Algebraická geometrie

Bc. Lukáš Vokřínek, PhD.

9. června 2016

Obsah

Úvod

Tady bude úvod.

Lukáš Vokřínek

Sylabus přednášky

Tady bude sylabus.

1. Motivace

Algebraická geometrie zkoumá množiny řešení algebraických (polynomiálních) rovnic, resp. soustav rovnic. Ve speciálním případě lineárních rovnic dostáváme afinní geometrii a pro kvadratické rovnice pak teorii nadkvadrik.

Zabývejme se nyní o něco zajímavější množinou, tzv. Descartovým listem o rovnici

$$f(x, y) = x^2 + x^3 - y^2 = 0$$

v $\mathbb{R}^2$. Tuto křivku lze poměrně jednoduše parametrizovat: když si namalujeme její obrázek a uvědomíme si, že počátkem prochází dvě větve, dostaneme jako průnik s $y = tx$ dvojnásobný počátek a zbylý průsečík pak lze jednoduše dopočítat,

$$x^2 + x^3 - t^2x^2 = x^2(1 + x - t^2) = 0$$

dává $x = t^2-1$ a dále pak $y = tx = t(t^2-1)$. Zúžením této parametrizace na $t \in \mathbb{Q}$ dostaneme právě všechna racionální řešení rovnice $f(x, y) = 0$.

Řekneme, že křivka je *racionální*, jestliže existuje parametrizace pomocí racionálních lomených funkcí, $t \mapsto (\frac{p(t)}{r(t)}, \frac{q(t)}{r(t)})$, kde všechna $p, q, r \in \mathbb{Q}[t]$.

Jednoduchým příkladem, kde si nevystačíme s polynomy jako v případě Descartova listu, je hyperbola $xy = 1$ s parametrizací $t \mapsto (t, \frac{1}{t})$.

Podobným způsobem lze racionálně parametrizovat všechny kuželosečky. Uvažme například bod $[0, -1]$ na kružnici $x^2 + y^2 - 1 = 0$ a veďme jím opět přímku o směrnici t, tj. $y = tx - 1$. Zase bude jedním průsečíkem bod $[0, -1]$ a druhý dopočítáme,

$$x^2 + (tx - 1)^2 - 1 = x((t^2 + 1)x - 2t) = 0$$

dává $x = \frac{2t}{t^2+1}$, $y = \frac{t^2-1}{t^2+1}$. (Tento výpočet samozřejmě souvisí s popisem Pythagorejských trojúhelníků $(2st, t^2 - s^2, t^2 + s^2)$.)

Velká Fermatova věta se zabývá racionálními řešeními $x^n+y^n-1 = 0$ (ty zjevně odpovídají celočíselným řešením $x^n + y^n - z^n = 0$), konkrétně jejich neexistencí pro $n > 2$. My zde ukážeme, že výše uvedená křivka nemá racionální parametrizaci (tj. zhruba řečeno těchto řešení neexistuje moc).

Předpokládejme, že $\varphi(t) = \frac{p(t)}{r(t)}$, $\psi(t) = \frac{q(t)}{r(t)}$ je racionální parametrizace, kde $p, q, r \in \mathbb{Q}[t]$ a můžeme předpokládat, že $\gcd(p, q, r) = 1$. Platí $p(t)^n + q(t)^n - r(t)^n = 0$ a derivací podle t dostaneme $p(t)^{n-1}p'(t) + q(t)^{n-1}q'(t) - r(t)^{n-1}r'(t) = 0$. Tedy $(p^{n-1}, q^{n-1}, -r^{n-1})$ je řešením soustavy lineárních rovnic nad $\mathbb{Q}[x]$ s maticí

$$\begin{pmatrix} p & q & r \\ p' & q' & r' \end{pmatrix}.$$

Podle "Cramerova pravidla" je řešením také $(qr' - rq', rp' - pr', pq' - qp')$. Toto řešení je nenulové, protože z $rp' - pr' = 0$ plyne $(\frac{p}{r})' = 0$, tj. $\frac{p}{r}$ by muselo být konstantní, nutně pak i $\frac{q}{r}$ a nejednalo by se o parametrizaci. Tedy prostor řešení je jednorozměrný a protože $\gcd(p^{n-1}, q^{n-1}, -r^{n-1}) = 1$, mělo by být víceméně jasné, že

$$(qr' - rq', rp' - pr', pq' - qp') = h(p^{n-1}, q^{n-1}, -r^{n-1})$$

pro $h \in \mathbb{Q}[t]$ (zřejmě tento vztah platí v rozkladovém tělese $\mathbb{Q}(t)$; pokud bychom psali $h = \frac{f}{g}$ s $\gcd(f, g) = 1$, dostali bychom $g \mid p^{n-1}, q^{n-1}, r^{n-1}$ a z jejich nesoudělitelnosti pak $g = 1$). Porovnáním stupňů $\deg p = a$, $\deg q = b$, $\deg r = c$ dostáváme

$$b + c - 1 \geq \deg(qr' - rq') \geq \deg p^{n-1} = a(n - 1),$$

a anlogicky $c+a-1 \geq b(n-1)$, $a+b-1 \geq c(n-1)$; sečtením $2(a+b+c)-3 \geq (a+b+c)(n-1)$, tj. $(a + b + c)(3 - n) \geq 3$ a $n < 3$.

2. Rezultanty

Hlavním objektem našeho studia bude okruh polynomů $\mathbb{k}[x_1, \ldots, x_n]$ ve více proměnných nad tělesem $\mathbb{k}$. Z algebry víme, že se jedná o obor integrity. Pro induktivní důkazy bývá často užitečné uvažovat tento okruh jako okruh $\mathbb{k}[x_1, \ldots, x_{n-1}][x_n]$ polynomů v jedné proměnné nad okruhem $\mathbb{k}[x_1, \ldots, x_{n-1}]$. Při této identifikaci se však nezachovává stupeň polynomu – v prvním případě jej budeme značit $\deg f$, ve druhém $\deg_{x_n} f$, tj. stupeň polynomu f vzhledem k proměnné x_n. Platí $\deg(fg) = \deg f + \deg g$ (vedoucí člen fg je součinem vedoucích členů f a g a je nenulový, protože je $\mathbb{k}[x_1, \ldots, x_n]$ obor integrity).

Nechť A je okruh, přičemž všechny naše okruhy budou komutativní s jedničkou. To stejné potom platí pro okruh polynomů $A[x]$.

Věta 2.1. *Pokud A je UFD, pak také $A[x]$ je UFD.*

Před vlastním důkazem uvedeme důležité tvrzení, tzv. Gaussovo lemma, ke kterému potřebujeme následující pojmy. Pro polynom $f \in A[x]$ nad UFD A definujeme jeho *obsah* $c(f)$ jako největší společný dělitel jeho koeficientů. Řekneme, že polynom f je *primitivní*, pokud je $c(f) = 1$.

Lemma 2.2 (Gauss). *Nechť A je UFD. Pak součin primitivních polynomů je primitivní. Pro obecné polynomy f, g platí $c(fg) = c(f) \cdot c(g)$.*

Důkaz. Předpokládejme, že f, g jsou primitivní. Pro každý ireducibilní prvek $p \in A$ je $A/(p)$ obor integrity (v GCD je ireducibilní prvek prvočíslem) a protože f je nenulový v $A/(p)$ (jinak by $p \mid c(f)$), stejně tak g, je nenulový i součin fg, takže nějaký koeficient fg není dělitelný p a $p \nmid c(fg)$. Protože toto platí pro libovolný ireducibilní prvek p, je $c(fg) = 1$.

Druhé tvrzení plyne jednoduše z prvního a z vyjádření $f = c(f) \cdot g$, kde $g = f/c(f)$ je primitivní. $\square$

Důkaz Věty 2.1. Nechť $\mathbb{k}$ je podílové těleso A. Víme, že $\mathbb{k}[x]$ je UFD.

Zjevně jednotky $A[x]$ jsou právě jednotky A, který chápeme jako podokruh konstantních polynomů. Každý ireducibilní prvek $\mathbb{k}[x]$ je asociovaný primitivnímu polynomu z $A[x]$ (převedeme na společný jmenovatel a vytkneme největší společný dělitel koeficientů), přičemž tento je jednoznačný až na asociovanost v $A[x]$: jsou-li $p, q \in A[x]$ primitivní a asociované v $\mathbb{k}[x]$, tj. $q = a/b \cdot p$ pro $a, b \in A$, pak $b \mid a \cdot c(p) = a$ a symetricky také $a \mid b$.

Uvažme rozklad polynomu f v okruhu $\mathbb{k}[x]$, přičemž ireducibilní činitele budeme předpokládat primitivní z $A[x]$:

$$f = a/b \cdot p_1 \cdots p_r.$$

Podle Gaussova lemmatu 2.2 máme $b \mid a \cdot c(p_1 \cdots p_r) = a$, takže $a/b \in A$; protože A je UFD, má a/b jednoznačný rozklad na součin ireducibilních v A, tedy i v $A[x]$.

Zbývá dokázat jednoznačnost. Protože je rozklad v $\Bbbk[x]$ jednoznačný, plyne z druhého odstavce jednoznačnost činitelů p_i až na asociovanost, tedy i jednoznačnost a/b až na asociovanost. Rozklad tohoto čísla je pak jednoznačný, protože A je UFD. □

Iterací dostáváme, že také $A[x_1, \ldots, x_n] \cong A[x_1, \ldots, x_{n-1}][x_n]$ je obor s jednoznačným rozkladem. Pokud je $\Bbbk$ těleso, pak podílové těleso $\Bbbk[x_1, \ldots, x_n]$, tj. těleso racionálních funkcí, značíme symbolem $\Bbbk(x_1, \ldots, x_n)$.

Zatímco dělení obecným polynomem je nad obecným okruhem problematické, dělení *normovaným* polynomem funguje stejně jako nad tělesem – toho využijeme později. Zejména platí $p(x_0) = 0 \Leftrightarrow (x - x_0) \mid p$. Protože pro polynomy vyšších stupňů dělení se zbytkem nefunguje, nefunguje ani Eukleidův algoritmus a tedy ani Bezoutova rovnost, která v případě okruhu polynomů $\Bbbk[x]$ nad tělesem vyjadřuje největší společný dělitel jako kombinaci $\gcd(f, g) = kf + lg$.

Nyní popíšeme, kdy mají f a g nějaký společný dělitel, pro polynomy ve více proměnných nad tělesem, začneme však případem jedné proměnné. Pro polynomy $f, g \in A[x]$ definujme *Sylvesterovu matici* $\mathrm{Syl}(f, g)$ jako matici $(r + s) \times (r + s)$, kde $r = \deg f$, $s = \deg g$, pomocí koeficientů polynomů f a g,

$$f = a_r x^r + \cdots + a_0, \quad g = b_s x^s + \cdots + b_0,$$

takto:

$$\mathrm{Syl}(f, g) = \begin{pmatrix} a_r & 0 & \cdots & 0 & b_s & 0 & \cdots & 0 \\ a_{r-1} & a_r & \cdots & 0 & b_{s-1} & b_s & \cdots & 0 \\ \vdots & a_{r-1} & \ddots & 0 & \vdots & b_{s-1} & \ddots & 0 \\ a_1 & \ddots & \ddots & a_r & b_1 & \ddots & \ddots & b_s \\ a_0 & a_1 & \ddots & a_{r-1} & b_0 & b_1 & \ddots & b_{s-1} \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & & \ddots & a_1 & \vdots & & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

s koeficienty a_i v prvních s sloupcích a b_j v posledních r sloupcích (akorát a_0 v prvním sloupci a b_0 v $(s+1)$-ním sloupci nemusí být ve stejném řádku). Dále definujeme *rezultantu* f, g jako $\mathrm{Res}(f, g) = \det \mathrm{Syl}(f, g)$.

Protože jsme předpokládali, že $r = \deg f$, je $a_r \neq 0$ a analogicky $b_s = 0$. V následujícím se nám však bude hodit i rozšíření na případ, kdy některý z těchto koeficientů může být nulový. Budeme pak determinant výše uvedené matice značit $\mathrm{Res}_{r,s}(f, g)$.

Věta 2.3. *Nechť $\Bbbk$ je těleso. Pak nekonstantní polynomy $f, g \in \Bbbk[x]$ mají společný faktor (tj. $f = hf_1$, $g = hg_1$ pro nějaký nekonstantní polynom h), právě když $\mathrm{Res}(f, g) = 0$.*

Lemma 2.4. *Nechť $\Bbbk$ je těleso, $f, g \in \Bbbk[x]$ nekonstantní polynomy. Potom f, g mají společný faktor, právě když existují polynomy $k, l \in \Bbbk[x]$ takové, že $kf + lg = 0$, $k \neq 0$, $l \neq 0$, $\deg k < \deg g$, $\deg l < \deg f$.*

Důkaz. Jestliže $f = hf_1$, $g = hg_1$, stačí vzít $k = g_1$, $l = -f_1$.

Předpokládejme naopak, že pro $k \neq 0$, $l \neq 0$ je $kf + lg = 0$ a přitom $\gcd(f, g) = 1$. Potom existují $\widetilde{k}$, $\widetilde{l}$ tak, že $1 = \widetilde{k}f + \widetilde{l}g$. Po vynásobení k dostáváme

$$k = k\widetilde{k}f + k\widetilde{l}g = -\widetilde{k}lg + k\widetilde{l}g = (-\widetilde{k}l + k\widetilde{l})g.$$

Protože $k \neq 0$, dostáváme $\deg k \geq \deg g$, takže k, l nesplňují podmínku na stupeň. □

Důkaz věty. Podle předchozího lemmatu mají f, g společný faktor, právě když existují $k = c_{s-1}x^{s-1} + \cdots + c_0$, $l = d_{r-1}x^{r-1} + \cdots + d_0$ nenulové takové, že $kf + lg = 0$. Rozepsáním koeficientů dostáváme soustavu rovnic

$$\mathrm{Syl}(f,g)(c_{s-1},\ldots,c_0,d_{r-1},\ldots,d_0)^T = 0.$$

Ta má nenulové řešení, právě když $\det \mathrm{Syl}(f,g) = 0$. □

Nyní vyjádříme rezultantu pomocí kořenů polynomů f a g. Pišme tedy

$$f = a_r(x-\alpha_1)\cdots(x-\alpha_r), \qquad g = b_s(x-\beta_1)\cdots(x-\beta_s),$$

kde obecně α_i a β_j leží v algebraickém uzávěru $\Bbbk$.

Věta 2.5. *Platí* $\mathrm{Res}(f,g) = {a_r}^s {b_s}^r \prod_{i,j}(\alpha_i - \beta_j)$.

Důkaz. Pracujme v okruhu polynomů $\Bbbk[a_r,\alpha_1,\ldots,\alpha_r,b_s,\beta_1,\ldots,\beta_s]$, případně v jeho podílovém tělese. Podle Vietových vztahů

$$a_{r-k} = (-1)^k a_r \sigma_k(\alpha), \quad b_{s-l} = (-1)^l b_s \sigma_l(\beta),$$

kde $\sigma_k(\alpha)$ značí k-tý symetrický polynom v proměnných $\alpha = (\alpha_1,\ldots,\alpha_r)$. Dosazením do determinantu Sylvesterovy matice je pak zřejmé, že $\mathrm{Res}(f,g) = {a_r}^s {b_s}^r p(\alpha,\beta)$, kde p je polynom stupně rs v proměnných α_i a stupně rs v proměnných β_j (každý sloupec je dělitelný a_r nebo b_s; v levých sloupcích jsou $\sigma_k(\alpha)$, $k \le r$, v pravých se α_i nevyskytují; symetricky pro β_j). Jelikož víme, že $\mathrm{Res}(f,g) = 0$ v případě, že $\alpha_i = \beta_j$ pro nějakou dvojici i, j, platí $(\alpha_i - \beta_j) \mid p(\alpha,\beta)$ a díky jednoznačnosti rozkladu také

$$\prod\nolimits_{i,j}(\alpha_i - \beta_j) \mid p(\alpha,\beta),$$

protože všichni činitelé jsou ireducibilní a různí. Porovnáním stupňů se musí tyto polynomy rovnat až na konstantu. To, že ve skutečnosti se rovnají přesně, pak plyne například z $\mathrm{Res}(x^r,(x+1)^s) = 1$. □

Příklad 2.6. Základním příkladem je $\mathrm{Res}(f,f') = a_r \operatorname{disc}(f)$ (platí totiž, že první řádek Sylvesterovy matice je dělitelný a_r). Zřejmě pak f obsahuje násobný ireducibilní faktor, právě když $\operatorname{disc}(f) = 0$. V případě kvadratického polynomu $f = ax^2 + bx + c$ dostáváme

$$\mathrm{Res}(f,f') = \det\begin{pmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{pmatrix} = ab^2 - 2a(b^2 - 2ac) = a(-b^2 + 4ac)$$

s tedy $\operatorname{disc}(f) = -b^2 + 4ac$.

Příklad 2.7. Spočtěte diskriminant $\operatorname{disc}(x^3 + px + q)$.

Řešení. Protože je $x^3 + px + q$ normovaný, je diskriminant roven determinantu

$$\det\begin{pmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{pmatrix} = 4p^3 + 27q^2$$ ◇

Pro polynomy $f, g \in \mathbb{k}[x_1, \ldots, x_n]$ definujeme rezultantu vzhledem k proměnné x_n tak, že chápeme f, g jako polynomy v proměnné x_n nad okruhem $\mathbb{k}[x_1, \ldots, x_{n-1}]$ a značíme $\operatorname{Res}(f, g; x_n) \in \mathbb{k}[x_1, \ldots, x_{n-1}]$. Analogicky bychom mohli definovat rezultantu vzhledem k ostatním proměnným x_i.

Lemma 2.8. *Nekonstantní polynomy f, g mají společný faktor s kladným stupněm v proměnné x_n, právě když $\operatorname{Res}(f, g; x_n) = 0$.*

Důkaz. Podle předchozího je $\operatorname{Res}(f, g; x_n) = 0$ ekvivalentní tomu, že f, g mají společný faktor jako prvky $\mathbb{k}(x_1, \ldots, x_{n-1})[x_n]$. Je tedy implikace $\Rightarrow$ zřejmá. Nechť naopak $f = \frac{h}{e}\frac{f_1}{c}$, $g = \frac{h}{e}\frac{g_1}{d}$, kde $c, d, e \in \mathbb{k}[x_1, \ldots, x_{n-1}]$ a $f_1, g_1, h \in \mathbb{k}[x_1, \ldots, x_n]$ a h má kladný stupeň v proměnné x_n. Potom obsahuje h ireducibilní faktor h_1 s kladným stupněm v x_n a z

$$fec = hf_1, \qquad fed = hg_1$$

musí také $h_1 \mid fec$. Protože jsou však c, e stupně 0 v proměnné x_n, musí být $h_1 \mid f$, analogicky pak také $h_1 \mid g$. □

Zabývejme se nyní významem kořenů $\operatorname{Res}(f, g; x_n)$.

Věta 2.9. *Nechť je $\mathbb{k}$ algebraicky uzavřené těleso. Bod $(p_1, \ldots, p_{n-1}) \in \mathbb{k}^{n-1}$ je kořenem rezultanty $\operatorname{Res}(f, g; x_n)$, právě když buď*

- *$(p_1, \ldots, p_{n-1})$ je kořenem vedoucích koeficientů $f, g \in \mathbb{k}[x_1, \ldots, x_{n-1}][x_n]$ nebo*
- *existuje $p_n \in \mathbb{k}$ tak, že $f(p_1, \ldots, p_{n-1}, p_n) = 0 = g(p_1, \ldots, p_{n-1}, p_n)$.*

Důkaz. Zabývejme se $\operatorname{Res}_{r,s}(f, g)$. V případě, že $b_s = 0$, platí

$$\operatorname{Res}_{r,s}(f, g) = a_r \operatorname{Res}_{r,s-1}(f, g)$$

a v případě, že $a_r = 0$, platí podobně $\operatorname{Res}_{r,s}(f, g) = (-1)^s b_s \operatorname{Res}_{r-1,s}(f, g)$.

Je-li nyní $(p_1, \ldots, p_{n-1})$ libovolné a $r = \deg_{x_n} f$, $s = \deg_{x_n} g$, pak

$$\operatorname{Res}(f, g; x_n)(p_1, \ldots, p_{n-1}) = \operatorname{Res}_{r,s}(f(p_1, \ldots, p_{n-1}, -), g(p_1, \ldots, p_{n-1}, -))$$

a toto je rovno buď

- 0 v případě, že jsou vedoucí koeficienty obou $f(p_1, \ldots, p_{n-1}, -)$, $g(p_1, \ldots, p_{n-1}, -)$ nulové, nebo
- nenulovému konstantnímu násobku $\operatorname{Res}(f(p_1, \ldots, p_{n-1}, -), g(p_1, \ldots, p_{n-1}, -))$; v tomto případě je tedy hodnota nulová, právě když mají tyto polynomy společný faktor, tedy společný kořen. □

Důsledek 2.10. *Nechť $\mathbb{k}$ je algebraicky uzavřené těleso. Pokud f, g nemají společný faktor, mají rovnice $f(x, y) = 0$ a $g(x, y) = 0$ pouze konečně mnoho společných řešení.*

Důkaz. Předpokládejme, že rovnice ze zadání mají nekonečně mnoho společných řešení. Nechť tato společná řešení mají nekonečně mnoho různých prvních souřadnic. Potom $\operatorname{Res}(f, g; y) \in \mathbb{k}[x]$ má nekonečně mnoho kořenů, a proto je nulový. To ale znamená, že f, g mají společný faktor (kladného stupně v proměnné x). □

Příklad 2.11. Mají $f = xy - 1$, $g = x^2 + y^2 - 4$ společný faktor?

Řešení. Spočítáme $\mathrm{Res}(f,g;x) = y^2(y^2-4)+1 \neq 0$ a $\mathrm{Res}(f,g;y) = x^2(x^2-4)+1 \neq 0$, takže nemají. ◇

Příklad 2.12. Spočtěte společná řešení rovnic $x^2+y^2-4=0$, $16x^2+y^2-16=0$.

Řešení. Spočítáme $\mathrm{Res}(f,g;x) = -9(5y^2-16)^2$. Platí, že $\mathrm{Res}(f,g;x)$ je nulové v $y=y_0$, právě když $f(-,y_0)$, $g(-,y_0)$ mají společný kořen, tj. právě když $f=0$, $g=0$ mají společné řešení s $y=y_0$. V našem případě tak dostáváme $y=\pm\frac{4}{\sqrt{5}}$. Analogicky bychom dostali $\mathrm{Res}(f,g;y) = 9(5x^2-4)$, tj. $x=\pm\frac{2}{\sqrt{5}}$. Obecnější metodu, fungující pro více polynomů, probereme později. ◇

Příklad 2.13. Spočtěte diskriminant $x^2+2xy^2+y+1 \in \mathbb{C}[y][x]$. Interpretujte kořeny tohoto diskriminantu.

Řešení. Protože je polynom normovaný, je diskriminant roven determinantu

$$\det\begin{pmatrix} 1 & 2 & 0 \\ 2y^2 & 2y^2 & 2 \\ y+1 & 0 & 2y^2 \end{pmatrix} = 4(-y^4+y+1).$$

Kořeny jsou ta y_0, pro něž $f(-,y_0)$ má násobný kořen; z Bezoutovy věty bude jasné, že to jsou právě horizontální přímky $y=y_0$, které se „dotýkají“ křivky $f(x,y)=0$ (další možnost by byla, že protínají křivku v jejím singulárním bodě). ◇

** **Věta 2.14.** *Existují nenulové polynomy $k,l \in \Bbbk[x_1,\dots,x_n]$ takové, že $\mathrm{Res}(f,g;x_n) = kf+lg$ a pro stupně v proměnné x_n platí $\deg_{x_n} k < \deg_{x_n} g$, $\deg_{x_n} l < \deg_{x_n} f$.*

Důkaz. V případě, že f, g mají společný faktor kladného stupně v proměnné x_n, tj. $f=hf_1$, $g=hg_1$, tvrzení plyne z $\mathrm{Res}(f,g;x_n) = 0 = g_1f+(-f_1)g$.

Nechť jsou naopak f, g nesoudělné jako prvky $\Bbbk(x_1,\dots,x_{n-1})[x_n]$. Pak řešme soustavu $\widetilde{k}f+\widetilde{l}g = \mathrm{Res}(f,g;x_n)$, tj.

$$\mathrm{Syl}(f,g)(c_{m-1},\dots,c_0,d_{n-1},\dots,d_0)^T = (0,\dots,0,\mathrm{Res}(f,g;x_n))^T.$$

Podle Cramerova pravidla

$$c_j = \frac{\det(-)}{\mathrm{Res}(f,g;x_n)}, \quad d_i = \frac{\det(-)}{\mathrm{Res}(f,g;x_n)},$$

přičemž každý čitatel je $\mathrm{Res}(f,g;x_n)$-násobkem jistého minoru Sylvesterovy matice (díky tvaru pravé strany) a všechny podíly c_j, d_i tedy leží v $\Bbbk[x_1,\dots,x_{n-1}]$. □

3. Bezoutova věta

Budeme značit $\mathbb{A}^n$ množinu $\Bbbk^n$ chápanou jako afinní prostor nad $\Bbbk$, zatímco $\Bbbk^n$ budeme používat pro stejnou množinu chápanou jako vektorový prostor. V následujícím bude hrát zásadní roli vztah mezi polynomy, tj. prvky $F \in \Bbbk[x_1,\dots,x_n]$ a polynomiálními funkcemi $f\colon \mathbb{A}^n \to \Bbbk$, $(p_1,\dots,p_n) \mapsto f(p_1,\dots,p_n)$. Volba souřadnic na $\mathbb{A}^n$ zadává interpretaci proměnných

x_i jako afinních funkcí na $\mathbb{A}^n$ (standardně je x_i funkce posílající bod na jeho i-tou souřadnici) a takto dostáváme homomorfismus okruhů

$$\Bbbk[x_1, \ldots, x_n] \to \mathrm{Map}(\mathbb{A}^n, \Bbbk).$$

Zjevně výsledná polynomiální funkce závisí na zvolených souřadnicích. Algebraicky odpovídá afinní změna souřadnic $x = Ay + b$ tomu, že veškeré polynomy přepíšeme do nových proměnných $x_i = \sum a_{ij} y_j + b_i$ (navíc jsou možné i obecnější změny souřadnic).

Zobecněním známé věty pro polynomy v jedné proměnné je následující tvrzení.

Tvrzení 3.1. *Je-li $\Bbbk$ nekonečné těleso (zejména je-li $\Bbbk$ algebraicky uzavřené), pak každý polynom je jednoznačně určen svou polynomiální funkcí.*

Důkaz. Jelikož je přiřazení $F \mapsto f$ zjevně homomorfismus okruhů, stačí se zabývat případem, kdy $f = 0$ a dokázat, že pak i $F = 0$. Pišme $F \in \Bbbk[x_1, \ldots, x_{n-1}][x_n]$ ve tvaru

$$F = G_r {x_n}^r + \cdots + G_1 x_n + G_0,$$

kde $G_i \in \Bbbk[x_1, \ldots, x_{n-1}]$. Podle předpokladu má polynom $F(p_1, \ldots, p_{n-1}, -) \in \Bbbk[x_n]$, vzniklý dosazením za proměnné $x_1, \ldots, x_{n-1}$, nulové hodnoty a je tedy nulový, tj. $G_i(p_1, \ldots, p_{n-1}) = 0$. Indukcí pak musí platit $G_i = 0$ a tedy i $F = 0$. □

Důsledek 3.2. *Pro každý polynom $F \in \Bbbk[x_1, \ldots, x_n]$ stupně r existují souřadnice tak, že koeficient u ${x_n}^r$ je nenulový.*

Důkaz. Píšeme-li $F = G_r + \mathrm{lot}$, kde G_r je homogenní stupně r a "lot" značí členy nižšího stupně, pak stačí volit souřadnice tak, aby $G_r(0, \ldots, 0, 1) \neq 0$; to lze, protože polynomiální funkce zadaná G_r je nenulová. □

Aplikací na součin $F = F_1 \cdots F_k$ lze najít souřadnice tak, že koeficient každého F_i u ${x_n}^{r_i}$, je nenulový, kde $r_i = \deg F_i$. Vhodnou volbou lineárního F_i lze navíc některé směry osy x_n zakázat, konkrétně ty z $\ker F_i$.

Věta 3.3 (Bezoutova věta, první verze)**.** *Nechť $\Bbbk$ je algebraicky uzavřené těleso. Pokud f, g nemají společný faktor, mají rovnice $f(x, y) = 0$ a $g(x, y) = 0$ maximálně $\deg f \cdot \deg g$ společných řešení.*

Důkaz. Již víme, že je těchto společných řešení pouze konečně mnoho. Zvolme souřadnou soustavu tak, aby žádné dva z těchto průsečíků neměly stejnou x-ovou souřadnici, a zároveň aby oba f, g jako polynomy v proměnné y byly stupňů $r = \deg f$, $s = \deg g$, tj. aby obsahovaly y^r, y^s s nenulovým koeficientem – to lze díky předchozímu důsledku a jeho následného zobecnění. Potom tyto souřadnice musí být kořeny rezultanty $\mathrm{Res}(f, g; y) \in \Bbbk[x]$. Zabývejme se nyní stupněm tohoto polynomu. Zjevně na pozici (i, j) příslušné matice je polynom stupně maximálně $i - j$ v případě $j \leq s$ a stupně maximálně $i - j + s$ v případě $j > s$. Protože druhá možnost nastává právě pro r voleb j, dostáváme pro každou permutaci $i = \sigma(j)$ stupeň odpovídajícího členu determinantu maximálně

$$\sum_{j \leq s} (\sigma(j) - j) + \sum_{j > s} (\sigma(j) - j + s) = rs.$$

Zároveň je rezultanta nenulová, protože f, g nemají společný faktor, a proto může mít maximálně rs kořenů. □

Přesnější tvrzení Bezoutovy věty bude naším hlavním cílem v této přednášce, konkrétně tvrzení, že v jistém smyslu je těchto průsečíků přesně $\deg f \cdot \deg g$. Upřesnění Bezoutovy věty je ve své podstatě podobné tvrzení, že každý polynom z $\Bbbk[x]$ stupně d má právě d kořenů. Prvně je potřeba přejít k projektivnímu rozšíření, ve kterém se vyskytují některé průsečíky, které bychom jinak vynechali (například $y = 0$, $y - 1 = 0$ má společné řešení v nekonečnu ve směru společném těmto přímkám) – na úrovni polynomů to odpovídá případu, kdy koeficient u x^d je nulový a příslušnému "kořenu $x = \infty$". Za druhé je potřeba vzít v úvahu násobnost průsečíků (na úrovni polynomů násobnost kořenů).

4. Lokalizace

Definice 4.1. *Lokální okruh* je okruh (komutativní s jedničkou) s jediným maximálním ideálem.

Věta 4.2. *Nechť A je okruh a $I \subsetneq A$ vlastní ideál. Potom I je jediný maximální ideál A, právě když $A \setminus I$ obsahuje pouze jednotky.*

Důkaz. Implikace $\Rightarrow$ je zřejmá – každá nejednotka $a \in A \setminus I$ generuje ideál (a), který je obsažem v nějakém maximálním ideálu $\mathfrak{m} \neq I$.

Naopak, nechť $A \setminus I$ obsahuje pouze jednotky. Potom I je zřejmě maximální (přidáním libovolného prvku dostaneme A) a také každý vlastní ideál $J \subsetneq A$ leží v I. □

Definice 4.3. Nechť A je okruh a $S \subseteq A$ *multiplikativní podmnožina*, tj. podmnožina splňující $1 \in S$; $x, y \in S \Rightarrow xy \in S$. Definujme na $A \times S$ relaci

$$(a_1, s_1) \sim (a_2, s_2) \quad \Leftrightarrow \quad \exists s \in S\colon (a_1 s_2 - a_2 s_1)s = 0.$$

Příslušný rozklad budeme značit $S^{-1}A$, říkáme mu *lokalizace* okruhu A vzhledem k podmnožině S, a jeho třídy značíme $[a, s] = \frac{a}{s}$. Na $S^{-1}A$ lze zavést strukturu okruhu

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}, \qquad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

Zobrazení $\lambda\colon A \to S^{-1}A$, $a \mapsto \frac{a}{1}$ je homomorfismus okruhů.

Lokalizace má následující univerzální vlastnost. Ta říká, že se jedná o univerzální okruh, kde všechny prvky $s \in S$ mají inverzi.

Věta 4.4. *Nechť $\rho\colon A \to B$ je homomorfismus okruhů takový, že $\rho(s) \in B$ je jednotka pro každé $s \in S$. Potom existuje jediný homomorfismus okruhů $\widetilde{\rho}\colon S^{-1}A \to B$ takový, že $\rho = \widetilde{\rho}\lambda$.*

$$\begin{tikzcd} A \arrow[r, "\rho"] \arrow[d, "\lambda"'] & B \\ S^{-1}A \arrow[ur, dashed, "\widetilde{\rho}"'] & \end{tikzcd}$$

Důkaz. Protože $\frac{a}{s} = \lambda(a)\lambda(s)^{-1}$, jsme nuceni položit $\widetilde{\rho}(\frac{a}{s}) = \rho(a)\rho(s)^{-1}$. Ukážeme, že je zobrazení dobře definované; to, že se jedná o homomorfismus okruhů, se ukáže podobně. Nechť tedy $\frac{a_1}{s_1} = \frac{a_2}{s_2}$, tj. existuje $s \in S$ takové, že $(a_1 s_2 - a_2 s_1)s = 0$. Proto také

$$(\rho(a_1)\rho(s_2) - \rho(a_2)\rho(s_1))\rho(s) = 0.$$

Vzhledem k tomu, že $\rho(s)$ je jednotka, je také $\rho(a_1)\rho(s_2) - \rho(a_2)\rho(s_1) = 0$, z čehož jednoduše plyne $\rho(a_1)\rho(s_1)^{-1} = \rho(a_2)\rho(s_2)^{-1}$. □

Speciálními případy jsou

- $S = \{1, a, a^2, \ldots\}$, potom $S^{-1}A$ vznikne z A přidáním inverze k prvku a, značíme jej $A[a^{-1}]$.
- $S = A \setminus \mathfrak{p}$, kde $\mathfrak{p} \subseteq A$ je prvoideál. Potom S je vskutku multiplikativní a $S^{-1}A$ značíme $A_\mathfrak{p}$ – je to lokalizace A v prvoideálu $\mathfrak{p}$.
- Zejména, pokud je A obor integrity, pak 0 je prvoideál a A_0 je podílové těleso okruhu A.

DÚ 1. Dokažte následující izomorfismy:

- $A[a^{-1}] \cong A[t]/(at - 1)$,
- $(A/I)[t] \cong A[t]/J$ a popište ideál J,
- $A/(I + J) \cong (A/I)/J'$ a popište ideál J' ve stylu "je to v zásadě J, jenom…".

Věta 4.5. *Lokalizace v prvoideálu $\mathfrak{p}$ je lokální okruh.*

Důkaz. Jednoduše se vidí, že doplněk ideálu $\mathfrak{m} = \{\frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p}\}$ se skládá z jednotek. □

Definice 4.6. Nechť A je okruh. Potom A-*modul* je komutativní grupa M společně s operací

$$M \times A \to M, \quad (x, a) \mapsto xa$$

splňující axiomy vektorového prostoru, tj.

$$\begin{aligned} x1 &= x, & (xa)b &= x(ab) \\ x(a + b) &= xa + xb, & (x + y)a &= xa + ya. \end{aligned}$$

Důležitým příkladem je ideál – ten je uzavřený na sčítání a násobení prvky okruhu.

Věta 4.7 (Nakayamovo lemma)**.** *Nechť A je lokální okruh s maximálním ideálem $\mathfrak{m}$. Nechť N je konečně generovaný A-modul takový, že $N\mathfrak{m} = N$. Potom $N = 0$.*

Důkaz. Nechť $x_1, \ldots, x_n$ generují N. Pišme

$$x_j = x_1 a_{1j} + \cdots + x_n a_{nj}$$

pro vhodná $a_{ij} \in \mathfrak{m}$. Převedením na levou stranu dostaneme $(x_1, \ldots, x_n)(E - M) = 0$, kde M je matice složená z prvků a_{ij}. Vynásobením adjungovanou maticí dostaneme

$$(x_1, \ldots, x_n) \det(E - M) = 0,$$

tedy $x_j \det(E - M) = 0$. Násobení prvkem $\det(E - M)$ tedy zadává na N nulové zobrazení. Přitom $\det(E - M) \in 1 + \mathfrak{m}$ a jedná se tedy o jednotku (neleží v $\mathfrak{m}$). Proto $N = 0$. □

5. Noetherovské okruhy

Definice 5.1. Nechť A je okruh. Řekneme, že A-modul M je *Noetherovský*, jestliže splňuje *podmínku rostoucích řetězců* pro podmoduly, tj. jestliže neexistuje ostře rostoucí posloupnost

$$M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n \subsetneq \cdots$$

podmodulů M. Speciálně řekneme, že A je Noetherovský, jesliže je Noetherovský jako A-modul, tj. jestliže je splněna podmínka rostoucích řetězců pro ideály v A.

Věta 5.2. *A-modul M je Noetherovský, právě když je každý jeho podmodul konečně generovaný.*

Důkaz. Předpokládejme, že M je Noetherovský, ale $L \subseteq M$ není konečně generovaný. Definujme induktivně posloupnost ostře rostoucí posloupnost konečně generovaných podmodulů $L_n \subseteq L$ takto: $L_0 = 0$; v indukčním kroku $L_n \neq L$, protože jinak by byl L konečně generovaný a položíme $L_{n+1} = L_n + (x_{n+1})$, kde $x_{n+1} \in L \setminus L_n$.

Předpokládejme nyní naopak, že každý podmodul M je konečně generovaný a $M_0 \subseteq M_1 \subseteq \cdots$ je posloupnost podmodulů M. Potom $M_\infty = \cup_n M_n$ je také podmodul, nechť je generovaný $M_\infty = (x_1, \ldots, x_k)$, přičemž $x_1, \ldots, x_k \in M_n$. Potom $M_n = M_{n+1} = \cdots$. □

Věta 5.3. *Nechť $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ je krátká exaktní posloupnost A-modulů. Potom M je Noetherovský, právě když jsou Noetherovské M' a M''.*

Důkaz. Pokud je M Noetherovský, pak svazy podmodulů M' a $M'' \cong M/M'$ jsou podsvazy svazu podmodulů M a neobsahují tedy nekonečný rostoucí řetězec.

Nechť naopak M', M'' jsou Noetherovské a nechť $M_0 \subseteq M_1 \subseteq \cdots$ je posloupnost podmodulů. Potom $M'_n = \alpha^{-1}(M_n)$ je konstantní pro $n \gg 0$ a stejně tak $M''_n = \beta(M_n)$. Potom ale musí být konstantní i M_n: je-li $x \in M_{n+1}$, pak $\beta(x) \in M''_{n+1} = M''_n$ a tedy $\beta(x) = \beta(y)$ pro nějaké $y \in M_n$. Analogicky, $x - y = \alpha(z)$ pro nějaké $z \in M'_n$, a proto $x = y + \alpha(z) \in M_n$. (Alternativně: inkluze $M_n \to M_{n+1}$ je rozšířením inkluzí $M'_n \to M'_{n+1}$ a $M''_n \to M''_{n+1}$, které jsou pro $n \gg 0$ izomorfismy, a podle 5-lemmatu je izomorfismus i inkluze $M_n \to M_{n+1}$, tj. $M_n = M_{n+1}$.) □

Důkaz. Nechť naopak M', M'' jsou Noetherovské a nechť $L \subseteq M$ je podmodul. Potom pro $L' = \alpha^{-1}(L)$, $L'' = \beta(L)$ dostáváme krátkou exaktní posloupnost

$$0 \to L' \to L \to L'' \to 0.$$

Protože jsou oba $L' \subseteq M'$ a $L'' \subseteq M''$ konečně generované, je konečně generovaný i L.

Důsledek 5.4. *Je-li A Noetherovský okruh, pak každý konečně generovaný modul M je Noetherovský.*

Důkaz. Protože lze součet dvou modulů vyjádřit pomocí krátké exaktní posloupnosti

$$0 \to M' \to M' \oplus M'' \to M'' \to 0,$$

je podle předpokladu a předchozí věty Noetherovský každý konečně generovaný volný modul A^n a potom i každý jeho kvocient. To jsou přesně konečně generované A-moduly. □

V následující definici je podstatný předpoklad komutativity.

Definice 5.5. *A-algebrou* budeme rozumět homomorfismus okruhů $\rho \colon A \to B$, ve všech našich případech se bude jednat o inkluzi podokruhu a bude tedy B nadokruhem A.

Příklad 5.6. $A[x_1, \ldots, x_n]$ je A-algebra.

Protože je B kanonickým způsobem B-modulem, můžeme jej zúžením skalárů podél ρ považovat také za A-modul. Alternativně můžeme A-algebru definovat jako A-modul B společně s A-bilineárním zobrazením $B \times B \to B$ (násobením), které, společně se sčítáním, dělá z B okruh.

Definice 5.7. Řekneme, že A-algebra B je *konečně generovaná*, jestliže existují $b_1, \ldots, b_n \in B$, které generují B jako A-algebru, tj. pomocí sčítání, násobení a násobení skaláry z A. Budeme psát $B = A[b_1, \ldots, b_n]$.

Řekneme, že A-algebra B je *konečná*, jestliže je B konečně generovaný A-modul (tj. existují $b_1, \ldots, b_n \in B$, které generují B pomocí sčítání a násobení skaláry z B). Budeme psát $B = A\{b_1, \ldots, b_n\}$.

Podotkněme, že konečná generovanost je ekvivalentní existenci surjektivního homomorfismus A-algeber $A[x_1, \ldots, x_n] \to B$ (ten posílá x_i na b_i a tyto generují B; je to proto, že $A[x_1, \ldots, x_n]$ je volná A-algebra na generátorech $x_1, \ldots, x_n$). Pro konečnou A-algebru existuje surjektivní homomorfismus A-modulů $A\{x_1, \ldots, x_n\} \to B$.

Věta 5.8. *Nechť A je Noetherovský okruh a B konečná A-algebra. Pak B je také Noetherovský okruh.*

Důkaz. Podle důsledku je B Noetherovský A-modul, tedy každý A-podmodul B je konečně generovaný jako A-modul. Tím spíš je každý jeho ideál (tj. B-podmodul $\Rightarrow$ A-podmodul) koečně generovaný jako ideál (tj. B-modul). $\square$

Příklad 5.9. Okruh $\mathbb{Z}$ je Noetherovský. Proto také $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ je Noetherovský.

Věta 5.10. *Nechť A je Noetherovský okruh, $S \subseteq A$ multiplikativní podmnožina. Potom také lokalizace $S^{-1}A$ je Noetherovský okruh.*

Důkaz. Připomeňme kanonické zobrazení $\lambda\colon A \to S^{-1}A$. Nechť $I \subseteq S^{-1}A$ je ideál a uvažme ideál
$$\lambda^{-1}(I) = \{a \in A \mid \lambda(a) = \tfrac{a}{1} \in I\} \subseteq A.$$
Nechť $\lambda^{-1}(I) = (a_1, \ldots, a_k)$. Potom $I = (\lambda(a_1), \ldots, \lambda(a_k))$, neboť pro $\frac{a}{s} \in I$ platí
$$\frac{a}{s} = \frac{b_1a_1 + \cdots + b_ka_k}{s} = \frac{b_1}{s}\,\lambda(a_1) + \cdots + \frac{b_k}{s}\,\lambda(a_k). \qquad \square$$

Věta 5.11 (Hilbertova věta o bázi)**.** *Je-li A Noetherovský okruh, pak také $A[x]$ je Noetherovský okruh.*

Důkaz. Nechť $I \subseteq A[x]$ je ideál. Definujme ideál
$$J = \{a \in A \mid \exists p \in I\colon p = ax^r + \mathrm{lot}\},$$
tj. ideál vedoucích koeficientů polynomů z I. Nechť $J = (a_1, \ldots, a_k)$ a zvolme polynomy $p_i \in I$ s vedoucím koeficientem a_i, můžeme předpokládat, že mají všechny stupeň r. Množina $A_{<r}[x]$ polynomů stupně menšího než r je konečně generovaný A-modul, a proto Noetherovský. Pišme $A_{<r}[x] \cap I = A\{q_1, \ldots, q_l\}$. Potom je $I = (p_1, \ldots, p_k, q_1, \ldots, q_l)$: protože každý $p \in I$ stupně menšího než r leží v $(q_1, \ldots, q_l)$, uvažme $p \in I$ stupně alespoň r. Potom $p = ax^s + \mathrm{lot}$, kde $a \in J$. Proto
$$p = (b_1a_1 + \cdots + b_ka_k)x^s + \mathrm{lot} = b_1x^{s-r}p_1 + \cdots + b_kx^{s-r}p_k + \mathrm{lot},$$
kde prvních k členů leží v $(p_1, \ldots, p_k)$ a zbytek je menšího stupně a leží v $(p_1, \ldots, p_k, q_1, \ldots, q_l)$ podle indukčního předpokladu. $\square$

Důsledek 5.12. *Nechť A je Noetherovský okruh. Pokud je B konečně generovaná A-algebra, je také B Noetherovský okruh.*

Důkaz. Platí $B \cong A[x_1, \ldots, x_n]/I$. Přitom $A[x_1, \ldots, x_n]$ je Noetherovský podle předchozí věty a proto i jeho kvocient B: svaz ideálů v $A[x_1, \ldots, x_n]/I$ je podsvazem svazu ideálů v $A[x_1, \ldots, x_n]$. □

Hilbertova věta o bázi dává naději, že bychom s ideály v okruhu polynomů $\Bbbk[x_1, \ldots, x_n]$ mohli efektivně počítat – můžeme totiž každý takový ideál popsat konečným množstvím dat, totiž jeho generátory. Otázkou samozřejmě zůstává, jak například efektivně rozhodnout, zda $x \in I$, $I = J$, spočítat $I \cap J$, atd. Ke všem těmto účelům se standardně používají Gröbnerovy báze. Gröbnerova báze obecně závisí na zvoleném uspořádání monomů v $\Bbbk[x_1, \ldots, x_n]$ a různá uspořádání se hodí k různým účelům. My se spokojíme s tzv. lexikografickým uspořádáním:

$$x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n} > x_1^{\beta_1} \cdots x_n^{\beta_n} = x^\beta,$$

právě když pro nějaké $i \geq 1$ platí $\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i$. Vzhledem k tomu, že se jedná o lineární uspořádání, můžeme hovořit o vedoucím členu polynomu $f \in \Bbbk[x_1, \ldots, x_n]$: když

$$f = a_\alpha x^\alpha + \sum_{\beta < \alpha} a_\beta x^\beta = a_\alpha x^\alpha + \mathrm{lot}$$

s $a_\alpha \neq 0$, hovoříme o $\mathrm{LC}\, f = a_\alpha$ jako o *vedoucím koeficientu*, o $\mathrm{LM}\, f = x^\alpha$ jako o *vedoucím monomu* a o $\mathrm{LT}\, f = a_\alpha x^\alpha$ jako o *vedoucím členu.*

Nechť $I \subseteq \Bbbk[x_1, \ldots, x_n]$ je ideál. Definujme $\mathrm{LT}\, I = (\mathrm{LM}\, f \mid f \in I)$, ideál generovaný vedoucími monomy polynomů z I. Zjevně se $\mathrm{LT}\, I$ skládá právě ze všech polynomů, jejichž každý člen je vedoucím členem nějakého polynomu z I.

Věta 5.13. *Nechť $I \subseteq \Bbbk[x_1, \ldots, x_n]$ je ideál a $g_1, \ldots, g_k \in I$. Jestliže $\mathrm{LT}\, I = (\mathrm{LM}\, g_1, \ldots, \mathrm{LM}\, g_k)$, tak $I = (g_1, \ldots, g_k)$. Množina prvků $g_1, \ldots, g_k \in I$ s touto vlastností vždy existuje a nazývá se* Gröbnerova báze.

Důkaz. Předpokládejme sporem, že $f \in I \smallsetminus (g_1, \ldots, g_k)$ má nejmenší možný vedoucí monom. Protože $\mathrm{LM}\, f \in \mathrm{LT}\, I$ a jedná se o monom, musí být $\mathrm{LM}\, f = x^\alpha\, \mathrm{LM}\, g_i$. Potom

$$f - \frac{\mathrm{LC}\, f}{\mathrm{LC}\, g_i} x^\alpha g_i$$

leží také v $I \smallsetminus (g_1, \ldots, g_k)$ a má menší vedoucí monom, neboť se vedoucí členy vyruší. To je spor s minimalitou.

Nechť $\mathrm{LT}\, I = (h_1, \ldots, h_l)$, potom každý člen h_j je vedoucím členem nějakého polynomu $g_i \in I$. Uvážením všech takových g_i dostaneme Gröbnerovu bázi. □

Pomocí Gröbnerovy báze lze jednoduše testovat příslušnost $f \in I$: prvně ověříme, jestli $\mathrm{LM}\, f \in \mathrm{LT}\, I$, tj. jestli je dělitelný nějakým $\mathrm{LM}\, g_i$. Pokud ne, dostáváme $f \notin I$. Pokud $\mathrm{LM}\, f = x^\alpha\, \mathrm{LM}\, g_i$, nahradíme f polynomem

$$f - \frac{\mathrm{LC}\, f}{\mathrm{LC}\, g_i} x^\alpha g_i$$

a pokračujeme s testováním.

Poznámka. Řekneme, že Gröbnerova báze ideálu I je *redukovaná*, jestliže jsou všechny g_i normované a $\mathrm{LM}\, g_i$ nedělí žádný člen g_j (je to analogie redukovaného schodovitého tvaru matice, který je zároveň speciálním případem).

Platí, že každý ideál má *jedinou* redukovanou Gröbnerovu bázi (nebudeme to dokazovat). V dalším si vysvětlíme, jak lze takovou bázi spočítat. Potom lze jednoduše testovat rovnost dvou ideálů zadaných pomocí generátorů – spočítáme redukované Gröbnerovy báze a tyto porovnáme.

5.1. Buchbergerův algoritmus

Algoritmus na hledání Gröbnerovy báze $I = (f_1, \dots, f_l)$ probíhá v krocích takto: prvně spočítáme pro f_i, f_j tzv. *S-polynom* $S(f_i, f_j)$ tak, že určíme nejmenší společný násobek x^α monomů $\mathrm{LM}\, f_i$, $\mathrm{LM}\, f_j$ a položíme

$$S(f_i, f_j) = \frac{x^\alpha}{\mathrm{LT}\, f_i} f_i - \frac{x^\alpha}{\mathrm{LT}\, f_j} f_j.$$

Poté tento polynom zredukujeme pomocí $f_1, \dots, f_l$ tak, že postupně odečítáme vhodné násobky f_k, abychom vždy přesně zrušili vedoucí člen. Pokud dostaneme nenulový polynom, jehož vedoucí člen již nyní není dělitelný žádným z f_k, přidáme jej k množině generátorů, takže se l zvětší o jedna a zvětšený systém polynomů samozřejmě také generuje I (přidaný polynom může záviset na redukci, která není jednoznačná, protože není jasné násobek kterého z f_k máme odečítat). Protože v každém kroku se zvětšuje $(\mathrm{LM}\, f_1, \dots, \mathrm{LM}\, f_l)$ a $\Bbbk[x_1, \dots, x_n]$ je Noetherovský, dospějeme po konečném počtu kroků do situace, kdy redukce všech S-polynomů jsou již nulové. Potom je naše množina generátorů Gröbnerovou bází: nechť $f \in I = (f_1, \dots, f_l)$, takže $f = p_1 f_1 + \cdots + p_l f_l$, a předpokládejme, že v tomto vyjádření f je

$$\max\{\mathrm{LM}(p_i f_i) \mid i = 1, \dots, l\}$$

nejmenší možné; vyberme index, pro který nastává maximum a označme jej i_0. Nastávají dvě možnosti:

- vedoucí členy se nevyruší, tj. $\mathrm{LM}\, f = \mathrm{LM}(p_{i_0} f_{i_0})$; pak $\mathrm{LM}\, f \in (\mathrm{LM}\, f_1, \dots, \mathrm{LM}\, f_l)$;
- vedoucí členy se vyruší; pak lze pro indexy $i \neq i_0$ s $\mathrm{LM}(p_i f_i)$ maximálním psát

$$p_i f_i - \frac{\mathrm{LC}(p_i f_i)}{\mathrm{LC}(p_{i_0} f_{i_0})} p_{i_0} f_{i_0} = q_i S(f_i, f_{i_0}) + \mathrm{lot}$$

  (S-polynom se získal jako *nejmenší* kombinace, ve které se ruší vedoucí členy – ty odpovídají vedoucím členům p_i a p_{i_0}, členy v “lot” odpovídají nevedoucím členům p_i a p_{i_0}). Podle konstrukce pak lze každý S-polynom $S(f_i, f_{i_0})$ nahradit kombinací f_j s menšími vedoucími členy, členy v “lot” už jsou tohoto tvaru; to dává spor s minimalitou.

Příklad 5.14. Spočtěte Gröbnerovu bázi $I = (f_1, f_2)$, kde $f_1 = x^3 - 2xy$, $f_2 = x^2 y + x - 2y^2$.

Řešení. V prvním kroku

$$S(f_1, f_2) = y f_1 - x f_2 = -x^2 \qquad\qquad f_3 = x^2$$

a žádná redukce není potřeba. V dalším kroku je redukce $S(f_1, f_2) = -f_3$ nulová, dále

$$S(f_1, f_3) = f_1 - x f_3 = -2xy \qquad\qquad f_4 = xy$$

$$S(f_2, f_3) = f_2 - y f_3 = x - 2y^2 \qquad\qquad f_5 = x - 2y^2$$

a opět nejsou potřeba žádné redukce. Ve skutečnosti lze nyní zahodit f_1, f_2, protože leží v (f_3, f_4, f_5). Počítejme tedy

$$\begin{aligned} S(f_3,f_4) &= yf_3 - xf_4 = 0 \\ S(f_3,f_5) &= f_3 - xf_5 = 2xy^2 \equiv 0 \\ S(f_4,f_5) &= f_4 - yf_5 = 2y^3 && f_6 = y^3 \end{aligned}$$

nyní je možné vypustit $f_3 = xf_5 + 2yf_4$ a $f_4 = yf_5 + 2f_6$. V posledním kroku

$$S(f_5,f_6) = y^3 f_5 - xf_6 = -2y^5 \equiv 0$$

Proto (f_5, f_6) je redukovaná Gröbnerova báze. ◇

Příklad 5.15. Spočtěte Gröbnerovu bázi $I = (f_1, f_2, f_3)$, kde $f_1 = x^2 + y^2 + z^2 - 1$, $f_2 = x^2 - y + z^2$, $f_3 = x - z$.

Řešení. Bude výhodné používat odečítání násobků f_i jako redukce $x^2 \equiv -y^2 - z^2 + 1$, $x^2 \equiv y - z^2$, $x \equiv z$, atd. V prvním kroku dostaneme

$$\begin{aligned} S(f_1,f_2) &= f_1 - f_2 = \underline{y^2} + y - 1 && f_4 = y^2 + y - 1 \\ S(f_1,f_3) &= f_1 - xf_3 = y^2 + z^2 - 1 + \underline{xz} \equiv y^2 + 2z^2 - 1 && f_5 = y^2 + 2z^2 - 1 \\ S(f_2,f_3) &= f_2 - xf_3 = -y + z^2 + \underline{xz} \equiv -y + 2z^2 && f_6 = y - 2z^2 \end{aligned}$$

V tomto kroku lze vypustit $f_1 = f_2 + f_4$, $f_2 = (x+z)f_3 - f_4$, $f_4 = f_5 + f_6$ takže máme

$$\begin{aligned} S(f_3,f_5) &= y^2 f_3 - xf_5 = -y^2 z - \underline{2xz^2} + x \equiv -y^2 z - 2z^3 + \underline{x} \\ &\equiv \underline{-y^2 z} - 2z^3 + z \equiv -(1 - 2z^2)z - 2z^3 + z = 0 \\ S(f_3,f_6) &= yf_3 - xf_6 = -yz + \underline{2xz^2} \equiv \underline{-yz} + 2z^3 \\ &\equiv -2z^3 + 2z^3 \equiv 0 \\ S(f_5,f_6) &= f_5 - yf_6 = 2z^2 - 1 + \underline{2yz^2} \equiv 4z^4 + 2z^2 - 1 && f_7 = z^4 + (1/2)z^2 - 1/4 \end{aligned}$$

Opět lze zahodit $f_5 = (y + 2z^2)f_6 + 4f_7$, takže Gröbnerova báze je (f_3, f_6, f_7).

Jako aplikace lze nyní vyřešit soustavu rovnic $f_1 = f_2 = f_3 = 0$. Ta je ekvivalentní soustavě $f_3 = f_6 = f_7 = 0$ a stejně jako pro lineární soustavy můžeme nyní řešit soustavu "odzadu": vyřešením rovnice $f_7 = 0$ dostaneme $z = \frac{\sqrt{-1\pm\sqrt{5}}}{2}$. Dosazením do $f_6 = 0$ pak dostaneme $y = 2z^2 = -2 \pm 2\sqrt{5}$ a dosazením do $f_3 = 0$ konečně $x = z = \frac{\sqrt{-1\pm\sqrt{5}}}{2}$. ◇

Příklad 5.16. Spočtěte Gröbnerovu bázi $I = (f_1, f_2)$, kde $f_1 = x^2 - y$, $f_2 = x^2 + (y-1)^2 - 1$.

Řešení. V prvním kroku

$$S(f_1,f_2) = f_1 - f_2 = -y^2 + y \qquad f_3 = y^2 - y$$

a žádná redukce není potřeba. V dalším kroku lze vynechat $f_2 = f_1 - f_3$, dále

$$S(f_2,f_3) = y^2 f_2 - x^2 f_3 = \underline{x^2 y} + y^4 - 2y^3 \equiv y^2 + y^4 - 2y^3 \equiv 0$$

(libovolná mocnina y^k, $k \geq 1$ se redukuje na y jen s pomocí f_3) a redukovaná Gröbnerova báze je (f_1, f_3).

V dalším textu nám bude jasné, že $\mathbb{k}[x,y]/I$ nebo ještě lépe $\mathbb{k}[x,y]/\sqrt{I}$ souvisí s nulovou množinou $f_1 = 0$, $f_2 = 0$. Ta sestává za tří bodů $[0,0]$, $[-1,1]$, $[1,1]$ a proto $\dim \mathbb{k}[x,y]/\sqrt{I} = 3$. Přitom $\dim \mathbb{k}[x,y]/I = 4$, protože bod $[0,0]$ je brán „dvakrát“, konkrétně $x(y-1) \notin I$, ale přitom $(x(y-1))^2 \in I$, tedy $x(y-1) \in \sqrt{I} \smallsetminus I$ (funkce $x(y-1)$ je nulová na výše uvedené trojici bodů, ale nikoliv do dostatečného řádu). $\diamond$

Lemma 5.17. *Jsou-li* $\mathrm{LM}(f)$, $\mathrm{LM}(g)$ *nesoudělné, pak lze* $S(f,g)$ *redukovat pomocí* f, g *na nulu.*

Důkaz. Pro jednoduchost předpokládejme, že jsou f, g normované. Podle předpokladu platí $S(f,g) = \mathrm{LM}(g)f - \mathrm{LM}(f)g$ a v každém okamžiku budeme odečítat násobek tvaru tf, kde t je člen g, nebo přičítat násobek tvaru sg, kde s je člen f tak, že se nakonec S-polynom zredukuje na $gf - fg = 0$ (pointa je, že každý člen st se vyskytuje jednou se znaménkem plus a jednou minus, přičemž vedoucím členem v libovolném okamžiku může být pouze pokud s je vedoucím v f nebo t v g). $\square$

DÚ 2. Pomocí Gröbnerovy báze vyřešte soustavu polynomiálních rovnic

$$\begin{aligned} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{aligned}$$

6. Afinní variety

Odteď budeme předpokládat, že $\mathbb{k}$ je algebraicky uzavřené těleso.

Definice 6.1. *Afinní varieta* (přesněji *afinní uzavřená množina*) je množina řešení soustavy algebraických rovnic

$$f_s(x_1, \ldots, x_n) = 0, \quad s \in S,$$

kde $S \subseteq \mathbb{k}[x_1, \ldots, x_n]$ je libovolná podmnožina. Budeme ji značit

$$V(S) = \{x \in \mathbb{A}^n \mid \forall s \in S \colon f_s(x) = 0\}.$$

Jinými slovy, $V(S)$ je množina bodů, kde se nulují všechny polynomy z S. Přímo z definice lze jednoduše odvodit, že pro ideál $I = (S)$ generovaný množinou S platí

$$V(I) = V(S)$$

a lze tedy každou afinní varietu psát ve tvaru $V(I)$, kde I je ideál. Protože je každý ideál konečně generovaný, $I = (f_1, \ldots, f_k)$, platí také $V(I) = V(f_1, \ldots, f_k)$ a každou afinní varietu lze tedy ve skutečnosti zadat konečným systémem polynomiálních rovnic.

Z teorie nadkvadrik víme, že každá nadkvadrika určuje svou rovnici jednoznačně až na násobek. Pro afinní variety máme následující jednoduchý postup jak z podmnožiny $X \subseteq \mathbb{A}^n$ vyrobit ideál (není to však přímá analogie situace pro nadkvadriky):

$$I(X) = \{f \in \mathbb{k}[x_1, \ldots, x_n] \mid \forall x \in X \colon f(x) = 0\}.$$

Je jednoduché ověřit, že se jedná vskutku o ideál, konkrétně o ideál všech polynomiálních funkcí, které se nulují na X.

Lemma 6.2. *Zobrazení V a I mají následující vlastnosti*

- *obě V a I převrací uspořádání, tj.*

$$S \subseteq T \ \Rightarrow\ V(S) \supseteq V(T), \qquad\qquad X \subseteq Y \ \Rightarrow\ I(X) \supseteq I(Y),$$

- *platí následující ekvivalence $X \subseteq V(S) \Leftrightarrow S \subseteq I(X)$,*
- *platí $S \subseteq IV(S)$ a rovnost nastává právě když S je ideál tvaru $I(X)$.*
- *platí $X \subseteq VI(X)$ a rovnost nastává právě když X je afinní varieta,*

Důkaz. První bod je triviální. V druhého bodě jsou obě strany ekvivalentní podmínce $(\forall f \in S)(\forall x \in X) f(x) = 0$. Pro třetí bod začněme s $V(S) \subseteq V(S)$ a podle druhého bodu tak $S \subseteq IV(S)$. Pokud nastává rovnost, je S zřejmě tvaru $I(X)$ pro $X = V(S)$. Pokud naopak $S = I(X)$, můžeme použít druhý bod v opačném směru a dostat $X \subseteq V(S)$ a aplikací I poté $S = I(X) \supseteq IV(S)$; opačnou inkluzi jsme již dokázali. Čtvrtý bod je obdobný třetímu. □

Předchozí lemma zejména říká, že V a I jsou inverzní na ideálech tvaru $I(X)$ a afinních varietách. Dostáváme tak:

Věta 6.3. *Zobrazení V zadává bijekci mezi ideály tvaru $I(X)$ a afinními varietami.* □

Tato věta bude naším hlavním nástrojem pro přechod mezi algebrou (ideály tvaru $I(X)$) a geometrií (afinními varietami). Naším dalším cílem bude podrobněji popsat ideály tvaru $I(X)$. Podle předchozího to jsou právě ty ideály J, pro které platí $IV(J) = J$. O něco obecněji popíšeme ideál $IV(J)$ pomocí ideálu J.

Definice 6.4. *Radikál* $\sqrt{J}$ ideálu $J \subseteq A$ je definován jako

$$\sqrt{J} = \{f \in A \mid \exists k\colon f^k \in J\}.$$

Ideál J se nazývá *radikálový*, jestliže $J = \sqrt{J}$.

Příklad 6.5. Každý prvoideál je radikálový.

Cvičení 6.6. Dokažte, že se vskutku jedná o ideál.

Příklad 6.7. Nechť $g = g_1^{k_1} \cdots g_r^{k_r}$ je rozklad $g \in \Bbbk[x_1, \dots, x_n]$ na součin ireducibilních. Potom je $\sqrt{(g)} = (g_1 \cdots g_r)$. Platí totiž

$$\exists k\colon f^k \in (g) \Leftrightarrow \exists k \forall i\colon g_i^{k_i} \mid f^k \Leftrightarrow \forall i\colon g_i \mid f \Leftrightarrow g_1 \cdots g_r \mid f$$

díky ireducibilitě g_i a tomu, že jsou navzájem různé. Zejména $\sqrt{(x^k)} = (x)$, $\sqrt{(x^2+1)} = (x^2+1)$.

Poznámka. Platí, že radikál je také roven $\sqrt{J} = \bigcap_{J \subseteq \mathfrak{p}} \mathfrak{p}$, tj. průniku všech prvoideálů obsahujících J: je-li $f \in \sqrt{J}$, pak $f \in \sqrt{\mathfrak{p}} = \mathfrak{p}$ pro každý prvoideál $\mathfrak{p} \supseteq J$ a tedy leží i v jejich průniku; naopak, pro $f \notin \sqrt{J}$, využijeme toho, že ideál, maximální mezi disjunktními s danou multiplikativní množinou S, je vždy prvoideál (to ukážeme za chvíli); stačí pak vzít multiplikativní množinu $S = \{1, f, f^2, \dots\}$ a Zornovo lemma dá ideál $\mathfrak{p} \supseteq J$, maximální disjunktní s S, který je prvoideál, a tedy $f \notin \mathfrak{p}$ a neleží tedy v průniku.

Zbývá dokázat, že pro ideál $\mathfrak{p}$, maximální disjunktní s S, a $f, g \notin \mathfrak{p}$ je také $fg \notin \mathfrak{p}$. Díky maximalitě musí $\mathfrak{p} + (f)$ i $\mathfrak{p}+(g)$ protínat S, tedy S obsahuje prvek z $\mathfrak{p}+(f)$ a z $\mathfrak{p}+(g)$ a tedy i jejich součin, který patří do $(\mathfrak{p}+(f))(\mathfrak{p}+(g)) \subseteq \mathfrak{p}+(fg)$; protože však $\mathfrak{p} \cap S = \emptyset$, musí být $fg \notin \mathfrak{p}$.

Věta 6.8 (Hilbertova věta o nulách)**.** *Nechť $\Bbbk$ je algebraicky uzavřené těleso.*

- *Maximální ideály $\Bbbk[x_1,\dots,x_n]$ jsou v bijekci s body $\mathbb{A}^n$: bodu $P = (p_1,\dots,p_n) \in \mathbb{A}^n$ odpovídá $\mathfrak{m}_P = (x_1 - p_1,\dots,x_n - p_n)$.*
- *$V(J) = \emptyset$, právě když $1 \in J$, tj. $J = \Bbbk[x_1,\dots,x_n]$.*
- *Platí $IV(J) = \sqrt{J}$.*

Poznámka. Druhý bod lze interpretovat jako úplnost nějakého logického systému: pokud soustava $\{f(x) = 0 \mid f \in S\}$ nemá řešení, tak je to proto, že z tohoto systému lze odvodit spor $1 = 0$ pomocí (jednoduchých) odvozovacích pravidel, tj. jako lineární kombinaci zadaných rovnic s polynomiálními koeficienty ($1 = g_1f_1 + \dots + g_rf_r$, kde $f_i \in S$).

DÚ 3. Nechť $\Bbbk$ je algebraicky uzavřené těleso. Studujte vztah mezi nenulovými kvadratickými polynomy $f \in \Bbbk[x_1,\dots,x_n]$ a příslušnými afinními varietami $V(f) \subseteq \mathbb{A}^n$; konkrétně se zabývejte tím, nakolik je zobrazení $f \mapsto V(f)$ injektivní. Dále proveďte analogickou studii pro kubické polynomy.

Důkaz provedeme v Sekci 8. Nyní ukážeme, že předchozí věta neplatí pro $\Bbbk = \mathbb{R}$. Konkrétně uvažme ideál $J = (x^2 + 1) \subseteq \mathbb{R}[x]$. Protože je $x^2 + 1$ ireducibilní, je J maximální a přitom není tvaru $\mathfrak{m}_P$. Zároveň platí $V(J) = \emptyset$ a také $IV(J) = \mathbb{R}[x] \neq J = \sqrt{J}$.

Důsledek 6.9. *Zobrazení V a I zadávají bijekci mezi radikálovými ideály a afinními varietami.*

Důkaz. Zbývá ukázat, že obraz I tvoří právě radikálové ideály. Přitom ale ideál J leží v obraze I, právě když $J = IV(J) = \sqrt{J}$ díky Hilbertově větě. □

Pro následující lemma připomeneme definici *součinu* ideálů: pro ideály I, J definujeme IJ jako ideál generovaný součiny gh, kde $g \in I$, $h \in J$. Protože jsou zjevně takové součiny uzavřené na násobení libovolným prvkem okruhu, lze také psát

$$IJ = \{g_1h_1 + \dots + g_rh_r \mid g_i \in I,\ h_j \in J\}.$$

Lemma 6.10. *Platí následující vztahy*

- *$\bigcap_{p\in P} V(J_p) = V(\sum_{p\in P} J_p)$,*
- *$V(I) \cup V(J) = V(I \cap J) = V(IJ)$.*

Důkaz. První bod plyne z toho, že $\sum_{p\in P} J_p$ je nejmenší ideál obsahující $\bigcup_{p\in P} J_p$, takže pravá strana je zároveň $V(\bigcup_{p\in P} J_p)$, tedy množina bodů, kde se nulují všechny polynomy ze všech J_p, což je ale zároveň levá strana.

Platí $I, J \supseteq I \cap J \supseteq IJ$ a aplikace V obrací uspořádání, tedy

$$V(I), V(J) \subseteq V(I \cap J) \subseteq V(IJ).$$

Stačí tedy ověřit $V(IJ) \subseteq V(I) \cup V(J)$. Nechť $x \in V(IJ)$, ale $x \notin V(I)$, $x \notin V(J)$. Potom existují $g \in I$, $h \in J$ takové polynomy, že $g(x) \neq 0$, $h(x) \neq 0$. Proto také $gh(x) \neq 0$, ale $gh \in J$, což je spor s $x \in V(IJ)$. □

Díky předchozímu lemmatu na $\mathbb{A}^n$ existuje topologie, jejíž uzavřené množiny jsou právě afinní variety. Nazývá se *Zariského topologie.*

Cvičení 6.11. Popište Zariského topologii na $\mathbb{A}^1$ a dokažte, že je T_1, ale není T_2 (za chvílí uvidíme, že žádný afinní prostor není Hausdorffův).

7. Ireducibilita

Definice 7.1. Neprázdný topologický prostor V se nazývá *ireducibilní*, jestliže nelze psát jako sjednocení $V = V_1 \cup V_2$, kde $V_1 \subsetneq V$, $V_2 \subsetneq V$ jsou vlastní uzavřené podmnožiny.

Ekvivalentně, průnik dvou otevřených neprázdných podmnožin je neprázdný. Ekvivalentně, každá neprázdná otevřená podmnožina je hustá (podmnožina je hustá, právě když protíná každou otevřenou neprázdnou podmnožinu – to se vidí přejítím k doplňku u charakterizace "neleží v žádné vlastní uzavřené").

Lemma 7.2. *Nechť $U \subseteq V$ je podprostor. Pokud je U otevřená neprázdná a V ireducibilní, je i U ireducibilní. Pokud je U hustá podmnožina a U ireducibilní, pak je i V ireducibilní. Zejména, pokud je U otevřená hustá, je U ireducibilní, právě když je V ireducibilní.*

Důkaz. V prvním směru, nechť $W_1, W_2 \subseteq U$ jsou dvě otevřené neprázdné podmnožiny. Jelikož je V ireducibilní, mají neprázdný průnik. Ve druhém směru, pokud jsou $W_1, W_2 \subseteq V$ dvě otevřené neprázdné, pak $U \cap W_1, U \cap W_2 \subseteq U$ jsou opět otevřené neprázdné (protože je U hustá), takže se protínají. □

Příklad 7.3. $V(x_1x_2)$ je sjednocením osy x_1 a osy x_2, tj. $V(x_1x_2) = V(x_2) \cup V(x_1)$ a tedy není ireducibilní (je reducibilní).

Věta 7.4. *Nechť V je afinní varieta. Potom V je ireducibilní, právě když $I(V)$ je prvoideál.*

Důkaz. Nechť V je ireducibilní. Předpokládejme, že $g_1g_2 \in I(V)$, ale $g_1, g_2 \notin I(V)$. Potom $V_i = V \cap V(g_i) \subsetneq V$ a přitom $V_1 \cup V_2 = V \cap (V(g_1) \cup V(g_2)) = V \cap V(g_1g_2) = V$, neboť g_1g_2 je nula na V, tj. $V \subseteq V(g_1g_2)$.

Nechť naopak $V = V_1 \cup V_2$ je sjednocením vlastních uzavřených podmnožin a zvolme $g_1 \in I(V_1) \smallsetminus I(V)$, která je nula na V_1, ale nikoliv na V (zobrazení I je injektivní na varietách, takže $I(V_1) \supsetneq I(V)$). Analogicky, nechť $g_2 \in I(V_2) \smallsetminus I(V)$. Potom g_1g_2 je nula na $V_1 \cup V_2 = V$, tedy $g_1g_2 \in I(V)$, ale $g_1, g_2 \notin I(V)$. □

Příklad 7.5. Afinní prostor $\mathbb{A}^n$ je ireducibilní, protože $I(\mathbb{A}^n) = 0$ je prvoideál (neboť $\Bbbk[x_1, \ldots, x_n]$ je obor integrity). Zejména není $\mathbb{A}^n$ Hausdorffův, protože se každé dvě neprázdné otevřené podmnožiny protínají.

DÚ 4. Dokažte následující tvrzení:

- Afinní varieta X je ireducibilní, právě když pro libovolné afinní variety X_1, X_2 platí
$$X \subseteq X_1 \cup X_2 \Longrightarrow (X \subseteq X_1 \vee X \subseteq X_2).$$
- Ideál J je prvoideál, právě když pro libovolné ideály J_1, J_2 platí
$$J \supseteq J_1J_2 \Longrightarrow (J \supseteq J_1 \vee J \supseteq J_2).$$
- Pomocí předchozích dvou tvrzení dokažte, že X je ireducibilní, právě když $I(X)$ je prvoideál (není k tomu potřeba Hilbertova věta o nulách, ale klidně ji použijte).

Definice 7.6. Topologický prostor se nazývá *Noetherovský*, jestliže neexistuje nekonečná ostře klesající posloupnost
$$X_1 \supsetneq X_2 \supsetneq \cdots$$
uzavřených podmnožin.

Věta 7.7. *Afinní prostor $\mathbb{A}^n$ se Zariského topologií je Noetherovský topologický prostor.*

Důkaz. Ostře klesající posloupnost afinních variet by aplikací I zadávala ostře rostoucí posloupnost ideálů v $\Bbbk[x_1, \ldots, x_n]$ (na afinních varietách je I injektivní). □

Cvičení 7.8. Každý Noetherovský topologický prostor je kompaktní (algebraičtí geometrové říkají kvazikompaktní, aby zdůraznili, že není Hausdorffův – někdy se kompaktním prostorem totiž rozumí kompaktní Hausdorffův).

Věta 7.9. *Každou afinní varietu $V \subseteq \mathbb{A}^n$ lze napsat jako konečné sjednocení (rozklad)*

$$V = V_1 \cup \cdots \cup V_r$$

ireducibilních afinních variet V_i, přičemž platí $V_i \not\subseteq V_j$ pro $i \neq j$ (říkáme, že je rozklad iredundantní). Takový rozklad je jednoznačný až na pořadí a V_i se nazývají ireducibilní komponenty *V.*

Důkaz. Předpokládejme sporem, že V nelze napsat jako konečné sjednocení ireducibilních. Pak zejména V nemůže být prázdná ani ireducibilní. Tedy $V = V_1 \cup V_1'$ a opět jedna z V_1, V_1' musí být reducibilní. Bez újmy na obecnosti $V_1 = V_2 \cup V_2'$ a postupně dostáváme nekonečnou ostře klesající posloupnost $V_1 \supsetneq V_2 \supsetneq \cdots$ afinních variet, což je spor s Noetherovskostí $\mathbb{A}^n$. Existuje tedy rozklad V na konečné sjednocení ireducibilních a vynecháním těch V_i obsažených v nějakém V_j, $j \neq i$, se tento stane iredundantní.

Zbývá dokázat jednoznačnost. Nechť tedy

$$V_1 \cup \cdots \cup V_r = V = W_1 \cup \cdots \cup W_s.$$

Potom $V_i = V_i \cap V = \bigcup_{j=1}^{s} V_i \cap W_j$ a díky ireducibilitě V_i musí pro nějaké j platit $V_i = V_i \cap W_j$, tj. $V_i \subseteq W_j$. Symetricky pak $W_j \subseteq V_{i'}$ a díky iredundantnosti musí být $i = i'$ a následně $V_i = W_j$. □

8. Důkaz Hilbertovy věty o nulách

Je jednoduché ukázat, že $\mathfrak{m}_P$ je maximální ideál – je to totiž přesně jádro homomorfismu $\Bbbk[x_1, \ldots, x_n] \to \Bbbk$, $F \mapsto F(p_1, \ldots, p_n)$. Substituce $y_i = x_i - p_i$ totiž dá

$$F = F(p_1, \ldots, p_n) + \sum_{|\alpha| \geq 1} a_\alpha y^\alpha$$

(jedná se o Taylorův polynom v bodě P), kde suma leží v $\mathfrak{m}_P$.

Definice 8.1. Nechť $B \subseteq A$ je podokruh. Řekneme, že A je *integrální* nad B, jestliže každý prvek A je kořenem *normovaného* polynomu s koeficienty z B.

Věta 8.2 (o Noetherovské normalizaci)**.** *Nechť A je konečně generovaná $\Bbbk$-algebra. Existuje podalgebra $B \subseteq A$ izomorfní $\Bbbk[t_1, \ldots, t_r]$ taková, že A je integrální nad B.*

Větu dokážeme později, nyní budeme směřovat k donokčení důkazu Hilbertovy věty o nulách. Budeme potřebovat ještě jednu pomocnou větu.

Věta 8.3. *Nechť $B \subseteq A$ je podokruh tělesa A takový, že A je integrální nad B. Potom B je také těleso.*

Důkaz. Nechť $b \in B$ a nechť $b^{-1} \in A$ je kořenem

$$x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0.$$

Po vynásobení b^{n-1} a dosazení b^{-1} dostáváme rovnost

$$0 = b^{-1} + b_{n-1} + \cdots + b_1 b^{n-2} + b_0 b^{n-1}$$

se všemi členy s výjimkou b^{-1} ležícími v B. Proto také $b^{-1} \in B$. □

Začněme s důkazem Hilbertovy věty o nulách. Nechť J je libovolný maximální ideál. Potom $A = \Bbbk[x_1, \ldots, x_n]/J$ je rozšíření $\Bbbk$, které je konečně generované jako algebra, tj. A vznikne z $\Bbbk$ přidáním konečně mnoha prvků a následným uzavřením na sčítání, násobení skaláry z $\Bbbk$ a násobení (nikoliv dělení!).

V důsledku předchozích dvou vět je pak $\Bbbk[t_1, \ldots, t_r] \subseteq A$ těleso, což může nastat pouze pro $r = 0$. Proto je A konečné rozšíření $\Bbbk$ a díky algebraické uzavřenosti $\Bbbk$ je triviální, tj. složení

$$\Bbbk \subseteq \Bbbk[x_1, \ldots, x_n] \xrightarrow{\pi} \Bbbk[x_1, \ldots, x_n]/J = A$$

je izomorfismus. Proto je $\pi(x_i) = \pi(p_i)$ pro nějaké $p_i \in \Bbbk$. To ale znamená $x_i - p_i \in \ker \pi = J$ a $\mathfrak{m}_P \subseteq J$. Díky tomu, že je $\mathfrak{m}_P$ maximální, musí být $J = \mathfrak{m}_P$.

Druhá část je elementární: pokud je J vlastní ideál, pak je obsažen v nějakém maximálním ideálu $\mathfrak{m}_P$ a tedy $\{P\} = V(\mathfrak{m}_P) \subseteq V(J)$.

V třetí části je inkluze $\sqrt{J} \subseteq IV(J)$ zřejmá: pokud $f^k \in J$, pak se na $V(J)$ nuluje f^k a tedy také f, tj. $f \in IV(J)$.

V opačném směru nechť $f \in IV(J)$ a uvažme následující afinní varietu v $\mathbb{A}^{n+1}$ se souřadnicemi $x_1, \ldots, x_n, t$:

$$V(J, ft - 1) = \{(x, t) \in \mathbb{A}^n \times \mathbb{A}^1 \mid x \in V(J),\ t = 1/f(x)\}.$$

Protože je však $f(x) = 0$ na $V(J)$, je tato varieta prázdná a podle druhé části Hilbertovy věty musí být $1 \in (J, ft - 1)$ neboli

$$1 = g_1(x)h_1(x, t) + \cdots + g_r(x)h_r(x, t) + (f(x)t - 1)k(x, t)$$

s $g_i(x) \in J$. Po dosazení $t = 1/f(x)$ a vynásobením vhodnou mocninou $f(x)$ tak, abychom se zbavili jmenovatelů, dostaneme

$$f(x)^k = g_1(x)\widetilde{h}_1(x) + \cdots + g_r(x)\widetilde{h}_r(x) \in J.$$

Poznámka. Máme izomorfismy

$$\begin{aligned} \Bbbk[x_1, \ldots, x_n, t]/(J, ft - 1) &\cong (\Bbbk[x_1, \ldots, x_n, t]/(J))/(ft - 1) \\ &\cong (\Bbbk[x_1, \ldots, x_n]/J)[t]/(ft - 1) \\ &\cong (\Bbbk[x_1, \ldots, x_n]/J)[f^{-1}] \end{aligned}$$

Tato lokalizace je podle Hilbertovy věty nulová, $1 = 0$, což podle definice znamená $f^k = 0$ v algebře $\Bbbk[x_1, \ldots, x_n]/J$, tj. $f^k \in J$ v okruhu polynomů.

Zbývá tak dokázat větu o Noetherovské normalizaci.

Důkaz Věty 8.2. Důkaz se provede indukcí vzhledem k počtu generátorů A. Nechť $a_1, \ldots, a_n$ generují A. Tyto prvky pak zadávají surjektivní homomorfismus $\Bbbk[x_1, \ldots, x_n] \to A$, posílající $x_i \mapsto a_i$. Pokud se jedná o izomorfismus, není co dokazovat. Nechť tedy $f \neq 0$ stupně r leží v jeho jádře J. Díky Důsledku 3.2 můžeme po případné změně souřadnic předpokládat, že koeficient u ${x_n}^r$ je nenulový, řekněme rovný jedné, tj. v okruhu $\Bbbk[x_1, \ldots, x_{n-1}][x_n]$ lze psát

$$f = x_n^r + g_{r-1}(x_1, \ldots, x_{n-1})x_n^{r-1} + \cdots + g_0(x_1, \ldots, x_{n-1}) \in J.$$

Označíme-li $B = \Bbbk[a_1, \ldots, a_{n-1}]$ podalgebru generovanou $a_1, \ldots, a_{n-1}$, máme $A = B[a_n]$ a a_n je kořenem normovaného polynomu s koeficienty v B, je tedy A konečná B-algebra.

Protože jsou zřejmě konečné algebry uzavřené na skládání ($C \subseteq B$, $B \subseteq A$ konečné algebry, pak také $C \subseteq A$ je konečná), tvrzení se dokáže indukcí pomocí následujícího lemmatu. $\square$

Lemma 8.4. *Nechť $B \subseteq A$ je konečně generovaná algebra. Potom A je integrální, právě když je konečná.*

Důkaz. Směr $\Rightarrow$ je zřejmý, neboť pro integrální $B \subseteq A$ je

$$A = B[a_1, \ldots, a_k] = B\{a_1^{j_1} \cdots a_k^{j_k} \mid 0 \leq j_i < r_i\},$$

kde r_i je stupeň libovolného normovaného polynomu nad B s kořenem a_i (lze totiž $a_i^{r_i}$ vyjádřit jako kombinaci menších mocnin).

Pro směr $\Leftarrow$ předpokládejme, že A je konečný B-modul a $a \in A$. Uvažujme na $A = B\{a_1, \ldots, a_n\}$ zobrazení dané násobením a a pišme $a_j a = \sum_{i=1}^n a_i b_{ij}$. Maticově pak

$$(a_1, \ldots, a_n)(aE - M) = 0.$$

Vynásobením maticí algebraických doplňků k $aE - M$ dostaneme

$$0 = (a_1, \ldots, a_n)(aE - M)(aE - M)^a = (a_1, \ldots, a_n) \det(aE - M)$$

a tedy $a_i \det(aE - M) = 0$. Protože je však $1 \in A$ také kombinací a_i, dostáváme také

$$\det(aE - M) = \sum a_i b_i \det(aE - M) = 0.$$

Ve výsledku je pak a kořenem normovaného polynomu $\det(xE - M)$ s koeficienty v B. $\square$

9. Polynomiální funkce

Korespondence mezi afinní varietami a ideály vypadá na první pohled uspokojivě, ale ve skutečnosti nám vůbec neodpovídá na klasifikaci afinních variet, neboť jedna varieta může být do afinního prostoru vložena různými způsoby – například lze jistě tvrdit, že všechny body afinního prostoru jsou stejné, nezávisle na jejich souřadnicích, nicméně odpovídající ideály $\mathfrak{m}_P$ jsou různé. Prvně si uvědomme, že na otázku klasifikace variet, která by nebrala v úvahu konkrétní vložení variety do afinního prostoru, nelze odpovědět bez toho, abychom prvně popsali izomorfismy variet – jinak nelze říct, kdy jsou dvě variety stejné. Je tedy nutné popsat ta správná zobrazení mezi varietami; izomorfismy pak budou ta, která budou navíc invertibilní.

Definice 9.1. Nechť $V \subseteq \mathbb{A}^n$ je afinní varieta. Řekneme, že funkce $f\colon V \to \Bbbk$ je *polynomiální*, jestliže existuje polynom $F \in \Bbbk[x_1, \dots, x_n]$ takový, že pro každý bod $P = (p_1, \dots, p_n) \in V$ platí $f(P) = F(p_1, \dots, p_n)$.

Množina všech polynomiálních funkcí společně s operacemi sčítání a násobení po hodnotách tvoří tzv. *souřadnicový okruh* variety V; značíme jej $\Bbbk[V]$.

V dalším budeme používat $F(P) = F(p_1, \dots, p_n)$.

Zabývejme se nyní zobrazením $\Bbbk[x_1, \dots, x_n] \to \Bbbk[V]$, $F \mapsto f$. To je zřejmě surjektivní homomorfismus okruhů, jehož jádro se sestává právě z polynomů majících nulové hodnoty na V, tj. toto jádro je právě $I(V)$. Lze tedy psát

$$\Bbbk[V] \cong \Bbbk[x_1, \dots, x_n]/I(V).$$

Příklad 9.2. Platí $\Bbbk[\mathbb{A}^n] \cong \Bbbk[x_1, \dots, x_n]/0 = \Bbbk[x_1, \dots, x_n]$.

Definice 9.3. Okruh A se nazývá *redukovaný*, jestliže pro $x \in A$ platí $x^n = 0 \Rightarrow x = 0$.

Lemma 9.4. *Nechť $I \subseteq B$ je ideál. Potom kvocient B/I je redukovaný, právě když I je radikálový (viz podobné charakterizace těles a oborů integrity).*

Důkaz. Podle definice je B/I redukovaná, právě když $(b + I)^n = 0 \Rightarrow b + I = 0$, tj. právě když $b^n \in I \Rightarrow b \in I$, tedy když $\sqrt{I} \subseteq I$, tj. když I je radikálový. □

Důsledek 9.5. *Souřadnicová algebra $\Bbbk[V]$ každé afinní variety V je konečně generovaná redukovaná $\Bbbk$-algebra.*

Důkaz. Zjevně je $\Bbbk[V]$ generovaná souřadnicovými funkcemi $x_1, \dots, x_n$. Navíc je $I(V)$ radikálový, takže je $\Bbbk[V]$ redukovaná podle předchozího lemmatu. □

V opačném směru nechť nyní A je libovolná konečně generovaná redukovaná $\Bbbk$-algebra. Zvolme generátory $a_1, \dots, a_n \in A$ a uvažme homomorfismus algeber

$$\varphi\colon \Bbbk[x_1, \dots, x_n] \to A, \quad x_i \mapsto a_i.$$

Ten je surjektivní a jeho jádrem je nějaký ideál $J = \ker \varphi$; ten je radikálový, protože $A \cong \Bbbk[x_1, \dots, x_n]/J$ je redukovaná. Platí

$$\Bbbk[V(J)] \cong \Bbbk[x_1, \dots, x_n]/IV(J) = \Bbbk[x_1, \dots, x_n]/\sqrt{J} = \Bbbk[x_1, \dots, x_n]/J \cong A$$

a je tedy A izomorfní souřadnicové algebře afinní variety $V(J)$.

Naším dalším cílem bude ukázat, že existuje bijekce mezi afinními varietami a konečně generovanými redukovanými algebrami, obojí brané až na izomorfismus. Stále nám ale chybí říct, co to je izomorfismus afinních variet.

Definice 9.6. Nechť $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ jsou afinní variety a uvažme na $\mathbb{A}^n$ souřadnice $x_1, \dots, x_n$ a na $\mathbb{A}^m$ souřadnice $y_1, \dots, y_m$. Řekneme, že zobrazení $f\colon V \to W$ je *polynomiální*, jestliže existují polynomy $F_1, \dots, F_m \in \Bbbk[x_1, \dots, x_n]$ takové, že pro každý bod $P \in V$ platí

$$f(P) = (F_1(P), \dots, F_m(P)).$$

Lemma 9.7. *Každé polynomiální zobrazení je spojité v Zariského topologiích.*

Důkaz. Podle definice je každé polynomiální zobrazení $f\colon V \to W$ zúžením polynomiálního zobrazení $f\colon \mathbb{A}^n \to \mathbb{A}^m$ zadaného týmiž polynomy. Stačí tedy ověřit spojitost polynomiálního zobrazení mezi afinními prostory. Protože je každá uzavřená množina průnikem nadploch $V(g)$, stačí ověřit, že vzor nadplochy je uzavřený:

$$f^{-1}(V(g)) = \{P \in \mathbb{A}^n \mid f(P) \in V(g)\} = \{P \in \mathbb{A}^n \mid gf(P) = 0\} = V(gf),$$

kde složení gf je polynomiální funkce zadaná polynomem $G(F_1, \ldots, F_m)$, který získáme dosazením polynomu $F_j \in \Bbbk[x_1, \ldots, x_n]$ za každou proměnnou y_j vyskytující se v G. $\square$

Definice 9.8. Řekneme, že V, W jsou *izomorfní*, jestliže existují polynomiální zobrazení $f\colon V \to W$, $g\colon W \to V$ taková, že $gf = \mathrm{id}$, $fg = \mathrm{id}$.

Příklad 9.9. Parabola je izomorfní přímce, $V(x_2 - x_1^2) \cong \mathbb{A}^1$. Konkrétní izomorfismus je například

$$(x_1, x_2) \mapsto x_1, \quad (t, t^2) \mapsfrom t.$$

Každé polynomiální zobrazení $f\colon V \to W$ definuje homomorfismus algeber $f^*\colon \Bbbk[W] \to \Bbbk[V]$, daný předpisem $f^*(g) = gf$,

$$\begin{tikzcd} V \arrow[r, "f"] \arrow[dr, dashed, "gf"'] & W \arrow[d, "g"] \\ & \Bbbk \end{tikzcd}$$

například $f^*(g_1 + g_2) = (g_1 + g_2)f = g_1 f + g_2 f = f^*(g_1) + f^*(g_2)$.

Tvrzení 9.10. *Izomorfní variety mají izomorfní souřadnicové algebry.*

Důkaz. Vše plyne jednoduše z $(f_1 f_2)^* = f_2^* f_1^*$, $\mathrm{id}^* = \mathrm{id}$. $\square$

Příklad 9.11. Polynomiální zobrazení $f\colon \mathbb{A}^1 \to \mathcal{C} = V(x_2^2 - x_1^3)$, $t \mapsto (t^2, t^3)$, je polynomiální bijekce, navíc homeomorfismus, ale není izomorfismus.

Zjevně je f polynomiální a tedy spojité; navíc se jednoduše vidí, že to je bijekce. Jelikož jsou v $\mathbb{A}^1$ uzavřené pouze konečné a celá $\mathbb{A}^1$, je navíc f uzavřené. Podívejme se nyní na indukované zobrazení $f^*\colon \Bbbk[\mathcal{C}] \to \Bbbk[t]$. To posílá x_1 na kompozici $x_1 f = t^2$ (první složka zobrazení f) a $f^*(x_2) = t^3$. Ve výsledku je tak obrazem podalgebra generovaná t^2 a t^3 a neobsahuje tedy t. Proto není f^* izomorfismus a tedy ani f nemůže být izomorfismus.

K tomu, abychom dokončili důkaz korespondence mezi afinními varietami a konečně generovanými redukovanými algebrami, budeme potřebovat následující tvrzení.

Tvrzení 9.12. *Nechť $\varphi\colon \Bbbk[W] \to \Bbbk[V]$ je homomorfismus $\Bbbk$-algeber. Potom existuje jediné polynomiální zobrazení $f\colon V \to W$ takové, že $\varphi = f^*$.*

Důkaz. Nechť $V \subseteq \mathbb{A}^n$, $W \subseteq \mathbb{A}^m$ se souřadnicemi x_i, y_j. Pokud má být $\varphi = f^*$, musí být jeho komponenty rovny $f_j = y_j f = f^*(y_j) = \varphi(y_j)$. Položme tedy $f_j = \varphi(y_j)$ a

$$f = (f_1, \ldots, f_m)\colon V \to \mathbb{A}^m.$$

Potřebujeme ukázat, že obraz f skutečně leží ve W. Nechť tedy $G \in I(W)$ a počítejme

$$gf = Gf = G(f_1, \ldots, f_m) = G(\varphi(y_1), \ldots, \varphi(y_m)),$$

tedy polynomiální funkce vzniklá dosazením $\varphi(y_j)$ za proměnnou y_j v polynomu G. Protože je však φ homomorfismus (a G je vlastně term pro signaturu $\Bbbk$-algeber), je toto rovno

$$\varphi(G(y_1,\dots,y_m)) = \varphi(g) = 0,$$

neboť $g \in \Bbbk[W]$ je nulová funkce. Ve výsledku tak na obrazu $\operatorname{im} f$ platí $g = 0$ pro libovolný polynom $G \in I(W)$ a proto $\operatorname{im} f \subseteq W$. Zároveň $\varphi = f^*$, protože mají stejné hodnoty na generátorech y_j. □

Zabývejme se nyní podrobně vztahem afinních variet a konečně generovaných redukovaných algeber. Umíme přiřadit afinní varietě V algebru $\Bbbk[V]$ a konečně generované redukované algebře A varietu $V(J_A)$, kde J_A je jádro libovolného pevně zvoleného surjektivního homomorfismu $\Bbbk[x_1,\dots,x_n] \to A$. Již jsme ukázali, že $\Bbbk[V(J_A)] \cong A$, zabývejme se nyní vztahem mezi varietami V a $V(J_{\Bbbk[V]})$. Podle předchozího víme, že mají izomorfní souřadnicové algebry a podle tvrzení jsou tedy izomorfní. Dostáváme tak dva (kontravariantní) funktory

$$\{\text{afinní variety}\} \rightleftarrows \{\text{konečně generované redukované algebry}\}$$

takové, že obě složení jsou izomorfní identitě – hovoříme o (kontravariantní) ekvivalenci kategorií. (Podle tvrzení lze každému homomorfismu algeber $\varphi\colon A \to B$ jednoznačně přiřadit polynomiální zobrazení $V(J_B) \to V(J_A)$ tak, že indukuje $\Bbbk[V(J_A)] \cong A \xrightarrow{\varphi} B \cong \Bbbk[V(J_B)]$.)

V dalším budeme potřebovat Hilbertovu větu o nulách pro $\Bbbk[X]$. Pro ideál $J \subseteq \Bbbk[X]$ definujme

$$V^X(J) = \{x \in X \mid \forall f \in J\colon f(x) = 0\}$$

a pro podmnožinu $Y \subseteq X$ definujeme

$$I^X(Y) = \{f \in \Bbbk[X] \mid \forall x \in Y\colon f(x) = 0\}.$$

Věta 9.13 (Hilbertova věta o nulách v X)**.** *Platí $I^X(V^X(J)) = \sqrt{J}$, zejména $V^X(J) = \emptyset$, právě když $1 \in J$ a maximální ideály odpovídají přesně bodům.*

Důkaz. Pokud realizujeme $\Bbbk[X]$ jako $\Bbbk[x_1,\dots,x_n]/I(X)$, pak máme $J = \widetilde{J}/I(X)$, kde $\widetilde{J} \subseteq \Bbbk[x_1,\dots,x_n]$ je ideál obsahující $I(X)$ a platí $V^X(J) = V(\widetilde{J})$ a také $I^X(Y) = I(Y)/I(X)$. Tím se věta převede na klasickou Hilbertovu větu o nulách, neboť zřejmě $\sqrt{J} = \sqrt{\widetilde{J}}/I(X)$. □

10. Součin afinních variet

Věta 10.1. *Nechť $V \subseteq \mathbb{A}^n$ a $W \subseteq \mathbb{A}^m$ jsou afinní variety. Potom také $V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m \cong \mathbb{A}^{n+m}$ je afinní varieta.*

Důkaz. Nechť $V = V(f_1,\dots,f_r)$ a $W = V(g_1,\dots,g_s)$, kde polynomy f_i píšeme v proměnných x_i a polynomy g_j v proměnných y_j. Tímto způsobem je lze interpretovat jako

$$f_1,\dots,f_r,g_1,\dots,g_s \in \Bbbk[x_1,\dots,x_n,y_1,\dots,y_m]$$

a potom zjevně platí $V \times W = V(f_1,\dots,f_r,g_1,\dots,g_s)$. □

Projekce $\pi\colon V \times W \to W$ je zřejmě polynomiální, tedy i spojitá. V dalším se nám bude hodit následující věta, která neplyne z příslušného tvrzení v topologii, neboť součin $V \times W$ *nemá* součinovou topologii (má víc otevřených množin).

Věta 10.2. *Projekce $\pi\colon X \times Y \to Y$ je otevřená.*

Důkaz. Nechť je $U \subseteq X \times Y$ bázová otevřená množina, tedy doplněk $U = (X \times Y) \smallsetminus V(g)$ nulové množiny nějakého polynomu $g = g(x, y)$ (zde x značí systém proměnných x_i, podobně y). Potom $x \in X$ neleží v $\pi(U)$ právě když $g(x, -)$ je nulový na celém Y, tj. $g(x, -) \in I(Y)$. To je ale systém lineárních podmínek na koeficienty $g(x, -) \in K[y_1, \dots, y_m]$, které závisí polynomiálně na $x_1, \dots, x_n$. □

Věta 10.3. *Pokud jsou obě V, W ireducibilní, je také $V \times W$ ireducibilní.*

Důkaz. Nechť $V \times W = Z_1 \cup Z_2$. Potom

$$W_i = W \smallsetminus \pi((V \times W) \smallsetminus Z_i) \subseteq W$$

jsou uzavřené množiny, přičemž díky ireducibilitě $V \times \{Q\} \cong V$ leží každé $V \times \{Q\}$ v nějakém Z_i, a proto také Q leží v příslušném W_i. Protože bylo Q libovolné, máme $W = W_1 \cup W_2$. Díky ireducibilitě W pak $W = W_i$ pro nějaké i a následně $V \times W = Z_i$. □

Důkaz. Nechť $V \times W = Z_1 \cup Z_2$. Nechť $Q \in W$ a uvažujme podvarietu $V \times \{Q\} \cong V$, která je podle předpokladu ireducibilní. Musí tedy být $V \times \{Q\} \subseteq Z_i$ pro nějaké i. Uvažme nyní množinu $W_i = \{Q \in W \mid V \times \{Q\} \subseteq Z_i\}$ a dokážeme, že je uzavřená. Protože je $W = W_1 \cup W_2$, musí pak být $W = W_i$ pro nějaké i a potom $V \times W = Z_i$. Platí

$$W_i = \bigcap_{P \in V} \mathrm{pr}_W((\{P\} \times W) \cap Z_i),$$

přičemž každá $(\{P\} \times W) \cap Z_i$ je uzavřená a projekce $\mathrm{pr}_W\colon \{P\} \times W \to W$ je izomorfismus, takže i obraz je uzavřený.

Zabývejme se nyní obrazem polynomiálního zobrazení. Uvidíme, že se obecně nejedná o afinní varietu, nicméně budeme celkem snadno schopni tento obraz popsat. V první fázi problém převedeme na problém výpočtu obrazu při lineární projekci. Je-li totiž zobrazení $f\colon V \to W$ polynomiální, můžeme uvážit jeho graf $\Gamma_f \subseteq \mathbb{A}^{n+m}$ a obraz f je pak stejný jako obraz Γ_f při projekci na posledních m souřadnic. Přitom graf Γ_f je afinní varieta, $\Gamma_f = V(I(V), y_j - f_j(x))$.

Příklad 10.4. Popište obraz zobrazení $f\colon \mathbb{A}^1 \to \mathbb{A}^2$, $f(t) = (t^2 - 1, t^3 - t)$.

Řešení. Graf $\Gamma_f = V(t^2 - 1 - x, t^3 - t - y)$. Přitom tyto polynomy v proměnné t mají společné řešení, právě když $\mathrm{Res}(t^2 - 1 - x, t^3 - t - y; t) = 0$. Vypočtěme nyní tento rezultant

$$\det \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ -1-x & 0 & 1 & -1 & 0 \\ 0 & -1-x & 0 & -y & -1 \\ 0 & 0 & -1-x & 0 & -y \end{pmatrix} = y^2 - x^2 - x^3.$$

Platí tedy $\mathrm{im}\, f = V(y^2 - x^2 - x^3)$. ◇

Stejným postupem lze ukázat, že obraz libovolného polynomiálního zobrazení $f\colon \mathbb{A}^1 \to \mathbb{A}^2$ je afinní varieta $V(\mathrm{Res}(f_1(t) - x_1, f_2(t) - x_2; t))$. Časem toto tvrzení zobecníme na zobrazení $f\colon \mathbb{A}^1 \to \mathbb{A}^m$.

Věta 10.5. *Nechť je $V \subseteq \mathbb{A}^{n+m}$ je afinní varieta. Potom pro její obraz při projekci $\pi\colon \mathbb{A}^{n+m} \to \mathbb{A}^m$ platí $I(\pi(V)) = I(V) \cap \Bbbk[y_1, \dots, y_m]$.*

Důkaz. Tvrzení je jasné z toho, že polynom $f \in \Bbbk[y_1, \ldots, y_m]$ je nulový na πV, právě když je nulový na V. $\square$

Nechť nyní $V = V(J)$. Protože je $I(\pi(V(J))) = \sqrt{J} \cap \Bbbk[y_1, \ldots, y_m]$ radikálem $J \cap \Bbbk[y_1, \ldots, y_m]$, lze psát $\overline{\pi(V(J))} = V(J \cap \Bbbk[y_1, \ldots, y_m])$. Toho lze využít k výpočtu obrazu, resp. jeho uzávěru v kombinaci s Gröbnerovými bázemi, neboť je zřejmé, že v případě uspořádání ve kterém $x_i > y_j$ je $J \cap \Bbbk[y_1, \ldots, y_m]$ generován prvky Gröbnerovy ležícími v $\Bbbk[y_1, \ldots, y_m]$ (každý vedoucí člen prvku z $J \cap \Bbbk[y_1, \ldots, y_m]$ je dělitelný vedoucím členem nějakého prvku Gröbnerovy báze, který ale může díky volbě uspořádání obsahovat pouze proměnné y_j).

Příklad 10.6. Popište uzávěr obrazu zobrazení $f\colon \mathbb{A}^2 \to \mathbb{A}^3$, $f(s,t) = (s^2 - t^2, 2st, s^2 + t^2)$.

Řešení. Graf $\Gamma_f = V(s^2 - t^2 - x, 2st - y, s^2 + t^2 - z)$. Spočítejme nyní Gröbnerovu bázi vzhledem k uspořádání $s > t > x > y > z$. Začneme s

$$s^2 - \tfrac{1}{2}x - \tfrac{1}{2}z,\ st - \tfrac{1}{2}y,\ t^2 + \tfrac{1}{2}x - \tfrac{1}{2}z$$

a S-polynomy vycházejí

$$\begin{aligned} t(s^2 - \tfrac{1}{2}x - \tfrac{1}{2}z) - s(st - \tfrac{1}{2}y) &= -\tfrac{1}{2}tx - \tfrac{1}{2}tz + \tfrac{1}{2}sy \\ t(st - \tfrac{1}{2}y) - s(t^2 + \tfrac{1}{2}x - \tfrac{1}{2}z) &= -\tfrac{1}{2}ty - \tfrac{1}{2}sx + \tfrac{1}{2}sz; \end{aligned}$$

přidáváme tedy $sy - tx - tz$, $sx - sz + ty$. V dalším kroku

$$\begin{aligned} y(s^2 - \tfrac{1}{2}x - \tfrac{1}{2}z) - s(sy - tx - tz) &= -\tfrac{1}{2}xy - \tfrac{1}{2}yz + stx + stz \equiv 0 \\ x(s^2 - \tfrac{1}{2}x - \tfrac{1}{2}z) - s(sx - sz + ty) &= -\tfrac{1}{2}x^2 - \tfrac{1}{2}xz + s^2z - sty \equiv -\tfrac{1}{2}x^2 - \tfrac{1}{2}y^2 + \tfrac{1}{2}z^2 \\ y(st - \tfrac{1}{2}y) - t(sy - tx - tz) &= -\tfrac{1}{2}y^2 + t^2x + t^2z \equiv -\tfrac{1}{2}x^2 - \tfrac{1}{2}y^2 + \tfrac{1}{2}z^2 \\ x(st - \tfrac{1}{2}y) - t(sx - sz + ty) &= -\tfrac{1}{2}xy - stz - t^2y \equiv 0 \\ x(sy - tx - tz) - y(sx - sz + ty) &= -tx^2 - txz + syz - ty^2 \equiv -tx^2 - ty^2 + tz^2 \end{aligned}$$

a přídáváme tedy pouze $x^2 + y^2 - z^2$. To je zároveň jediný prvek Gröbnerovy báze ležící v $\Bbbk[x,y,z]$. Proto $\overline{\operatorname{im} f} = V(x^2 + y^2 - z^2)$. $\diamond$

Z pohledu *uzávěru* obrazu je o dost méně zajimavý následující příklad. V jeho řešení ale zjistíme obraz přesně, nikoliv pouze jeho uzávěr.

Příklad 10.7. Popište obraz zobrazení $f\colon \mathbb{A}^2 \to \mathbb{A}^2$, $f(s,t) = (st, t)$.

Řešení. Opět $\Gamma_f = V(st - x, t - y)$ a zkoumáme, pro které body (x, y) mají tyto polynomy společný kořen. Podle Hilbertovy věty o nulách to nastane, právě když $1 \in (st - x, t - y) = J \subseteq \Bbbk[s,t]$. Počítejme proto Gröbnerovu bázi. V prvním kroku redukujeme na

$$J = (sy - x,\ t - y)$$

Nyní mohou nastat dva případy. Buď $y \neq 0$ a potom $J = (s - \frac{x}{y}, t - y)$ je maximální ideál odpovídající bodu $(\frac{x}{y}, y)$ a tedy neobsahuje 1. V případě $y = 0$ je $J = (-x, t)$ a opět nastávají dvě možnosti: pro $x \neq 0$ máme $J = (1)$ a pro $x = 0$ naopak $J = (t) \not\ni 1$ (jedná se o Gröbnerovu bázi a neobsahuje 1). Výsledek tedy je

$$\operatorname{im} f = \{(x,y) \in \mathbb{A}^2 \mid (y \neq 0) \vee (y = 0 \wedge x = 0)\}. \qquad \diamond$$

Abstrakcí předchozího příkladu je následující tvrzení. Řekneme, že podmnožina $X \subseteq \mathbb{A}^n$ je *zkonstruovatelná*, jestliže se jedná o množinu bodů splňujících logický výrok vzniklý z polynomiálních rovnic pomocí konečného množství konjunkcí, disjunkcí a negací. Ekvivalentně se jedná o konečné sejdnocení kvaziafinních variet (otevřených podmnožin afinních variet). Tvrzení říká, že obrazem zkonstruovatelné množiny je opět zkonstruovatelná množina. Z pohledu logiky je pak obraz dán existenčním kvantifikátorem,

$$\pi(X) = \{(y_1, \ldots, y_m) \in \mathbb{A}^m \mid \exists x_1, \ldots, x_n \colon (x_1, \ldots, x_n, y_1, \ldots, y_m) \in X\}.$$

Lze tedy toto tvrzení interpretovat následujícím způsobem: ke každému logickému výrazu tvořenému z polynomiálních rovnic pomocí logiky prvního řádu existuje ekvivalentní tvrzení bez kvantifikátoru. Hovoříme o „eliminaci kvantifikátorů“.

11. Projektivní variety

V případě průsečíku dvou kuželoseček dostáváme maximálně čtyři průsečíky. Tohoto čísla v některých nelze dosáhnout – například dvě kružnice $(x-p_i)^2 + (y-q_i)^2 - r_i^2$ mají právě dva průsečíky (v případě, že se dotýkají, pouze jeden dvojnásobný). Důvodem je, že se protínají ještě ve dvou nevlastních bodech $(0:1:\pm i)$, tzv. “circular points”. V případě, že počítáme i tyto nevlastní body a každý se správnou násobností, jsou průsečíky přesně 4. Toto tvrzení není zdaleka elementární, zejména pro křivky vyšších stupňů, a jeho důkaz bude vrcholem tohoto kurzu. Prvně zahrneme do hry nevlastní body – budeme tedy v dalším definovat projektivní variety.

Nechť V je vektorový prostor nad $\mathbb{k}$. Budeme označovat $\mathbb{P}(V) = (V \smallsetminus \{0\})/{\sim}$, $u \sim v \Leftrightarrow \exists k \in \mathbb{k} \colon v = ku$, projektivní prostor vektorového prostoru V. Zejména $\mathbb{P}^n = \mathbb{P}(\mathbb{k}^{n+1})$. Značíme $(x_0 : \cdots : x_n) \in \mathbb{P}^n$ třídu zadanou vektorem $(x_0, \ldots, x_n)$ a mluvíme o *homogenních souřadnicích.* Pro každé $i = 0, \ldots, n$ definujeme

$$U_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$$
$$H_i = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid x_i = 0\}$$

přičemž platí $H_i \cong \mathbb{P}^{n-1}$ a $U_i \cong \mathbb{A}^n$, $(x_0 : \cdots : x_n) \mapsto (\frac{x_0}{x_i}, \ldots, \widehat{\frac{x_i}{x_i}}, \ldots, \frac{x_n}{x_i})$. Dále platí $\mathbb{P}^n = U_0 \cup \cdots \cup U_n$, mluvíme o afinním pokrytí projektivního prostoru $\mathbb{P}^n$. Každý homogenní polynom $f \in \mathbb{k}^d[x_0, \ldots, x_n]$ stupně d splňuje $f(kx_0, \ldots, kx_n) = k^d f(x_0, \ldots, x_n)$ a lze proto definovat

$$V(f) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid f(x_0, \ldots, x_n) = 0\}$$

Definice 11.1. *Projektivní varieta* je podmnožina $\mathbb{P}^n$ tvaru $V(S) = \bigcap_{f \in S} V(f)$, kde S je nějaká množina homogenních polynomů.

Příklad 11.2. Nadrovina $H_i = V(x_i)$ je projektivní varieta.

Definice 11.3. *Graduovaný okruh* je okruh A společně s rozkladem $A = \bigoplus_{d \geq 0} A_d$ (vzhledem ke sčítání, tj. $A_d + A_d \subseteq A_d$) takový, že platí $A_d \cdot A_e \subseteq A_{d+e}$. Zejména $1 \in A_0$.

Prvky sčítanců A_d se nazývají *homogenní* stupně d. Každý prvek $a \in A$ má jednoznačný rozklad $a = a_0 + \cdots + a_r$, kde $a_d \in A_d$ se nazývají *(homogenní) komponenty* prvku a.

Příklad 11.4. Okruh polynomů $A = \mathbb{k}[x_0, \ldots, x_n] = \bigoplus_{d \geq 0} \mathbb{k}^d[x_0, \ldots, x_n]$, kde

$$\mathbb{k}^d[x_0, \ldots, x_n] = \{f \in \mathbb{k}[x_0, \ldots, x_n] \mid f \text{ homogenní stupně } d\}.$$

Definice 11.5. Ideál I se nazývá *homogenní*, jestliže pro každý prvek $f \in I$ s rozkladem $f = f_0 + \cdots + f_d$ do komponent platí také $f_i \in I$. V takovém případě platí $I = \bigoplus_{d \geq 0}(A_d \cap I)$.

Lemma 11.6. *Pro ideál I v graduovaném okruhu A platí*

- *I je homogenní, právě když je generovaný homogenními prvky;*
- *je-li I homogenní, pak I je prvoideál, právě když pro každé dva* homogenní *prvky $f, g \in A$ platí $fg \in I \Rightarrow f \in I$ nebo $g \in I$;*
- *homogenní ideály jsou uzavřené na součet, součin, průnik a radikál.*

Důkaz. Je-li I homogenní, pak je generovaný homogenními prvky $f \in A_d \cap I$. Naopak, pokud je I generovaný nějakou množinou S homogenních prvků, pak je každý $f \in I$ kombinací prvků z S, přičemž můžeme koeficienty rozložit do homogenních komponent a sdružit členy stejných stupňů a jsou tedy všechny komponenty f také kombinacemi prvků z S.

Pokud $fg \in I$, pak jeho komponenta největšího stupně je součinem komponent největšího stupně prvků f, g a tedy musí ležet alespoň jedna tato komponenta v I, řekněme $g = g_s + g'$, kde $g_s \in I$ a g' je menšího stupně. Potom $fg = fg_s + fg'$ a tedy i $fg' \in I$. Indukcí vzhledem k součtu stupňů f a g lze tedy předpokládat, že buď $f \in I$ nebo $g' \in I$, ale pak také $g = g_s + g' \in I$.

Součet a součin se vyřeší pomocí generujících množin, průnik bude homogenní přímo z definice. Pro radikál předpokládejme $f \in \sqrt{I}$, tj. $f^k = {f_r}^k + \mathrm{lot} \in I$, takže díky homogenitě I je ${f_r}^k \in I$, tedy $f_r \in \sqrt{I}$, a proto také $f' = f - f_r \in \sqrt{I}$. Dále indukcí vzhledem k r. □

Protože opět $V(I) \cup V(J) = V(IJ)$ a $\bigcap V(J_p) = V(\sum J_p)$, dostáváme díky předchozímu lemmatu na $\mathbb{P}^n$ opět *Zariského topologii*, jejíž uzavřené podmnožiny jsou právě projektivní variety. Definujme dále $V(J) = V(f \in J \mid f \text{ homogenní})$. Definujeme dále $I(X)$ jako ideál generovaný všemi homogenními polynomy f takovými, že $f|_X = 0$.

Lemma 11.7. *Platí $f \in I(X)$, právě když $f(x) = 0$ pro libovolný vektor $x \neq 0$ reprezentující bod $[x] \in X$.*

Důkaz. Pišme $f = f_0 + \cdots + f_d$ a zabývejme se tím, co se stane při změně reprezentanta, $f(kx) = f_0(x) + \cdots + k^d f_d(x)$. Tento výraz je nulový pro *všechna* $k \in \mathbb{k}^\times$, právě když $f_0(x) = \cdots = f_d(x) = 0$, tj. $f_i \in I(X)$ a tedy $f \in I(X)$. □

V projektivním případě je vztah mezi ideály a varietami o něco složitější, neboť $(x_0, \ldots, x_n)$ je vlastní radikálový ideál s $V(x_0, \ldots, x_n) = \emptyset$. Toto je však jediná komplikace.

Věta 11.8 (projektivní věta o nulách). *Nechť $\mathbb{k}$ je algebraicky uzavřené těleso. Potom pro homogenní ideál $J \subseteq \mathbb{k}[x_0, \ldots, x_n]$ platí*

- *$V(J) = \emptyset \Leftrightarrow \sqrt{J} \supseteq (x_0, \ldots, x_n)$;*
- *jestliže $V(J) \neq \emptyset$, pak $I(V(J)) = \sqrt{J}$.*

Důkaz. Je-li $1 \in J$, pak zjevně J splňuje obě tvrzení. V dalším tedy předpokládejme, že $1 \notin J$. Protože se jedná o homogenní ideál, znamená to, že každý prvek $f \in J$ má nulový absolutní člen, tj. $f(0) = 0$.

Pro afinní varietu $V^{\mathrm{af}}(J) \subseteq \mathbb{A}^{n+1}$ zadanou homogenním ideálem $J \not\ni 1$ platí

$$V^{\mathrm{af}}(J) = \pi^{-1}(V(J)) \cup \{0\}$$

(na obou stranách bereme nulové body generujících homogenních prvků, pro které je rovnost zřejmá), jedná se o tzv. *afinní kužel* nad $V(J)$. Potom $V(J) = \emptyset$, právě když $V^{\mathrm{af}}(J) = \{0\} = V(x_0, \dots, x_n)$, tedy právě když $(x_0, \dots, x_n) \subseteq I^{\mathrm{af}}(V^{\mathrm{af}}(J)) = \sqrt{J}$ podle afinní věty o nulách. Podle předchozího lemmatu $I(V(J)) = I^{\mathrm{af}}(\pi^{-1}(V(J))) = I^{\mathrm{af}}(V^{\mathrm{af}}(J)) = \sqrt{J}$ (protože 0 leží v uzávěru $\pi^{-1}([x]) = \Bbbk^{\times}x$ pro libovolné $[x] \in V(J)$ – uzávěr každé nekonečné podmnožiny přímky je celá přímka). $\square$

Ideál $(x_0, \dots, x_n)$ nazveme *irelevantní*. Dostáváme tak bijekci mezi radikálovými ideály různými od $(x_0, \dots, x_n)$ (tedy relevantními) a projektivními varietami.

Věta 11.9. *Vložení $j_i \colon U_i \to \mathbb{A}^n$, $j_i(x_0 : \dots : x_n) = (\frac{x_0}{x_i}, \dots, \widehat{\frac{x_i}{x_i}}, \dots, \frac{x_n}{x_i})$, je homeomorfismus.*

Důkaz. Nechť $i = 0$. Protože jsou obě topologie generovány nadplochami, počítejme

$$j_0(V^{\mathrm{pr}}(f)) = \{(x_1, \dots, x_n) \in \mathbb{A}^n \mid f|_{x_0=1} = 0\} = V^{\mathrm{af}}(f|_{x_0=1}).$$

Naopak,

$$j_0^{-1}(V^{\mathrm{af}}(g)) = \{(x_0 : \dots : x_n) \in U_0 \mid x_0^{\deg g} g(\tfrac{x_1}{x_0}, \dots, \tfrac{x_n}{x_0}) = 0\} = U_0 \cap V^{\mathrm{pr}}(\widetilde{g}),$$

kde $\widetilde{g} = x_0^{\deg g} g(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$ je homogenní polynom, tzv. *homogenizace g*. $\square$

Důsledek 11.10. *Zobrazení $j_0 \colon U_0 \to \mathbb{A}^n$ indukuje bijekci*

$$\left\{\begin{matrix}\textit{ireducibilní projektivní variety}\\ \textit{v } \mathbb{P}^n \textit{ neobsažené v } H_0\end{matrix}\right\} \xrightarrow{\cong} \{\textit{ireducibilní afinní variety v } \mathbb{A}^n\},$$

posílající ireducibilní projektivní varietu $V \subseteq \mathbb{P}^n$ na $j_0(U_0 \cap V)$.

Důkaz. Díky předchozí větě stačí ověřit, že $V \mapsto U_0 \cap V$ zadává bijekci mezi ireducibilními projektivními varietami neobsaženými v H_0 a ireducibilními uzavřenými podmnožinami U_0. Inverzní zobrazení je dáno uzávěrem, $W \mapsto \overline{W}$, protože $V = \overline{U_0 \cap V}$ – každá *neprázdná* otevřená podmnožina ireducibilního prostoru je hustá. $\square$

Algebraicky je projektivní rozšíření (tj. uzávěr obrazu v $\mathbb{P}^n$) realizováno jako

$$\overline{V^{\mathrm{af}}(J)} = V^{\mathrm{pr}}(\widetilde{J}),$$

kde $\widetilde{J} = (\widetilde{g} \mid g \in J)$ (toto vyžaduje algebraickou uzavřenost $\Bbbk$; protipříkladem nad $\mathbb{R}$ je $J = (x_1^2 + x_2^4)$): pokud se pro $f \in \Bbbk^d[x_0, \dots, x_n]$ homogenní nuluje $f|_{x_0=1}$ na $V^{\mathrm{af}}(J)$, pak $f^k|_{x_0=1} = g \in J$, a proto $f^k = x_0^{d-\deg g} \cdot \widetilde{g} \in \widetilde{J}$; opačná implikace je zřejmá, tedy

$$\overline{V^{\mathrm{af}}(J)} = V^{\mathrm{pr}}(I^{\mathrm{pr}}(V^{\mathrm{af}}(J))) = V^{\mathrm{pr}}(f \mid f^k \in \widetilde{J}) = V^{\mathrm{pr}}(\widetilde{J}).$$

Poznámka. Tvrzení, které platí i nad algebraicky neuzavřenými tělesy: $\overline{X} = V^{\mathrm{pr}}(\widetilde{I(X)})$. Je totiž $f|_{x_0=1}$ nulové na X, jestliže $f|_{x_0=1} \in I(X)$, nutně pak $f \in \widetilde{I(X)}$ a zbytek je stejný. Toto je však značně nepraktické – spočítat radikál je obecně dost těžké, podstatnou výjimkou jsou hlavní ideály.

DÚ 5. Označme $\widetilde{J} = (\widetilde{g} \mid g \in J)$ ideál generovaný homogenizacemi $\widetilde{g} = x_0^{\deg g} g(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$. Uvažujme následující uspořádání monomů

$$x^\alpha >_{\mathrm{gr}} x^\beta \quad \Leftrightarrow \quad |\alpha| > |\beta| \vee (|\alpha| = |\beta| \wedge x^\alpha > x^\beta).$$

Dokažte, že v případě, že $J = (g_1, \dots, g_r)$ je Gröbnerova báze vzhledem k $>_{\mathrm{gr}}$, je také $\widetilde{J} = (\widetilde{g}_1, \dots, \widetilde{g}_r)$ Gröbnerovou bází vzhledem k podobném uspořádání $>_{\mathrm{gr}}$, jen s x_0 navíc a menším než zbylé proměnné, tj. $x_1 > \dots > x_n > x_0$.

Příklad 11.11. Pokud $C_0 = V^{\mathrm{af}}(x_2^2 - x_1(x_1-1)(x_1-2))$, pak projektivní rozšíření je $C = V(x_0x_2^2 - x_1(x_1-x_0)(x_1-2x_0))$.

12. Regulární zobrazení a funkce

Pokusme se nyní definovat „polynomiální" zobrazení mezi projektivními varietami. Nechť $f_0, \dots, f_m \in \Bbbk[x_0, \dots, x_n]$ jsou polynomy a uvažme

$$f\colon \mathbb{P}^n \to \mathbb{P}^m, \quad (x_0 : \dots : x_n) \mapsto (f_0(x_0, \dots, x_n) : \dots : f_m(x_0, \dots, x_n));$$

k tomu, aby výsledek nezávisel na volbě homogenních souřadnic je potřeba, aby polynomy f_j byly homogenní téhož stupně d – potom $f_j(kx_0, \dots, kx_n) = k^d f(x_0, \dots, x_n)$. Dvě lokální vyjádření se rovnají, $(f_0 : \dots : f_m) = (g_0 : \dots : g_m)$, právě když $f_jg_k = f_kg_j$.

Příklad 12.1. Uvažme projektivní varietu $V = V(x_0x_3 - x_1x_2)$ a dvě zobrazení do $\mathbb{P}^1$ daná $f = (x_0 : x_1)$, $g = (x_2 : x_3)$. Na V platí $(x_0 : x_1) = (x_2 : x_3)$.

Nyní popíšeme jeden problém s „polynomiálními" zobrazeními mezi projektivními varietami – nejsou definované všude. V předchozím příkladu je $(x_0 : x_1)$ korektní bod $\mathbb{P}^1$ pouze pokud $x_0 \neq 0$ nebo $x_1 \neq 0$. Ve výsledku je tedy možné definovat zobrazení $f\colon V \to \mathbb{P}^1$ předpisem

$$f(x_0 : x_1 : x_2 : x_3) = \begin{cases} (x_0 : x_1) & x_0 \neq 0 \text{ nebo } x_1 \neq 0 \\ (x_2 : x_3) & x_2 \neq 0 \text{ nebo } x_3 \neq 0 \end{cases}$$

Přitom neexistuje žádné vyjádření $f = (h_0 : h_1)$, definované na celém V. To plyne nejrychleji z faktu, který dokážeme později, že totiž každé tři homogenní polynomy mají na $\mathbb{P}^3$ společný kořen, $V(x_0x_3 - x_1x_2, h_0, h_1) \neq \emptyset$.

Definice 12.2. *Kvaziprojektivní varieta* je libovolná otevřená podmnožina projektivní variety, tj. libovolný průnik uzavřené a otevřené podmnožiny. Zejména každá projektivní i každá afinní varieta je kvaziprojektivní (druhý případ plyne z toho, že sám afinní prostor $\mathbb{A}^n \cong U_0 \subseteq \mathbb{P}^n$ je otevřenou podmnožinou projektivního prostoru).

Kvaziafiní varieta je libovolná otevřená podmnožina afinní variety; každá kvaziafinní varieta je tedy kvaziprojektivní.

Definice 12.3. Zobrazení $f\colon V \to W$ mezi kvaziprojektivními varietami se nazývá *regulární*, jestliže pro každý bod $P \in V$ existují homogenní polynomy $f_0, \dots, f_m \in \Bbbk^d[x_0, \dots, x_n]$ téhož stupně tak, že platí $f = (f_0 : \dots : f_m)$ na nějakém okolí bodu P ve V; zejména musí být alespoň jedno $f_j(P) \neq 0$.

Lemma 12.4. *Každé regulární zobrazení je spojité v Zariského topologiích.*

Důkaz. Stačí dokázat lokálně, tedy na každé otevřené podmnožině $V \smallsetminus V(f_0, \dots, f_m)$, kde lze f vyjádřit jako $f = (f_0 : \dots : f_m)$; důkaz je pak analogický případu polynomiálního zobrazení mezi afinními varietami. $\square$

Regulární zobrazení ve skutečnosti nejsou ani tak polynomiální jako spíše racionální – přepsáním do afinních map $U_0 \subseteq \mathbb{P}^n$, $U_0 \subseteq \mathbb{P}^m$ totiž dostaneme

$$(x_1, \dots, x_n) \mapsto \left(\tfrac{f_1(1, x_1, \dots, x_n)}{f_0(1, x_1, \dots, x_n)}, \dots, \tfrac{f_m(1, x_1, \dots, x_n)}{f_0(1, x_1, \dots, x_n)}\right).$$

Naopak, každé (částečně definované) zobrazení mezi kvaziafinními varietami, jehož komponenty jsou racionální funkce lze převést na společný jmenovatel $\left(\frac{g_1}{g_0}, \dots, \frac{g_m}{g_0}\right)$. Potom pro vhodná d_j je

$$(x_0^{d_0}\widetilde{g}_0 : x_0^{d_1}\widetilde{g}_1 \cdots : x_0^{d_m}\widetilde{g}_m)$$

rozšířením původního zobrazení. Budeme tedy zobrazením jako výše říkat *racionální* zobrazení, pokud nejsou nutně definované všude:

Definice 12.5. *Racionální zobrazení* $f\colon V \dashrightarrow W$ mezi kvaziprojektivními varietami je třída regulárních zobrazení $f'\colon V' \to W$, definovaných na libovolné otevřené husté podmnožině $V' \subseteq V$, vzhledem k relaci $f' \sim f'' \Leftrightarrow f' = f''$ na $V' \cap V''$.

Říkáme, že f je *regulární* v bodě P, jestliže existuje reprezentant f, který je na P definovaný. *Definiční obor* f je množina všech regulárních bodů f; značíme jej $\operatorname{dom} f$.

Příklad 12.6. Důležitým příkladem jsou polynomiální zobrazení mezi afinními varietami – podle předchozího je lze chápat jako racionální funkce, které jsou navíc definované všude, tedy jsou regulární. V Důsledku 12.8 ukážeme, že žádná jiná regulární zobrazení mezi afinními varietami neexistují.

Obecněji, taktéž podle předchozího jsou zobrazení mezi kvaziprojektivními varietami, jejichž komponenty jsou racionální lomenné funkce, racionálními zobrazeními.

Protože jsou regulární zobrazení definována lokálně, existuje reprezentant f' každého racionálního zobrazení definovaný na *maximálním* možném $V' = \operatorname{dom} f$. Na druhou stranu existuje reprezentant tvaru $(f_0 : \cdots : f_m)$ (alespoň pro ireducibilní V); oba dva reprezentanti se hodí k různým účelům.

Zabývejme se nyní případem racionálních funkcí na *ireducibilní* varietě V, tj. racionálních zobrazení $f\colon V \dashrightarrow \Bbbk \subseteq \mathbb{P}^1$. Ta jsou tvaru f_1/f_0, přičemž dvě taková vyjádření jsou stejná, $f_1/f_0 = g_1/g_0$, právě když platí $f_1g_0 = g_1f_0$ na nějaké otevřené husté podmnožině V a tedy i na celém V.

Protože má $f_1/f_0 \neq 0$ (tj. $f_1 \notin I(V)$) inverzi f_0/f_1, tvoří racionální funkce na V těleso, které značíme $\Bbbk(V)$. Přímo z definice plyne, že pro libovolnou otevřenou hustou podmnožinu $U \subseteq V$ platí $\Bbbk(U) = \Bbbk(V)$. Zejména tedy lze přejít k afinní podvarietě $\Bbbk(V) = \Bbbk(\mathbb{A}^n \cap \overline{V})$. V dalším nechť tedy $V \subseteq \mathbb{A}^n$ je afinní varieta. Každá polynomiální funkce g na V je regulární, tím spíše racionální, dostaneme tak injektivní homomorfismus $\Bbbk[V] \to \Bbbk(V)$. Protože $f_1/f_0 = (f_1/x_0^d)/(f_0/x_0^d)$, kde obě racionální funkce f_i/x_0^d jsou zjevně polynomiální, lze $\Bbbk(V)$ ztotožnit s podílovým tělesem $\Bbbk[V]$. Bez důkazu poznamenejme, že pro V reducibilní by $\Bbbk(V)$ nebylo těleso a bylo by izomorfní lokalizaci $\Bbbk[V]$ v prvoideálu všech dělitelů nuly.

Věta 12.7. *Racionální funkce $f\colon V \dashrightarrow \Bbbk$ na afinní varietě V je regulární, právě když je polynomiální. Obecněji funkce f regulární na $V \smallsetminus V(h)$ jsou právě prvky lokalizace $\Bbbk[V][h^{-1}]$.*

Důkaz. Definujeme ideál jmenovatelů $D_f = \{h \in \Bbbk[V] \mid fh \in \Bbbk[V]\}$. V druhém odstavci dokážeme, že platí $\operatorname{dom} f = V \smallsetminus V(D_f)$. Pak je f regulární, právě když $V(D_f) = \emptyset$, tj. právě když $1 \in D_f$ (podle Hilbertovy věty 9.13 o nulách ve V). To ale přesně znamená, že f má vyjádření ve tvaru $f = g/1$ a $f = g$ je polynomiální. V obecném případě $\operatorname{dom} f \supseteq V \smallsetminus V(h)$ $\Leftrightarrow V(D_f) \subseteq V(h) \Leftrightarrow h \in I(V(D_f)) = \sqrt{D_f} \Leftrightarrow f$ lze vyjádřit ve tvaru $f = g/h^k$, tj. $f \in \Bbbk[V][h^{-1}]$.

Zbývá tedy dokázat $\operatorname{dom} f = V \smallsetminus V(D_f)$. Pokud $P \in V \smallsetminus V(D_f)$, pak existuje polynomiální funkce $h \in D_f$ taková, že $h(P) \neq 0$. Označíme-li $g = fh \in \Bbbk[V]$, pak na okolí $V \smallsetminus V(h) \ni P$

platí $f = g/h$ a $P \in \operatorname{dom} f$. Nechť naopak $P \in \operatorname{dom} f$. Potom na nějakém okolí $U \ni P$ platí $f = f_1/f_0$, kde $f_0, f_1 \in \Bbbk[V]$. Nechť nyní $h \in I(V \smallsetminus U) \smallsetminus I(P)$. Potom $ff_0h = f_1h$ na celém V a je polynomiální, tj. $f_0h \in D_f$, a přitom $f_0h(P) \neq 0$, takže $P \notin V(D_f)$. □

Poznámka. Druhá část předchozího důkazu je jednoduchá pro V ireducibilní: je-li $f = g/h$, pak $fh = g$ na celém V, takže D_f obsahuje 0 a pak právě všechny jmenovatele, z čehož $V = V(D_f)$ plyne okamžitě.

Důsledek 12.8. *Regulární zobrazení mezi afinními varietami jsou právě polynomiální zobrazení.*

Důkaz. Každá komponenta je regulární funkce, tedy polynomiální. □

Definice 12.9. Řekneme, že kvaziprojektivní varieta je *afinní*, jestliže je izomorfní afinní varietě. Analogicky řekneme, že kvaziprojektivní varieta je *projektivní*, jestliže je izomorfní projektivní varietě.

Cvičení 12.10. Nechť V je afinní. Dokažte, že pak také $V_h = V \smallsetminus V(h)$ je afinní.

Cvičení 12.11. Dokažte, že každé racionální zobrazení $\mathbb{P}^1 \dashrightarrow \mathbb{P}^n$ je regulární.

Cvičení 12.12. Dokažte, že každá racionální funkce $\mathbb{A}^2 \dashrightarrow \Bbbk$, regulární na $\mathbb{A}^2 \smallsetminus \{0\}$, je regulární. (Nápověda: protože je $\Bbbk[\mathbb{A}^2]$ UFD, existuje nejlepší vyjádření.)

Cvičení 12.13. Dokažte, že $\mathbb{A}^2 \smallsetminus \{0\}$ není afinní.

Cvičení 12.14. Dokažte, že $\mathbb{P}^2 \smallsetminus \{0\}$ není afinní.

13. Dominantní zobrazení a biracionální ekvivalence

Předpokládejme, že V, W jsou ireducibilní kvaziprojektivní variety a $f\colon V \dashrightarrow W$ racionální zobrazení. Pro $g \in \Bbbk(W)$ se může jednoduše stát, že gf není definované nikde (stačí aby $\operatorname{im} f \cap \operatorname{dom} g = \emptyset$) a obecně tedy nelze definovat $f^*\colon \Bbbk(W) \to \Bbbk(V)$ jako pro polynomiální zobrazení mezi afinními varietami a jejich souřadnicové okruhy.

Příklad 13.1. Nelze složit $\mathbb{A}^1 \to \mathbb{A}^2$, $t \mapsto (t, 0)$ s racionální funkcí $\mathbb{A}^2 \to \Bbbk$, $(x, y) \mapsto x/y$.

Zabývejme se nyní podmínkou na racionální zobrazení f, aby byla kompozice gf vždy definovaná. Protože je $\operatorname{dom} g$ neprázdná otevřená podmnožina, musí platit, že $\operatorname{im} f$ protne každou neprázdnou otevřenou podmnožinu, tj. $\operatorname{im} f$ musí být hustá podmnožina. Naopak, v takovém případě je gf definováno na neprázdné otevřené podmnožině $f^{-1}(\operatorname{dom} g) \subseteq \operatorname{dom} f$.

Definice 13.2. Řekneme, že racionální zobrazení $f\colon V \dashrightarrow W$ je *dominantní*, jestliže $\operatorname{im} f \subseteq W$ je hustá podmnožina.

Podle předhozí analýzy pak každé dominantní zobrazení $f\colon V \dashrightarrow W$ indukuje homomorfismus algeber $f^*\colon \Bbbk(W) \to \Bbbk(V)$.

Lemma 13.3. *Jsou-li $f\colon V \dashrightarrow W$ a $g\colon W \dashrightarrow X$ dvě dominantní zobrazení, pak $gf\colon V \dashrightarrow X$ je opět dominantní zobrazení.*

Důkaz. Výše jsme zdůvodnili, proč je gf definované na neprázdné otevřené podmnožině, zjevně se jedná o racionální zobrazení. Přitom

$$\operatorname{im} gf = g(\operatorname{im} f \cap \operatorname{dom} g)$$

a uzávěr obrazu tedy musí obsahovat obraz uzávěru $\overline{\operatorname{im} f \cap \operatorname{dom} g} = \operatorname{dom} g$, tedy $\operatorname{im} g$; přitom $\overline{\operatorname{im} g} = X$. (Jinak – z topologie asi znáte, že spojitost je ekvivalentní $g(\overline{A}) \subseteq \overline{g(A)}$; vezměte $A = \operatorname{im} f \cap \operatorname{dom} g$.) □

Definice 13.4. Řekneme, že dominantní zobrazení $f\colon V \dashrightarrow W$ je *biracionální ekvivalence*, jestliže existuje dominantní zobrazení $g\colon W \dashrightarrow V$ takové, že $gf = \mathrm{id}$, $fg = \mathrm{id}$.

Podle předchozího pak každá biracionální ekvivalence indukuje izomorfismus algeber $\Bbbk(W) \cong \Bbbk(V)$. Naším dalším cílem bude ukázat i obrácené tvrzení. K tomu bude výhodné přejít k afinním varietám. To je možné proto, že pro ireducibilní kvaziprojektivní varietu V a její libovolnou neprázdnou otevřenou podmnožinu U je inkluze $U \hookrightarrow V$ biracionální ekvivalence s inverzí "id" $: V \dashrightarrow U$ (reprezentovanou $\mathrm{id}\colon U \to U$). Každá kvaziprojektivní varieta V je tedy biracionálně ekvivalentní projektivní varietě $\overline{V}$ a dále pak afinní varietě $\mathbb{A}^n \cap \overline{V}$.

Zabývejme se tedy nyní případem ireducibilních afinních variet, pro které lze jednoduše spočítat $\Bbbk(V)$ jako podílové těleso souřadnicového okruhu $\Bbbk[V]$. Takto lze určit i algebru racionálních funkcí na kvaziprojektivních varietách, např. $\Bbbk(\mathbb{P}^n) \cong \Bbbk(\mathbb{A}^n) = \Bbbk(x_1/x_0, \ldots, x_n/x_0)$.

Lemma 13.5. *Racionální zobrazení $f\colon V \dashrightarrow W$ mezi afinními varietami je dominantní, právě když je $f^*\colon \Bbbk[W] \to \Bbbk(V)$ injektivní. (Stačí V afinní.)*

Důkaz. Dominantnost znamená, že na $\operatorname{im} f$ se nulují pouze polynomy z $I(W)$, tj. z rovnosti $gf = 0$ pro $g \in \Bbbk[W]$ plyne $g = 0$. To je ale přesně injektivita f^*. □

Předchozí lemma dává algebraický popis dominantnosti. Indukované zobrazení na tělesech racionálních funkcí pak dostaneme jako jednoznačné rozšíření f^* na $f^*\colon \Bbbk(W) \to \Bbbk(V)$, $f^*(g/h) = f^*(g)/f^*(h)$ (každý injektivní homomorfismus z oboru integrity do tělesa lze jednoznačně rozšířit na podílové těleso).

Tvrzení 13.6. *Ke každému homomorfismu $\Bbbk$-algeber $\varphi\colon \Bbbk(W) \to \Bbbk(V)$ existuje jediné dominantní zobrazení $f\colon V \dashrightarrow W$ takové, že $\varphi = f^*$.*

Důkaz. Tvrzení stačí dokázat pro afinní variety. Opět jsme nuceni položit $f = (\varphi(y_1), \ldots, \varphi(y_m))$ a stejně jako v polynomiálním případě platí $\operatorname{im} f \subseteq W$ a $\varphi = f^*$. Díky tomu je $f^*\colon \Bbbk[W] \hookrightarrow \Bbbk(W) \xrightarrow{\varphi} \Bbbk(V)$ injektivní a tedy je f dominantní. □

Věta 13.7. *Existuje kontravariantní ekvivalence kategorií*

$$\left\{\begin{matrix}\textit{ireducibilní kvaziprojektivní variety}\\ \textit{a dominantní zobrazení}\end{matrix}\right\} \overset{\cong}{\rightleftarrows} \left\{\begin{matrix}\textit{konečně generovaná rozšíření těles}\\ \Bbbk \subseteq K \textit{ a jejich homomorfismy}\end{matrix}\right\}$$

posílající $V \mapsto \Bbbk(V)$.

Důkaz. Stačí opět najít ke každému konečně generovanému rozšíření K afinní varietu V takovou, že $K \cong \Bbbk(V)$. Nechť $K = \Bbbk(a_1, \ldots, a_n)$, potom K je podílové těleso podalgebry $\Bbbk[a_1, \ldots, a_n]$, která je konečně generovaná a redukovaná, existuje tedy afinní varieta V taková, že

$$\Bbbk[a_1, \ldots, a_n] \cong \Bbbk[V]$$

a tedy budou izomorfní i podílová tělesa, $K \cong \Bbbk(V)$. Protože je $\Bbbk[a_1, \dots, a_n]$ obor integrity, je V ireducibilní. □

Důsledek 13.8. *Dvě kvaziprojektivní variety V, W jsou biracionálně ekvivalentní, právě když $\Bbbk(V) \cong \Bbbk(W)$.*

Definice 13.9. Kvaziprojektivní varieta V se nazývá *racionální*, jestliže je biracionálně ekvivalentní $\mathbb{A}^d$ (ekvivalentně $\mathbb{P}^d$).

Zejména je tedy V racionální, právě když je $\Bbbk(V)$ čistě transcendentní, tj. $\Bbbk(V) \cong \Bbbk(x_1, \dots, x_d)$.

Příklad 13.10. Hyperbola je racionální. Uvažujme ji projektivně, tj. $H = V(y_1 y_2 - y_0^2)$. Potom

$$\mathbb{P}^1 \to H, \quad (x_0 : x_1) \mapsto (x_0 x_1 : x_1^2 : x_0^2)$$

(vycházející z afinního předpisu $t \mapsto (t, 1/t)$) je regulární zobrazení s inverzí

$$H \to \mathbb{P}^1, \quad (y_0 : y_1 : y_2) \mapsto (y_0 : y_1).$$

Proto máme $H \cong \mathbb{P}^1$ a díky tomu také $H_0 \simeq \mathbb{A}^1$ (afinní hyperbola je biracionálně ekvivalentní afinní přímce).

V předchozím příkladu lze jednoduše popsat potřebná racionální zobrazení $H_0 \longrightarrow \mathbb{A}^1$ a $\mathbb{A}^1 \dashrightarrow H_0$ a dokázat, že indukují izomorfismus $H_0 \cong \mathbb{A}^1 \smallsetminus \{0\}$. Toto je obecný fenomén:

Věta 13.11. *Ireducibilní kvaziprojektivní variety V, W jsou biracionálně ekvivalentní, právě když existují otevřené husté podmnožiny $V' \subseteq V$, $W' \subseteq W$ takové, že V', W' jsou izomorfní.*

Důkaz. Dostatečnost podmínky je zřejmá, neboť $V \simeq V' \cong W' \simeq W$. Nechť tedy naopak $f\colon V \dashrightarrow W$ je biracionální ekvivalence s inverzí $g\colon W \dashrightarrow V$. Označme

$$V' = \operatorname{dom} f \cap f^{-1}(\operatorname{dom} g), \quad W' = \operatorname{dom} g \cap g^{-1}(\operatorname{dom} f).$$

Potom platí $f(V') \subseteq \operatorname{dom} g$ a můžeme tedy uvažovat obraz $gf(V') = \operatorname{id}(V') \subseteq \operatorname{dom} f$; tedy $f(V') \subseteq W'$ a symetricky také $g(W') \subseteq V'$. Přitom f a g jsou inverzní všude, kde jsou definované, tedy zejména na V', W'. □

DÚ 6. Ukažte, že zobrazení $f\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^2$, $(x_0 : x_1 : x_2) \mapsto (x_1 x_2 : x_2 x_0 : x_0 x_1)$ je biracionální ekvivalence a najděte otevřené podmnožiny $\mathbb{P}^2$, na nichž je f izomorfismus. (Nápověda: napíšete-li si zobrazení afinně, inverze by měla být jasná.)

14. Součin projektivních variet

Uvažujme projektivní prostory $\mathbb{P}^n$, $\mathbb{P}^m$. Jejich součin lze zrealizovat jako podvarietu $\mathbb{P}(\Bbbk^{n+1} \otimes \Bbbk^{m+1}) = \mathbb{P}^{nm+n+m}$, konkrétně uvážíme tzv. *Segreho zobrazení*

$$s_{nm}\colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{nm+n+m}, \quad ([v], [w]) \mapsto [v \otimes w].$$

Jeho obraz nazveme *Segreho varietou* a značíme Σ_{nm}.

Věta 14.1. *Segreho zobrazení je bijekce a Σ_{nm} je projektivní varieta.*

Důkaz. Souřadnice v $\Bbbk^{n+1}$ budeme značit x_i, souřadnice v $\Bbbk^{m+1}$ jako y_j a v $\Bbbk^{n+1} \otimes \Bbbk^{m+1}$ potom z_{ij}. Potom Segreho zobrazení má vyjádření

$$s_{nm}((x_0 : \cdots : x_n), (y_0 : \cdots : y_m)) = \begin{pmatrix} x_0 y_0 : \cdots : x_0 y_m \\ \vdots \quad\quad\quad \vdots \\ x_n y_0 : \cdots : x_n y_m \end{pmatrix} = (\cdots : x_i y_j : \cdots),$$

tj. homogenní souřadnice z_{ij} je rovna $x_i y_j$ (koeficient $\sum x_i e_i \otimes \sum y_j \widetilde{e}_j$ u $e_i \otimes \widetilde{e}_j$ je $x_i y_j$). Zjevně pro souřadnice obrazu platí $z_{ij} z_{kl} = z_{il} z_{kj}$. Nechť Z je varieta zadaná těmito rovnicemi, platí tedy $\Sigma_{nm} \subseteq Z$. Nechť naopak $R = (z_{ij}) \in Z$ a hledejme $P = (x_i) \in \mathbb{P}^n$, $Q = (y_j) \in \mathbb{P}^m$ tak, že $s_{nm}(P, Q) = R$. Alespoň jedna ze souřadnic R je nenulová, nechť je to z_{kl}. Protože má být

$$P = (x_0 : \cdots x_n) = (x_0 y_l : \cdots : x_n y_l) = (z_{0l} : \cdots : z_{nl}),$$

jsme nuceni položit $P = (z_{0l} : \cdots : z_{nl})$ a analogicky $Q = (z_{k0} : \cdots : z_{km})$ (jsou dobře definovány, protože obsahují komponentu $z_{kl} \neq 0$). Potom je $s_{nm}((z_{0l} : \cdots : z_{nl}), (z_{k0} : \cdots : z_{km}))$ rovno

$$(\cdots : z_{il} z_{kj} : \cdots) = (\cdots : z_{ij} z_{kl} : \cdots) = (\cdots : z_{ij} : \cdots). \qquad \square$$

Odteď budeme $\mathbb{P}^n \times \mathbb{P}^m$ ztotožňovat se Σ_{nm} a chápat tedy jako projektivní varietu. Z předchozího důkazu navíc vidíme, že obě projekce $\pi_1 \colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^n$ a $\pi_2 \colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$ jsou regulární (v prvním případě zadané $(\cdots : z_{ij} : \cdots) \mapsto (z_{0l} : \cdots : z_{nl})$ a každý bod leží v definičním oboru takového zobrazení pro vhodné l).

Řekneme, že polynom $f \in \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_m]$ je *bihomogenní* stupně (r, s), jestliže je homogenní stupně r v proměnných x_i a homogenní stupně s v proměnných y_j.

Věta 14.2. *Nechť $V \subseteq \mathbb{P}^n$, $W \subseteq \mathbb{P}^m$ jsou projektivní variety. Potom $V \times W \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je také projektivní varieta. Jsou-li obě V, W ireducibilní, pak $V \times W$ je také ireducibilní.*

Obecněji, nechť $S \subseteq \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_m]$ je množina bihomogenních polynomů. Potom $V(S) \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je projektivní varieta. Naopak, každá varieta $X \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je tohoto tvaru.

Důkaz. Platí $V \times W = {\pi_1}^{-1}(V) \cap {\pi_2}^{-1}(W)$ (nebo lze použít obecnější druhé tvrzení na bihomogenní polynomy zadávající V a W). Ireducibilita se dokáže stejně jako u afinních variet.

Je-li f bihomogenní stupně (r, r), pak jej lze psát jako homogenní polynom stupně r v proměnných $x_i y_j = z_{ij}$ a je tedy $(\mathbb{P}^n \times \mathbb{P}^m) \cap V(f)$ projektivní varieta. Přitom platí $V(f) = V(x_0 f, \ldots, x_n f)$ a takto lze změnit stupeň polynomu f z (r, s) na $(r+1, s)$, analogicky na $(r, s+1)$, a lze tedy dosáhnout stejného stupně v obou skupinách proměnných. $\square$

Důsledek 14.3. *Segreho varieta je ireducibilní.*

Důkaz. To plyne z toho, že projektivní prostor $\mathbb{P}^n$ je ireducibilní (protože je $\mathbb{P}^n = \overline{\mathbb{A}^n}$, plyne toto jednoduše z ireducibility $\mathbb{A}^n$). $\square$

Tvrzení 14.4. *Nechť W je kvaziprojektivní varieta. Potom $\Delta_W \subseteq W \times W$ je uzavřená. Jsou-li $f, g \colon V \to W$ dvě regulární zobrazení mezi kvaziprojektivními varietami, pak podmnožina $\{P \in V \mid f(P) = g(P)\}$ je uzavřená ve V.*

Důkaz. Zjevně platí $\Delta_W = (W \times W) \cap \Delta_{\mathbb{P}^m}$, takže stačí ukázat uzavřenost $\Delta_{\mathbb{P}^m} \subseteq \mathbb{P}^m \times \mathbb{P}^m$. Přitom platí $(x_0 : \cdots : x_m) = (y_0 : \cdots : y_m)$, právě když $x_i y_j = x_j y_i$. Pro druhou část si pak stačí uvědomit, že množina ze zadání je $(f, g)^{-1}(\Delta_W)$, kde $(f, g) \colon V \to W \times W$. $\square$

Věta 14.5 (o projekci). *Projekce $\pi\colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$ je uzavřená.*

K důkazu věty budeme potřebovat následující úvahu. Nechť $P_0 \in \mathbb{P}^n$ je bod, pro jednoduchost budeme předpokládat $P_0 = (0 : \cdots : 0 : 1)$, a $X \subseteq \mathbb{P}^n$ projektivní varieta. Budeme uvažovat projekci p z P_0 na komplementární podprostor $\mathbb{P}^{n-1}$; geometricky je $p(Q)$ průsečík přímky $\overline{P_0Q}$ s $\mathbb{P}^{n-1}$. V souřadnicích pak $p(x_0 : \cdots : x_{n-1} : x_n) = (x_0 : \cdots : x_{n-1})$.

Uvažujme pro F, G homogenní stupňů d, e oba jako $F, G \in \Bbbk[x_0, \ldots, x_{n-1}][x_n]$ stupňů d a e, tj. může se jednoduše stát, že vedoucí koeficient F je 0. Vzhledem k tomu, že je to přesně koeficient u ${x_n}^d$, nastane to, právě když $F(P_0) = 0$. Budeme potom psát

$$\mathrm{Res}'(F, G; x_n) = \mathrm{Res}_{d,e}(F, G; x_n)$$

pro rezultantu polynomů F, G chápaných v tomto smyslu – jedná se tedy o determinant čtvercové matice o rozměru $d + e$.

Tvrzení 14.6. *Nechť J je homogenní ideál a $X = V(J)$. Označme $Y = V(\mathrm{Res}'(F, G; x_n) \mid F, G \in J$ homogenní$)$. Potom platí*

- *pokud $P_0 \notin X$, je $Y = p(X)$,*
- *pokud $P_0 \in X$, je $Y = \mathbb{P}^{n-1}$.*

Důkaz. Pokud $P_0 \in X$, bude vedoucí člen každých $F, G \in J$ nulový a tedy $\mathrm{Res}'(F, G; x_n) = 0$. V dalším budeme předpokládat $P_0 \notin X$.

Pokud je $(x_0 : \cdots : x_{n-1}) \in p(X)$, tj. pokud existuje x_n takové, že $(x_0 : \cdots : x_{n-1} : x_n) \in X$, pak mají $F(x_0, \ldots, x_{n-1}, -)$ a $G(x_0, \ldots, x_{n-1}, -)$ společný kořen x_n a jejich rezultanta je tedy nulová. Proto $p(X) \subseteq Y$.

Nechť nyní $(x_0 : \cdots : x_{n-1}) \notin p(X)$. Zvolme $F \in J$ takový, že $F(P_0) \neq 0$. Potom $F(x_0, \ldots, x_{n-1}, -)$ má pouze konečně mnoho kořenů, označme odpovídající body $P_1, \ldots, P_k$. Podle předpokladu neleží v X. Ukážeme, že pak existuje polynom $G \in J$ takový, že $G(P_0) \neq 0, G(P_1) \neq 0, \ldots, G(P_k) \neq 0$. Potom F, G nebudou mít společný kořen a zároveň budou mít koeficient u ${x_n}^d$ nenulový (protože $F(P_0) \neq 0$ a $G(P_0) \neq 0$) a tedy rezultanta $\mathrm{Res}'(F, G; x_n)$ bude nenulová v $(x_0, \ldots, x_{n-1})$. Proto $(x_0 : \cdots : x_{n-1}) \notin Y$.

Zbývá najít polynom G. Předně existuje polynom $G_i \in J$ nenulový na P_i. Vynásobením vhodným polynomem H_i, nulovým na ostatních bodech, ale nenulovým na P_i, a vhodného stupně dostaneme sečtením hledaný $G = H_0G_0 + \cdots + H_kG_k \in J$. □

Důkaz Věty 14.5. Uvažme zobrazení $p\colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{n-1} \times \mathbb{P}^m$, které je v první složce projekcí z libovolného bodu $P_0 \in \mathbb{P}^n$ a ve druhé složce identita, tj. ve vhodných souřadnicích

$$p((x_0 : \cdots : x_{n-1} : x_n), (y_0 : \cdots : y_m)) = ((x_0 : \cdots : x_{n-1}), (y_0 : \cdots : y_m)).$$

Nechť $X \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je projektivní varieta a položme

$$I = (f \in \Bbbk[x_0, \ldots, x_n, y_0, \ldots, y_m] \mid f \text{ bihomogenní, } f|_X = 0);$$

platí $X = V(I)$, protože X je zadána bihomogenními polynomy. Uvažujme nyní

$$J = (\mathrm{Res}'(f, g; x_n) \mid f, g \in I \text{ bihomogenní}),$$

kde varianta rezultanty je definovaná pomocí stupňů f, g vzhledem k proměnným x_i a jedná se o bihomogenní polynom v proměnných $x_0, \ldots, x_{n-1}, y_0, \ldots, y_m$. Zřejmě je

$$\mathrm{Res}'(f, g; x_n)(-, y) = \mathrm{Res}'(f(-, y), g(-, y); x_n),$$

takže předchozí tvrzení říká, že

$$Y = V(J) = p(X) \cup (\mathbb{P}^{n-1} \times \{Q \mid (P_0, Q) \in X\}),$$

a proto $\pi(X) = \pi(Y)$. Věta plyne n-násobnou iterací tohoto kroku. □

Důkaz. Nechť $Z \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je zadaná bihomogenními polynomy $g_1, \dots, g_r$. Pro bod $Q \in \mathbb{P}^m$ je pak v obraze $\pi(Z)$, právě když $V(g_1(-,Q), \dots, g_r(-,Q)) \neq \emptyset$. Podle projektivní věty o nulách to nastane, právě když $\sqrt{(g_1(-,Q), \dots, g_r(-,Q)} \not\supseteq (x_0, \dots, x_n)$, tj. právě když $(g_1(-,Q), \dots, g_r(-,Q)$ neobsahuje žádnou mocninu $(x_0, \dots, x_n)^d$. Stačí tedy ukázat, že

$$T_d = \{Q \in \mathbb{P}^m \mid (g_1(-,Q), \dots, g_r(-,Q)) \not\supseteq (x_0, \dots, x_n)^d\}$$

je uzavřená, neboť $\pi(Z) = \bigcap_{d \geq 0} T_d$. Přitom definující podmínka je zjevně ekvivalentní tomu, že ideál $(g_1(-,Q), \dots, g_r(-,Q))$ neobsahuje všechny monomy stupně d. Uvážíme tedy $\mathbb{k}^d[x_0, \dots, x_n] \cap (g_1(-,Q), \dots, g_r(-,Q))$, což je vektorový prostor generovaný

$$\{g_k(-,Q)x^\alpha \mid \deg g_k(-,Q) + |\alpha| = d\}.$$

To je vlastní podprostor $\mathbb{k}^d[x_0, \dots, x_n]$, právě když každých $D-1$ polynomů $g_k(-,Q)x^\alpha$ je lineárně závislých, kde $D = \dim \mathbb{k}^d[x_0, \dots, x_n]$. Podmínka lineární závislosti lze ekvivalentně napsat jako nulování všech minorů řádu $D-1$ v matici tvořené souřadnicemi všech $g_k(-,Q)x^\alpha$. Přitom každý takový minor je polynomiální výraz v souřadnicích Q.

Důsledek 14.7. *Nechť X je projektivní varieta a Y kvaziprojektivní varieta. Potom projekce $\pi\colon X \times Y \to Y$ je uzavřená.*

Důkaz. Nechť $Z \subseteq X \times Y$ je uzavřená; proto je také Z uzavřená v $\mathbb{P}^n \times Y$. Potom

$$Z = (\mathbb{P}^n \times Y) \cap \overline{Z}$$

a platí $\pi(Z) = Y \cap \pi(\overline{Z})$ a podle předchozí věty je tato množina uzavřená v Y (protože $\pi(\overline{Z}) \subseteq \mathbb{P}^m$ je uzavřená). □

Věta 14.8. *Nechť X je projektivní varieta a $f\colon X \to Y$ libovolné regulární zobrazení. Potom obraz* $\operatorname{im} f \subseteq Y$ *je uzavřený.*

Důkaz. Uvažme graf Γ_f, ten tvoří uzavřenou podmnožinu součinu $X \times Y$, neboť se skládá právě z těch $([x],[y]) \in X \times Y$, pro které pro libovolné lokální vyjádření $f = (f_0 : \dots : f_m)$ platí $y_j f_k(x) = y_k f_j(x)$ (tam, kde není lokální vyjádření definované jsou beztak obě strany nulové). Podle předchozího důsledku je $\operatorname{im} f = \pi(\Gamma_f) \subseteq Y$ uzavřená podmnožina. □

Věta 14.9. *Každá regulární funkce $f\colon X \to \mathbb{k}$ na ireducibilní projektivní varietě X je konstantní.*

Důkaz. Uvažme složení $X \xrightarrow{f} \mathbb{k} \subseteq \mathbb{P}^1$, $P \mapsto (1 : f(P))$. Jedná se o regulární zobrazení a podle předchozí věty je jeho obraz uzavřený. Zároveň ale není roven $\mathbb{P}^1$, neboť je obsažen v $\mathbb{A}^1 = \mathbb{k}$, takže tímto obrazem musí být konečná podmnožina $\mathbb{k}$. Jednoduše se ukáže, že obraz ireducibilní variety při spojitém zobrazení je ireducibilní a proto musí být $\operatorname{im} f$ jednoprvková, tj. f je konstantní. □

Věta 14.10. *Projektivní varieta je afinní, právě když je konečná.*

Důkaz. Ukážeme, že každá ireducibilní komponenta musí být jednoprvková. Nechť X je tedy ireducibilní projektivní varieta a $f\colon X \hookrightarrow \mathbb{A}^n$ vložení. Podle předchozí věty je každá komponenta f konstantní a tedy i f je konstantní. Proto je X vskutku jednobodová. □

Příklad 14.11. Afinní prostor $\mathbb{A}^n$ je projektivní, právě když $n = 0$.

DÚ 7. Dokažte, že obraz regulárního zobrazení $\mathbb{A}^1 \to \mathbb{A}^n$ je uzavřený (nápověda: použijte, že $\mathbb{P}^1 \to \mathbb{P}^n$ je regulární a zkoumejte obraz nevlastního bodu).

Cvičení 14.12. Dokažte, že $\mathbb{A}^2 \smallsetminus \{0\}$ není afinní ani projektivní.

Cvičení 14.13. Dokažte, že $\mathbb{P}^2 \smallsetminus \{0\}$ není afinní ani projektivní.

Cvičení 14.14. Dokažte, že $\mathbb{P}^n \times \mathbb{P}^m$ je biracionálně ekvivalentní $\mathbb{P}^{n+m}$.

Cvičení 14.15. Dokažte, že $\mathbb{P}^1 \times \mathbb{A}^1$ není afinní ani projektivní.

15. Veroneseho zobrazení

Označme $D + 1$ počet všech homogenních monomů stupně d a uvažujme zobrazení

$$\mathbb{P}^n \to \mathbb{P}^D, \quad (x_0 : \cdots : x_n) \mapsto (\cdots : x^\alpha : \cdots)_{|\alpha|=d}.$$

Ukážeme, že je to vložení na podvarietu, které říkáme *Veroneseho varieta.* Předně je jasné, že se jedná o regulární zobrazení, neboť některá ze složek ${x_i}^d$ je vždy nenulová. Podle věty o uzavřeném obraze je pak Veroneseho varieta vskutku projektivní varieta. Popíšeme nyní inverzní zobrazení. Pro ${x_i}^d \neq 0$ lze tuto inverzi reprezentovat jako

$$(\cdots : x^\alpha : \cdots) \mapsto ({x_i}^{d-1} x_0 : \cdots : {x_i}^{d-1} x_n).$$

Nechť $f \in \mathbb{k}^d[x_0, \ldots, x_n]$. Potom varieta $V(f) \subseteq \mathbb{P}^n$ má ve Veroneseho vložení rovnici $\widehat{f} = 0$, která je lineární v souřadnicích x^α. Jinak řečeno, obraz $V(f)$ je průnik Veroneseho variety s projektivní nadrovinou v $\mathbb{P}^D$.

Věta 15.1. *Nechť X je ireducibilní projektivní varieta mající více než jeden bod. Pokud je f libovolný nekonstantní polynom, pak $X \cap V(f) \neq \emptyset$ a $X_f = X \smallsetminus V(f)$ je afinní.*

Důkaz. Díky Veroneseho vložení můžeme předpokládat, že f je lineární. Pokud by $X \cap V(f) = \emptyset$, znamenalo by to, že $X \subseteq \mathbb{P}^D \smallsetminus V(f) \cong \mathbb{A}^D$ a X by byla afinní varieta, což je možné pouze pro bod. Zároveň $X \smallsetminus V(f) \subseteq \mathbb{A}^D$ a je tedy afinní. □

Pro afinní variety předchozí věta neplatí: libovolné dvě rovnoběžné přímky v rovině $\mathbb{A}^2$ mají prázdný průnik, $V(x_1) \cap V(x_1 - 1) = \emptyset$.

Z předchozí věty lze jednoduše vyvodit, že $X_f = X \smallsetminus V(f)$ je afinní také pro každou afinní varietu X. Je totiž zadaná komplementem nulové množiny x_0 ve svém projektivním uzávěru, $X = \overline{X}_{x_0}$, takže $X_f = \overline{X}_{x_0 \widetilde{f}}$. O něco přímější důkaz používá konkrétní konstrukci

$$X_f \cong \{(x,t) \in \mathbb{A}^{n+1} \mid x \in X,\ f(x)t = 1\} = V(I(X), ft - 1);$$

izomorfismus posílá $x \mapsto (x, f(x)^{-1})$ a v opačném směru se jedná o projekci.

Věta 15.2. *Nechť $P \in X$ je bod kvaziprojektivní variety X. Potom afinní otevřená okolí P, tj. otevřená okolí izomorfní nějaké afinní varietě, tvoří bázi okolí P.*

Důkaz. Uvažujme libovolné otevřené okolí $U \ni P$ bodu $P \in X$ kvaziprojektivní variety X. Potom $\overline{X} \smallsetminus U$ je projektivní varieta neobsahující P a existuje tedy homogenní polynom $f \in I(\overline{X} \smallsetminus U) \smallsetminus I(P)$. Proto $P \in \overline{X}_f = \overline{X} \smallsetminus V(f) \subseteq U$ a tedy afinní otevřená okolí tvoří bázi okolí. □

Předchozí věta se hodí k lokálnímu studiu kvaziprojektivních variet, neboť můžeme vždy přejít k afinním varietám.

16. Lokální vlastnosti variet

Pro (ireducibilní) kvaziprojektivní varietu V definujeme tzv. *strukturní svazek* jako soubor algeber $\mathcal{O}(U)$ pro každou otevřenou podmnožinu $U \subseteq V$,

$$\mathcal{O}(U) = \{f \in \Bbbk(V) \mid f \text{ je regulární na } U, \text{ tj. } \operatorname{dom} f \supseteq U\}$$

Je-li $U_0 \subseteq U_1$, pak každá funkce regulární na U_1 je zejména regulární na U_0 a máme tedy inkluzi $r_{U_0U_1} \colon \mathcal{O}(U_1) \to \mathcal{O}(U_0)$. Přitom platí $r_{UU} = \mathrm{id}$ a $r_{U_0U_1}r_{U_1U_2} = r_{U_0U_2}$ a v takovém případě mluvíme o *předsvazku* algeber. (Jedná se o kontravariantní funktor z uspořádané množiny všech otevřených podmnožin do kategorie algeber.)

Nyní vysvětlíme a dokážeme vlastnost svazku. Ta zhruba říká, že regulární funkce lze definovat lokálně, tj. máme-li nějaké otevřené pokrytí $U = \bigcup U_\alpha$, tak ke každému systému $f_\alpha \in \mathcal{O}(U_\alpha)$ takovému, že

$$r_{U_\alpha \cap U_\beta, U_\alpha}(f_\alpha) = r_{U_\alpha \cap U_\beta, U_\beta}(f_\beta)$$

(podmínka kompatibility – funkce se shodují na průniku jejich definičních oborů), existuje jediná $f \in \mathcal{O}(U)$ taková, že $r_{U_\alpha U}(f) = f_\alpha$. Tato vlastnost plyne jednoduše z toho, že jsme regulární funkce definovali jako funkce mající lokálně vyjádření f_1/f_0.

Naše předchozí výsledky říkají například $\mathcal{O}(V) = \Bbbk[V]$, $\mathcal{O}(V_h) = \Bbbk[V]_h$ pro afinní varietu V a $\mathcal{O}(X) = \Bbbk$ pro projektivní varietu X.

Definujeme *lokální okruh variety* X v bodě $P \in V$ jako

$$\mathcal{O}_P = \{f \in \Bbbk(V) \mid f \text{ je regulární v bodě } P\}$$

Jelikož je racionální funkce g/h regulární v bodě P, právě když $h(P) \neq 0$, tj. právě když $h \notin \mathfrak{m}_P$, lze ekvivalentně psát $\mathcal{O}_P = \Bbbk[V]_{\mathfrak{m}_P}$. Díky tomuto má $\mathcal{O}_P$ jediný maximální ideál

$$\mathfrak{M}_P = \mathfrak{m}_P\mathcal{O}_P = \{g/h \in \mathcal{O}_P \mid g \in \mathfrak{m}_P\}$$

a je to tedy lokální okruh.

17. Grassmannovy variety

Grassmannova varieta $G(k,n)$ má velice bohatou strukturu. Začneme s tím, že ji popíšeme jako množinu, teprve poté ji nadefinujeme jako projektivní varietu. Jako množina je $G(k,n)$ množina všech k-rozměrných podprostorů ve vektorovém prostoru $\mathbb{K}^n$. Je-li $(v_1,\dots,v_k)$ lineárně nezávislá k-tice vektorů z $\mathbb{K}^n$, pak označme $[v_1,\dots,v_k]$ vektorový podprostor jimi generovaný. Máme tak zobrazení

$$(\mathbb{K}^n)^k \supseteq V(k,n) \xrightarrow{\gamma} G(k,n), \quad (v_1,\dots,v_k) \mapsto [v_1,\dots,v_k]$$

a $G(k,n)$ je jistý kvocient definičního oboru $V(k,n)$ (tj. množiny lineárně nezávislých k-tic vektorů). Není špatné si uvědomit, že se jedná o kvocient podle akce grupy $\mathrm{GL}(k)$ lineárních izomorfismů $\mathbb{K}^k$, která působí na k-ticích vektorů pomocí maticového násobení, tj. nahradí tuto k-tici jinou, složenou z odpovídajících lineárních kombinací,

$$(v_1,\dots,v_k)(a_{ij}) = (\sum v_i a_{i1}, \dots, \sum v_i a_{ik}).$$

Našim cílem nyní bude $G(k,n)$ popsat jako podmnožinu nějakého projektivního prostoru. K tomu využijeme vnější mocninu $\Lambda^k\mathbb{K}^n$ vektorového prostoru $\mathbb{K}^n$. Platí totiž, že vnější součin $v_1 \wedge \cdots \wedge v_k$ se při změně báze změní pouze vynásobením skalárem (konkrétně při změně o akci matice A se součin vynásobí $\det A$). Zobrazení

$$G(k,n) \longrightarrow \mathbb{P}(\Lambda^k\mathbb{K}^n), \quad [v_1,\dots,v_k] \longmapsto [v_1 \wedge \cdots \wedge v_k]$$

je tedy dobře definované, nazývá se *Plückerovo vložení*. Ukážeme nyní, že je injektivní a jeho obrazem je projektivní varieta. K obojímu se budeme snažit z tenzoru $\omega = v_1 \wedge \cdots \wedge v_k$ získat zpět podprostor $[v_1,\dots,v_k]$. Definujme zobrazení

$$\varphi_\omega : \mathbb{K}^n \longrightarrow \Lambda^{k+1}\mathbb{K}^n, \quad v \longmapsto \omega \wedge v.$$

Zřejmě platí

$$[v_1,\dots,v_k] = \ker \varphi_\omega,$$

neboť $v_1 \wedge \cdots \wedge v_k \wedge v = 0$, právě když $v_1,\dots,v_k,v$ jsou lineárně závislé. Z tohoto ihned plyne injektivita Plückerova vložení. Popišme nyní jeho obraz pomocí polynomiálních rovnic. Hlavní ideou je, že jádro zobrazení φ_ω má vždy dimenzi nejvýše k. Platí totiž:

Lemma 17.1. *Jsou-li $u_1,\dots,u_r$ lineárně nezávislé, pak $u_1,\dots,u_r \in \ker\varphi_\omega$, právě když*

$$\omega = u_1 \wedge \cdots \wedge u_r \wedge \omega'.$$

Důkaz. Doplňme $u_1,\dots,u_r$ do báze $\mathbb{K}^n$. Potom $u_{i_1} \wedge \cdots \wedge u_{i_k}$ s $i_1 < \cdots < i_k$ tvoří bázi $\Lambda^k\mathbb{K}^n$. Zapíšeme-li ω v této bázi, je podmínka $u_i \in \ker\varphi_\omega$, tj. $\omega \wedge u_i = 0$ ekvivalentní tomu, že všechny koeficienty u bázových prvků, ve kterých se nevyskytuje u_i, jsou nulové. Proto se ve všech členech musí vyskytovat všechna $u_1,\dots,u_r$ a ω má kýžený tvar. □

Vidíme tedy, že obrazem Plückerova vložení jsou právě ta $\omega \in \Lambda^k\mathbb{K}^n$, pro něž $\ker\varphi_\omega$ má dimenzi alespoň k (přitom větší dimenzi mít nemůže) nebo ekvivalentně φ_ω má hodnost nejvýše $n-k$. To lze říct také tak, že matice φ_ω má všechny minory řádu $n-k+1$ nulové. Protože jsou tyto minory polynomiální výrazy v souřadnicích projektivního prostoru $\mathbb{P}(\Lambda^k\mathbb{K}^n)$, je obrazem Plückerova vložení projektivní varieta. Odteď budeme vždy $G(k,n)$ uvažovat jako varietu v $\mathbb{P}(\Lambda^k\mathbb{K}^n)$.

V následujícím budeme potřebovat, že $G(k,n)$ je ireducibilní. To se jednoduše vidí pomocí zobrazení $\gamma : V(k,n) \to G(k,n)$ definovaného výše. Toto zobrazení je zřejmě regulární a surjektivní (stačilo by i dominantní). Protože je $(\mathbb{K}^n)^k$, a tedy i $V(k,n)$, ireducibilní, bude ireducibilní i obraz $G(k,n)$.

V následujícím se nám bude hodit, že zobrazení γ je otevřené. Základní příklad otevřeného zobrazení v topologii je projekce součinu $X \times Y \to X$ (v algebraické geometrii se toto musí dokázat znovu, protože součin má více otevřených množin). Jednoduchým zobecněním jsou pak tzv. bandly, které vypadají jako součin pouze lokálně. Naše zobrazení je bandl, jak za chvíli ukážeme.

Lemma 17.2. *Nechť X a Y jsou kvaziprojektivní variety. Pak je projekce $X \times Y \to X$ otevřená.*

Důkaz. Tvrzení stačí dokázat pro projektivní variety, protože zúžení otevřeného zobrazení na otevřené podmnožiny je otevřené. Nechť je $U \subseteq X \times Y$ bázová otevřená množina, tedy doplněk $U = (X \times Y) \smallsetminus V(g)$ nulové množiny nějakého polynomu $g = g(x, y)$ (zde x značí systém proměnných x_i, podobně y). Potom $x \in X$ neleží v $\pi(U)$ právě když $g(x, -)$ je nulový na celém Y, tj. $g(x, -) \in I(Y)$. To je ale systém lineárních podmínek na koeficienty $g(x, -) \in K[y_0, \ldots, y_m]$, které závisí polynomiálně na $x_0, \ldots, x_n$. □

Uvažujme podmnožinu $\widehat{U} \subseteq V(k, n)$ danou k-ticemi $(v_1, \ldots, v_k)$, jejichž projekce do $\mathbb{K}^k$ generovaného prvními k bázovými vektory jsou lineárně nezávislé. Jejich vhodnou kombinací, tj. vynásobením vhodnou invertibilní maticí A, můžeme dosáhnout toho, že tyto projekce tvoří standardní bázi $\mathbb{K}^k$. To znamená

$$(v_1, \ldots, v_k)A^{-1} = \begin{pmatrix} A \\ B \end{pmatrix} A^{-1} = \begin{pmatrix} E \\ BA^{-1} \end{pmatrix} = (e_1 + w_1, \ldots, e_k + w_k)$$

Potom $[v_1, \ldots, v_k] = [e_1 + w_1, \ldots, e_k + w_k]$ a navíc báze $(e_1 + w_1, \ldots, e_k + w_k)$ uvedeného tvaru (projekce do $\mathbb{K}^k$ dávají kanonickou bázi) je jediná. To znamená, že zobrazení

$$(\mathbb{K}^{n-k})^k \longrightarrow G(k, n), \quad (w_1, \ldots, w_k) \longmapsto [e_1 + w_1, \ldots, e_k + w_k]$$

je regulární bijekce a není těžké napsat předpis pro jeho inverzi, která je regulární na jisté otevřené množině $U \subseteq G(k, n)$, konkrétně na obraze předchozího zobrazení. Vzhledem k tomu, jak jsme tento izomorfismus odvodili, je zřejmé, že $\gamma(\widehat{U}) = U$ a při uvedené identifikaci $U \cong (\mathbb{K}^{n-k})^k$ má zobrazení předpis

$$\begin{pmatrix} A \\ B \end{pmatrix} \longmapsto BA^{-1}.$$

Ač to tak na první pohled možná nevypadá, jedná se o projekci. To je dáno tím, že $\widehat{U} \cong (\mathbb{K}^{n-k})^k \times \mathrm{GL}(k)$ pomocí

$$\begin{pmatrix} A \\ B \end{pmatrix} \longmapsto (BA^{-1}, A).$$

Shrňme situaci následujícím diagramem

$$\begin{tikzcd}
\mathbb{K}^{(n-k)k} \times \mathrm{GL}(k) \arrow[d, "\mathrm{pr}"'] & \cong & \widehat{U} \arrow[d] & \subseteq & V(k, n) \arrow[d, "\gamma"] \\
\mathbb{K}^{(n-k)k} & \cong & U & \subseteq & G(k, n)
\end{tikzcd}$$

Konstrukci lze provést i s jinými složkami než právě s prvními k. Vzniklé množiny U pokrývají $G(k, n)$ a množiny $\widehat{U}$ pokrývají $V(k, n)$. Jelikož je každé zúžení $\widehat{U} \to U$ otevřené, jednoduše se ukáže, že i celé $\gamma : V(k, n) \to G(k, n)$ je otevřené.

Poznámka. Předchozí izomorfismy mají geometrický význam. Uvažujme $\Bbbk^n = \Bbbk^k \times \Bbbk^{n-k}$. Potom množina U odpovídá těm podprostorům, které protínají $\Bbbk^{n-k}$ pouze v nule a jsou to potom grafy lineárních zobrazení $\Bbbk^k \to \Bbbk^{n-k}$, takže $\hom(\Bbbk^k, \Bbbk^{n-k}) \cong U$. Samozřejmě komplementární podprostory $\Bbbk^n = K \oplus L$ lze volit nezávisle na souřadnicích a dostáváme tak bezsouřadnicovou verzi předchozího; dostaneme pak $\hom(K, L) \cong U$ a $\hom(K, L) \times \mathrm{iso}(\Bbbk^k, K) \cong \widehat{U}$.

Projektivní verze Grassmannovy variety je varieta k-rozměrných projektivních podprostorů v $\mathbb{P}^n$, kterým budeme v dalším říkat *k-roviny*. To je ale to samé, co $(k+1)$-rozměrné vektorové prostory v $\mathbb{K}^{n+1}$, máme tedy

$$\mathbb{G}(k,n) = G(k+1, n+1).$$

Nad $\mathbb{G}(k,n)$ krom $\mathbb{V}(k,n)$ existuje ještě celá řada dalších bandlů (přičemž všechny v jistém smyslu vzniknou z $\mathbb{V}(k,n)$ – jsou k němu tzv. asociované). My budeme potřebovat následující "tautologický bandl"

$$\Sigma = \{(\Lambda, x) \in \mathbb{G}(k,n) \times \mathbb{P}^n \mid x \in \Lambda\} \subseteq \mathbb{G}(k,n) \times \mathbb{P}^n$$

Pomocí Σ definujme pro projektivní varietu $X \subseteq \mathbb{P}^n$ tzv. incidenční varietu $\mathcal{C}_k(X)$ jako

$$\mathcal{C}_k(X) = \{\Lambda \in \mathbb{G}(k,n) \mid X \cap \Lambda \neq \emptyset\} \subseteq \mathbb{G}(k,n).$$

Ukážeme nyní, že se skutečně jedná o variety. V případě Σ to plyne z následujícího

$$([\omega],[v]) \in \Sigma \iff \omega \wedge v = 0.$$

Označíme-li projekce $\pi_1 : \Sigma \to \mathbb{G}(k,n)$ a $\pi_2 : \Sigma \to \mathbb{P}^n$, pak $\mathcal{C}_k(X) = \pi_1(\pi_2^{-1}(X))$ a jde tedy také o projektivní varietu. Poznamenejme, že $\Sigma \to \mathbb{G}(k,n)$ je opět bandl s fibrem $\mathbb{P}^k$.

Řekneme, že *obecný bod x* variety *X má vlastnost P*, jestliže množina bodů $x \in X$ majících tuto vlastnost je otevřená hustá (v případě ireducibilní X tedy otevřená neprázdná) nebo obecněji, pokud množina bodů $x \in X$ majících tuto vlastnost obsahuje nějakou otevřenou hustou podmnožinu.

Věta 17.3. *Nechť $X \subseteq \mathbb{P}^n$ je projektivní varieta. Pak buď každá k-rovina protne X nebo obecná k-rovina neprotne X.*

Důkaz. Ukázali jsme, že $\mathcal{C}_k(X) \subseteq \mathbb{G}(k,n)$ je projektivní varieta. Protože je $\mathbb{G}(k,n)$ ireducibilní, je buď $\mathcal{C}_k(X) = \mathbb{G}(k,n)$ nebo je doplněk otevřená hustá podmnožina. □

Tvrzení 17.4. *Je-li $k \geq l$, tak obecná k-rovina obsahuje obecnou l-rovinu a obecná l-rovina je obsažena v obecné k-rovině.*

Důkaz. Nechť $U \subseteq \mathbb{G}(l,n)$ je otevřená neprázdná. Smysl prvního tvrzení je, že množina

$$V = \{\Lambda \in \mathbb{G}(k,n) \mid \exists \Gamma \in U : \Gamma \subseteq \Lambda\}$$

je otevřená neprázdná. Uvažujme následující zobrazení

$$\delta : \mathbb{K}^{(n+1)(k+1)} \longrightarrow \mathbb{G}(l,n)$$

posílající $(k+1)$-tici vektorů $(v_0, \ldots, v_k)$ na l-rovinu $[v_0, \ldots, v_l]$. Potom $V = \gamma(\delta^{-1}(U))$ a první tvrzení plyne z otevřenosti γ. Druhé tvrzení se ukáže podobně z otevřenosti δ (ta plyne z toho, že to je složení projekce a γ pro l-roviny). □

DÚ 8. Řekneme, že k-rovina K a l-rovina L se protínají *transverzálně* v $\mathbb{P}^n$, jestliže jejich průnik je $(k+l-n)$-rovina. Ukažte, že obecná dvojice $(K, L) \in \mathbb{G}(k,n) \times \mathbb{G}(l,n)$ se protíná transverzálně.

18. Dimenze

Definice 18.1. Řekneme, že projektivní varieta $X \subseteq \mathbb{P}^n$ má *kodimenzi* k, jestliže každá k-rovina protíná X a existuje $(k-1)$-rovina, která X neprotíná. *Dimenzí* X pak nazveme číslo $\dim X = d = n - k$.

V případě, že X má kodimenzi k, existuje podle definice $(k-1)$-rovina neprotínající X, podle Věty 17.3 dokonce obecná $(k-1)$-rovina neprotíná X.

Pro libovolnou projektivní varietu X platí, že každá $(n+1)$-rovina protne X a existuje (-1)-rovina neprotínající X (formálně je (-1)-rovina jediná, a to prázdná množina). Proto je dimenze dobře definovaná a jednoznačná.

Příklad 18.2. Ve dvou triviálních (extrémních) případech, lze zcela charakterizovat variety určité dimenze. Podle definice varieta $X \subseteq \mathbb{P}^n$ má dimenzi 0, tj. kodimenzi n, právě když každá n-rovina (ta existuje jediná a to $\mathbb{P}^n$) protne X, tedy X je neprázdná, a navíc existuje $(n-1)$-rovina, která je s X disjunktní. Potom je ale X afinní a tedy konečná.

Varieta $X \subseteq \mathbb{P}^n$ má dimenzi n, tj. kodimenzi 0, právě když každá 0-rovina, tj. bod, protíná X. To ale znamená, že $X = \mathbb{P}^n$.

Ještě jeden případ, byť poněkud formální, se nám bude v dalším výkladu hodit. Varieta má dimenzi -1, pokud je prázdná (existuje n-rovina disjunktní s X). To sedí s případem variety dimenze 0, která je konečná *neprázdná.*

Lemma 18.3. *Dimenze projektivní variety X je rovna maximu z dimenzí jejích ireducibilních komponent.*

Důkaz. Označme komponenty X_i. Jelikož je každá X_i obsažena v X, plyne přímo z definice, že $\dim X_i \leq \dim X$. Pokud by tato nerovnost byla striktní pro všechna i, byla by pro každé i obecná k-rovina je disjunktní s X_i a následně by byla obecná k-rovina disjunktní s jejich sjednocením X, což by byl spor s $k = \operatorname{codim} X$. □

Víme, že obecná $(k-1)$-rovina je disjunktní s X, takže obecná k-rovina Λ obsahuje $(k-1)$-rovinu Γ disjunktní s X; proto je $X \cap \Lambda$ konečná – leží v afinním $\Lambda \smallsetminus \Gamma$. Platí tedy, že obecná k-rovina protíná X v konečně mnoha bodech (toto by šlo také použít jako definice dimenze).

Ve skutečnosti platí, že počet průsečíků $X \cap \Lambda$ je pro obecnou k-rovinu maximální možný a roven tzv. stupni variety X, kterým se budeme zabývat později v souvislosti s Bezoutovou větou.

V současné chvíli není vůbec jasné, zda dimenze závisí pouze na varietě, nebo i na jejím vložení do $\mathbb{P}^n$. K tomu, abychom tuto nezávislost ukázali, bude potřeba dimenzi popsat jiným, invariantním způsobem. Nechť P je libovolný bod $(k-1)$-roviny $\Lambda \subseteq \mathbb{P}^n$ disjunktní s X. Uvažujme projekci z bodu P. To je regulární zobrazení

$$\pi : \mathbb{P}^n \smallsetminus \{P\} \longrightarrow \mathbb{P}^{n-1}$$

dané volbou nadroviny $\Gamma \subseteq \mathbb{P}^n$. Obraz $\pi(Q)$ je potom jediný průsečík přímky $\overline{PQ}$ s $\Gamma \cong \mathbb{P}^{n-1}$. Ve vhodných souřadnicích, ve kterých $P = (0 : \cdots : 0 : 1)$ a $\Gamma = \mathbb{P}^{n-1}$ má π předpis

$$\pi(x_0 : \cdots : x_n) = (x_0 : \cdots : x_{n-1}).$$

Ukážeme nyní, že obraz $\pi(X)$ má stejnou dimenzi jako X. Zároveň porovnáme další invariant, stupeň transcendence $\operatorname{tr\,deg} \Bbbk(X)$ tělesa $\Bbbk(X)$ racionálních funkcí na X. Jedná se o maximální počet prvků $\Bbbk(X)$ algebraicky nezávislých nad $\Bbbk$. Jsou-li tyto prvky $a_1, \dots, a_s$, je $\Bbbk(a_1, \dots, a_s)$ izomorfní tělesu racionálních funkcí v s proměnných. Každý prvek $\Bbbk(X)$ je algebraický nad $\Bbbk(a_1, \dots, a_s)$. Jelikož je $\Bbbk(X)$ konečně generované, je už rozšíření $\Bbbk(X) : \Bbbk(a_1, \dots, a_s)$ konečné. Platí, že libovolný maximální systém algebraicky nezávislých prvků má stejný počet.

Důkaz. Pokud $a_1, \dots, a_s$ a $b_1, \dots, b_t$ jsou dva maximální systémy algebraicky nezávislých prvků, pak postupně nahradíme první systém maximálním algebraicky nezávislým systémem $a_{i_1}, \dots, a_{i_{s-k}}, b_1, \dots, b_k$ (v indukčním kroku jsou $a_{i_1}, \dots, a_{i_{s-k}}, b_1, \dots, b_k, b_{k+1}$ algebraicky závislé a proto splňují nějakou polynomiální rovnici, která ovšem musí obsahovat jak b_{k+1}, tak některou z a_{i_j} a nahradíme $a_{i_j} \to b_{k+1}$).

$$\begin{tikzcd}
& \Bbbk(X) \arrow[d, no head] \arrow[ddr, no head, "<\infty"] & \\
& \Bbbk(a_{i_1}, \dots, a_{i_{s-k}}, b_1, \dots, b_k, b_{k+1}) \arrow[dl, no head, "<\infty"'] \arrow[dr, no head] & \\
\Bbbk(a_{i_1}, \dots, \widehat{a_{i_j}}, \dots, a_{i_{s-k}}, b_1, \dots, b_k, b_{k+1}) \arrow[dr, no head] & & \Bbbk(a_{i_1}, \dots, a_{i_{s-k}}, b_1, \dots, b_k) \arrow[dl, no head, "\infty"] \\
& \Bbbk(a_{i_1}, \dots, \widehat{a_{i_j}}, \dots, a_{i_{s-k}}, b_1, \dots, b_k) &
\end{tikzcd}$$

Pro $k = s$ dostaneme, že $b_1, \dots, b_s$ je maximální algebraicky nezávislý systém a tedy $s = t$. $\square$

Tvrzení 18.4. *Platí* $\dim \pi(X) = \dim X$ *a* $\operatorname{tr\,deg} \Bbbk(\pi(X)) = \operatorname{tr\,deg} \Bbbk(X)$.

Důkaz. Prvně si uvědomme, že pro první rovnost chceme dokázat $\operatorname{codim} \pi(X) = \operatorname{codim} X - 1$. Nechť tedy $\Delta \subseteq \mathbb{P}^{n-1}$ je libovolná $(k-1)$-rovina. Potom $\pi^{-1}(\Delta) \cup \{P\}$ je k-rovina a proto protíná X. To ale znamená, že Δ protíná $\pi(X)$. Zároveň $\pi(\Lambda)$ je $(k-2)$-rovina disjunktní s $\pi(X)$, protože Λ je disjuktní s X.

Pro výpočet stupňů transcendence připomeňme, že za předpokladu $X \not\subseteq H_0$ je $\Bbbk(X)$ generované $x_1/x_0, \dots, x_n/x_0$, kde předpokládáme, že x_0 není nulové na X, tj. $x_0 \notin I(X)$. Zobrazení $X \to \pi(X)$ je dominantní, lze tedy chápat $\Bbbk(X)$ jako rozšíření $\Bbbk(\pi(X))$. Jako takové je generované jediným prvkem x_n/x_0. Uvažme libovolný homogenní polynom $f \in I(X)$ stupně r, který je nulový na X, ale nikoliv na $P = (0 : \cdots : 0 : 1)$. To znamená, že jeho koeficient u x_n^r je nenulový a fakt, že $f/x_0^r = 0$ v $\Bbbk(X)$ vyjadřuje přesně, že prvek x_n/x_0 je algebraický nad $\Bbbk(\pi(X))$. Je tedy rozšíření $\Bbbk(X) : \Bbbk(\pi(X))$ konečné a proto se stupně transcendence rovnají. $\square$

Důsledek 18.5. *Platí* $\dim X = \operatorname{tr\,deg} \Bbbk(X)$.

Důkaz. Důkaz provedeme indukcí vzhledem ke $k = \operatorname{codim} X$. Pro $k = 0$ máme $X = \mathbb{P}^n$ a

$$\operatorname{tr\,deg} \Bbbk(X) = \operatorname{tr\,deg} \Bbbk(x_1/x_0, \dots, x_n/x_0) = n = \dim X.$$

Je-li X vlastní podvarieta, zvolíme projekci π jako výše a dostáváme

$$\dim X = \dim \pi(X) = \operatorname{tr\,deg} \Bbbk(\pi(X)) = \operatorname{tr\,deg} \Bbbk(X)$$

podle předchozího tvrzení a indukčního předpokladu. $\square$

Důsledek 18.6. *Je-li $X' \subseteq X$ podvarieta projektivní variety X, která neobsahuje žádnou její komponentu, pak* $\dim X' < \dim X$.

Důkaz. Stačí se omezit na případ, kdy X je ireducibilní a tedy X' vlastní podvarieta. Předpokládejme sporem, že $\dim X' = \dim X$ a zvolme $(k-1)$-rovinu Λ disjunktní s X, tím pádem i s X', a uvažme projekci π z Λ (opakovanou projekci z bodů Λ). Stačí ukázat $\pi(X') \subsetneqq \mathbb{P}^d$, protože pak

$$\dim X' = \dim \pi(X') < d = \dim X.$$

Nyní dokážeme, že zúžení $\pi' = \pi|_{X'} \colon X' \to \mathbb{P}^d$ nemůže být surjektivní. Přejděme k afinní podmnožině $\mathbb{A}^d = \mathbb{P}^d{}_{x_0}$ a jejím odpovídajícím vzorům v X a X'. Zvolme libovolný polynom $f \in I(X') \smallsetminus I(X)$, tedy polynom nulový na X', ale nikoliv na X. Protože $x_1, \dots, x_d \in \Bbbk(X)$ tvoří maximální algebraicky nezávislý systém, existuje polynomiální relace

$$p(x_1, \dots, x_d, f) = 0 \text{ v } \Bbbk(X),$$

kde můžeme předpokládat, že $p \in \Bbbk[s_1, \dots, s_d, t]$ je ireducibilní. Protože je $f \neq 0$ na X, není tento polynom rovný t, a tedy ani dělitelný t. Po zúžení na X' tak dostáváme nenulovou polynomiální relaci

$$p(x_1, \dots, x_d, 0) = 0 \text{ v } \Bbbk(X').$$

Proto nejsou $x_1, \dots, x_d$ algebraicky nezávislé v $\Bbbk(X')$ a tedy $(\pi')^* \colon \Bbbk[\mathbb{A}^d] \to \Bbbk(X')$ není injektivní. To ale přesně znamená, že π' není dominantní a tedy ani surjektivní. $\square$

Věta 18.7. *Je-li X projektivní varieta a $V(f)$ nadplocha neobsahující žádnou komponentu X, pak platí* $\dim(X \cap V(f)) = \dim X - 1$.

Důkaz. Podle předchozího důsledku je jistě $\dim(X \cap V(f)) \leq \dim X - 1$. Předpokládejme nyní, že je tato dimenze striktně menší. Potom existuje $(k+1)$-rovina Λ disjunktní s $X \cap V(f)$. Potom ale $X \cap \Lambda$ musí být konečná (leží totiž v afinním $\Lambda \smallsetminus V(f)$) a jistě lze najít k-rovinu $\Gamma \subseteq \Lambda$, která bude s X disjunktní. To je ale spor s tím, že k je kodimenze X. $\square$

Důsledek 18.8. *Každá ireducibilní projektivní varieta $X \subseteq \mathbb{P}^n$ dimenze $n-1$ (tj. kodimenze 1) je nadplocha, tj. $X = V(f)$.*

Důkaz. Je-li $f \in I(X)$ libovolný ireducibilní homogenní polynom (takový existuje, protože je $I(X)$ prvoideál), pak $X \subseteq V(f)$. Protože je však X ireducibilní a téže dimenze, musí být $X = V(f)$. $\square$

Důsledek 18.9. *Je-li* $\operatorname{char} \Bbbk = 0$, *pak každá kvaziprojektivní varieta je biracionálně ekvivalentní nadploše.*

Důkaz. Nechť $x_1, \dots, x_d \in \Bbbk(X)$ je maximální algebraicky nezávislý systém prvků. Potom $\Bbbk(X) : \Bbbk(x_1, \dots, x_d)$ je konečné, proto jednoduché (podle věty o primitivním prvku), řekněme generované prvkem x_{d+1}. Protože je $\Bbbk(X)$ konečně generované, je izomorfní tělesu racionálních funkcí afinní variety $Y \subseteq \mathbb{A}^{d+1}$. Protože je $\operatorname{tr\,deg} \Bbbk(X) = d$, má Y dimenzi d a jedná se o nadplochu. $\square$

Důsledek 18.10. *Každých n homogenních polynomů má společný nenulový kořen, tj. $\emptyset \neq V(f_1, \dots, f_n) \subseteq \mathbb{P}^n$.* $\square$

O počtu těchto řešení pak mluví Bezoutova věta, kterou dokážeme později.

Pomocí předchozí věty lze dimenzi ireducibilní projektivní variety X charakterizovat jako "délku" d nejdelšího řetězce
$$\emptyset \subsetneqq X_d \subsetneqq \cdots \subsetneqq X_0 = X$$
ireducibilních variet (index značí kodimenzi). Podle předchozí věty má totiž každý řetězec délku maximálně d. Navíc ale lze najít $X_1 \subsetneqq X_0$ dimenze přesně $d-1$ a indukcí pak řetězec délky d. V řeči souřadnicových okruhů má tato charakterizace následující vyjádření, ve které je nyní X ireducibilní afinní varieta. Dimenze X je rovna tzv. Krullově dimenzi $\Bbbk[X]$, která je definována jako "délka" d nejdelšího řetězce
$$0 = I_0 \subsetneqq \cdots \subsetneqq I_d \subsetneqq \Bbbk[X]$$
prvoideálů v $\Bbbk[X]$.

Tato definice má tu výhodu, že je vyjádřena v řeči variety samotné (dokonce pouze její topologie) a nezávisí na jejím vložení do projektivního prostoru a je tedy zjevně invariantní vzhledem k izomorfismům.

Věta 18.11. *Nechť je $f : X \to Y$ surjektivní zobrazení mezi projektivními varietami takové, že $d = \dim f^{-1}(y)$ nezávisí na $y \in Y$. Potom*
$$\dim X = \dim Y + d.$$

Důkaz. Můžeme předpokládat, že Y je ireducibilní – jinak ji rozložíme na ireducibilní komponenty. Nechť $Y_0 = Y \cap V(g)$, kde g není nulová na obrazu žádné komponenty X a položme $X_0 = f^{-1}(Y_0) = X \cap V(gf)$. Potom indukcí
$$\dim X = \dim X_0 - 1 = (\dim Y_0 + d) - 1 = \dim Y + d. \qquad \square$$

Jako důsledek vidíme, že není potřeba technický předpoklad v Tvrzení 18.4, totiž že projekce má být z bodu obsaženého v nějaké $(k-1)$-rovině disjunktní s X (nebo lze také nyní nahlédnout, že každý bod je obsažený v takové $(k-1)$-rovině).

Je-li X ireducibilní projektivní varieta, Věta 18.7 říká, že *maximum* z dimenzí komponent $X \cap V(f)$ je rovno $\dim X - 1$. Ve skutečnosti ale platí, že všechny komponenty $X \cap V(f)$ mají dimenzi $\dim X - 1$ (nebo ekvivalentně, že Věta 18.7 platí také pro kvaziprojektivní variety):

Věta 18.12. *Je-li X kvaziprojektivní varieta a $V(f)$ nadplocha neobsahující žádnou komponentu X, pak platí $\dim(X \cap V(f)) = \dim X - 1$.*

DÚ 9. Nechť $f\colon X \to Y$ je surjektivní uzavřené zobrazení mezi Noetherovskými topologickými prostory takové, že pro každou dvojici uzavřených podmnožin $A \subsetneqq B \subseteq X$, kde B je ireducibilní, je $f(A) \subsetneqq f(B)$. Dokažte, že f je otevřené.

** *Důkaz věty.* Uvažme opět konečnou projekci $p\colon X \to \mathbb{P}^d$ takovou, že $V(f) = p^{-1}(\mathbb{P}^{d-1})$ je vzor nadroviny v této projekci – toho se dosáhne pomocí Veroneseho vložení a volbou projekce z podprostoru obsaženého v nadrovině $V(f)$. Nechť $X_0 \subseteq X$ je libovolná komponenta $X \cap V(f)$ a X_1 sjednocení ostatních. Potom $U = X \smallsetminus X_1$ je otevřená a jejím obrazem $p(U) \subseteq \mathbb{P}^d$ je podle předchozího opět otevřená podmnožina. Proto $\mathbb{P}^{d-1} \cap p(U) \subseteq p(X_0)$ a $p(X_0)$ obsahuje otevřenou neprázdnou podmnožinu $\mathbb{P}^{d-1}$. Protože je sama uzavřená, musí být $p(X_0) = \mathbb{P}^{d-1}$ a $\dim X_0 = d - 1$ (tady používáme Větu 18.11 pro projektivní variety). $\square$

S pomocí tohoto rozšíření pak lze rozšířit rozličné definice dimenze i na kvaziprojektivní variety X – pro porovnání ji provizorně definujme jako $\dim \overline{X}$. První definice je, že kodimenze je rovna k, jestliže obecná k-rovina protne X (neprotne totiž vlastní uzavřenou $\overline{X} \smallsetminus X$ menší dimenze) a obecná $(k-1)$-rovina neprotne X (neprotne totiž ani $\overline{X}$). Druhá definice je $\operatorname{tr\,deg} \Bbbk(X)$. Třetí je pak délka d nejdelšího řetězce

$$\emptyset \subsetneqq X_d \subsetneqq \cdots \subsetneqq X_0 = X$$

ireducibilních podmnožin (díky předchozí větě je průnik s nadplochou opět kodimenze 1).

Dále se dá Věta 18.11 rozšířit i na kvaziprojektivní variety; uveďme jednoduchou aplikaci takového rozšíření.

Příklad 18.13. Spočítejme dimenzi Grassmannovy variety $G(k,n)$ elementárním způsobem. Uvažme zobrazení

$$\gamma : V(k,n) \longrightarrow G(k,n), \quad (v_1,\ldots,v_k) \longmapsto [v_1,\ldots,v_k]$$

s definičním oborem $V(k,n)$. Jelikož se jedná o otevřenou podmnožinu v K^{nk}, je $\dim V(k,n) = nk$. Spočítejme dimenzi fibru $f^{-1}(\Lambda)$. Ten se zjevně skládá právě ze všech bází Λ a lze jej tedy ztotožnit s otevřenou podmnožinou K^{k^2} a má dimenzi k^2. Proto

$$nk = \dim V(k,n) = \dim G(k,n) + k^2$$

a konečně $\dim G(k,n) = nk - k^2 = k(n-k)$.

** **Věta 18.14.** *Nechť $f : X \to Y$ je surjektivní zobrazení mezi projektivními varietami a položme*

$$d = \min\{\dim f^{-1}(y) \mid y \in Y\}.$$

Potom množina $U = \{y \in Y \mid \dim f^{-1}(y) = d\}$ je neprázdná otevřená. Jsou-li obě X, Y ireducibilní, pak platí $\dim X = \dim Y + d$.

Důkaz. Nahraďme $X \subseteq \mathbb{P}^n$ grafem f a zobrazení f pak projekcí

$$g \colon X = \Gamma_f \subseteq \mathbb{P}^n \times Y \longrightarrow Y.$$

Nechť minimální dimenze fibru je $d = \dim f^{-1}(y_0)$. Zvolme libovolnou $(n-d-1)$-rovinu $\Lambda \subseteq \mathbb{P}^n$ disjunktní s $f^{-1}(y_0)$. Potom U zřejmě obsahuje komplement vlastní uzavřené množiny $Y_0 = g(\Gamma_f \cap (\Lambda \times Y))$, tj. množinu těch $y \in Y$, pro něž je $f^{-1}(y)$ disjunktní s Λ.

Ukážeme nyní, že U je skutečně otevřená. Kdyby $(Y \smallsetminus Y_0) \subsetneqq U$, zužíme f na Y_0 a použijeme předchozí tvrzení znova. Opět tedy množina těch $y \in Y_0$, pro něž je $\dim f^{-1}(y)$ minimální, obsahuje komplement nějaké vlastní uzavřené množiny $Y_1 \subsetneqq Y_0$. Protože je prostor Y Noetherovský, musí se posloupnost $Y_0 \supsetneqq Y_1 \supsetneqq \cdots$ stabilizovat od nějakého Y_n a tedy $U = Y \smallsetminus Y_n$ je otevřená.

Jsou-li nyní obě X, Y ireducibilní, tak zúžením na U dostáváme $f : f^{-1}(U) \to U$ splňující předpoklady předchozí věty (bez tohoto předokladu by mohlo nastat $\dim f^{-1}(U) < \dim X$ nebo $\dim U < \dim Y$). $\square$

Zajímavým důsledkem je následující.

** **Důsledek 18.15.** *Nechť $f : X \to Y$ je zobrazení mezi projektivními varietami takové, že všechny fibry $f^{-1}(y)$ mají tutéž dimenzi. Jsou-li Y a všechny fibry $f^{-1}(y)$ ireducibilní, je ireducibilní i X.*

Důkaz. Nechť $X = X_1 \cup \cdots \cup X_r$ je rozklad X na sjednocení ireducibilních komponent a nechť $f_i : X_i \to Y$ značí zúžení f na jednotlivé komponenty. Označme d_i minimální dimenzi fibru f_i a nechť d_1 je maximální z nich. Díky předpokladu konstantní dimenze fibrů je pak dimenze $f_1^{-1}(y)$ konstantní a rovna dimenzi $f^{-1}(y)$. Z ireducibility fibrů pak $f_1^{-1}(y) = f^{-1}(y)$ a tedy $X = X_1$ je ireducibilní. □

** 19. Blow-up

Nechť $X \subseteq \mathbb{A}^n$ je ireducibilní afinní varieta dimenze alespoň 1 a $P_0 \in X$ její bod; pro jednoduchost budeme předpokládat $P_0 = 0$. Definujeme *blow-up* variety X v bodě P_0 jako uzávěr

$$\{(P, \ell) \mid P \in X \cap \ell,\ P \neq P_0\} \subseteq \mathbb{A}^n \times \mathbb{P}^{n-1};$$

značíme jej $\widetilde{X}$ (výše uvedená podmnožina je zjevně izomorfní $X \smallsetminus P_0$).

Tečný kužel variety X v bodě P_0 je afinní kužel na průniku tohoto blow-upu s rovinou $P = P_0$ (přímky ℓ jsou sečny X procházející P_0, takže tečný kužel sestává z tečen procházejících P_0).

Zabývejme se nyní rovnicemi zadávajícími blow-up a tečný kužel. Označíme souřadnice na $\mathbb{A}^n$ jako x_i a homogenní souřadnice na $\mathbb{P}^{n-1}$ jako $\widetilde{x}_i$. Pak polynom $g(x, \widetilde{x})$, homogenní v proměnných $\widetilde{x}_i$ stupně d, je nulový na $\widetilde{X}$, právě když $0 = g(x, tx) = t^d g(x, x)$ pro každé $x \in X$, $x \neq 0$, $t \neq 0$. Protože je $X \neq \{P_0\}$, je toto ekvivalentní $g(x, x) = 0$ pro $x \in X$, tj. $g(x, x) \in I(X)$. Pišme $g(x, \widetilde{x}) = \sum_{|\alpha|=d} g_\alpha(x)\widetilde{x}^\alpha$, pak rovnice tečného kužele jsou

$$0 = g(0, \widetilde{x}) = \sum_{|\alpha|=d} g_\alpha(0)\widetilde{x}^\alpha,$$

což je zjevně buď nulový polynom nebo iniciální člen (člen nejmenšího stupně) polynomu $f(x) = g(x, x)$; značíme jej f_{in}. Vidíme tedy, že tečný kužel X v bodě $P_0 = 0$ je

$$V^{\mathrm{af}}(f_{\mathrm{in}} \mid f \in I(X)).$$

Příklad 19.1. Zabývejme se křivkou $V(y^2 - x^3 - x^2)$. Její tečný kužel v počátku je $V(y^2 - x^2) = V(y-x) \cup V(y+x)$ (iniciální člen libovolného násobku $f = y^2 - x^3 - x^3$ je násobkem f_{in}) a je sjednocením dvou přímek které bychom jistě chtěli za tečny považovat. V další kapitole definujeme tečný prostor a uvidíme, že ten je dvourozměrný. Tečný kužel tedy lépe vystihuje intuitivní představu o tečnách.

Protože je X biracionálně ekvivalentní s $X \smallsetminus P_0$ a ta zase s otevřenou hustou podmnožinou $\widetilde{X}$, má blow-up $\widetilde{X}$ stejnou dimenzi jako X a je také ireducibilní. Přitom tečný kužel je afinní kužel na průniku s nadplochou $x = 0$; tento průnik má dimenzi $\dim X - 1$ a tečný kužel tedy opět dimenzi $\dim X$.

Zabývejme se nyní rovnicemi zadávajícími blow-up ještě jednou. Nechť $f = f_d + \mathrm{hot}$ a pišme $\widetilde{f}$ pro libovolný polynom vzniklý z f tím, že v každém jeho členu nahradíme libovolných d proměnných x_i proměnnými $\widetilde{x}_i$. Označme J ideál generovaný množinou

$$J = (\{x_i\widetilde{x}_j - x_j\widetilde{x}_i \mid i, j = 1, \dots, n\} \cup \{\widetilde{f} \mid f \in I(X)\}).$$

Tvrdíme nyní, že $\widetilde{X} = V(J)$. Zjevně $\widetilde{X} \subseteq V(J)$ a pro $(x, [\widetilde{x}]) \in V(J)$ s $x \neq 0$ je nutně $\widetilde{x} = tx$ nenulový násobek x a proto $\widetilde{f}(x, \widetilde{x}) = \widetilde{f}(x, tx) = t^d f(x)$, takže $x \in X$ a tedy $(x, [\widetilde{x}]) \in \widetilde{X}$. Zbývá tedy ověřit, že $\widetilde{X}$ a $V(J)$ se shodují i pro $x = 0$. Podle předchozího už známe tečný kužel a je jasné, že $(0, [\widetilde{x}]) \in V(J)$ musí splňovat $\widetilde{f}(0, \widetilde{x}) = f_{\mathrm{in}}(\widetilde{x})$, takže opravdu $(0, [\widetilde{x}]) \in \widetilde{X}$.

Příklad 19.2. Vraťme se ještě ke křivce $X = V(y^2 - x^3 - x^2)$ a popišme její blow-up v počátku. Podle předchozího je $\widetilde{X} = V(x\widetilde{y} - y\widetilde{x}, \widetilde{y}^2 - x\widetilde{x}^2 - \widetilde{x}^2)$.

Zajímavý je popis v nějakém afinním kusu $\mathbb{A}^2 \times \mathbb{P}^1$, konkrétně pro $\widetilde{x} = 1$, $\widetilde{y} = t$ je $y = \frac{x\widetilde{y}}{\widetilde{x}} = xt$. Potom rovnice vychází $t^2 - x - 1$ a bude se jednat o parabolu, zejména nebude obsahovat žádnou singularitu. Obecně pro křivku X platí, že opakovanou aplikací blow-upu v bodech singularity dostaneme po konečném počtu kroků nesingulární křivku.

Blow-up $\widetilde{\mathbb{A}}^2$ je pokryt afinními prostory následujícím způsobem:

$$\mathbb{A}^2 \to \widetilde{\mathbb{A}}^2, \quad (s, t) \mapsto (s(1, t), (1 : t))$$

(s inverzí $((x, y), (\widetilde{x} : \widetilde{y})) \mapsto (x, \widetilde{y}/\widetilde{x})$) a dále analogickou mapou $(s, t) \mapsto (t(s, 1), (s : 1))$. V této mapě je pak $\widetilde{X}$ popsáno rovnicemi $\widetilde{f}(s, st, 1, t)$. Předpokládáme-li, že původní polynom f obsahoval nějakou mocninu x^e (v opačném případě by byl $f = yg$ rozložitelný; lze řešit pro každou komponentu zvlášť), pak bude tato nahrazena $x^{e-d}\widetilde{x}^d$ v $\widetilde{f}$ a posléze s^{e-d}. **Co když** $e - d = 0$**?** Po konečném množství blow-upů pak bude tento polynom nižšího iniciálního stupně a po dalším konečném množství blow-upů pak dokonce lineární.

20. Tečný prostor

Definujme pro ideál $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ jeho *lineární část* v bodě $P \in \mathbb{A}^n$ jako

$$I_P^{(1)} = \{\mathrm{d}f(P) \mid f \in I\} \subseteq \mathbb{k}^{(1)}[x_1, \ldots, x_n],$$

kde $\mathrm{d}f(P) = \frac{\partial f(P)}{\partial x_0}\,\mathrm{d}x_0 + \cdots + \frac{\partial f(P)}{\partial x_n}\,\mathrm{d}x_n$ (a kde $\mathrm{d}x_i = x_i$ jakožto lineární forma na $\mathbb{k}^n$). (Pokud je $P = 0$, jedná se o množinu všech lineárních částí.) *Tečný prostor* $T_P X$ ireducibilní afinní variety X v bodě $P \in X$ je následující rovina

$$T_P X = \{v \in \mathbb{K}^n \mid \forall \alpha \in I(X)_P^{(1)} : \alpha(v) = 0\}.$$

Bod $P \in X$ se nazývá *nesingulární* nebo *hladký*, jestliže $\dim T_P X = \dim X$ (ekvivalentně $C_P X = T_P X$). Duální prostor k $T_P X$ je izomorfní

$$T_P^* X = \mathbb{K}^{(1)}[x_1, \ldots, x_n]/I(X)_P^{(1)},$$

je totiž zobrazení $\mathbb{K}^{(1)}[x_1, \ldots, x_n] \cong (\mathbb{K}^n)^* \longrightarrow (T_P X)^*$ (dané zúžením lineární formy na podprostor) surjektivní s jádrem právě $I(X)_P^{(1)}$.

Zabývejme se nyní krátce tečným prostorem projektivních variet. Uvažujme zobrazení

$$\mathbb{k}^{n+1} \smallsetminus \{0\} \to \mathbb{P}^n, \quad x \mapsto [x].$$

V afinní mapě U_i se jedná o zobrazení $(x_0, \ldots, x_n) \mapsto (x_0/x_i, \ldots, \widehat{x_i/x_i}, \ldots, x_n/x_i)$ a tedy jeho diferenciál v $x = (x_0, \ldots, x_n)$ je surjektivní s jádrem daným

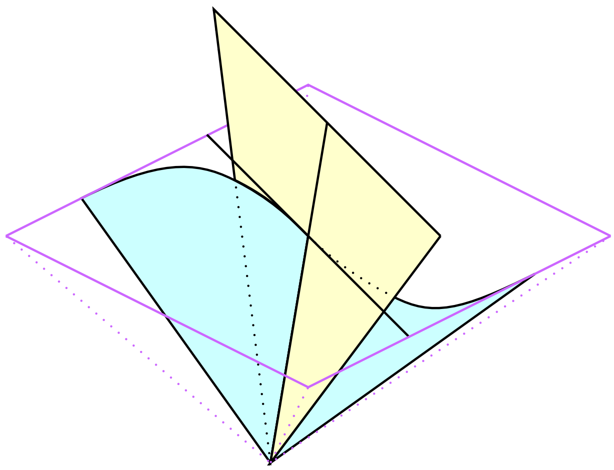
$$(x_i \mathrm{d}x_j - x_j \mathrm{d}x_i)/{x_i}^2 = 0, \quad j = 0, \ldots, \widehat{i}, \ldots, n.$$

Řešením této soustavy jsou právě násobky x, tedy $\Bbbk^{n+1}/[x] \xrightarrow{\cong} T_{[x]}\mathbb{P}^n$, nezávisle na volbě afinní mapy. Pro $f \in I(X)$ homogenní a $x = (1, x_1, \dots, x_n)$, $[x] \in X$, platí, že f je nulové na přímce $[x] \subseteq \Bbbk^{n+1}$, takže $\ker \mathrm{d}f(x) = [x] + \ker \mathrm{d}f|_{x_0=1}(x)$. Lze tedy ztotožnit

$$\ker \mathrm{d}f|_{x_0=1}(x) \cong \ker \mathrm{d}f(x)/[x]$$

a ve výsledku tak

$$T_{[x]}X = \bigcap_{f \in I(X) \text{ homog.}} \ker \mathrm{d}f(x)/[x].$$



Věta 20.1. *Nechť* $\operatorname{char} \Bbbk = 0$. *Množina nesingulárních bodů ireducibilní kvaziprojektivní variety tvoří neprázdnou otevřenou podmnožinu.*

Důsledek 20.2. *Dimenze ireducibilní variety* X *je rovna* $\dim X = \min\{\dim T_P X \mid P \in X\}$.

Důkaz. Popišme prvně množinu těch bodů P, pro něž má $T_P X$ minimální dimenzi $d = n - k$ ze všech tečných prostorů. Ta je dána tím, že nějakých k diferenciálů $\mathrm{d}f_1(P), \dots, \mathrm{d}f_k(P)$ je lineárně nezávislých, kde $f_1, \dots, f_k \in I(X)$, tedy nenulovostí nějakého determinantu. Je tedy vskutku otevřená.

Zbývá ukázat, že $d = \dim X$. Z následujícího tvrzení plyne, že dimenze tečných prostorů se zachovávají při biracionální ekvivalenci $f\colon X \dashrightarrow Y$ variet: prvně platí

$$T^*_{f(P)}Y \cong \mathfrak{M}_{f(P)}\mathfrak{M}^2_{f(P)} \cong \mathfrak{M}_P/\mathfrak{M}^2_P \cong T^*_P X,$$

pokud je $P \in \operatorname{dom} f$ a za druhé z otevřenosti množiny bodů, kde $\dim T_P X$ je minimální, plyne, že toto minimum pro nějaký bod $P \in \operatorname{dom} f$ nastane, takže $\dim X \leq \dim Y$; analogickým tvrzením pro inverzi dostaneme opačnou nerovnost. Protože je každá varieta biracionálně ekvivalentní s nadplochou, stačí rovnost $d = \dim X$ ověřit pro ireducibilní nadplochu $X = V(f)$ (tj. f je ireducibilní polynom). Přitom je zřejmé, že platí $T_P X = \ker \mathrm{d}f(P)$ a stačí tedy ukázat, že diferenciál $\mathrm{d}f$ je v nějakém bodě nadplochy X nenulový. Protože má ale $\frac{\partial f}{\partial x_i}$ menší stupeň než f, plyne z $\frac{\partial f}{\partial x_i} \in I(X) = (f)$, že $\frac{\partial f}{\partial x_i} = 0$ a f je potom konstantní, což je spor s ireducibilitou. $\square$

Tvrzení 20.3. *Tečný prostor T_PX afinní variety X je duální k $\mathfrak{m}_P/\mathfrak{m}_P^2 \cong \mathfrak{M}_P/\mathfrak{M}_P^2$, kde $\mathfrak{m}_P \subseteq K[X]$ je maximální ideál příslušný bodu P a $\mathfrak{M}_P \subseteq \mathcal{O}_{X,P}$ je maximální ideál lokálního okruhu X v P.*

Důkaz. Nechť polynomiální funkce $f \in \mathbb{K}[X]$ je zúžením polynomu F. Definujeme diferenciál f v bodě $P \in X$ jako $\mathrm{d}f(P) = \mathrm{d}F(P)|_{T_PX}$. Jelikož se každé dva polynomy F liší o prvek $I(X)$, jehož diferenciál je nulový na T_PX, je $\mathrm{d}f(P)$ dobře definované linearní forma na T_PX, tj. $\mathrm{d}f(P) \in (T_PX)^*$. Je-li $f \in \mathfrak{m}_P^2$, tedy součet polynomiálních funkcí tvaru gh, kde $g, h \in \mathfrak{m}_P$ jsou nulové v P, pak podle Leibnizova pravidla

$$\mathrm{d}f(P) = \mathrm{d}(gh)(P) = \mathrm{d}g(P) \cdot \underbrace{h(P)}_{0} + \underbrace{g(P)}_{0} \cdot \mathrm{d}h(P) = 0.$$

Máme tedy dobře definované zobrazení

$$D_P : \mathfrak{m}_P/\mathfrak{m}_P^2 \longrightarrow (T_PX)^* \cong \mathbb{K}^{(1)}[x_1, \ldots, x_n]/I(X)_P^{(1)}.$$

Jelikož je každá lineární funkce α diferenciálem afinní funkce $\alpha - \alpha(P) \in \mathfrak{m}_P$, je D_P surjektivní.

Pro injektivitu nechť $f \in \mathfrak{m}_P$. Taylorův „rozvoj“ v bodě P (ve skutečnosti polynom) dává

$$f(x) = \underbrace{f(P)}_{0} + \mathrm{d}f(P)(x - P) + \cdots,$$

kde další členy již zjevně leží v $\mathfrak{m}_P^2$, protože vždy obsahují součiny alespoň dvou lineárních činitelů $(x_i - p_i) \in \mathfrak{m}_P$. Je-li tedy $\mathrm{d}f(P) = 0$, pak $f \in \mathfrak{m}_P^2$ a D_P je izomorfismus.

Zobrazení D_P má zjevné rozšíření na $\mathfrak{M}_P/\mathfrak{M}_P^2$, totiž

$$D_P\left(\frac{g}{h}\right) = \frac{\mathrm{d}g(P) \cdot h(P) - g(P) \cdot \mathrm{d}h(P)}{h(P)^2} = \frac{\mathrm{d}g(P)}{h(P)}$$

(neboť je $g(P) = 0$), a proto je nutně zobrazení $\mathfrak{m}_P/\mathfrak{m}_P^2 \to \mathfrak{M}_P/\mathfrak{M}_P^2$ injektivní. Surjektivita plyne z toho, že každý prvek $\mathfrak{M}_P$ lze vyjádřit jako $\frac{g}{h}$, kde $h(P) = 1$ a pak platí

$$\frac{g}{h} = \frac{g}{1 + (h-1)} \equiv g(1 - (h-1)) \pmod{\mathfrak{M}_P^2}$$

(totiž $(1 + (h-1))(1 - (h-1)) = 1 - (h-1)^2 \equiv 1$), kde pravá strana leží v $\mathfrak{m}_P$. □

21. Stupeň

Věta 21.1 (Bezoutova věta, elementární verze)**.** *Nechť $X, Y \subseteq \mathbb{P}^2$ jsou dvě křivky zadané homogenními polynomy $X = V(f), Y = V(g)$. Potom počet jejich průsečíků je maximálně $|X \cap Y| \leq \deg f \cdot \deg g$.*

Důkaz. Zvolme souřadnice tak, že $(0 : 0 : 1) \notin X \cup Y$ a že žádné dva průsečíky neleží na přímce procházející tímto bodem. To znamená, že můžeme předpokládat

$$f = x_2^d + \cdots, \quad g = x_2^e + \cdots.$$

Bod $(x_0 : x_1 : x_2)$ je průsečíkem, právě když polynomy $f, g \in \mathbb{K}[x_0, x_1][x_2]$ mají společný kořen, tj. právě když rezultant

$$\mathrm{Res}(f, g; x_2) \in \mathbb{K}[x_0, x_1]$$

má kořen $(x_0 : x_1)$. Snadným výpočtem se lze přesvědčit, že $\mathrm{Res}(f, g, x_2)$ je homogenní stupně $d \cdot e$. Platí totiž, že v matici zadávající $\mathrm{Res}(f, g, x_2)$ je na pozici (i, j) buď polynom stupně $i - j$ nebo $i - j + d$, přičemž druhé platí, právě když $j > d$, tj. mezi $(\sigma(1), 1), \ldots, (\sigma(n), n)$ je to právě e-krát. Tvrzení plyne z toho, že každý kořen $\mathrm{Res}(f, g; x_2)$ odpovídá nejvýše jednomu průsečíku. □

Poznámka. S trochou práce lze ukázat, že v případě, že se X, Y protínají v bodě $(x_0 : x_1 : x_2)$ transverzálně, je $(x_0 : x_1)$ jednoduchým kořenem rezultanty $\mathrm{Res}(f, g, x_2)$. To znamená, že když se X, Y protínají transverzálně všude, je počet průsečíků roven přesně součinu stupňů $\deg f \cdot \deg g$ definujících polynomů.

Značí-li $\alpha_1, \ldots, \alpha_d : \mathbb{P}^1 \to \mathbb{P}^2$ nějaké lokální parametrizace kořenů f (například v podobě formálních mocninných řad $\alpha_j(x_0 : x_1) = (x_0 : x_1 : \widetilde{\alpha}_j(x_0 : x_1))$, kde $\widetilde{\alpha}_j \in \mathbb{K}[\![x_0 : x_1]\!]$), lze rezultantu psát (obecně ve vzorci vystupuje vedoucí člen f, který jsme ale prohlásili za 1)

$$\mathrm{Res}(f, g, x_2) = g(\alpha_1) \cdots g(\alpha_d).$$

Derivací v $P = (x_0 : x_1)$ dostáváme za předpokladu, že kořenem f je $\alpha_1(P)$, vztah

$$\mathrm{d}\big(\mathrm{Res}(f, g, x_2)\big)(P) = \mathrm{d}\big(g(\alpha_1)\big)(P) \cdot g(\alpha_2(P)) \cdots g(\alpha_d(P))$$

(ostatní členy vypadnou, protože obsahují $g(\alpha_1(P)) = 0$). Protože tečný prostor $V(f)$ v bodě $\alpha_1(P)$ je dán přesně obrazem $\mathrm{d}\alpha_1(P)$, a jelikož tento neleží v $\ker \mathrm{d}g(\alpha_1(P))$ díky předpokladu transverzality, je diferenciál $\mathrm{d}(g(\alpha_1))(P)$ nenulový a proto je nenulový i celý součin. Ve výsledku je P jednoduchým kořenem rezultanty $\mathrm{Res}(f, g, x_2)$.

V obecném případě (kdy se X, Y neprotínají transverzálně) je potřeba každý průsečík brát s vhodnou násobností, abychom dostali jejich počet rovný $\deg f \cdot \deg g$. V moderní algebraické geometrii se tato násobnost zavádí s pomocí schémat. Průnik $X \cap Y$ ve smyslu schémat obsahuje totiž mnohem více informace než jen body tohoto průniku. Veškerá informace je obsažena v součtu ideálů $I(X) + I(Y)$, který není obecně radikálový a neodpovídá tedy varietě. Radikálový není dokonce ani v případě transverzálního průniku, ale rozdíl mezi $I(X) + I(Y)$ a $I(X \cap Y)$ se vyskytuje pouze v nízkých stupních polynomů, pro $k \gg 0$ je

$$I^{(k)}(X) + I^{(k)}(Y) = I^{(k)}(X \cap Y).$$

V takovém případě říkáme, že tyto ideály mají stejnou saturaci a z hlediska schémat je považujeme za totožné. Stejně jako projektivní variety jsou v bijekci s radikálovými homogenními ideály (po odebrání irelevantního), podschémata projektivního prostoru jsou v bijekci se saturovanými homogenními ideály. Budeme tedy v následujícím pracovat s (téměř) obecnými homogenními ideály a tvářit se, že jsou to geometrické objekty. V případě, že tyto ideály budou radikálové, budeme je ztotožňovat s odpovídajícími projektivními varietami.

Nechť $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ je homogenní ideál. Řekneme, že je *saturovaný*, jestliže pro každý polynom f platí $x_0 f, \ldots, x_n f \in I \Rightarrow f \in I$. Saturace ideálu je nejmenší saturovaný ideál

$$\bar{I} = \{f \in \mathbb{K}[x_0, \ldots, x_n] \mid (\exists k \geq 0) : (\mathfrak{m}_0)^k f \subseteq I\}$$

obsahující I.

Lemma 21.2. *Pro homogenní ideály $I, J \subseteq \mathbb{K}[x_0, \dots, x_n]$ jsou následující podmínky ekvivalentní.*

1. $\bar{I} = \bar{J}$,
2. *pro* $d \gg 0$ *platí* $I^{(d)} = J^{(d)}$.

Důkaz. Prvně dokážeme implikaci (1) $\Rightarrow$ (2) přičemž zjevně stačí, že $I^{(d)} = \bar{I}^{(d)}$ pro $d \gg 0$. To je proto, že $\bar{I} = (f_1, \dots, f_r)$ a každý prvek $f = a_1 f_1 + \cdots + a_r f_r \in \bar{I}$ dostatečně velkého stupně má každé a_i tak velkého stupně, že $a_i f_i \in (\mathfrak{m}_0)^k f_i \subseteq I$. Pro implikaci (2) $\Rightarrow$ (1) si stačí uvědomit, že to, zda $f \in \bar{I}$, závisí pouze na $I^{(d)}$, $d \gg 0$. $\square$

Dejme nyní do souvislosti saturované ideály s projektivní větou o nulách. Platí, že zobrazení

$$\{\text{saturované ideály}\} \xrightarrow{V} \{\text{projektivní variety}\}$$

se zužuje na bijekce mezi radikálovými saturovanými ideály a projektivními varietami (irelevantní ideál $\mathfrak{m}_0$ není saturovaný) a $V(I) = \emptyset$, právě když $1 \in I$.

Nyní vysvětlíme, jaký geometrický objekt lze saturovanému ideálu přiřadit. Předně je to jeho množina nulových bodů $V(I) \subseteq \mathbb{P}^n$, ta však opovídá ideálu $\sqrt{I}$. Nejjednodušším příkladem neradikálového ideálu je $I(X)^2$, o kterém budeme uvažovat jako o množině X "násobnosti dva". Zjemněním $V(I)$ je množina ireducibilních komponent ideálu I, která obsahuje všechny ireducibilní komponenty $V(I)$, ale ještě některé variety navíc. Ty jsou zásadní pro počítání v souřadnicovém okruhu $\mathbb{K}[x_0, \dots, x_n]/I$. Ireducibilní komponenty I se definují pomocí tzv. primárního rozkladu (lze to i příměji, my ale budeme primární rozklad stejně potřebovat).

Řekneme, že homogenní ideál I je *ireducibilní*, jestliže nelze napsat jako průnik dvou striktně větších homogenních ideálů[1]. Protože je $S = \mathbb{K}[x_0, \dots, x_n]$ Noetherovský okruh, tj. neexistuje nekonečná rostoucí posloupnost ideálů, lze každý ideál rozložit jako konečný průnik

$$I = I_1 \cap \cdots \cap I_r$$

ireducibilních homogenních ideálů. Poznamenejme, že tento rozklad není jednoznačný v žádném smyslu. Řekneme, že homogenní ideál I je *primární*, jestliže pro homogenní prvky $f, g \in S$ platí

$$fg \in I \Longrightarrow (f \in I) \vee (g \in \sqrt{I}).$$

Lemma 21.3. *Každý ireducibilní homogenní ideál je primární.*

Důkaz. Nechť $I \subseteq S$ je ireducibilní ideál a $f, g \in S$ dva homogenní prvky splňující $fg \in I$. Definujme homogenní ideály

$$(I : g^k) = \{h \in S \mid hg^k \in I\}$$

které zjevně tvoří neklesající posloupnost

$$(I : g) \subseteq (I : g^2) \subseteq \cdots .$$

[1] Standardně se toto definuje pro nehomogenní, dá se však ukázat, že pro homogenní ideál stačí podmínku zkontrolovat pouze pro průnik homogenních ideálů. To stejné se týká primárnosti.

Díky Noetherovskosti S musí pro nějaké k platit $(I : g^{k+1}) = (I : g^k)$. Jelikož chceme ukázat, že buď $g^k \in I$ nebo $f \in I$ stačí nám díky ireducibilitě I dokázat, že $(I + (f)) \cap (I + (g^k)) = I$. Nechť tedy h leží v tomto průniku a můžeme předpokládat, že je homogenní. Máme

$$hg \in I + (fg) = I,$$

tedy při rozkladu $h = k + lg^k$ musí být $lg^{k+1} \in I$, což znamená $l \in (I : g^{k+1}) = (I : g^k)$ a proto $lg^k \in I$ a konečně $h \in I$. □

Tvrzení 21.4. *Je-li I primární, pak $\sqrt{I}$ je prvoideál.*

Důkaz. Je-li $fg \in \sqrt{I}$, tj. $f^k g^k \in I$, pak buď $f^k \in I$ nebo $g^k \in \sqrt{I}$, každopádně však $f \in \sqrt{I}$ nebo $g \in \sqrt{I}$. □

V dalším nás nebude zajímat rozklad na průnik ireducibilních ideálů, ale primárních ideálů. Platí, že $I \cap J$ je primární, pokud $\sqrt{I} = \sqrt{J} (= \sqrt{I \cap J})$:

$$fg \in I \cap J \Leftrightarrow ((f \in I) \vee (g \in \sqrt{I})) \wedge ((f \in J) \vee (g \in \sqrt{J})) \Leftrightarrow (f \in (I \cap J)) \vee (g \in \sqrt{I \cap J})$$

Můžeme tedy sloučit ty činitele, jejichž radikály jsou stejné a dostaneme rozklad na průnik primárních ideálů, který ovšem stále není jednoznačný. Je-li však $I = I_1 \cap \cdots \cap I_r$ takovýto iredundantní rozklad na primární, tj. takový, že vynecháním libovolného člene se průnik změní, pak $\sqrt{I_1}, \ldots, \sqrt{I_r}$ už na rozkladu nezávisí[2] a příslušné ireducibilní variety $V(I_1), \ldots, V(I_r)$ se nazývají *ireducibilní komponenty* (projektivního schématu zadaného ideálem I). Samozřejmě platí

$$V(I) = V(I_1 \cap \cdots \cap I_r) = V(I_1) \cup \cdots \cup V(I_r).$$

Důležitou výjimku v nejednoznačnosti rozkladu tvoří ideály I_j, pro které je $V(I_j)$ maximální, tj. není obsažené v žádné jiné $V(I_k)$.[3]

Příklad 21.5. $I = (x^2, xy) = (x) \cap (x, y)^2 = (x) \cap (x^2, y)$ (plus obrázek). Ireducibilními komponentami tedy jsou přímka $V(x)$ (tedy osa y) a bod $V(x, y)$ (tedy počátek).

Tvrzení 21.6. *Je-li $V(I) = \{P\}$, pak $I^{(k)} \subseteq S^{(k)}$ má pro $k \gg 0$ konstantní kodimenzi, která je rovna dimenzi "afinního souřadnicového okruhu".*

Důkaz. Předpokládejme, že $P = (1 : 0 : \cdots : 0)$ a uvažme (surjektivní) homomorfismus

$$\varphi : \mathbb{K}[x_0, \ldots, x_n] \longmapsto \mathbb{K}[x_1, \ldots, x_n], \quad f(x_0, \ldots, x_n) \mapsto f(1, x_1, \ldots, x_n)$$

a zúžením na homogenní polynomy stupně k nalevo a polynomy stupně nejvýše k napravo jím indukovaný izomorfismus

$$\varphi_k : \mathbb{K}^{(k)}[x_0, x_1, \ldots, x_n] \xrightarrow{\cong} \mathbb{K}^{(\leq k)}[x_1, \ldots, x_n].$$

Vezmeme nyní kvocient podle obrazů ideálu I a dostaneme izomorfismus

$$\mathbb{K}^{(k)}[x_0, x_1, \ldots, x_n]/I^{(k)} \xrightarrow{\cong} \mathbb{K}^{(\leq k)}[x_1, \ldots, x_n]/\varphi_k(I^{(k)}).$$

[2] Nebudeme to dokazovat, jen uvedeme základní myšlenkou. Tou je charakterizovat tyto prvoideály alternativním způsobem jako ty, které se vyskytují mezi ideály $(I : f)$, $f \in S$.

[3] To se ukáže tak, že $I_j = \ker(S \to (S/I)_{p_j})$, kde $(S/I)_{p_j}$ je lokalizace vzhledem k prvoideálu $p_j = \sqrt{I_j}$.

Ukážeme nyní, že pravá strana je izomorfní "souřadnicovému okruhu" $\mathbb{K}[x_1,\dots,x_n]/\varphi(I)$ pro $k \gg 0$. Podle projektivní věty o nulách $\mathfrak{m}_P = \sqrt{I}$, tj. $(x_1,\dots,x_n)^\ell = (\mathfrak{m}_P)^\ell \subseteq I$ a proto $(\mathfrak{m}_0)^\ell \subseteq \varphi(I)$. Díky tomu je každý prvek $\mathbb{K}[x_1,\dots,x_n]/\varphi(I)$ reprezentován polynomem stupně menšího než ℓ. Je-li tedy $k \geq \ell - 1$ je přirozené zobrazení

$$\mathbb{K}^{(\leq k)}[x_1,\dots,x_n]/\varphi_k(I^{(k)}) \longrightarrow \mathbb{K}[x_1,\dots,x_n]/\varphi(I)$$

surjektivní. Potřebujeme dále ukázat, že pro $k \gg 0$ je

$$\varphi(I) \cap \mathbb{K}^{(\leq k)}[x_1,\dots,x_n] = \varphi_k(I^{(k)}).$$

Implikace $\supseteq$ je triviální. Dále $(\mathfrak{m}_0)^\ell \cap \mathbb{K}^{(\leq k)}[x_1,\dots,x_n] \subseteq \varphi_k(I^{(k)})$ vždy. Jelikož je $\varphi(I)/(\mathfrak{m}_0)^\ell$ konečně rozměrný vektorový prostor generovaný řekněme $\varphi(g_1) + (\mathfrak{m}_0)^\ell, \dots, \varphi(g_r) + (\mathfrak{m}_0)^\ell$, bude pro libovolné $k \geq \max\{\deg g_1, \dots, \deg g_r\}$ platit, že $\varphi(I)$ je generovaný (jako vektorový prostor)

$$\{\varphi(g_1),\dots,\varphi(g_r)\} \cup (\mathfrak{m}_0)^\ell \subseteq \varphi_k(I^{(k)}). \qquad \square$$

Definujeme Hilbertovu funkci homogenního ideálu $I \subseteq \mathbb{K}[x_0,\dots,x_n]$ jako

$$h_I(k) = \dim \mathbb{K}^{(k)}[x_0,\dots,x_n]/I^{(k)}.$$

V následujícím ukážeme, že pro $k \gg 0$ je $h_I(k)$ polynom nad $\mathbb{Q}$ (a to sice tzv. *numerický*, tj. jeho hodnoty v celých číslech jsou celočíselné). Zatím jsme to ukázali pro ideál, jehož asociovaná varieta má jediný bod. K rozšíření na libovolné konečné množiny využijeme rozklad ideálu na ireducibilní komponenty. Je-li $I = I_1 \cap \dots \cap I_r$, kde $V(I_j) = \{P_j\}$, tvrdíme, že pro $k \gg 0$ platí

$$h_I(k) = h_{I_1}(k) + \dots + h_{I_r}(k).$$

Ve skutečnosti nám bude stačit předpokládat $V(I_j)$ po dvou disjunktní, takže se můžeme omezit na $r = 2$, tj. $I = I_1 \cap I_2$. Potom

$$0 \to S/(I_1 \cap I_2) \to S/I_1 \oplus S/I_2 \to S/(I_1 + I_2) \to 0$$

je exaktní[4], přičemž $I_1 + I_2 = S$, alespoň pro $k \gg 0$, neboť $V(I_1 + I_2) = V(I_1) \cap V(I_2) = \emptyset$ a tedy $\overline{I_1 + I_2} = S$. Ve výsledku $h_{I_1 \cap I_2}(k) = h_{I_1}(k) + h_{I_2}(k)$ pro $k \gg 0$.

Primární rozklad pro nás bude užitečný zejména kvůli tomu, že nám umožní poznat dělitele nuly v S/I. Ideál I je totiž primární, právě když každý dělitel nuly v S/I je nilpotentní. Rozklad $I = I_1 \cap \dots \cap I_r$ na primární potom dává následující kritérium:

[4]První zobrazení je $\binom{\mathrm{pr}}{\mathrm{pr}}$ a druhé $(\mathrm{pr}, -\mathrm{pr})$. To je zjevně surjektivní, přičemž jeho jádro jsou právě dvojice $(f + I_1, g + I_2)$ takové, že $f - g \in I_1 + I_2$; změnou reprezentantů pak lze dosáhnout $f = g$ a tedy je tato dvojice obrazem $f + (I_1 \cap I_2)$. Přitom je $f + (I_1 \cap I_2)$ v jádře, právě když $f \in I_1$ a $f \in I_2$, tedy f reprezentuje 0.

Jinak: dvojitý komplex

$$\begin{array}{ccccc} I_1/(I_1 \cap I_2) & \longrightarrow & S/(I_1 \cap I_2) & \longrightarrow & S/I_1 \\ \downarrow & & \downarrow & & \downarrow \\ (I_1 + I_2)/I_2 & \longrightarrow & S/I_2 & \longrightarrow & S/(I_1 + I_2) \end{array}$$

má exaktní řádky, takže totální komplex je exaktní. Navíc je levé vertikální zobrazení izomorfismus, takže kvocient tvořený těmito dvěma členy je také exaktní, tudíž i příslušný podkomplex. To je ale přesně naše posloupnost.

Lemma 21.7. *Jestliže f není nulový na žádné ireducibilní komponentě I, pak $f + I \in S/I$ je nedělitel nuly.*

Důkaz. Pokud $fg \in I$, pak $fg \in I_j \Rightarrow g \in I_j$ pro všechna j, tedy $g \in I$. □

Věta 21.8. *Hilbertova funkce $h_I(k) = \dim \mathbb{K}^{(k)}[x_0, \ldots, x_n]/I^{(k)}$ je pro $k \gg 0$ rovna hodnotě (jediného) numerického polynomu, jehož stupeň je roven $d = \dim V(I)$. Vedoucí koeficient tohoto polynomu je $1/d!$-násobkem přirozeného čísla $\deg I$, které nazýváme stupněm I.*

Důkaz. Větu dokážeme indukcí vzhledem k $\dim V(I)$. Je-li tato dimenze nula, větu jsme již dokázali. Nechť tedy má $V(I)$ nenulovou dimenzi a zvolme libovolný lineární polynom f, který je nenulový na každé ireducibilní komponentě I. Potom násobení f zadává injektivní homomorfismus $S/I \to S/I$ jehož kojádro je zjevně $S/(I + (f))$. Označíme-li $J = I + (f)$ máme tedy exaktní posloupnost

$$0 \to S^{(k-1)}/I^{(k-1)} \to S^{(k)}/I^{(k)} \to S^{(k)}/J^{(k)} \to 0.$$

Pro dimenze tedy platí $h_I(k) - h_I(k-1) = h_J(k)$, neboli $h_I(k) = h_J(k) + h_I(k-1)$ a indukcí pak

$$h_I(k) = h_J(k) + \cdots + h_J(k_0 + 1) + h_I(k_0).$$

Protože $V(J) = V(I + (f)) = V(I) \cap V(f)$, má $V(J)$ dimenzi o jedna menší a můžeme indukcí předpokládat, že pro $k \gg 0$ je

$$h_J(k) = c_{d-1}\tbinom{k}{d-1} + \cdots + c_0\tbinom{k}{0}.$$

Sečtením pak dostáváme pro $k \gg 0$ vyjádření

$$\begin{aligned} h_I(k) &= c_{d-1} \underbrace{\left(\tbinom{k}{d-1} + \cdots + \tbinom{k_0+1}{d-1}\right)}_{\binom{k+1}{d} - \text{const}} + \cdots + c_0 \underbrace{\left(\tbinom{k}{0} + \cdots + \tbinom{k_0+1}{0}\right)}_{\binom{k+1}{1} - \text{const}} + \underbrace{h_I(k_0)}_{\text{const}} \\ &= c_{d-1}\tbinom{k+1}{d} + \cdots + c_0\tbinom{k+1}{1} + \text{const} = \widetilde{c}_d\tbinom{k}{d} + \cdots + \widetilde{c}_1\tbinom{k}{1} + \widetilde{c}_0\tbinom{k}{0} \end{aligned}$$

(poslední rovnost plyne z $\binom{k+1}{i} = \binom{k}{i} + \binom{k}{i-1}$). Z tohoto tvaru je jasné, že vedoucí koeficient je $\widetilde{c}_d/d!$, přičemž $\widetilde{c}_d = c_{d-1}$ je podle indukce přirozené číslo. □

Věta 21.9 (Bezoutova)**.** *Nechť $I \subseteq S$ je libovolný homogenní ideál a nechť $f \in S$ je homogenní polynom, který není nulový na žádné ireducibilní komplonentě I. Potom platí*

$$\deg(I + (f)) = \deg I \cdot \deg f$$

Důkaz. Využijeme exaktní posloupnost z důkazu předchozí věty, tentokrát s posunem o $\deg f$. Označíme $J = I + (f)$ a dostáváme

$$\begin{aligned} h_J(k) &= h_I(k) - h_I(k - \deg f) \\ &= \left(c_d k^d + c_{d-1}k^{d-1} + \text{lot}\right) - \Big(\underbrace{c_d(k - \deg f)^d}_{c_d \cdot k^d - c_d d \deg f \cdot k^{d-1} + \text{lot}} + \underbrace{c_{d-1}(k - \deg f)^{d-1}}_{c_{d-1} \cdot k^{d-1} + \text{lot}} + \text{lot}\Big) \\ &= c_d d \deg f \cdot k^{d-1} + \text{lot} \\ &= \deg I/d! \cdot d \deg f \cdot k^{d-1} + \text{lot} \\ &= \deg I \cdot \deg f \cdot k^{d-1}/(d-1)! + \text{lot} \end{aligned}$$

□

Příklad 21.10. Spočítejme stupeň ideálu (f). V případě, že f nemá násobné činitele v rozkladu na součin ireducibilních polynomů, tedy počítáme stupeň $I(V(f))$, tj. nadplochy $V(f)$. Aplikujeme Bezoutovu větu na ideál $I = 0$, pro který máme

$$h_0(k) = \dim \mathbb{K}^{(k)}[x_0, \dots, x_n] = \binom{k+n}{n}$$

a tedy $\deg \mathbb{P}^n = \deg 0 = 1$; proto je stupeň ideálu (f) roven stupni polynomu f.

Nechť X je křivka. V případě, že je f lineární polynom, je jeho stupeň 1 a je tedy počet průsečíků X s $V(f)$ včetně násobnosti roven stupni $\deg X$. Obecněji toto platí pro průniky variety kodimenze k s k-rovinami. Jelikož lze najít k-rovinu, jejíž všechny průsečíky jsou násobnosti 1, je pak počet průsečíků roven $\deg X$.[5]

Řekneme, že varieta X kodimenze k je *úplný průnik*, jestliže $I(X)$ je generovaný k polynomy. Jsoul-li nyní X, Y úplné průniky komplementární dimenze, které se protínají v konečně mnoha bodech, pak $X \cap Y$ má právě $\deg(I(X)+I(Y)) = \deg X \cdot \deg Y$ bodů počítaných včetně násobnosti.

Důsledek 21.11. *Každý izomorfismus $\mathbb{P}^n \to \mathbb{P}^n$ je lineární.*

Důkaz. Idea důkazu je, že nadroviny jsou právě nadplochy stupně jedna a ty jsou při každém izomorfismu zachovávány. Přitom ale zobrazení zachovávající nadroviny je (alespoň pro $n > 1$ nebo 2) nutně lineární. □

Příklad 21.12. Kubická křivka $X = \{(s^3 : s^2t : st^2 : t^3) \mid (s : t) \in \mathbb{P}^1\} \subseteq \mathbb{P}^3$ není “úplný průnik”, tj. $I(X)$ není generovaný dvěma homogenními polynomy. Skládání s parametrizací dává $\Bbbk[x_0, x_1, x_2, x_3] \to \Bbbk[s, t]$, které posílá polynomy stupně k surjektivně na polynomy stupně $3k$, a jehož jádrem je právě $I(X)$. Proto $h_X(k) = h_{\mathbb{P}^1}(3k) = 3k + 1$. Máme tedy $\deg X = 3$.

Podle Bezoutovy věty by za předpokladu $I(X) = (f, g)$ musel být jeden z polynomů f, g stupně 1, což by ale znamenalo, že X leží v rovině. Jednoduše se lze přesvědčit, že tomu tak není (parametry s, t nesplňují žádnou kubickou rovnici). Dodejme, že existují homogenní polynomy f, g takové, že $X = V(f, g)$ (přičemž vyjde nejspíš $I(X)^2 = (f, g)$, protože polynomy jsou stupňů 2 a 3). V takové, případě říkáme, že X je množinový úplný průnik.

Navíc existují i příklady variet, které nejsou ani množinovým úplným průnikem, například Segreho varieta $\Sigma_{1,2} \subseteq \mathbb{P}^5$ je dimenze 2, ale nelze zadat 3 rovnicemi; stejně to dopadne pro obraz Veroneseho vložení $\mathbb{P}^2 \to \mathbb{P}^5$.

Zabývejme se nyní tím, jak spočítat stupeň nula rozměrného ideálu. Předně pomocí primárního rozkladu zredukujeme problém na ideál “soustředěný” v jednom bodě. Toho dosáhneme pomocí následujícího lemmatu.

Lemma 21.13. *Nechť $I = I_1 \cap I_2$, přičemž $d = \dim V(I_1) = \dim V(I_2) > \dim V(I_1) \cap V(I_2)$. Potom platí $\deg I = \deg I_1 + \deg I_2$.*

[5]Stačí ukázat pro X ireducibilní a $r = \deg X$, že podmnožina $\{(\Lambda, P_1, \dots, P_r) \in \mathbb{G}(k,n) \times X^r \mid P_i \in \Lambda\}$ těch prvků splňujících $P_i = P_j$ pro nějaké $i \neq j$ nebo P_i singulární bod X pro nějaké i nebo $\Lambda \not\pitchfork T_{P_i}X$ pro nějaké i je vlastní. Zřejmě se jedná o sjednocení uzavřených podmnožin, přičemž se jednoduše ukáže, že každá z těchto podmnožin je vlastní. Zbytek plyne z ireducibility.

Důkaz. Využijeme exaktní posloupnosti

$$0 \to S/(I_1 \cap I_2) \to S/I_1 \oplus S/I_2 \to S/(I_1 + I_2) \to 0.$$

Podle ní platí

$$\begin{aligned} h_{I_1 \cap I_2}(k) &= h_{I_1}(k) + h_{I_2}(k) - h_{I_1+I_2}(k) \\ &= \Big(\deg I_1 \cdot k^d/d! + \mathrm{lot}\Big) + \Big(\deg I_2 \cdot k^d/d! + \mathrm{lot}\Big) - \Big(\mathrm{lot}\Big) \\ &= (\deg I_1 + \deg I_2) \cdot k^d/d! + \mathrm{lot}. \end{aligned}$$

□

Je-li tedy I nula rozměrný ideál s primárním rozkladem $I = I_1 \cap \cdots \cap I_r$, pak platí

$$\deg I = \deg I_1 + \cdots + \deg I_r$$

a v následujícím postačí spočítat primární ideál odpovídající bodu $P \in V(I)$, který označme I_P. Stupeň $\deg I_P$ se nazývá *lokálním stupněm* I v bodě P.

Lemma 21.14. *Primární ideál I_P odpovídající bodu $P \in V(I)$ je roven $I + (\mathfrak{m}_P)^k$ pro $k \gg 0$.*

Důkaz. Nechť $I = \bigcap I_j$ je rozklad na průnik primárních ideálů s ireducibilními komponentami $V(I_j) = P_j$. Podle Hilbertovy věty o nulách platí $\sqrt{I_j} = \mathfrak{m}_{P_j}$ a tedy $(\mathfrak{m}_{P_j})^k \subseteq I_j$ pro nějaké $k \gg 0$, takže

$$I + (\mathfrak{m}_{P_j})^k \subseteq I_j.$$

Protože je $V(I + (\mathfrak{m}_{P_j})^k) = \{P_j\}$, má ideál $I + (\mathfrak{m}_{P_j})^k$ jedinou ireducibilní komponentu a jedná se tedy o primární ideál (v rozkladu je pouze jeden člen) a zjevně platí

$$I \subseteq \bigcap (I + (\mathfrak{m}_{P_j})^k) \subseteq \bigcap I_j = I,$$

takže se všechny členy rovnají a první průnik je tedy také rozkladem na průnik primárních ideálů (v tomto případě je navíc rozklad jednoznačný). □

Přejděme nyní k afinním souřadnicím; pak $\varphi(I_P) = \varphi(I + (\mathfrak{m}_P)^k) = \varphi(I) + (\mathfrak{m}_P)^k$. Poznamenejme, že jakmile $\varphi(I) + (\mathfrak{m}_P)^k = \varphi(I) + (\mathfrak{m}_P)^{k+1}$, je již tato společná hodnota rovna $\varphi(I_P)$ (platí $\varphi(I) + (\mathfrak{m}_P)^{k+2} = \varphi(I) + \mathfrak{m}_P(\varphi(I) + (\mathfrak{m}_P)^{k+1}) = \varphi(I) + \mathfrak{m}_P(\varphi(I) + (\mathfrak{m}_P)^k) = \varphi(I) + (\mathfrak{m}_P)^{k+1}$). Toho lze využít pro výpočet $\varphi(I_P)$ – postupně počítat $\varphi(I), \varphi(I) + \mathfrak{m}_P, \varphi(I) + (\mathfrak{m}_P)^2, \ldots$ do okamžiku, kdy se posloupnost zastaví. Jelikož $R/(\mathfrak{m}_P)^k$ lze kanonicky ztotožnit s vektorovým prostorem polynomů stupně menšího než k, lze spočítat kodimenzi

$$\varphi(I_P)/(\mathfrak{m}_P)^k \subseteq R/(\mathfrak{m}_P)^k$$

většinou relativně snadno. Tato kodimenze je rovna dimenzi kvocientu $R/\varphi(I_P)$, tedy $\deg I_P$.

Příklad 21.15. Určete stupně průsečíků $C_2 \cap C_3 = V(x_2 - x_1^2) \cap V(x_2 - x_1^3)$.

Řešení. V projektivním rozšíření dostáváme se průnik $V(x_0 x_2 - x_1^2) \cap V(x_0^2 x_2 - x_1^3)$ skládá právě z bodů

$$P_0 = (1 : 0 : 0),\ P_1 = (1 : 1 : 1),\ P_2 = (0 : 0 : 1).$$

Pro bod P_0 počítejme v afinních souřadnicích $x_0 = 1$:

$$\begin{aligned} \varphi(I) + (\mathfrak{m}_{P_0})^1 &= (x_1, x_2) \\ \varphi(I) + (\mathfrak{m}_{P_0})^2 &= (x_1^2, x_2) = I + (\mathfrak{m}_{P_0})^3 \end{aligned}$$

a tedy $\deg_{P_0} C_2 \cap C_3 = 2$. Pro bod P_2 počítejme v afinních souřadnicích $x_2 = 1$:

$$\begin{aligned} \psi(I) + (\mathfrak{m}_{P_2})^1 &= (x_0, x_1) \\ \psi(I) + (\mathfrak{m}_{P_2})^2 &= (x_0, x_1^2) \\ \psi(I) + (\mathfrak{m}_{P_2})^3 &= (x_0 - x_1^2, x_0^2, x_1^3) = I + (\mathfrak{m}_{P_2})^4 \end{aligned}$$

a tedy $\deg_{P_2} C_2 \cap C_3 = 3$ (průnik s $\Bbbk\{1, x_0, x_1, x_1^2\}$ je právě $\Bbbk\{x_0 - x_1^2\}$). Poslední stupeň lze dopočítat z Bezoutovy věty jako $\deg_{P_1} C_2 \cap C_3 = 6 - 2 - 3 = 1$ nebo přímo v afinních souřadnicích $x_0 = 1$, ideálně s pomocí posunutí $y_1 = x_1 - 1$, $y_2 = x_2 - 1$, ve kterých jsou $C_2 = V(y_2 - y_1^2 - 2y_1)$, $C_3 = V(y_2 - y_1^3 - 3y_1^2 - 3y_1)$, takže:

$$\varphi(I) + (\mathfrak{m}_{P_1})^1 = (y_1, y_2) = I + (\mathfrak{m}_{P_1})^2 \qquad \diamond$$

Poslední výpočet se značně zjednodušil, protože lineární části $y_2 - 2y_1$, $y_2 - 3y_1$ byly lineárně nezávislé. Zabývejme se nyní touto situací obecně. Řekneme, že dvě variety $X, Y \subseteq \mathbb{P}^n$ se v bodě $P \in X \cap Y$ *protínají transverzálně*, jestliže je P nesingulárním bodem obou X, Y a platí $T_P X + T_P Y = T_P \mathbb{P}^n$.

Tvrzení 21.16. *Jestliže se variety $X, Y \subseteq \mathbb{P}^n$ komplementární dimenze protínají v bodě P transverzálně, pak $\deg(I(X) + I(Y))_P = 1$. Pokud průnik není transverzální v P, potom*

$$\deg(I(X) + I(Y))_P \geq 1 + \dim(T_P X \cap T_P Y).$$

Důkaz. Počítejme afinně s $P = 0$. Potom $I(X)$ obsahuje polynomy tvaru $f^{(1)} + \mathrm{hot}$, kde $f^{(1)}$ je nulové na $T_0 X$ a podobně pro $I(Y)$. Pokud je tedy průnik transverzální, máme

$$x_1 + \mathrm{hot}, \dots, x_n + \mathrm{hot} \in I(X) + I(Y).$$

Snadno se lze přesvědčit, že $I(X) + I(Y) + (\mathfrak{m}_0)^k$ obsahuje induktivně všechny monomy stupně $k, k-1, \dots, 1$ a proto

$$I(X) + I(Y) + (\mathfrak{m}_0)^k = \mathfrak{m}_0$$

má kodimenzi 1 v R.

Není-li průnik transverzální, lze podobně ukázat, že

$$I(X) + I(Y) + (\mathfrak{m}_0)^2 \subseteq R$$

se skládá právě z těch polynomů s nulovým absolutním členem, jejichž lineární část je nulová na $T_P X \cap T_P Y$. Kodimenze tohoto ideálu je proto rovna $1 + \dim(T_P X \cap T_P Y)$ (jednička odpovídá absolutnímu členu). Kodimenze $(I(X) + I(Y))_P = I(X) + I(Y) + (\mathfrak{m}_0)^k \subseteq R$ je buď stejná nebo vyšší, proto platí nerovnost z tvrzení. $\square$

Poznamenejme, že Bezoutova věta platí mnohem obecněji, než jak jsme ji zde formulovali a dokázali. Zejména, pokud je průnik $X \cap Y$ transverzální ve všech bodech, platí, že

$$\#(X \cap Y) = \deg X \cdot \deg Y$$

(obecně to myslím nebude platit ani po nahrazení $\#(X \cap Y)$ stupněm $\deg(I(X) + I(Y))$, ačkoliv pro úplné průniky by to platit mělo).

** **Tvrzení 21.17.** *Ideál $I \subseteq S$ je primární, právě když množina $\{(I : x) \mid x \notin I\}$ obsahuje jediný prvoideál P. V tom případě říkáme, že I je P-primární a platí $P = \sqrt{I}$.*

Důkaz. Počítejme $(I : x)$ v případě, že I je primární. Jelikož $x \notin I$, je součin $xy \in I$ pouze, pokud $y \in \sqrt{I}$, tedy vždy $I \subseteq (I : x) \subseteq \sqrt{I} = P$. Vzítím radikálů dostáváme $\sqrt{(I : x)} = P$ a jediný prvoideál mezi $(I : x)$ tedy může být P. V dalším ukážeme, že nějaký prvek x, pro nějž je $(I : x)$ prvoideál, existuje. Budeme však postupovat obecněji.

Předpokládejme, že $I = I_1 \cap \cdots \cap I_r$ je minimální rozklad na průnik primárních ideálů. Potom pro libovolný $x \in (I_2 \cap \cdots \cap I_r) \smallsetminus I_1$ platí $(I : x) = (I_1 : x)$ a podle předchozího pak $\sqrt{(I : x)} = P_1$. Díky konečné generovanosti P_1 také $(P_1)^k \subseteq (I : x)$, tedy $(P_1)^k(x) \subseteq I$. Zvolme k minimální s touto vlastností. Potom $(P_1)^{k-1}(x) \not\subseteq I$ a nechť $y \in (P_1)^{k-1}(x) \smallsetminus I$. Dostáváme $P_1 y \in (P_1)^k(x) \subseteq I$ a tedy $P_1 \subseteq (I : y)$. Zároveň však podle předchozího také $(I : y) = (I_1 : y) \subseteq P_1$ a dostáváme tedy rovnost. Platí tedy, že každý z asociovaných prvoideálů se vyskytuje jako $(I : x)$ pro nějaké $x \notin I$.

Pro úplnost ještě ukážeme, že v obecném případě z předchozího odstavce každý prvoideál tvaru $(I : x)$ musí být některý z P_j. To je proto, že

$$P_1 \cap \cdots \cap P_r = \sqrt{I} \subseteq \sqrt{(I : x)} = \sqrt{(I_1 : x)} \cap \cdots \cap \sqrt{(I_r : x)} = \bigcap_{x \notin P_j} P_j$$

Je-li tedy $(I : x)$ prvoideál, pak musí být roven některému z P_j (je roven průniku některých z nich a proto musí být roven jednomu z nich). $\square$

Poznámka. Z předchozího tvrzení lze jednoduše vyvodit, že každý ireducibilní ideál je primární. Předpokládejme, že existují $x, y \notin I$ takové, že $(I : x), (I : y)$ jsou dva různé prvoideály. Pak pro libovolný $z \in I + (x) \smallsetminus I$ je $(I : z) = (I : x)$ (inkluze "$\supseteq$" je zřejmá a druhá plyne z toho, že z $t(wx) \in I$ plyne $tw \in (I : x)$ a tedy $t \in (I : x)$, protože $wx \notin I$, tj. $w \notin (I : x)$). Stejně tak $(I : z) = (I : y)$ pokud $z \in I + (y) \smallsetminus I$. Proto $(I + (x)) \cap (I + (y)) = I$, což je spor s ireducibilitou. Podobný důkaz lze vést v homogenním případě, jakmile se ukáže, že v případě, že $(I : x)$ je prvoideál, musí být automaticky homogenní a je roven $(I : x_i)$, kde x_i je nějaká homogenní komponenta x. Důkaz tohoto tvrzení viz Eisenbud.

* 22. Divizory na křivkách

Nechť je $\mathcal{C} \subseteq \mathbb{P}^2$ křivka a nechť g je nenulový homogenní polynom. Potom definujeme (g) jako formální celočíselnou kombinaci

$$(g) = a_1 \cdot P_1 + \cdots + a_r \cdot P_r,$$

kde $a_i = \deg(I(\mathcal{C}) + (g))_{P_i}$ je stupeň primární komponenty ideálu $I(\mathcal{C}) + (g)$ odpovídající komponentě $\{P_i\}$, kde jsou tedy $P_1, \ldots, P_r$ právě průsečíky $\mathcal{C} \cap V(g)$. Zřejmě závisí (g) pouze na třídě g v kvocientu $S/I(\mathcal{C})$.

Definujeme grupu divizorů $\operatorname{Div} \mathcal{C} = \mathbb{Z}\mathcal{C}$, tedy volnou komutativní grupu na množině $\mathcal{C}$ (jsou to právě formální celočíselné kombinace prvků $\mathcal{C}$); její prvky nazýváme *divizory.* Pro koeficient divizoru D u bodu P používáme značení D_P, takže máme $D = \sum_{P \in \mathcal{C}} D_P \cdot P$. *Stupeň* divizoru je součet koeficientů, $\deg D = \sum_{P \in \mathcal{C}} D_P$ (jinými slovy je homomorfismus $\deg\colon \operatorname{Div} \mathcal{C} \to \mathbb{Z}$ jednoznačně zadán tím, že každý bod posílá na 1). Pro divizory D, E budeme psát $D \leq E$, pokud pro každý bod P platí $D_P \leq E_P$.

Pro nenulový homogenní polynom g tedy máme divizor $(g) \in \operatorname{Div} \mathcal{C}$ a podle Bezoutovy věty je $\deg(g) = \deg \mathcal{C} \cdot \deg g$. Zejména je $(g) \geq 0$ a $(g)_P > 0$, právě když $g(P) = 0$.

Lemma 22.1. *Platí* $(gh) = (g) + (h)$.

Důkaz. Pro libovolný homogenní ideál I máme exaktní posloupnost

$$S/(I + (g)) \xrightarrow{h\times} S/(I + (gh)) \longrightarrow S/(I + (h)) \longrightarrow 0$$

díky které dostáváme v případě, že jsou všechny ideály dimenze 0, nerovnost

$$\deg(I + (gh)) \leq \deg(I + (g)) + \deg(I + (h)).$$

Pokud volíme $I = I(\mathcal{C}) + (\mathfrak{m}_P)^k$ pro libovolný bod P a $k \gg 0$, dostáváme lokální stupně a tedy nerovnost $(gh)_P \leq (g)_P + (h)_P$. Protože jsou si však podle Bezoutovy věty globální stupně rovny, musí nastat rovnost pro každý bod P. $\square$

Nechť je nyní f nenulová racionální funkce na $\mathcal{C}$, pišme $f = g/h$, a definujme

$$(f) = (g) - (h).$$

Podle předchozího lemmatu výsledek nezávisí na vyjádření $f = g/h$ a navíc opět dostáváme $(f_1 f_2) = (f_1) + (f_2)$. Divizory tvaru (f) nazýváme *hlavní* a definujeme *Picardovu grupu* nebo také *grupu tříd divizorů*

$$\operatorname{Cl} \mathcal{C} = \operatorname{Div} \mathcal{C} / \operatorname{PDiv} \mathcal{C}$$

Ještě se definuje $\operatorname{Div}^0 \mathcal{C}$ jako podgrupa divizorů stupně nula a

$$\operatorname{Cl}^0 \mathcal{C} = \operatorname{Div}^0 \mathcal{C} / \operatorname{PDiv} \mathcal{C}$$

(protože mají g a h stejný stupeň, je $\deg(f) = 0$, tedy každý hlavní divizor má stupeň nula). Pokud je f regulární v bodě P, pak zjevně $(f)_P \geq 0$ (lze volit $h(P) \neq 0$ a tedy $(h)_P = 0$; navíc $(f)_P > 0 \Leftrightarrow g(P) = 0 \Leftrightarrow f(P) = 0$). Nyní ukážeme, že pro hladké křivky platí i opačná implikace.

Lemma 22.2. *Nechť $\mathcal{C}$ je hladká křivka a f nenulová racionální funkce na $\mathcal{C}$. Pak f je regulární v bodě P, právě když $(f)_P \geq 0$.*

Důkaz. Zvolme lokální parametr[6] t v bodě P. Potom lze psát $f = g/h = (g/k)/(h/k)$ pro vhodný homogenní polynom k takový, že $k(P) \neq 0$, tedy $f = g'/h'$ je podíl dvou nenulových funkcí z $\mathcal{O}_P$. Můžeme proto psát $g' = t^r g''$, $h' = t^s h''$ kde $g'', h'' \in \mathcal{O}_P \smallsetminus \mathfrak{m}_P$. Dohromady tak

$$f = g'/h' = t^{r-s} \cdot g''/h''$$

a $f'' = g''/h''$ je v P regulární a nenulová, proto $(f'')_P = 0$. Dohromady

$$(f)_P = (r - s) \cdot (t)_P,$$

přičemž $(t)_P > 0$. Pokud $(f)_P \geq 0$, tedy $r - s \geq 0$, je t^{r-s} regulární v bodě P a tedy i f. $\square$

[6] Lokální parametr je funkce $t \in \mathcal{O}_P$ generující $\mathfrak{m}_P/\mathfrak{m}_P^2$. Podle Nakayamova lemmatu $\mathfrak{m}_P/(t) = 0$ (protože $\mathfrak{m}_P^2 \equiv \mathfrak{m}_P$ modulo (t)), takže $\mathfrak{m}_P = (t)$ a tím pádem $\mathfrak{m}_P^k = (t^k)$. Další aplikací Nakayamova lemmatu platí $\bigcap_k \mathfrak{m}_P^k = 0$ (každý prvek tohoto průniku je t-násobkem jediného prvku – $\mathcal{O}_P$ je obor integrity – tento tedy musí také ležet v tomto průniku), takže každý nenulový prvek $\mathcal{O}_P$ lze vyjádřit jednoznačně jako $f = t^r g$, kde $g \notin \mathfrak{m}_P$.

Poznámka. Protože existuje funkce, pro níž vyjde $(f)_P = 1$ (stačí vzít podíl dvou lineárních funkcí, z nichž jedna má v bodě P nulový bod, ale jejíž diferenciál není nulový na $T_P\mathcal{C}$, a druhá je v bodě P nenulová), musí být nutně $(t)_P = 1$. Dostáváme tak alternativní definici hlavního divizoru (f): koeficient $(f)_P$ je exponent r ve vyjádření $f = t^r \cdot f'$, kde f' je v bodě P regulární a nenulová.

Věta 22.3. *Platí* $\mathrm{Cl}^0\,\mathbb{P}^1 = 0$ *a tedy* $\mathrm{Cl}\,\mathbb{P}^1 = \mathbb{Z}$.

Důkaz. Stačí ukázat, že každý divizor $P - Q$ je hlavní. Nechť $P = (p_0 : p_1)$, pak lineární funkce $g(x_0, x_1) = p_0x_1 - p_1x_0$ splňuje $V(g) = \{P\}$ a tedy $(g) = P$. Podobně dostaneme lineární funkci h takovou, že $(h) = Q$. Pro $f = g/h$ pak $(f) = P - Q$. □

Věta 22.4. *Nechť* $\mathcal{C} \subseteq \mathbb{P}^2$ *je hladká kubická křivka, tj.* $I(\mathcal{C})$ *je generovaný kubickým polynomem, jehož derivace je na* $\mathcal{C}$ *nenulová. Pak pro libovolný bod* $P_0 \in \mathcal{C}$ *je zobrazení*

$$\begin{aligned} \mathcal{C} &\to \mathrm{Cl}^0\,\mathcal{C} \\ P &\mapsto P - P_0 \end{aligned}$$

bijekce. Zejména je $\mathcal{C}$ *komutativní grupou s nulovým prvkem* P_0.

Důkaz. Prvně ukážeme, že je toto zobrazení surjektivní. Nechť P_1, P_2 jsou dva body $\mathcal{C}$ a veďme jimi přímku; v případě, že $P_1 = P_2$, vezmeme tečnu $\mathcal{C}$ procházející tímto bodem. Pak je tato přímka tvaru $V(g)$ pro nějakou lineární funkci g a platí

$$(g) = P_1 + P_2 + Q'$$

Podobně pro body Q_1, Q_2 dostáváme $(h) = Q_1 + Q_2 + P'$ a tedy hlavní divizor

$$(g/h) = P_1 + P_2 + Q' - Q_1 - Q_2 - P'$$

Díky tomu v $\mathrm{Cl}^0\,\mathcal{C}$ platí relace

$$P_1 + P_2 - Q_1 - Q_2 = P' - Q'.$$

Takto lze snadno každý prvek $\mathrm{Cl}^0\,\mathcal{C}$ vyjádřit ve tvaru $P - Q$. Zvolíme-li dále $(g) = P + P_0 + P'$ a $(h) = Q + P' + R$, pak

$$(g/h) = P + P_0 + P' - Q - P' - R$$

a tedy v $\mathrm{Cl}^0\,\mathcal{C}$ platí $P - Q = R - P_0$.

Pro injektivitu pak stačí, že jediný hlavní divizor tvaru $P - P_0$ je nula. Zvolme souřadnice tak, že $P_0 \in V(x_0)$, a pišme $(x_0) = P_0 + P_1 + P_2$. Předpokládejmě nyní, že $P - P_0 = (f) = (g/h) = (g) - (h)$. Protože zjevně $(h) \leq (gx_0)$, máme podle následujícího lemmatu $h \mid gx_0$ a tedy $f = g/h = gx_0/hx_0 = \ell/x_0$ a $(\ell) = P + P_1 + P_2$. Protože však body P_1, P_2 prochází jediná přímka, a to $V(x_0)$, musí být $(\ell) = (x_0) = P_0 + P_1 + P_2$, a proto $P = P_0$. □

Lemma 22.5. *Pokud je* $\mathcal{C}$ *hladká křivka a pro homogenní polynomy* g, h *platí* $(h) \leq (g)$, *pak* $h \mid g$ *v okruhu* $S/I(\mathcal{C})$.

Důkaz. Nechť $r = \deg g - \deg h$. Racionální funkce $g/(x_0^r h)$ je regulární na $\mathbb{A}^n$, takže je $(g/h)|_{x_0=1} = k$ polynomiální. Zpětně pak $g/h = x_0^s\widetilde{k}$. □

Uvedeme ještě jednu hezkou aplikaci Bezoutovy věty na hladké kubické křivky. Řekneme, že bod $P \in \mathcal{C}$ je *inflexní*, jestliže tečna v bodě $\mathcal{C} \cap T_P\mathcal{C}$ má v bodě P násobnost (alespoň) 3. V takovém případě pro lineární funkci ℓ zadávající $T_P\mathcal{C}$ platí $(\ell) = 3P$. Je-li nyní samotný bod P_0 inflexní, pak také $3(P - P_0) = 3P - 3P_0 = 0$, takže bod P je 3-torzní.

Věta 22.6. *Na hladké rovinné kubické křivce existuje právě 9 inflexních bodů.*

Důkaz. Ukáže se, že inflexní body jsou právě body průniku $\mathcal{C} \cap V(\det \mathrm{d}^2 f)$, kde $\mathrm{d}^2 f(P)$ je matice druhých derivací v bodě P generujícího polynomu $f \in I(\mathcal{C})$, ty jsou lineární, takže determinant je opět kubický. Podle Bezoutovy věty je těchto průsečíků právě 9, pokud se počítá každý s příslušnou násobností. Přitom je tato násobnost ale vždy 1 (ono je to **jakože celkem logické** – kdyby ta násobnost byla větší, musel by se ten polynom nulovat až do řádu 3, což nelze). □