) \in \mathbb{K}(x_1, \dots x_{r-1}).$$

6.10 Věta. *Nechť f, g jsou polynomy v $\mathbb{K}[x_1, \dots, x_{r-1}][x_r]$ stupňů m a n. Potom*

1. $\operatorname{Res}(f, g, x_r) \in \mathbb{K}[x_1, \dots, x_{r-1}]$
2. *polynomy f a g mají společný faktor s kladným stupněm v proměnné x_r právě, když* $\operatorname{Res}(f, g, x_r) = 0$
3. *existují nenulové polynomy $A, B \in \mathbb{K}[x_1, \dots, x_{r-1}]$ takové, že* $\operatorname{Res}(f, g, x_r) = Af + Bg$

Důkaz: Zvolme libovolné

$$f = a_n(x_1, \dots, x_{r-1})x_r^n + \cdots + a_0(x_1, \dots, x_{r-1})$$
$$g = b_m(x_1, \dots, x_{r-1})x_r^m + \cdots + b_0(x_1, \dots, x_{r-1})$$

kde $a_i, b_i \in \mathbb{K}[x_1, \dots, x_{r-1}]$, $a_n \neq 0$, $b_m \neq 0$. Polynomy f, g chápejme jako prvky $\mathbb{K}(x_1, \dots, x_{r-1}[x_r]$. Potom použijeme větu 6.7 (to lze, protože $\mathbb{K}[x]$ v odkazovaném tvrzení je libovolné těleso, tedy zejména platí pro $\mathbb{K}(x_1, \dots, x_{r-1})[x_r]$) a podle ní f a g mají společný faktor právě, když $\operatorname{Res}(f, g, x_r) \in \mathbb{K}(x_1, \dots, x_{r-1})$ je *nulový*. Podle lemmatu 6.8 mají f a g společný faktor v $\mathbb{K}(x_1, \dots, x_{r-1})[x_r]$ právě, když mají společný faktor v $\mathbb{K}[x_1, \dots, x_r]$ s kladným stupněm v x_r. Tím jsou dokázána první dvě tvrzení.

(3) Je-li resultant nulový, je tvrzení zřejmé. Nechť $\operatorname{Res}(f, g, x_r) \neq 0$, pak je to nenulový polynom v $\mathbb{K}[x_1, \ldots, x_{r-1}]$. Pak jistě lze najít $\tilde{A}, \tilde{B}$ ve tvaru:

$$\begin{aligned}\tilde{A} &= c_{m-1}(x_1, \ldots, x_{r-1})x_r^{m-1} + \cdots + c_0(x_1, \ldots x_{r-1}) \\ \tilde{B} &= d_{n-1}(x_1, \ldots, x_{r-1})x_r^{n-1} + \cdots + d_0(x_1, \ldots x_{r-1})\end{aligned}$$

takové, aby byla splněna rovnice $\tilde{A}f + \tilde{B}g = 1$.

Porovnáním koeficientů u jednotlivých mocnin x_r v předchozí rovnosti dostáváme

$$\begin{aligned} x^{n+m}: &\quad a_n c_{m-1} + b_m d_{n-1} = 0 \\ x^{n+m-1}: &\quad a_{n-1}c_{m-1} + a_n c_{m-2} + b_{m-1}d_{n-1} + b_m d_{n-2} = 0 \\ \vdots \\ x_0 : a_0 c_0 + b_0 d_0 = 1 \end{aligned}$$

V maticovém tvaru opět získáme rovnost

$$K.L = M$$

kde matice K a L jsou stejné jako v důkazu 6.7 a $M^T = (0, \ldots, 0, 1)$. Zejména je matice zhomogenizovaného systému opět právě Sylvestrova matice polynomů f a g.

Všechna a_i, b_i, c_i, d_i jsou prvky $\mathbb{K}[x_1, \ldots, x_{r-1}] \subset \mathbb{K}(x_1, \ldots, x_{r-1})$. Takže budeme opět řešit soustavu lineárních rovnic nad tělesem $\mathbb{K}(x_1, \ldots, x_{r-1})$ a vzhledem k předpokládané nenulovosti determinantu matice systému můžeme použít Cramerovo pravidlo. Připomeňme, že pro systém $R \cdot S = T$ s nenulovým $\det R$

$$\begin{pmatrix} r_{11} & r_{12} & \ldots & r_{1n} \\ r_{21} & r_{22} & \ldots & r_{2n} \\ \vdots & \vdots & & \\ r_{n1} & r_{n2} & \ldots & r_{nn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

má (jednoznačně určené) řešení $(x_1, \ldots, x_n)^T$ se souřadnicemi

$$x_i = \begin{vmatrix} a_{11} & a_{12} & \ldots & b_1 & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & b_2 & \ldots & a_{2n} \\ \vdots & \vdots & & & & \\ a_{n1} & a_{n2} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix} \Big/ \det R$$

kde zaměněný sloupec je na i-tém místě.

V našem případě získáváme

$$c_{m-1}(x_1, \ldots, x_{r-1}) = \frac{\begin{vmatrix} 0 & 0 & \ldots & 0 & b_n & 0 & \ldots & 0 \\ 0 & & & & & & & \\ \vdots & \vdots & & & & & & \\ 1 & \ldots & \ldots & & & & & \end{vmatrix}}{\operatorname{Res}(f, g, x_r)}$$

což je polynom v $x_1, \dots x_{r-1}$. Podobně dostaneme i ostatní koeficienty. Tedy

$$\tilde{A} = \frac{A(x_1, \dots, x_{r-1})}{\operatorname{Res}(f, g, x_r)}$$
$$\tilde{B} = \frac{B(x_1, \dots x_{r-1})}{\operatorname{Res}(f, g, x_r)}$$

Nyní A, B jsou hledané polynomy, tj.

$$Af + Bg = \operatorname{Res}(f, g, x_r).$$

□

6.11 Věta. *Nechť f, g jsou homogenní polynomy v $\mathbb{K}[x_0, \dots x_r]$ mající stupně $n, m > 0$ v $\mathbb{K}[x_0, \dots, x_{r-1}][x_r]$. Pak $\operatorname{Res}(f, g, x_r)$ je buď 0 nebo homogenní polynom stupně mn v $\mathbb{K}[x_0, \dots x_{r-1}][x_r]$. Navíc, jestliže vznikly f, g homogenizací polynomů $\tilde{f}, \tilde{g} \in \mathbb{K}[x_1, \dots, x_r]$, pak dehomogenizací resultantu $\operatorname{Res}(f, g, x_r)$ získáme $\operatorname{Res}(\tilde{f}, \tilde{g}, x_r)$.*

Důkaz: Dehomogenizace znamená

$$\tilde{f}(x_1, \dots, x_r) = f(1, x_1, \dots, x_r)$$
$$\tilde{g}(x_1, \dots, x_r) = g(1, x_1, \dots, x_r)$$

a chceme tedy ukázat, že

$$\operatorname{Res}(\tilde{f}, \tilde{g}, x_r) = \operatorname{Res}(f(1, x_1, \dots, x_r),\ g(1, x_1, \dots, x_r), x_r) = \operatorname{Res}(f, g, x_r)(1, x_1, \dots, x_r).$$

Dále chceme dokázat, že $\operatorname{Res}(f, g, x_r)$ je homogenní polynom vhodného stupně k (nebo nula), což je ekvivalentní vztahu

$$\operatorname{Res}(f, g, x_r)(tx_0, \dots, tx_{r-1}) = t^k \operatorname{Res}(f, g, x_r)(x_0, \dots, x_{r-1}).$$

Zbývá tedy pouze vypočíst

$$\operatorname{Res}(f, g, x_r)(tx_0, \dots, tx_{r-1}) = \begin{vmatrix} a_n(tx_0, \dots, tx_{r-1}) & a_{n-1}(tx_0, \dots, tx_{r-1}) & \dots \\ \vdots & & \\ b_m(tx_0, \dots, tx_{r-1}) & \dots & \end{vmatrix}$$

Všechny koeficienty a_i, b_j jsou homogenní polynomy stupňů $(n-i)$, $(m-j)$. Můžeme proto vynásobit vhodně řádky mocninami t tak, abychom mohli vytýkat ze sloupců. K cíli vede násobení i-tého řádku s koeficienty a mocninou t^{i-1} a podobně j-tého řádku mocninou t^{j-1}. Dostáváme

$$\begin{vmatrix} a_n & ta_{n-1} & t^2a_{n-2} & t^3a_{n-3} & \dots & t^na_0 & 0 & \dots & \dots & 0 \\ 0 & ta_n & t^2a_{n-1} & t^3a_{n-2} & \dots & \dots & t^{n+1}a_0 & 0 & \dots & 0 \\ \vdots & \vdots & & & & & & & & \\ \dots & \dots & & & & & & & & t^{n+m-1}a_0 \\ b_m & tb_{m-1} & \dots & & & & t^mb_0 & 0 & \dots & 0 \\ 0 & tb_m & \dots & & & & & t^{m+1}b_0 & 0\dots & 0 \\ \vdots & & \vdots & & & & & & & \\ \dots & \dots & & & & & & & & t^{n+m-1}b_0 \end{vmatrix}$$

Po provedení úprav tak zíkáme vztah (stačí se přesvědčit, že platí $\frac{(m+n-1)(m+n)}{2} - \frac{n(n-1)}{2} - \frac{m(m-1)}{2} = mn$)

$$t^{\frac{(m+n-1)(m+n)}{2}} \operatorname{Res}(f,g,x_r)(x_0,\dots,x_{r-1}) = t^{\frac{m(m+1)}{2}+\frac{(n+1)n}{2}} \operatorname{Res}(f,g,x_r)(tx_0,\dots,tx_{r-1})$$

a odtud vyplývá

$$\operatorname{Res}(f,g,x_r)(tx_0,\dots,tx_{r-1}) = t^{mn} \operatorname{Res}(f,g,x_r)(x_0,\dots,x_{r-1})$$

což je požadovaný vztah □

6.12 Příklad.
(1) Nechť $f = xy - 1$, $g = x^2 + y^2 - 4$. Jak vypadá resultant těchto dvou polynomů (v proměnné x)?

$$\operatorname{Res}(f,g,x) = \begin{vmatrix} y & -1 & 0 \\ 0 & y & -1 \\ 1 & 0 & y^2 4 \end{vmatrix} = yy(y^2-4)+1$$
$$= y^4 - 4y^2 + 1 = (y^2-2)^2 - (\sqrt{3})^2$$

Podle předchozí teorie tedy f a g nemají společný nenulový faktor.
(2) Pro polynomy $f = x^2y - x$, $g = x^3 + xy - 4x$ určíme resultant v proměnné x.

$$\operatorname{Res}(f,g,x) = \begin{vmatrix} y & -1 & 0 & 0 & 0 \\ 0 & y & -1 & 0 & 0 \\ 0 & 0 & y & -1 & 0 \\ 1 & 0 & y-4 & 0 & 0 \\ 0 & 1 & 0 & y-4 & 0 \end{vmatrix} = 0$$

tzn., že polynomy mají společný nenulový faktor.
(3) Pro polynomy $f = xy - z^2$, $g = x^2 + y^2 - 4z$

$$\operatorname{Res}(f,g,x) \begin{vmatrix} y & -z^2 & 0 \\ 0 & y & -z^2 \\ 1 & 0 & y^2-4z \end{vmatrix} = y^2(y^2-4z) + z^4 = y^4 - 4y^2z^2 + z^4$$

tzn. tyto polynomy nemají společný nenulový faktor nenulového stupně v x.

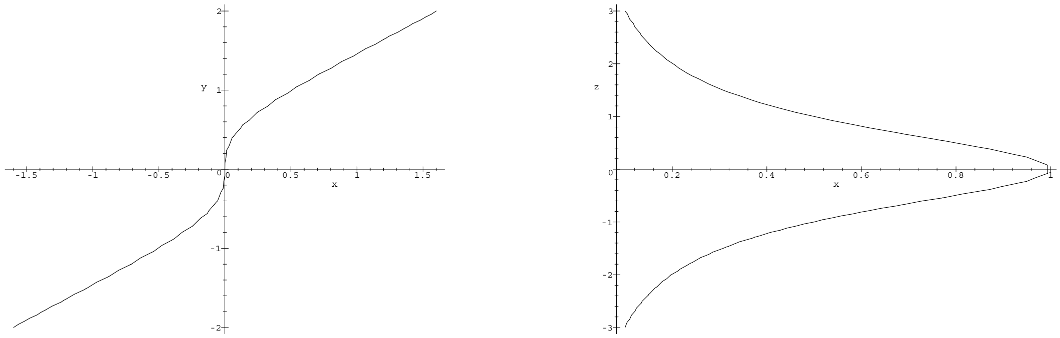
6.13 Věta. *Polynom $f \in \mathbb{K}[x]$, kde $\mathbb{K}$ je algebraicky uzavřené, má vícenásobný kořen právě, když* $\operatorname{Res}(f,f') = 0$.

Důkaz: Polynom f má vícenásobný kořen právě, když $f = g^2h$, tzn. $f' = 2gg'h$, a to je možné právě, když f a f' mají společný faktor g. □

6.14 Definice. Resultant $\operatorname{Res}(f,f')$ se nazývá *diskriminant* polynomu f.

6.15 Příklad. Pro polynom druhého stupně $f = ax^2 + bx + c$; $f' = 2ax + b$ je jeho diskriminant

$$\operatorname{Res}(f,f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a \begin{vmatrix} 1 & b & c \\ 2 & b & 0 \\ 0 & 2a & b \end{vmatrix}$$
$$= a[b^2 - 2(b^2 - 2ac)] = -a(b^2 - 4ac).$$



Obr. 16: Dvě různé homogenizace $\mathcal{V}(xz^2 - y^3 + xy^2)$, vlevo $\mathcal{V}(x - y^3 + xy^2)$, vpravo $\mathcal{V}(xz^2 - 1 + x)$.

6.16 Poznámka. Pomocí resultantů můžeme počítat průniky křivek. Resultant dvou homogenních polynomů v proměnných x_0, x_1, x_2 podle x_2 bude polynom v x_0, x_1. Homogenní polynom $f \in \mathbb{K}[x_0, x_1]$ nad algebraicky uzavřeným $\mathbb{K}$ má, až na pořadí a konstantní násobky jednoznačné vyjádření $f = f_1 f_2 \dots f_s$, kde s je stupeň f a f_i jsou lineární polynomy. Jistě existuje bod $(x_0 : x_1)$ pro který $f(x_0, x_1) \neq 0$. Vhodnou volbou projektivních souřadnic docílíme $(x_0 : x_1) = (1 : 0)$. (Tj. polynom nemá kořen v nekonečnu). Hledáme pak $f(x_0, x_1) = (a_1 x_0 + b_1 x_1) \dots (a_s x_0 + b_s x_1)$. Dosazením $x_1 = 1$ dostaneme $f(x_0, 1) = (a_1 x_0 + b_1) \dots (a_s x_0 + b_s)$.

7 Rovinné algebraické křivky

Budeme zpravidla uvažovat křivky v $\mathbb{P}_2(\mathbb{C})$, pokud možno zadané redukovanou rovnicí. Jako rozcvičku si prodiskutujme singulární body v několika příkladech.

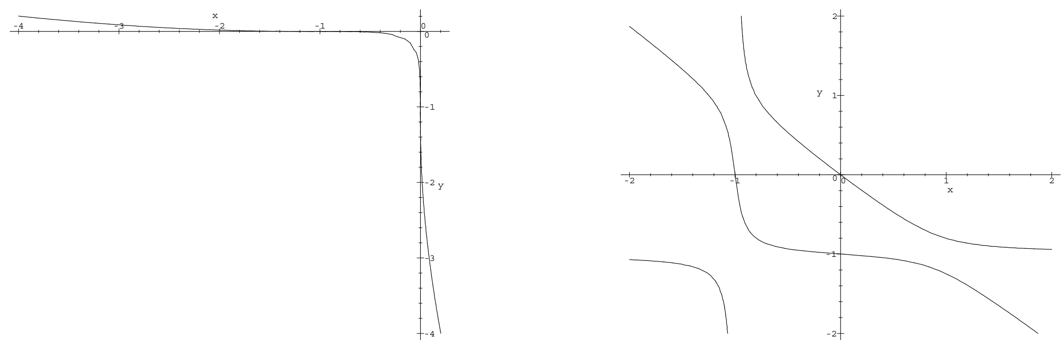
7.1 Příklad.

1. Uvažme nejprve $V = \mathcal{V}(xz^2 - y^3 + xy^2) \subset \mathbb{P}_2(\mathbb{R})$. Homogenizací pomocí $z = 1$ dostáváme afinní varietu $V_{af} = \mathcal{V}(x - y^3 + xy^2)$ s jediným nevlastním bodem $(1 : 0 : 0)$ a bez singulárních bodů. Homogenizací s $y = 1$ dostaneme křivku $\mathcal{V}(xz^2 - 1 + x)$ s asymptotou $x = 0$. Rozmyslete si, jak existence této asymptoty souvisí s tecnou k V_{af} v pocatku.

2. Křivka $K = \mathcal{V}((x + y + z)^3 - 27xyz)$ má všechny tři homogenizace stejné a jediný singulární bod $(1 : 1 : 1)$. Tečný kužel v tomto bodě je ale imaginární, proto se musí jednat o izolovaný bod křivky. Část této křivky (bez izolovaného bodu $(1, 1)$) je na levé části obrázku 17.

3. Jednoparametrický systém křivek

$$K_\alpha = xy^2 + yz^2 + x^2 z + x^2 y + y^2 z + xz^2 + \alpha xyz$$



Obr. 17: Ilustrace druhého a třetího příkladu v 7.1.

obsahuje skoro samé regulární křivky. Pouze při $\alpha = -6$ dostáváme jeden singulární bod $(1:1:1)$ s imaginárním tečným kuželem (tedy je izolovaný), při $\alpha = 3$ existuje pouze jeden nereálný singulární bod a pro hodnotu $\alpha = 2$ celá křivka třetího stupně degeneruje na sjednocení tří přímek protínajících se ve třech bodech $(-1:1:1)$, $(-1:-1:1)$, $(1:-1:1)$. Na obrázku 17 je zobrazena křivka pro hodnotu α blízkou dvěma ($\alpha = 2.1$).

7.2 Definice. Redukovaná rovnice rovinné algebraické křivky $K = \mathcal{V}(F)$ je dána homogenním polynomem $F = F_1 \dots F_k$, kde polynomy $F_1, \dots, F_k$ jsou různé nerozložitelné homogenní.[9] Stupeň polynomu F nazýváme *stupeň* křivky K. Křivky $K_i = \mathcal{V}(F_i)$ nazýváme *komponenty křivky* K.

7.3 Násobnost průniků. Pro přímku $L \subset \mathbb{P}_2(\mathbb{C})$ zadanou parametricky rovnicemi $x_0 = a_0 s_0 + b_0 s_1$, $x_1 = a_1 s_0 + b_1 s_1$, $x_2 = a_2 s_0 + b_2 s_1$ (tzn. L je obrazem $\mathbb{P}_1(\mathbb{C})$ ve vhodném homomorfismu) a homogenní polynom F stupně m bude

$$\bar{F}(s_0, s_1) = F(a_0 s_0 + b_0 s_1, a_1 s_0 + b_1 s_1, a_2 s_0 + b_2 s_1)$$

buď nulový polynom v $\mathbb{K}[s_0, s_1]$, nebo homogenní polynom stupně m. V druhém případě má $\bar{F}$ právě m kořenů $(s_0 : s_1) \in \mathbb{P}_1(\mathbb{C})$, včetně násobností. Získáme tedy, včetně násobností, právě m průniků L s křivkou $K = \mathcal{V}(F)$. Pro takový bod průniku $c \in K$ označme násobnost príslušného kořene $\bar{F}$ výrazem $n(c, K, L)$. Je-li $\bar{F} = 0$, pak jistě $L \subset \mathcal{V}(F)$ a klademe $n(c, K, L) = \infty$, pro $c \notin K$ definujeme $n(c, K, L) = 0$. Skalár $n(c, K, L)$ nazýváme násobností průniku L a K v bodě c.

7.4 Věta. *Nechť K je křivka v $\mathbb{P}_2(\mathbb{C})$ stupně m, L přímka, která není komponentou K. Pak*

$$m = \sum_{a \in K \cap L} n(a, K, L)$$

Důkaz: Tvrzení plyne okamžitě přímo z definice násobnosti průniků. □

[9] Za stejné považujeme přitom polynomy, které se liší jen o násobek skalárem.

7.5 Věta. *Nechť $K = \mathcal{V}(F)$ je křivka stupně m s redukovanou rovnicí $F = 0$. Pak $a \in \mathbb{P}_2(\mathbb{C})$ je singulární bod křivky K právě, když derivace $(\frac{\partial F}{\partial x_0}, \frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2})(a) = 0$. Je-li a regulární bod křivky K, je tečna v a (tj. tečný prostor T_aK) dána rovnicí*

$$\frac{\partial F}{\partial x_0}(a)u_0 + \frac{\partial F}{\partial x_1}(a)u_1 + \frac{\partial F}{\partial x_2}(a)u_2 = 0.$$

Důkaz: Jde o speciální případ obecných tvrzení z kapitoly čtvrté. □

7.6 Věta. *Nechť K_1 je křivka stupně m a K_2 křivka stupně n a nechť K_1 a K_2 mají více než mn průsečíků. Pak mají společnou komponentu.*

Důkaz: Předpokládejme, že K_1, K_2 mají více než mn průsečíků a vyberme z nich pevně $mn+1$ bodů $a^{(i)} = (a_0^{(i)} : a_1^{(i)} : a_2^{(i)})$. Vhodnou volbou projektivních souřadnic dosáhneme, že bod $(0:0:1)$ neleží na žádné přímce spojující libovolné dva z vybraných bodů, ani na $K_1 \cup K_2$. Zejména pak rovnice křivek mají tvar

$$K_1 : \; F(x) = p_0 x_2^m + p_1(x_0, x_1)x_2^{m-1} + \cdots + p_m(x_0, x_1) = 0$$
$$K_1 : \; G(x) = q_0 x_2^m + q_1(x_0, x_1)x_2^{m-1} + \cdots + q_m(x_0, x_1) = 0$$

kde $p_0, q_0 \in \mathbb{C}$ a p_i, q_i jsou homogenní polynomy stupně i.

Pak resultant $\mathrm{Res}(F, G, x_2)$ je buď nula, nebo homogenní polynom stupně mn. V každém případě je $\mathrm{Res}(F, G, x_2)(a_0^{(i)}, a_1^{(i)}) = 0$, protože resultant náleží ideálu polynomů $\langle F, G\rangle$. Kdyby $(a_0^{(i)}, a_1^{(i)}) = (a_0^{(j)}, a_1^{(j)})$ pro jisté $i \neq j$, pak by přímka zadaná body $a^{(i)}$, $a^{(j)}$ byla zadána rovnicí $a_0^{(i)}x_1 - a_1^{(i)}x_0 = 0$ a obsahovala by bod $(0:0:1)$. Proto jsou všechny $(a_0^{(i)} : a_1^{(i)}) \in \mathbb{P}_1(\mathbb{C})$ různé kořeny resultantu. Protože ale polynom stupně mn má nejvýše mn různých kořenů, je $\mathrm{Res}(F, G, x_2) = 0$ a křivky proto mají společnou komponentu. □

7.7 Lemma. *Nechť křivky K_1, K_2 mají rovnice $F(x) = G(x) = 0$ s polynomy stejného tvaru jako v 7.6. Je-li $a = (a_0 : a_1 : a_2) \in K_1 \cap K_2$ takový, že a je r-násobný bod[10] křivky K_1 a s-násobný bod křivky K_2, pak $(a_0 : a_1)$ je kořenem $\mathrm{Res}(F, G, x_2)$ s násobností alespoň rs, nebo je $\mathrm{Res}(F, G, x_2)$ nulový polynom.*

Důkaz: Nejprve ukážeme, že vhodnou volbou souřadnic lze dosáhnout $a = (1:0:0)$. Potom tvrzení snadno dokážeme ve vložené afinní rovině $x_0 = 1$ v $\mathbb{P}_2(\mathbb{C})$. Předpokládejme $\mathrm{Res}(F, G, x_2) \neq 0$. Z volby našich polynomů vyplývá, že $a \neq (0:0:1)$, a můžeme předpokládat, že $a_0 \neq 0$ (jinak přehodíme první dvě souřadnice). Transformace souřadnic

$$x_0' = \frac{1}{a_0}x_0, \; x_1' = x_1 - \frac{a_1}{a_0}x_0, \; x_2' = x_2$$

převede bod $(a_0 : a_1 : a_2)$ na $(1:0:a_2)$ a zřejmě má $\mathrm{Res}(F', G', x_2')$ ztransformovaných polynomů v $(1:0)$ kořen stejného stupně jako původní resultant v $(a_1 : a_2)$. Jako další se nabízí transformace

$$x_0' = x_0, \; x_1' = x_1, \; x_2' = x_2 - a_2 x_0$$

[10] Připomeňme, že to znamená, že všechny derivace definujícího polynomu až do stupně $r-1$ včetně jsou nulové.

po které by $a = (1 : 0 : 0)$, musíme ale zjistit co se při této transformaci stane s resultantem (nyní měníme proměnnou x_2, vzhledem ke které se resultant počítá).

Zaveďme do uvažované transformace volný parametr $\lambda \in \mathbb{C}$ místo a_2, tj.

$$x'_0 = x_0,\ x'_1 = x_1,\ x'_2 = x_2 - \lambda x_0$$

a označme $\operatorname{Res}(F_\lambda, G_\lambda, x'_2) \in \mathbb{C}[\lambda]$ resultant transformovaných polynomů, tj.

$$F_\lambda(x'_0, x'_1, x'_2) = F(x'_0, x'_1, x'_2 + \lambda x'_0)$$

a podobně pro G. Pro $\lambda = 0$ dostáváme původní $\operatorname{Res}(F, G, x_2) \neq 0$, je tedy

$$\operatorname{Res}(F_\lambda, G_\lambda, x'_2) = c_0(x'0, x'_1) + c_1(x'0, x'_1)\lambda + \cdots + c_N(x'0, x'_1)\lambda^N$$

pro jisté $N \geq 0$. Stačí nám ukázat, že $c_1 = \cdots = c_N = 0$, pak dokonce resultant polynomů F_λ, G_λ na hodnotě λ vůbec nezávisí.

Přepdokládejme tedy, že $c_N \neq 0$, $N \geq 1$. Jistě pak existují $b_0, b_1 \in \mathbb{C}$ takové, že $c_0(b_0, b_1) \neq 0$ a $c_N(b_0, b_1) \neq 0$. Existuje ale také $\lambda_0 \in \mathbb{C}$ takové, že $\operatorname{Res}(F_{\lambda_0}(b_0, b_1), G_{\lambda_0}(b_0, b_1), x'_2)$ polynomů v proměnné x'_2 je nulový. Tzn., že polynomy $F_{\lambda_0}(b_0, b_1, x'_2), G_{\lambda_0}(b_0, b_1, x'_2) \in \mathbb{C}[x'_2]$ mají společný kořen b_2. Pak ovšem polynomy F_{λ_0} a G_{λ_0} mají společný kořen (b_0, b_1, b_2) a proto původní polynomy F a G mají společný kořen $(b_0, b_1, b_2 + \lambda_0 b_0)$. To je ve sporu s předpokladem $\operatorname{Res}(F, G, x_2)(b_0, b_1) = c_0(b_0, b_1) \neq 0$. Proto je $c_N = 0$ pro všechny $N \geq 1$.

Zbývá studovat násobnost kořene $(1 : 0 : 0)$ pro $\operatorname{Res}(F, G, x_2)$, můžeme to provést v afinní rovině $x_0 = 1$. Uvažujme tedy polynomy f, g vzniklé dehomogenizací F, G, které mají v $(0, 0)$ parciální derivace až do řádu $r - 1$, resp. $s - 1$, nulové. Tj.

$$\begin{aligned} f(x, y) &= f_0 x^r + f_1 x^{r-1} + \cdots + f_r y^r + \cdots + f_m y^m \\ g(x, y) &= g_0 x^s + g_1 x^{s-1} + \cdots + g_s y^s + \cdots + g_n y^n \end{aligned}$$

kde f_i a g_i jsou polynomy v proměnné x. Nyní

$$\operatorname{Res}(f, g, y) = \begin{vmatrix} f_m & f_{m-1} & \dots & f_r & \dots & f_1 x^{r-1} & f_0 x^r & \dots & \dots \\ 0 & f_m & \dots & f_{r+1} & \dots & f_2 x^{r-2} & f_1 x^{r-1} & f_0 x^r & \dots \\ & & & & \dots & & & & \\ g_n & \dots & \dots & \dots & \dots & \dots & g_0 x^s & \dots & \dots \\ & & & & \dots & & & & \\ \dots & \dots & g_n & \dots & \dots & \dots & \dots & \dots & g_0 x^s \end{vmatrix}$$

Vynásobíme řádky mocninami x tak, abychom pak mohli vytýkat ze sloupců: U řádků s f postupně vynásobíme $(n - j)$-tý mocninou x^{s-j}, $j = 0, \dots, s - 1$, u g postupně $(m - j)$-tý mocninou x^{r-j}. Pak v $(m + n + 1 - i)$-tém sloupci máme společný faktor $x^{r+s+1-i}$, a to pro $i = +, \dots, r + s$. Celkem tedy máme

$$x^{\sum_{i=1}^{s} i + \sum_{i=1}^{r} i} \operatorname{Res}(f, g, y) = x^{\sum_{i=1}^{r+s} (r+s+1-i)} h(x)$$

kde h je jistý polynom. Odtud plyne, že resultant bude dělitelný mocninou x s exponentem

$$\frac{1}{2}((r + s + 1)(r + s) - (s + 1)s - (r + 1)r) = rs$$

címž je důkaz ukončem. $\square$

7.8 Důsledek. *Nechť F a G jsou redukované rovnice křivek K_1 a K_2. Je-li bod $a = (a_0 : a_1 : a_2) \in K_1 \cap K_2$ r-násobný bod K_1 a s-násobný bod K_2, pak $(a_0 : a_1)$ je rs-násobný bod resultantu $\mathrm{Res}(F, G, x_2)$.*

7.9 Věta. *Nechť K_1 a K_2 jsou křivky v $\mathbb{P}_2(\mathbb{C})$ stupňů m a n, bez společné komponenty. Jsou-li $a^{(1)}, \dots, a^{(k)}$ všechny průsečíky křivek K_1 a K_2, přičemž každý $a^{(i)}$ je r_i-násobný bod K_1 a s_i-násobný bod K_2, pak $\sum_{i=1}^k r_i s_i \leq mn$.*

Důkaz: Zvolíme opět zouřadnice tak, aby redukované rovnice měly tvar jako v 7.6 a aby žádné přímky procházející dvěma průsečíky neobsahovaly bod $(0 : 0 : 1)$. Pak $(a_0^{(i)} : a_1^{(i)})$ jsou různé kořeny $\mathrm{Res}(F, G, x_2)$. Přitom je $\mathrm{Res}(F, G, x_2)$ polynom stupně mn a každý z průsečíků dává kořen stupně alespoň $r_i s_i$. □

7.10 Důsledek.

- *Nerozložitelná křivka stupně $m \geq 2$ má singulární bod nejvýše stupně $m - 1$.*
- *Má-li nerozložitelná křivka $(m - 1)$-násobný bod, pak již nemá žádné další singulární body.*

Důkaz: Nechť je K nerozložitelná křivka stupně $m \geq 2$, $a \in K$ nechť má násobnost k. Pak pro $b \neq a$, $b \in K$ splňuje přímka L zadaná body a, b rovnost $k \cdot 1 + 1 \cdot 1 = k + 1 \leq m \cdot 1$, tj. $k \leq m - 1$. Pokud je přitom a m-násobný bod, pak b už nemůže mít násobnost větší než 1. □

7.11 Poznámka (Bezoutova věta). Tvrzení věty 7.9 lze podstatně rozšířit. Ve skutečnosti totiž nastává v nerovnosti $\sum_i r_i s_i \leq mn$ vždy rovnost, pokud se křivky protínají „dostatečně regulárně", např. když se protínají v regulárních bodech, ve kterých mají různé tečny. Obecně musíme započítat násobné protínání křivek způsobené „stykem vyššího stupně", viz. například dotyk tečny ke křivce. Budeme-li potom počítat každý bod s koeficientem daným touto násobností, získáme skutečně rovnost. Pro čistě algebraickou definici řádu dotyku křivek nemáme vybudovaný dostatečný aparát[11] a využití prostředků diferenciální geometrie se chci vyhnout. Tento výsledek je známý pod jménem *Bezoutova věta* a říká že počet průsečíků dvou nerozložitelných křivek bez společné komponenty, včetně násobností, je roven součinu jejich stupňů. Všimněme si, že speciálním případem, kdy je jedna z křivek stupně 1, je věta 7.4.

7.12 Lineární systémy křivek. Všechny křivky K stupně m v $\mathbb{P}_2(\mathbb{C})$ jsou dány homogenními polynomy tvaru

$$F(x) = \sum_{\alpha+\beta+ga=m} c_{\alpha\beta\gamma} x_0^\alpha x_1^\beta x_2^\gamma$$

kde počet koeficientů $c_{\alpha\beta\gamma}$ je roven

$$\sum_{i=0}^{m} (m - i + 1) = (m + 1)((m + 1) - \frac{1}{2} m) = \frac{1}{2}(m + 1)(m + 2).$$

[11] Výhodné je používat parametrizace křivek pomocí podílového tělesa formálních mocninných řad, pak jde o shodné koeficienty až do určitého stupně včetně.

Polynomy lišící se o násobek skalárem ovšem zadávají stejnou křivku, tj. křivky stupně m jsou parametrizovány[12] body $\mathbb{P}_{N_m}(\mathbb{C})$, kde

$$N_m = \frac{1}{2}(m+1)(m+2) - 1 = \frac{1}{2}m(m+3).$$

Zvolíme-li body $a^{(i)}$, $i = 1, \dots, N_m$, a požadujeme $F(a^{(i)}) = 0$ (tj. zvolené body mají ležet na uvažované křivce), dostáváme N_m lineárních rovnic na koeficienty $c_{\alpha\beta\gamma}$. Jsou-li tyto rovnice nezávislé, pak je body $a^{(i)}$ jednoznačně určena křivka K. Např. pro $m = 2$ je $N_2 = 5$ a je známo, že křivky zadané homogenními polynomy druhého stupně jsou dány pěti svými body v obecné poloze, tj. žádné čtyři z nich neleží na přímce.

Množina N_m bodů křivky K zadané polynomem stupně m se nazývá *obecná množina bodů křivky* K, je-li K jediná taková křivka,která jimi prochází.

Každý projektivní podprostor v $\mathbb{P}_{N_m}(\mathbb{C})$ zadává *lineární systém křivek*. Např. požadavek $a \in K$ pro pevně zvolené $a \in \mathbb{C}_2$ zadává křivky parametrizované nadplochou v $\mathbb{P}_{N_m}(\mathbb{C})$.

7.13 Příklad. Obecně bohužel neplatí, že k zvolenými body prochází $(N_m - k)$-rozměrný systém křivek. Např. pro $m = 2$, je $N_2 = 5$ a pokud 3 ze zvolených 4 bodů jsou v přímce L, pak každá kuželosečka jimi procházející obsahuje celou přímku L (viz. věta 7.9). Pokud je čtvrtý zvolený bod také na L, nezadává pak nezávislou podmínku. Proto výsledný systém není 1-rozměrný, ale je to dvourozměrný systém všech rozložitelných kuželoseček obsahujících danou přímku L.

Zvolme ještě $m = 3$, tj. $N_m = 9$. Lze snadno najít dvě kubiky $K_1 = \mathcal{V}(F)$ a $K_2 = \mathcal{V}(G)$, které se protínají v devíti bodech (např. každá z nich může být sjednocení 3 přímek). Pak jednorozměrný systém křivek $\mathcal{V}(\lambda_1 F + \lambda_2 G)$ prochází těmito devíti body. Přitom je $N_m - 9 = 0$.

7.14 Definice. Lineární systémy dimenze jedna se nazývají *svazky*, systémy dimenze jsou *sítě* a trojrozměrné jsou *tkáně*. U vyšších dimenzí také hovoříme o vícerozměrných sítích.

Svazky mají důležitou vlastnost: průsečíky dvou nezávislých křivek ve svazku prochází i všechny ostatní křivky tohoto svazku. Jednoduchou aplikaci této skutečnosti ukazuje následující věta.

7.15 Věta. *Jestliže se dvě křivky stupně m protínají v m^2 bodech a jestliže je právě mn z nich na nerozložitelné křivce stupně n, pak zbylých $m(m-n)$ bodů leží na křivce stupně nejvýše $m - n$.*

Důkaz: Nechť K_1, K_2 jsou dvě takové křivky zadané polynomy F, G. Nechť $K_3 = \mathcal{V}(H)$ je nerozložitelná křivka stupně n obsahující právě mn z m^2 průsečíků. Vhodnou volbou prametrů λ_1, λ_2 lze najít křivku ve svazku $\mathcal{V}(\lambda_1 F + \lambda_2 G)$, která prochází libovolným předem daným bodem. Zvolme takový bod na K_3, ale mimo $K_1 \cup K_2$. Potom K_3 a $\mathcal{V}(\lambda_1 F + \lambda_2 G)$ mají nejméně $nm + 1$ společných bodů, proto mají společnou komponentu. Touto komponentou ovšem musí být celá K_3, neboť je podle předpokladu nerozložitelná. Odtud plyne $\lambda_1 F + \lambda_2 G = HH'$ a $\mathcal{V}(HH')$ prochází všemi m^2 průsečíky K_1 a

[12] Nyní počítáme komponenty křivek včetně násobností, např. dvojnásobná přímka je kuželosečkou a zadáme ji polynomem druhého stupně.

K_2. Zejména je stupeň H' roven $m-n$ a $\mathcal{V}(H')$ musí obsahovat všechny zbylé průsečíky. □

7.16 Důsledek (Pascalova věta). *Dvojice protějších stran šestiúhelníku vepsaného regulární kuželosečce se protínají ve třech kolineárních bodech.*

Důkaz: Označme strany šestiúhelníka $L_1, \ldots, L_6$. Pak kubiky tvořené sjednocením $L_1 \cup L_3 \cup L_5$ a $L_2 \cup L_4 \cup L_6$ se protínají v šesti vrcholech šestiúhelníku a třech průsečících protilehlých stran, tj. v $3^2 = 9$ bodech. Nerozložitelná kuželosečka prochází právě šesti z nich, musí proto existovat křivka stupně 1, na které jsou zbývající 3. □

7.17 Poznámka. Jestliže se dvě kubiky $\mathcal{V}(F)$, $\mathcal{V}(G)$ protínají v právě 9 bodech, pak přímá diskuse využívající toho, že všechny kubiky ve svazku $\mathcal{V}(\lambda_1 F + \lambda_2 G)$ procházejí těmito devíti průsečíky, ukazuje, že každá kubika, která prochází osmi z nich prochází i posledním. Použitím tohoto výsledku můžeme v předchozí větě rozšířit tvrzení pro případ $m = 3$, $n = 2$ i na rozložitelné kuželosečky. Pascalova věta platí tedy i pro singulární kuželosečky, tj. dvojici přímek. Toto tvrzení je známo pod názvem Pappova věta.

Ve zbytku kapitoly se budeme podrobněji zabývat tečnami ke křivkám.

7.18 Definice. Nechť $K = \mathcal{V}(F)$ a $a \in K$ je regulární bod. Dále nechť L je tečna K v bodě a s násobností protínání $n(a, K, L) \geq 3$. Pak L nazýváme *inflexní tečnou* křivky K, bod a *inflexním bodem* křivky K a číslo $(n(a, K, L) - 2)$ *násobností inflexe* v bodě a.

Všimněme si, že každý bod přímkové komponenty křivky K je inflexní (s nekonečnou násobností inflexe).

7.19 Definice. Pro křivku K stupně $m \geq 3$ s redukovanou rovnicí $F = 0$ definujeme její *hessián* jako křivku H_K zadanou hessiánem polynomu F, tj.

$$H_K = \mathcal{V}(\det(\frac{\partial^2 F}{\partial x_i \partial x_j})).$$

7.20 Věta. *Nechť K je křivka stupně $m \geq 3$ bez přímkových komponent s redukovanou rovnicí F. Pak inflexní body křivky K jsou všechny regulární body K ležící na na průniku $K \cap H_K$.*

Důkaz: Nechť $a = (a_0 : a_1 : a_2) \in K$ je regulární bod a $b \in \mathbb{P}_2(\mathbb{C})$ je libovolný. Rozvineme kompozici F s parametrizací přímky procházející a, b.

$$F(sa + tb) = F(a)s^m + \sum_i \frac{\partial F}{\partial x_i}(a) b_i s^{m-1} t + \frac{1}{2} \sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) b_i b_j s^{m-2} t^2 + \ldots$$

Označme L a Q přímku a kuželosečku zadané rovnicemi

$$\sum_i \frac{\partial F}{\partial x_i}(a) x_i = 0, \qquad sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) x_i x_j = 0.$$

Je zřejmé, že L je tečnou v bodě a, a násobnost $n(a, L, K) > 2$ právě, když $L \subset Q$. Kuželosečka Q má ovšem přímkovou komponentu právě, když je singulární, tj. když hessián F je v a nulový.

Naopak, nechť a je regulární bod křivky K, $a \in K \cap H_K$. Vždy platí

$$\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) a_i a_j = m(m-1)F(a)$$

proto $a \in Q$. Dále

$$\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) a_i x_j = (m-1) \sum_i \frac{\partial F}{\partial x_i}(a) x_i$$

je tedy přímková komponenta $\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) a_i x_j$ kvadriky Q skutečně tečnou křivky K.

□

7.21 Důsledek. *Křivka stupně $m \geq 3$ bez singulárních bodů a přímkových komponent má alespoň jeden inflexní bod a nejvýše $3m(m-2)$ inflexních bodů.*

Důkaz: Dvě křivky v $\mathbb{P}_2(\mathbb{C})$ mají jistě alespoň jeden společný bod. (Plyne z toho, že resultant jejich polynomů má jistě kořen, nebo je identicky nulový.)

Hessián $H_K = \mathcal{V}(\det(\frac{\partial^2 F}{\partial x_i \partial x_j}))$ je dán polynomem stupně $3(m-2)$, je to proto křivka stupně alespoň 1 a nejvýše $3(m-2)$. Proto buď mají K a H_K společnou komponentu, nebo mají nejvýše $3m(m-2)$ společných bodů. Protože předpokládáme, že K nemá ani singulární body ani přímkové komponenty, jsou všechny tyto společné body inflexní body K, podle předchozí věty.

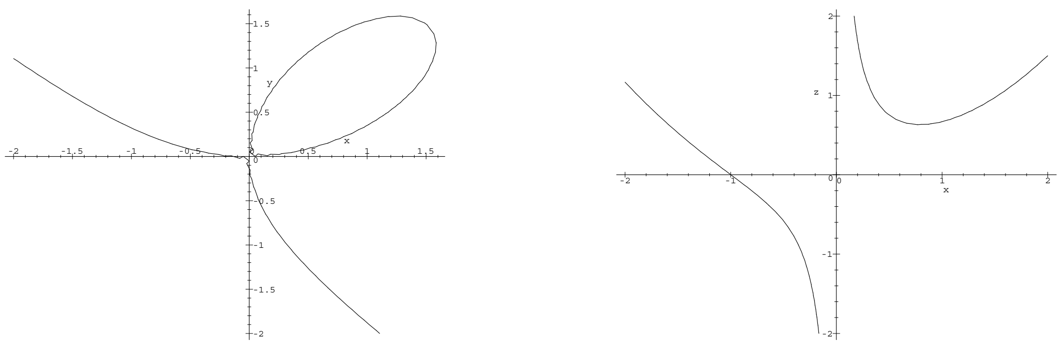
Pokud by ale existovala společná komponenta K' v $K \cap H_K$, pak by tečny ve všech bodech K' měly dotyk řádu většího než jedna. Parametrizujme hladce K' v okolí nějakého takového bodu v afinní rovině funkcemi $(f(t), g(t))$. Dotyk alespoň druhého stupně pak znamená, že druhé derivace $(\frac{d^2}{dt} f(t), \frac{d^2}{dt} g(t))$ zmizí identicky na otevřené množině. To ale znamená, že parametrizujeme přímku. K tomuto závěru dojdeme v okolí kteréhokoliv bodu K', je to tedy přímková komponenta, což není možné. Proto K a H_K nemohou mít společnou komponentu. □

7.22 Důsledek. *Nechť K nemá přímkové komponenty. Pak v $K \cap H_K$ jsou právě všechny singulární body a inflexní body křivky K.*

Důkaz: Zbývá jenom dokázat, že každý singulární bod je bodem hessiánu křivky K. Pro body násobnosti větší než 3 je přímo matice druhých derivací identicky nulová. Zbývají tedy dvojnásobné body. Pro ty platí

$$\sum_{i,j} \frac{\partial^2 F}{\partial x_i \partial x_j}(a) a_i x_j = (m-1) \sum_i \frac{\partial F}{\partial x_i}(a) x_i = 0$$

proto $\mathcal{V}(\frac{\partial^2 F}{\partial x_i \partial x_j})$ obsahuje přímkovou komponentu, je tedy příslušná kvadratická forma singulární, neboli $\det(\frac{\partial^2 F}{\partial x_i \partial x_j}) = 0$. □



Obr. 18: Descartův list v afinní rovině $z = 1$ a jeho chování v okolí inflexní tečny (zobrazeno v afinní rovině $y = 1$).

7.23 Příklad. Křivce $K = \mathcal{V}(x^3 + y^3 - 3axyz) \subset \mathbb{P}_2(\mathbb{R})$, $a \neq 0$, se říká *Descartův list*. Její vyobrazení (v afinní rovině $z = 1$) je na obrázku 18. Snadno se spočte, že jediný singulární bod je $(0 : 0 : 1)$, jediný reálný nevlastní bod je $(-1 : 1 : 0)$ (další dva komlexně združené nás teď nezajímají) a tečna v nevlastním bodě má rovnici $x + y + az = 0$. Hessián K_H je zadán rovnicí $x^3 + y^3 + axyz$ a společné body $K_H \cap K$ jsou dva reálné $(0 : 0 : 1)$, $(-1 : 1 : 0)$ (a další dva komplexně združené). Jediná reálná inflexní tečna je tedy asymptota $y = -x - a$.

7.24 Asociované symetrické formy. Nechť $F \in \mathbb{K}[x_0, \ldots, x_n]$ je homogenní polynom stupně k. Pišme na chvíli multiindexy velikosti k jako posloupnosti k celých čísel $(i_1, \ldots, i_k)$, $0 \leq i_j \leq m$. Polynom F pak můžeme vyjádřit

$$F(x_0, \ldots, x_n) = \sum_{0 \leq i_1, \ldots, i_k \leq n} c_{i_1, \ldots, i_k} x_{i_1} \ldots x_{i_k}$$

kde koeficienty $c_{i_1, \ldots, i_k}$ jsou symetrické ve všech indexech i_j. Pro každý polynom existuje právě jedna volba takových symetrických koeficientů. Stejné koeficienty nám definují k-lineární zobrazení $\hat{F} : \mathbb{K} \times \cdots \times \mathbb{K}$ vztahem[13]

$$\hat{F}((x_0^{(1)}, \ldots, x_n^{(1)}), \ldots, (x_0^{(k)}, \ldots, x_n^{(k)})) = \sum_{0 \leq i_1, \ldots, i_k \leq n} c_{i_1, \ldots, i_k} x_{i_1}^{(1)} \ldots x_{i_k}^{(k)}.$$

Zobrazení $\hat{F}$ je jediné symetrické k-lineární zobrazení splňující

$$\hat{F}(x, x, \ldots, x) = F(x)$$

pro všechny vektory $x \in \mathbb{K}^{n+1}$. Říkáme mu *polární forma* homogenního polynomu F.

[13] k-lineárnost znamená, že všechna zobrazení vzniklá z daného dosazením pevných souřadnic za některých $k - 1$ argumentů jsou lineární.

7.25 Definice. Nechť K je křivka v $\mathbb{P}_2(\mathbb{C})$ stupně $m \geq 2$ s redukovanou rovnicí $F = 0$. Pro libovolný bod $a \in \mathbb{C}^3$ definujeme polynomy $F_a^{[i]} \in \mathbb{C}[x_0, x_1, x_2]$

$$\begin{aligned} F_a^{[1]}(x) &= \hat{F}(a, x, x, \dots, x) \\ F_a^{[2]}(x) &= \hat{F}(a, a, x \dots, x) \\ &\vdots \\ F_a^{[m-1]}(x) &= \hat{F}(a, a, \dots, a, x) \end{aligned}$$

Zřejmě je vždy $F_a^{[j]}$ buď nulový polynom, nebo homogenní polynom stupně $m - j$. Hodnoty polynomů $F_a^{[j]}$ sice závisejí na výběru homogenních souřadnic bodů $a, x \in \mathbb{P}_2(\mathbb{C})$, je ovšem $F_{\alpha a}^{[j]}(\beta x) = \alpha^j \beta^{m-j} F_a^{[j]}(x)$. Proto jsou dobře definovány křivky

$$K_a^{[j]} = \mathcal{V}(F_a^{[j]})$$

pro všechny body $a \in \mathbb{P}_2(\mathbb{C})$, pro které jsou příslušné polynomy nenulové. Tyto křivky nazýváme j-té *poláry bodu* a *vzhledem ke křivce* K.

Ve formulaci další věty budeme jako argumenty a polynomů $F_a^{[j]}$ uvádět přímo body projektivního prostoru. Je tedy třeba i tyto polynomy chápat „až na násobek skalárem“. Přesné značení by vedlo k nepřehlednosti.

7.26 Věta. *Nechť je K křivka v $\mathbb{P}_2(\mathbb{C})$ stupně m s redukovanou rovnicí $F = 0$.*

1. *Je-li $a \in K$ r-násobný bod křivky, pak platí $F_a^{[m-1]} = \cdots = F_a^{[m-r+1]} = 0$ a polára $K_a^{[m-r]}$ již existuje.*
2. *Platí-li $F_a^{[m-1]} = \cdots = F_a^{[m-r+1]} = 0$, $F_a^{[m-r]} \neq 0$, pro nějaký bod a, pak je a r-násobný bod křivky K.*
3. *Je-li $a \in K$ regulární bod křivky, je $K_a^{[m-1]}$ přímka, která je tečnou křivky K v bodě a.*
4. *Pro libovolné dva body $a, b \in \mathbb{P}_2(\mathbb{C})$ je $a \in K_b^{[j]}$ právě, když $b \in K_a^{[m-j]}$.*
5. *Nechť $a \in \mathbb{P}_2(\mathbb{C})$ a nechť polára $K_a^{[r+s]}$ existuje. Pak s-tá polára bodu a vzhledek k r-té poláře bodu a (vzhledem ke K) je $(r+s)$-tá polára bodu a vzhledem ke K.*
6. *Každý s-násobný bod křivky K je bodem polár $K_b^{[r]}$, pro všechny $r < s$ a libovolný bod b.*

Důkaz: (1), (2): Přímka procházející body $a, x \in \mathbb{P}_2(\mathbb{C})$ má parametrický tvar $u = \lambda a + \mu x$. Hodnota polynomu ve vektoru u je

$$\begin{aligned} F(u) &= \hat{F}(u, \dots, u) = \hat{F}(\lambda a + \mu x, \dots, \lambda a + \mu x) \\ &= \lambda^m F(a) + m\lambda^{m-1}\mu \hat{F}(a, \dots, a, x) + \cdots + \mu^m F(x) \end{aligned}$$

Je-li $a \in K$ r-násobný, pak $(\lambda : \mu) = (1 : 0)$ je r-násobný kořen $F(\lambda a + \mu x)$ pro každé $x \neq a$, tzn.

$$F(a) = \hat{F}(a, \dots, a, x) = \hat{F}(a, \dots, a, \underbrace{x, \dots, x}_{r-1}) = 0$$

a další už musí být nenulové. To dokazuje (1). Naopak, z platnosti těchto rovností vyplývá, že a je skutečně r-násobný bod křivky. Tím jsme ověřili i (2).

(3): Je-li bod $a \in K$ regulární, pak naše vyjádření hodnoty $F(u)$ ukazuje, že polára $K^{[m-1]}$ jistě existuje, a volba $x \in K_a^{[m-1]}$ nám dá přímku s násobným průnikem, tj. tečnu.

(4): Je $a \in K_b^{[j]}$ právě, když $\hat{F}(\underbrace{b,\dots,b}_{j},\underbrace{a,\dots,a}_{m-j}) = 0$. Protože je $\hat{F}$ symetrické ve svých argumentech, je tvrzení zřejmé.

(5): r-tá polára bodu a vzhledem ke K je dána polynomem

$$G(x) = \hat{F}(\underbrace{a,\dots,a}_{r},x,\dots,x)$$

a s-tá polára vzhledem k ní je tedy zadána polynomem

$$\hat{G}(\underbrace{a,\dots,a}_{s},x,\dots,x) = \hat{F}(\underbrace{a,\dots,a}_{r+s}x,\dots,x).$$

(6): Již jsme ukázali, že pro s-násobný bod existuje polára $K_a^{[m-s]}$. Pak tedy j-tá polára vzhledem ke $K_a^{[m-s-j]}$ je právě $K_a^{[m-s]}$. Podle (1), (2) je ovšem bod a s-násobný právě, když

$$\hat{F}(\underbrace{b,\dots,b}_{j},\underbrace{a,\dots,a}_{m-j}) = 0$$

pro libovolné $b \in \mathbb{P}_2(\mathbb{C})$ a $j = 1,\dots,s-1$. Tzn. skutečně $a \in K_b^{[j]}$ pro $j = 1,\dots,s-1$. $\square$

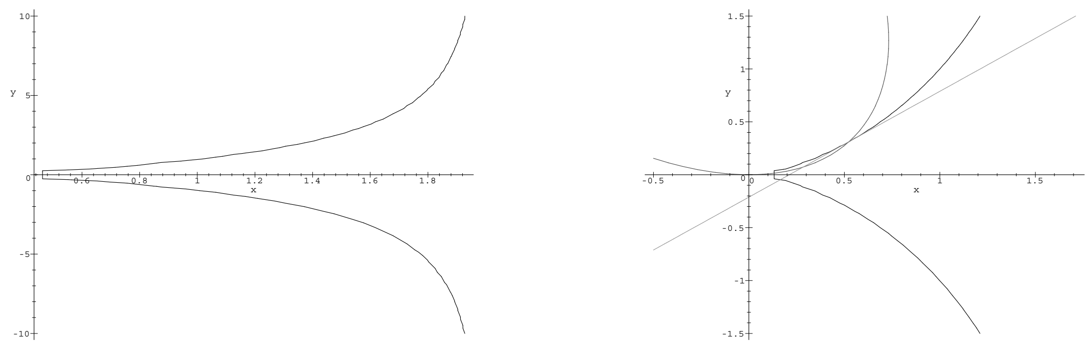
7.27 Poznámka. Pro každý bod $a = (a_0, a_1, a_2)$ označme D_a „diferenciální operátor“ $a_0\frac{\partial}{\partial x_0} + a_1\frac{\partial}{\partial x_1} + a_2\frac{\partial}{\partial x_2}$ na polynomech. Bodem $(a_0 : a_1 : a_2) \in \mathbb{P}_2(\mathbb{C})$ je D_a samozřejmě určeno až na násobek. Pro homogenní polynom $F \in \mathbb{K}[x_0, x_1, x_2]$ stupně m platí (viz. Eulerova věta)

$$\sum_i \frac{\partial F}{\partial x_i}(a)a_i = m\hat{F}(a,x,\dots,x).$$

Proto, pokud existuje polára $K_a^{[1]}$ bodu a vzhledem k varietě $\mathcal{V}(F)$, je rovna $\mathcal{V}(D_aF)$. Iterací tohoto postupu dostáváme $K_a^{[i]} = \mathcal{V}((D_a)^iF)$, pokud tato polára existuje. Jsou tedy rovnice poláry dány iterovaným derivováním polynomu F ve směru vektoru a.

7.28 Příklad. Budeme zkoumat tzv. *Dioclesovu cissoidu* $K = \mathcal{V}(x(y^2+x^2) - 2ay^2z)$. Je to opět nerozložitelná křivka, jejíž afinní část v rovině $z = 1$ má jediný reálný nevlastní bod $(0 : 1 : 0)$ (a dva imaginární komplexně sdružené) a jediný singulární bod $(0 : 0 : 1)$. Jediným inflexním bodem je nevlastní bod $(0 : 1 : 0)$ křivky a inflexní tečna je asymptota $x = 2a$. Afinní část křivky vidíme na levém obrázku 19.

Spočtěme tečnu ve směru $(1 : 1 : 0)$. Za tím účelem najdeme poláru $K_{(1:1:0)}^{[1]}$ a její průnik s K bude obsahovat právě singulární bod $(0 : 0 : 1)$ a bod $a \in K$ dotyku hledané tečny. Pak spočteme $K_a^{[2]}$, což je přímo hledaná tečna. Výsledné křivky jsou zobrazeny na pravém obrázku 19.



Obr. 19: Dioclesova cissoida a její tečna ve směru (1 : 1 : 0).

8 Dodatek

V této části jsou vytištěny zápisníky programového systému MAPLE V, které vznikly během výuky při ukázkách ilustračních příkladů. Všechny zápisníky jsou k nalezení na síti ve stejném adresáři jako tyto texty. Věřím, že si posluchači po úvodním seznámení MAPLE V oblíbí a ocení možnost interaktivní práce se systémem a experimentování na jejich základě.

8.1 Několik obrázků křivek (ag0.ms)

```
> with(plots);
```

[*animate*, *animate3d*, *conformal*, *contourplot*, *cylinderplot*, *densityplot*, *display*, *display3d*, *fieldplot*, *fieldplot3d*, *gradplot*, *gradplot3d*, *implicitplot*, *implicitplot3d*, *loglogplot*, *logplot*, *matrixplot*, *odeplot*, *pointplot*, *polarplot*, *polygonplot*, *polygonplot3d*, *polyhedraplot*, *replot*, *setoptions*, *setoptions3d*, *spacecurve*, *sparsematrixplot*, *sphereplot*, *surfdata*, *textplot*, *textplot3d*, *tubeplot*]

```
> implicitplot(x^3-y^2, x=-0.5..2, y=-2..2,grid=[50,50]);
```

```
> implicitplot(x^3+x^2-y^2, x=-1.5..2, y=-2..2,grid=[50,50]);
```

```
> implicitplot(2*x^4-3*x^2*y+y^2-2*y^3+y^4, x=-2.5..2.5, y=-1..3,
> grid=[100,100]);
```

```
> implicitplot(x^2-y^2,x=-3..3, y=-3..3,grid=[50,50]);
```

8.2 Komplexní kružnice, singulární body, tečny (ag1.ms)

```
> ph3:=(x1*y2-x2*y1)/(sqrt(x1^2+x2^2));
```

$$ph3 := \frac{x1\,y2 - x2\,y1}{\sqrt{x1^2 + x2^2}}$$

```
> -x2*ph3/(sqrt(x1^2+x2^2));
```

$$-\frac{x2\,(\,x1\,y2 - x2\,y1\,)}{x1^2 + x2^2}$$

```
> simplify(subs(x2=-x1*y1/y2, "));
```

$$y1$$

```
> x1*ph3/(sqrt(x1^2+x2^2));
```

$$\frac{x1\,(\,x1\,y2 - x2\,y1\,)}{x1^2 + x2^2}$$

```
> simplify(subs(x2=-x1*y1/y2, "));
```

$$y2$$

```
> ps3:=-v*w/sqrt(u^2+v^2);ps4:=u*w/sqrt(u^2+v^2);
```

$$ps3 := -\frac{v\,w}{\sqrt{u^2 + v^2}}$$

$$ps4 := \frac{u\,w}{\sqrt{u^2 + v^2}}$$

```
> (u*ps4-v*ps3)/sqrt(u^2+v^2);
```

$$\frac{\dfrac{u^2\,w}{\sqrt{u^2 + v^2}} + \dfrac{v^2\,w}{\sqrt{u^2 + v^2}}}{\sqrt{u^2 + v^2}}$$

```
> simplify(subs(x2=-x1*y1/y2, "));
```

$$w$$

```
> with(plots);
```

$[animate, animate3d, conformal, contourplot, cylinderplot, densityplot, display, display3d, fieldplot, fieldplot3d, gradplot, gradplot3d, implicitplot, implicitplot3d, loglogplot, logplot, matrixplot, odeplot, pointplot, polarplot, polygonplot, polygonplot3d, polyhedraplot, replot, setoptions, setoptions3d, spacecurve, sparsematrixplot, sphereplot, surfdata, textplot, textplot3d, tubeplot]$

```
> implicitplot(x^2+x^3-y^2, x=-1..1, y=-1..1, grid=[40,40]);
> f:=x^2+x^3-y^2;diff(f,x); diff(f,y);
```

$$f := x^2 + x^3 - y^2$$

$$2\,x + 3\,x^2$$

$$-2\,y$$

```
> solve({diff(f,x)=0,diff(f,y)=0,f=0},{x,y});
```

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

```
> solve(subs(x=0,y=0,diff(f,x$2)*v^2 +diff(f,x,y)*v*w +diff(f,y$2)*w^2=0),
> {v,w});
```

$$\{\, v = w, w = w \,\}, \{\, v = -w, w = w \,\}$$

```
> implicitplot({x^2+x^3-y^2, x+y, x-y}, x=-1..1, y=-1..1, grid=[40,40]);
```

8.3 Křivky v prostoru, tečny a tečné kužely (ag2.ms)

```
> with(plots):
> plot([t^2,t^3,t=-1..1]);
> f:=2*x^4 - 3*x^2*y+y^2-2*y^3+y^4;
```

$$f := 2\,x^4 - 3\,x^2\,y + y^2 - 2\,y^3 + y^4$$

```
> solve({diff(f,x)=0, diff(f,y)=0, f=0},{x,y});
```

$$\{\, x = 0, y = 0 \,\}, \{\, x = 0, y = 1 \,\}$$

```
> r:=diff(f,x,x)*u*u + diff(f,x,y)*u*v + diff(f,y,y)*v*v;
```

$$r := (\, 24\,x^2 - 6\,y \,)\,u^2 - 6\,x\,u\,v + (\, 2 - 12\,y + 12\,y^2 \,)\,v^2$$

```
> r1:=subs(x=0,y=0,r);
```

$$r1 := 2\,v^2$$

```
> r2:=subs(x=0,y=1,r);
```

$$r2 := -6\,u^2 + 2\,v^2$$

```
> implicitplot({2*x^4 - 3*x^2*y+y^2-2*y^3+y^4,y-sqrt(3)*x-1,y+sqrt(3)*x-1},
> x=-2..2, y=0..3, grid=[80,80]);
> g:=x^6-x^3*y^2-x^5;
```

$$g := x^6 - x^3\,y^2 - x^5$$

```
> solve({diff(g,x)=0,diff(g,y)=0,g=0},{x,y});
```

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

```
> implicitplot(g, x=-2..2, y=-2..2, grid=[80,80]);
> solve(u^3*v^2+10*u^5=0, {u,v});
```

$$\{v = v, u = 0\}, \left\{v = v, u = \frac{1}{10} I v \sqrt{10}\right\}, \left\{v = v, u = -\frac{1}{10} I v \sqrt{10}\right\}$$

V tomto pripade byly vsechny ostatni derivace nizsich radu v (0,0) nulove, ostatni derivace pateho radu jsou nulove take. Vychazi trojnasobna tecna x=0 a dve jednoduche imaginarni tecny.

```
> plot3d([t*(u^2-t^2),u,u^2-t^2], u=-2..2,t=-2..2);
> plot3d({[1.5*t,u+1.5,t],[-1.5*t,u+1.5,t],[t*(u^2-t^2),u,u^2-t^2]},
> u=-2..2,t=-2..2);
> plot3d({[0.5*t,u+0.5,t],[-0.5*t,u+0.5,t],[t*(u^2-t^2),u,u^2-t^2]},
> u=-2..2,t=-2..2);
> spacecurve([t,t^2,t^3], t=-1.5..1.5);
> plot3d({[x,x^2,u],[x,u,x^3]}, x=-1..1,u=-1..1);
```

8.4 Deformace singularit křivek (ag3.ms)

```
> f:= x^3 - y^2;
```

$$f := x^3 - y^2$$

```
> with(plots):
> implicitplot(f,x=0..1, y=-1..1, grid=[40,40]);
> plot3d(f, x=-1..1, y=-1..1);
> g:=x^3 + delta*x^2 - y^2;
```

$$g := x^3 + \delta x^2 - y^2$$

```
> obr:=seq(implicitplot(g, x=-1..1.5, y=-1..1,
> grid=[40,40]), delta=[-1,-0.65,-0.35,0,0.35,0.65,1]):
> display([obr], insequence=false);
> h:=x^3+x^2-y^2 - epsilon;
```

$$h := x^3 + x^2 - y^2 - \varepsilon$$

```
> obr:=seq(implicitplot(h, x=-1..1.5, y=-1..1, grid=[40,40]),
> epsilon=[-1,-0.65,-0.35,0,0.03,0.06,0.1,3.9/27,0.2]);
> display([obr], insequence=false);
```

8.5 Příklady ploch v $\mathbb{R}^3$ (ag4.ms)

```
> with(plots):
> implicitplot3d(x^2+y^2-z, x=-1..1, y=-1..1, z=-2..2);
> implicitplot3d(x^2+y^2-z^2, x=-0.1..0.1, y=-0.1..0.1, z=-0.1..0.1,
> grid=[15,15,15]);
> implicitplot3d(x^2+y^2-z^2+z^3, x=-1.5..1.5, y=-1.5..1.5,
```

```
> z=-2..2, grid=[20,20,20]);
> implicitplot3d(x*y+z^3, x=-1..1, y=-1..1, z=-1..1, grid=[20,20,20]);
> implicitplot3d(x*y+z^3, x=-10..10, y=-10..10, z=-5..5,
> grid=[20,20,20]);
> implicitplot3d(x^2-y^2*z, x=-8..8, y=-2..2, z=-2..2, grid=[20,20,20]);
> implicitplot3d(x^2+y^2-z^3, x=-1..1, y=-1..1, z=0..1.3,
> grid=[20,20,20]);
> implicitplot3d(x^2-y^2*z^2+z^3, x=-1..1, y=-1..1, z=-1..2,
> grid=[20,20,20]);
```

8.6 Tečné prostory a kužely ploch a křivek (ag5.ms)

```
> with(plots):
> implicitplot3d(x^2-y^2*z^2+z^3, x=-1..1, y=-1..1, z=-1..1,
> grid=[20,20,20]);
> plot3d([t*(u^2-t^2), u, u^2-t^2], u=-1..1, t=-1..1);
> k1:=spacecurve([t,t^2,t^3], t=-1.5..1.5):
> k2:=plot3d([1+s,1+2*s,1+r], s=-0.5..0.5, r=-0.5..0.5):
> k3:=plot3d([1+s, 1+r, 1+3*s], s=-0.5..0.5, r=-0.5..0.5):
> display({k1,k2,k3});
> plot3d([u*v,v, u^2], u=-1.2..1.2, v=-1.2..1.2);
```

8.7 Afinní variety (ag6.ms)

```
> f:=x^2-y^2-1;
```

$$f := x^2 - y^2 - 1$$

```
> diff(f,x);
```

$$2\,x$$

```
> diff(f,y);
```

$$-2\,y$$

```
> with(plots):
> implicitplot(f,x=-3..3,y=-3..3);
> p1:=":
> p2:=implicitplot(x+y-1,x=-3..3,y=-3..3):
> display({p1,p2});
> {x,x,y};
```

$$\{x, y\}$$

```
> [x,y,x];
```

$$[x, y, x]$$

```
> f:=y^2-x^3+3;
```

$$f := y^2 - x^3 + 3$$

```
> fx:=diff(f,x);
```

$$fx := -3\,x^2$$

```
> fy:=diff(f,y);
```

$$fy := 2\,y$$

```
> solve({f=0,fx=0,fy=0},{x,y});
> p1:=implicitplot(f,x=1.5..2.5,y=2..3):
> ?subs
> subs(x=2,y=sqrt(5),f);
```

$$0$$

```
> t:=subs(x=2,y=sqrt(5),fx)*(x-2)+subs(x=2,y=sqrt(5),fy)*(y-sqrt(5));
```

$$t := -12\,x + 24 + 2\sqrt{5}\,\left(y - \sqrt{5}\right)$$

```
> p2:=implicitplot(t,x=1.5..2.5,y=2..3):
> display({p1,p2});
> f1:=y^2-x^3+6*x^2-9*x;
```

$$f1 := y^2 - x^3 + 6\,x^2 - 9\,x$$

```
> fx:=diff(f1,x);
```

$$fx := -3\,x^2 + 12\,x - 9$$

```
> fy:=diff(f1,y);
```

$$fy := 2\,y$$

```
> solve({f1=0,fx=0,fy=0},{x,y});
```

$$\{x = 3, y = 0\}$$

```
> p1:=implicitplot(f1,x=0..6,y=-3..3):
> display(p1);
> subs(x=1,y=2,f1);
```

$$0$$

```
> t:=subs(x=1,y=2,fx)*(x-1)+subs(x=1,y=2,fy)*(y-2);
```

$$t := 4\,y - 8$$

```
> p2:=implicitplot(t,x=0..6,y=-3..3):
> display({p1,p2});
> fxx:=diff(f1,x,x);
```

$$fxx := -6\,x + 12$$

```
> fxy:=diff(f1,x,y);
```

$$fxy := 0$$

```
> fyy:=diff(f1,y,y);
```

$$fyy := 2$$

```
> tk:=subs(x=3,y=0,fxx)*(x-3)^2+subs(x=3,y=0,fxy)*(x-3)*y+
> subs(x=3,y=0,fyy)*y^2;
```

$$tk := -6\,(\,x-3\,)^2 + 2\,y^2$$

```
> p3:=implicitplot(tk,x=0..6,y=-3..3):
> display({p1,p3});
```

8.8 Projektivní rozšíření rovinných křivek (ag7.ms)

```
> homog:= proc(poly,stupen)
> expand(z^stupen*subs(x=x/z,y=y/z, poly)) end;

homog :=

proc(poly,stupen)
    expand(z^stupen*subs(x = x/z,y = y/z,poly))
end
```

```
> g:=homog(y-x^2,2);
```

$$g := z\,y - x^2$$

```
> dehomog := proc(poly,prom) subs(prom=1,poly) end;

dehomog :=

    proc(poly,prom) subs(prom = 1,poly) end
```

```
> dehomog(g, z);
```

$$y - x^2$$

```
> homog(x^2*y-y^3, 3);
```

$$x^2\,y - y^3$$

```
> hom := proc(poly, stupen, n)
> expand(subs(seq(x.i=x.i/x0, i=1..n),poly)*x0^stupen) end;
Warning, `i` is implicitly declared local


hom :=

proc(poly,stupen,n)
local i;
    expand(
        subs(seq(x.i = x.i/x0,i = 1 .. n),poly)
        *x0^stupen)
end
```

```
> hom(x3-x1^3, 3, 3);
```

$$x0^2\,x3 - x1^3$$

```
> dehomog(", x3);
```

$$x0^2 - x1^3$$

```
> f:=y-x^3+x;
```

$$f := y - x^3 + x$$

```
> g:=homog(f,3);
```

$$g := z^2\,y - x^3 + z^2\,x$$

```
> solve({g, diff(g,x), diff(g,y), diff(g,z)}, {x,y,z});
```

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

```
> h:=dehomog(g,y);
```

$$h := z^2 - x^3 + z^2\,x$$

```
> solve({g, diff(g,x), diff(g,z)}, {x,z});
```

$$\{x = 0, z = 0\}$$

```
> with(plots):
> implicitplot(h, x=-5..5, z=-5..5, grid=[50,50]);
> f1:=y-x^3; g1:=homog(f1,3); h1:=dehomog(g1,y);
```

$$f1 := y - x^3$$

$$g1 := z^2\,y - x^3$$

$$h1 := z^2 - x^3$$

```
> implicitplot(h1, x=0..4, z=-4..4, grid=[50,50]);
> f2:=y-x^4; g2:=homog(f2,4); h2:=dehomog(g2,y);
```

$$f2 := y - x^4$$

$$g2 := z^3\, y - x^4$$

$$h2 := z^3 - x^4$$

```
> implicitplot(h2, x=-2..2, z=0..4, grid=[50,50]);
> f:=y^2-x^3+6*x^2-9*x;
```

$$f := y^2 - x^3 + 6\, x^2 - 9\, x$$

```
> implicitplot(f, x=0..4, y=-3..3, grid=[30,30]);
> solve({f, diff(f,x), diff(f,y)},{x,y});
```

$$\{\, y = 0, x = 3\,\}$$

```
> D2:=subs(x=3,y=0,diff(f,x,x)*u^2 + 2*diff(f,x,y)*u*v +
> diff(f,y,y)*v^2);
```

$$D2 := -6\, u^2 + 2\, v^2$$

```
> solve(", {u,v});
```

$$\left\{u = u, v = \sqrt{3}\, u\right\}, \left\{u = u, v = -\sqrt{3}\, u\right\}$$

```
> g:=homog(f,3);
```

$$g := z\, y^2 - x^3 + 6\, z\, x^2 - 9\, z^2\, x$$

```
> h:=dehomog(g,y);
```

$$h := z - x^3 + 6\, z\, x^2 - 9\, z^2\, x$$

```
> solve({h,diff(h,x), diff(h,z)}, {x,z});
> implicitplot(h, x=-3..3, z=-3..3, grid=[50,50]);
> diff(h,x); diff(h,z);
```

$$-3\, x^2 + 12\, z\, x - 9\, z^2$$

$$1 + 6\, x^2 - 18\, z\, x$$

```
> f:=x^6 -x*y +y^6;
```

$$f := x^6 - x\, y + y^6$$

```
> sing := proc(poly) solve({poly, diff(poly,x), diff(poly,y)},
> {x,y}) end;
```

```
sing :=
```

```
proc(poly)
    solve(
        {poly,diff(poly,x),diff(poly,y)},{x,y})
end
```

```
> sing(f);
```

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

```
> implicitplot(f, x=-1..1, y=-1..1, grid=[50,50]);
> dehomog(homog(f,6),y);
```

$$x^6 - z^4\,x + 1$$

```
> implicitplot(", x=-2..2, z=-2..2, grid=[30,30]);
> f:=x^3-z*x*y +y^3;
```

$$f := x^3 - z\,x\,y + y^3$$

```
> sing3 := proc(poly) solve({poly, diff(poly,x), diff(poly,y),
> diff(poly, z)}, {x,y,z}) end;

sing3 :=

proc(poly)
    solve({
    poly,diff(poly,x),diff(poly,y),diff(poly,z)
    },{z,x,y})
end
```

```
> sing3(f);
```

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

```
> h:=dehomog(f, z);
```

$$h := x^3 - x\,y + y^3$$

```
> implicitplot(h, x=-1..1, y=-1..1, grid=[50,50]);
> implicitplot3d(f, x=-1..1, y=-1..1, z=0..1, grid=[25,25,25]);
```

8.9 Projektivní rozšíření prostorových křivek (ag8.ms)

```
> homog:= proc(poly,stupen)
> expand(z^stupen*subs(x=x/z,y=y/z, poly)) end;

homog :=

proc(poly,stupen)
    expand(z^stupen*subs(x = x/z,y = y/z,poly))
end
```

```
> dehomog := proc(poly,prom) subs(prom=1,poly) end;
```

```
dehomog :=

    proc(poly,prom) subs(prom = 1,poly) end
```

```
> hom := proc(poly, stupen, n)
> expand(subs(seq(x.i=x.i/x0, i=1..n),poly)*x0^stupen) end;
Warning, `i` is implicitly declared local
```

```
hom :=

proc(poly,stupen,n)
local i;
    expand(
        subs(seq(x.i = x.i/x0,i = 1 .. n),poly)
        *x0^stupen)
end
```

```
> hom(x3-x1^3, 3, 3);
```

$$x0^2\,x3 - x1^3$$

```
> dehomog(", x3);
```

$$x0^2 - x1^3$$

$$f := y - x^3 + x$$

```
> with(plots):
```

```
> singn := proc(poly, prom) solve({poly, seq(diff(poly,i),i=prom)},
> {op(prom)}) end;
Warning, `i` is implicitly declared local
```

```
singn :=

   proc(poly,prom)
   local i;
       solve({poly,seq(diff(poly,i),i = prom)},
           {op(prom)})
   end
```

```
> f:= x3-x1*x2; singn(f,[x1,x2,x3]);
```

$$f := x3 - x1\,x2$$

```
> hom(f,2,3);
```

$$x0\,x3 - x1\,x2$$

```
> dehomog(",x1);
```

$$x0\,x3 - x2$$

```
> singn(",[x0,x3,x2]);
> f:=x3-x1^2*x2;
```

$$f := x3 - x1^2\,x2$$

```
> plot3d(x1^2*x2, x1=-2..2, x2=-2..2);
> singn(f,[x1,x2,x3]);
> hom(f,3,3);
```

$$x0^2\,x3 - x1^2\,x2$$

```
> dehomog(",x3);
```

$$x0^2 - x1^2\,x2$$

```
> implicitplot3d(", x1=-2..2, x2=-2..2, x0=-2..2);
> singn("",[x0,x1,x2]);
```

$$\{\,x1 = 0, x2 = x2, x0 = 0\,\}$$

8.10 Homogenní polynomy (resultanty) (ag9.ms)

```
> f:=x*y-1:g:=x^2+y^2-4:
> resultant(f,g,x);
```

$$y^4 - 4\,y^2 + 1$$

```
> solve({"},y);
```

$$\left\{y = \frac{1}{2}\sqrt{6} + \frac{1}{2}\sqrt{2}\right\}, \left\{y = \frac{1}{2}\sqrt{6} - \frac{1}{2}\sqrt{2}\right\}, \left\{y = -\frac{1}{2}\sqrt{6} + \frac{1}{2}\sqrt{2}\right\},$$
$$\left\{y = -\frac{1}{2}\sqrt{6} - \frac{1}{2}\sqrt{2}\right\}$$

```
> sol:=["]:
> for a in sol do solve({subs(a,f),subs(a,g)}, x) od;
```

$$\left\{x = \frac{1}{2}\sqrt{6} - \frac{1}{2}\sqrt{2}\right\}$$

$$\left\{x = \frac{1}{2}\sqrt{6} + \frac{1}{2}\sqrt{2}\right\}$$

$$\left\{x = -\frac{1}{2}\sqrt{6} - \frac{1}{2}\sqrt{2}\right\}$$

$$\left\{x = -\frac{1}{2}\sqrt{6} + \frac{1}{2}\sqrt{2}\right\}$$

```
> f:=x*z^2 - y^3 + x*y^2;
```

$$f := x\,z^2 - y^3 + x\,y^2$$

```
> gz:=subs(z=1, ");
```

$$gz := x - y^3 + x\,y^2$$

```
> solve({gz, diff(gz,x), diff(gz,y)}, {x,y});
> with(plots): implicitplot(gz, x=-2..2, y=-2..2);
> gy:= subs(y=1, f);
```

$$gy := x\,z^2 - 1 + x$$

```
> solve({gy, diff(gy,x), diff(gy,z)},{x,z});
> f:=expand((x+y+z)^3 - 27*x*y*z);
```

$$f := x^3 + 3\,x^2\,y + 3\,x^2\,z + 3\,x\,y^2 - 21\,x\,y\,z + 3\,x\,z^2 + y^3 + 3\,y^2\,z + 3\,y\,z^2 + z^3$$

```
> gz:=subs(z=1, f);
```

$$gz := x^3 + 3\,x^2\,y + 3\,x^2 + 3\,x\,y^2 - 21\,x\,y + 3\,x + y^3 + 3\,y^2 + 3\,y + 1$$

```
> solve({gz, diff(gz,x), diff(gz,y)}, {x,y});
```

$$\{x = 1, y = 1\}$$

```
> hess:= diff(gz,x,x)*u^2 + 2*diff(gz,x,y)*u*v + diff(gz, y, y)*v^2;
```

$$hess := (6\,x + 6\,y + 6)\,u^2 + 2\,(6\,x + 6\,y - 21)\,u\,v + (6\,x + 6\,y + 6)\,v^2$$

```
> hess:=subs(x=1,y=1,  hess);
```

$$hess := 18\,u^2 - 18\,u\,v + 18\,v^2$$

```
> solve({hess}, {u,v});
```

$$\{u = RootOf(\_Z^2 - \_Z\,v + v^2), v = v\}$$

```
> implicitplot(gz, x=0..2, y=0..2);
> f:= x*y^2+ y*z^2 + z*x^2 + x^2*y + y^2*z + z^2*x + alpha*x*y*z;
```

$$f := x\,y^2 + y\,z^2 + x^2\,z + x^2\,y + y^2\,z + x\,z^2 + \alpha\,x\,y\,z$$

```
> gz:=subs(z=1,f);
```

$$gz := x\,y^2 + y + x^2 + x^2\,y + y^2 + x + \alpha\,x\,y$$

```
> solve({gz, diff(gz,x), diff(gz,y)}, {x,y,alpha});
```

$$\{\alpha = 2, x = -1, y = 1\}, \{\alpha = 2, x = -1, y = -1\}, \{x = 1, \alpha = 2, y = -1\}, \{x = 1, \alpha = -6, y = 1\}, \{y = RootOf(\_Z^2 + \_Z + 1), x = -1 - RootOf(\_Z^2 + \_Z + 1), \alpha = 3\}$$

```
> gz6:=subs(alpha=-6,gz);
```

$$gz6 := x\,y^2 + y + x^2 + x^2\,y + y^2 + x - 6\,x\,y$$

```
> hess:=subs(x=1,y=1,diff(gz6,x,x)*u^2 + 2*diff(gz6,x,y)*u*v +
> diff(gz6, y,y)*v^2);
```

$$hess := 4\,u^2 - 4\,u\,v + 4\,v^2$$

```
> solve({hess}, {u,v});
```

$$\{u = RootOf(\_Z^2 - \_Z\,v + v^2), v = v\}$$

8.11 Inflexe rovinných křivek (ag10.ms)

```
> F:=x^3+y^3-3*a*x*y*z;
```

$$F := x^3 + y^3 - 3\,a\,x\,y\,z$$

```
> param:=[3*a*t/(1+t^3), 3*a*t^2/(1+t^3), t=-.7..15];
```

$$param := \left[3\,\frac{a\,t}{1+t^3}, 3\,\frac{a\,t^2}{1+t^3}, t = -.7..15\right]$$

```
> ob2:=plot(subs(a=1,param)):ob1:=plot(subs(a=2,param)):
> with(plots):
> display([ob1,ob2]);
> f:=subs(z=1, F);
```

$$f := x^3 + y^3 - 3\,a\,x\,y$$

```
> solve({f, diff(f,x), diff(f,y)},{x,y});
```

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

```
> g:=subs(x=1,F);
```

$$g := 1 + y^3 - 3\,a\,y\,z$$

```
> bod:=solve({g, z},{y,z});
```

$$bod := \{z = 0, y = -1\}, \{z = 0, y = RootOf(\_Z^2 - \_Z + 1)\}$$

```
> der:=subs(x=1,z=0,y=-1,[diff(F,x),diff(F,y),diff(F,z)]);
```

$$der := [3, 3, 3\,a]$$

```
> hess:=linalg[matrix](3,3,[diff(F,x,x),diff(F,x,y),diff(F,x,z),
> diff(F,y,x),diff(F,y,y),diff(F,y,z),diff(F,z,x),diff(F,z,y),
> diff(F,z,z)]);
```

$$hess := \begin{bmatrix} 6\,x & -3\,a\,z & -3\,a\,y \\ -3\,a\,z & 6\,y & -3\,a\,x \\ -3\,a\,y & -3\,a\,x & 0 \end{bmatrix}$$

```
> H:=linalg[det](hess);
```

$$H := -54\,x^3\,a^2 - 54\,a^3\,z\,y\,x - 54\,a^2\,y^3$$

```
> solve({F,H},{x,y,z});
```

$$\{y = y, z = 0, x = -y\}, \{y = y, z = 0, x = RootOf(\_Z^2 - \_Z\,y + y^2)\},$$
$$\{y = 0, x = 0, z = z\}$$

```
> solve({H,diff(H,x),diff(H,y),diff(H,z)},{x,y,z});
```

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

8.12 Poláry rovinných křivek (ag11.ms)

```
> F:=x*(y^2+x^2) - 2*a*y^2*z;
```

$$F := x\,(y^2 + x^2) - 2\,a\,y^2\,z$$

```
> with(plots):
> implicitplot(subs(z=1,a=1,F), x=-1.5..2.5, y=-10..10,
> grid=[40,40]);
> solve({F,diff(F,x), diff(F,y), diff(F,z)},{x,y,z});
```

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

```
> f:=subs(z=1,F):solve(subs(x=0,y=0,{diff(f,x,x)*u^2+2*diff(f,x
> ,y)*u*v+diff(f,y,y)*v^2}),{u,v});
```

$$\{u = u, v = 0\}$$

```
> solve({F,z=0},{x,y,z});
```

$$\{x = 0, z = 0, y = y\}, \{z = 0, y = y, x = I\,y\}, \{x = -I\,y, z = 0, y = y\}$$

```
> tangent:=subs(x=0,y=1,z=0, diff(F,x)*X+diff(F,y)*Y+diff(F,z)*Z);
```

$$tangent := X - 2\,a\,Z$$

tecna ve smeru:

```
> Da:= proc(bod, F)
> op(1,bod)*diff(F,x)+op(2,bod)*diff(F,y)+op(3,bod)*diff(F,z) end;
```

```
Da :=

    proc(bod,F) op(1,bod)*diff(F,x)+op(2,bod)*diff(F,y)+op(3,bod)*
    diff(F,z) end
```

```
> K1:=Da([1,1,0],F);
```

$$K1 := y^2 + 3\,x^2 + 2\,x\,y - 4\,a\,y\,z$$

```
> implicitplot(subs(z=1,a=1,{F,K1}),x=-0.5..2.5, y=-1.5..1.5,
> grid=[40,40]);
> xxx:=solve(subs(a=1,{F,K1,z=1}),{x,y,z});
```

$$\begin{aligned} xxx := \{\, z = 1, x = 0, y = 0 \,\}, \Big\{ z = 1,\\ x = RootOf(\,2\,\_Z^3 - 12\,\_Z^2 + 21\,\_Z - 8\,), y =\\ -6\,RootOf(\,2\,\_Z^3 - 12\,\_Z^2 + 21\,\_Z - 8\,)^2\\ +\,19\,RootOf(\,2\,\_Z^3 - 12\,\_Z^2 + 21\,\_Z - 8\,) - 8 \Big\} \end{aligned}$$

```
> evalf(");
```

$$\{\, z = 1., x = 0, y = 0 \,\}, \{\, z = 1., x = .5243134822, y = .312528396 \,\}$$

```
> bod:=subs(op(op(2,["])),[x,y,z]);
```

$$bod := [\,.5243134822, .312528396, 1.\,]$$

```
> K2:=subs(a=1,Da(bod,Da(bod,F)));
```

$$K2 := 1.844775763\,x - 1.844775762\,y - .3906959932\,z$$

```
> implicitplot(subs(z=1,a=1,{F,K1,K2}),x=-0.5..2.5, y=-1.5..1.5,
> grid=[40,40]);
> F:=(x+z)*(x^2+y^2);
```

$$F := (\,x + z\,)(\,y^2 + x^2\,)$$