Algebraická geometrie

Bc. Lukáš Vokřínek, PhD.

1. dubna 2014

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 je $t \mapsto (t, \frac{1}{t})$.

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 $(2t, t^2 - 1, t^2 + 1)$.)

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

$$b + c - 1 \geq a(n - 1), \quad c + a - 1 \geq b(n - 1), \quad a + b - 1 \geq c(n - 1)$$

a sečtením pak $2(a + b + c) - 3 \geq (a + b + c)(n - 1)$, tj. $0 \geq (a + b + c)(n - 3) + 3$ a $n < 3$.

2. Rezultanty

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

$$A \text{ obor s jednoznačným rozkladem (UFD)} \Rightarrow A[x] \text{ obor s jednoznačným rozkladem}$$

(zásadním poznatkem je Gaussovo lemma – primitivní polynom, tj. polynom, jehož koeficienty jsou nesoudělné, je ireducibilní nad A, právě když je ireducibilní nad podílovým tělesem A – a to, že $\Bbbk[x]$ je obor s jednoznačným rozkladem). Iterací dostáváme, že také $A[x_1, \ldots, x_r] \cong A[x_1, \ldots, x_{r-1}][x_r]$ je obor s jednoznačným rozkladem. Podílové těleso $A[x_1, \ldots, x_r]$, tj. těleso racionálních funkcí, značíme symbolem $A(x_1, \ldots, x_r)$.

Zatímco dělení obecným polynomem je nad obecným okruhem problematické, dělení *normovaným* polynomem funguje stejně jako nad tělesem. Zejména platí $p(x_0) = 0 \Leftrightarrow (x - x_0) \mid p$.

V případě okruhu polynomů $\Bbbk[x]$ nad tělesem máme Bezoutovu rovnost, která vyjadřuje největší společný dělitel jako kombinaci $\gcd(f, g) = kf + lg$. Nyní popíšeme situaci, kdy mají f a g nějaký společný dělitel, pomocí polynomiální rovnice. Definujme *Sylvesterovu matici* $\operatorname{Syl}(f, g)$ jako matici $(n + m) \times (n + m)$, kde $n = \deg f$, $m = \deg g$, pomocí koeficientů polynomů f a g,

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

takto:

$$\operatorname{Syl}(f, g) = \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & b_{m-1} & b_m & \cdots & 0 \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & b_{m-1} & \ddots & 0 \\ a_1 & \ddots & \ddots & a_n & b_1 & \ddots & \ddots & b_m \\ a_0 & a_1 & \ddots & a_{n-1} & b_0 & b_1 & \ddots & b_{m-1} \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & & \ddots & a_1 & \vdots & & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

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

Věta 2.1. *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* $\operatorname{Res}(f, g) = 0$.

Lemma 2.2. *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 $k = g_1$, $l = -f_1$.

Naopak předpokládejme, že k, l splňují podmínky lemmatu 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 $\deg k \geq \deg g$, spor. □

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

$$\operatorname{Syl}(f, g)(c_{m-1}, \ldots, c_0, d_{n-1}, \ldots, d_0)^T = 0.$$

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

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

$$f = a_n(x - \alpha_1) \cdots (x - \alpha_n), \qquad g = b_m(x - \beta_1) \cdots (x - \beta_m),$$

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

Věta 2.3. *Platí* $\operatorname{Res}(f, g) = a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j)$.

Důkaz. Podle Vietových vztahů je

$$a_{n-k} = (-1)^k a_n \sigma_k(\alpha), \quad b_{m-l} = (-1)^l b_m \sigma_l(\beta),$$

kde $\sigma_k(\alpha)$ značí k-tý symetrický polynom v proměnných $\alpha = (\alpha_1, \ldots, \alpha_n)$. Dosazením do determinantu Sylvesterovy matice je pak zřejmé, že $\operatorname{Res}(f, g) = a_n^m b_m^n p(\alpha, \beta)$ pro nějaký symetrický polynom $p(\alpha, \beta)$ v proměnných α_i, β_j. Jelikož víme, že $\operatorname{Res}(f, g) = 0$ v případě, že $\alpha_i = \beta_j$ pro nějakou dvojici i, j, platí $(\alpha_i - \beta_j) \mid p$ a díky jednoznačnosti rozkladu také

$$\prod_{i,j}(\alpha_i - \beta_j) \mid p$$

protože všechny činitelé jsou ireducibilní a různí; pišme $p = q \prod_{i,j}(\alpha_i - \beta_j)$.

Zároveň platí $a_n^m b_m^n \prod_{i,j}(\alpha_i - \beta_j) = a_n^m g(\alpha_1) \cdots g(\alpha_n)$, z čehož je zřejmé, že má p stupeň mn v proměnných α. Nemůže tedy q obsahovat žádnou z proměnných α_i. Symetricky pak nemůže obsahovat ani žádnou z proměnných β_j a je tedy q konstantní. To, že ve skutečnosti $q = 1$, pak plyne například z $\operatorname{Res}(x^n, (x + 1)^m) = 1$. □

Příklad 2.4. Základním příkladem je $\operatorname{Res}(f, f') = a_n \operatorname{disc}(f)$ (platí totiž, že první řádek Sylvesterovy matice je dělitelný a_n). Zřejmě pak f obsahuje násobný ireducibilní faktor, právě když $\operatorname{disc}(f) = 0$. V případě kvadratického polynomu $f = ax^2 + bx + c$ dostáváme

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

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

Příklad 2.5. Spočtěte diskriminant $\mathrm{disc}(x^3+px+q)$.

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

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

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

Lemma 2.6. *Nekonstantní polynomy f, g mají společný faktor s kladným stupněm v proměnné x_r, právě když $\mathrm{Res}(f,g;x_r)=0$.*

Důkaz. Podle předchozího je $\mathrm{Res}(f,g;x_r)=0$ ekvivalentní tomu, že f, g mají společný faktor jako prvky $\Bbbk(x_1,\dots,x_{r-1})[x_r]$. Je tedy implikace $\Rightarrow$ zřejmá. Nechť naopak $f=\frac{h}{e}\frac{f_1}{c}$, $g=\frac{h}{e}\frac{g_1}{d}$, kde $c,d,e\in\Bbbk[x_1,\dots,x_{r-1}]$ a $f_1,g_1,h\in\Bbbk[x_1,\dots,x_r]$ a h má kladný stupeň v proměnné x_r. Potom obsahuje h ireducibilní faktor h_1 s kladným stupněm v x_r 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_r, musí být $h_1 \mid f$, analogicky pak také $h_1 \mid g$. □

Zabývejme se nyní významem kořenů $\mathrm{Res}(f,g;x_r)$. Jsou to body $(x_1,\dots,x_{r-1})$ takové, že buď

- $f(x_1,\dots,x_{r-1},-)$ a $g(x_1,\dots,x_{r-1},-)$ mají společný kořen, tedy obraz společné nulové množiny f a g při projekci $\Bbbk^r\to\Bbbk^{r-1}$, $(x_1,\dots,x_r)\mapsto(x_1,\dots,x_{r-1})$, nebo
- vedoucí koeficient f či g je nulový; toto nenastane pokud je vedoucí člen ${x_r}^n$, přičemž vhodnou změnou souřadnic tohoto lze dosáhnout, viz dále.

Věta 2.7 (nedělat). *Existují nenulové polynomy $k, l\in\Bbbk[x_1,\dots,x_r]$ takové, že* $\mathrm{Res}(f,g;x_r) = kf+lg$ *a pro stupně v proměnné x_r platí* $\deg_r k < \deg_r g$, $\deg_r l < \deg_r f$.

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

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

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

Podle Cramerova pravidla

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

přičemž každý čitatel $\mathrm{Res}(f,g;x_r)c_j$ je jistý minor Sylvesterovy matice a leží tedy v $\Bbbk[x_1,\dots,x_{r-1}]$. Proto

$$k(x_1,\dots,x_r) = \mathrm{Res}(f,g;x_r)\widetilde{k}(x_1,\dots,x_r) = \mathrm{Res}(f,g;x_r)(c_{m-1}{x_r}^{m-1}+\dots+c_0)$$

je polynom v $\Bbbk[x_1,\dots,x_r]$ a zjevně $kf+lg=\mathrm{Res}(f,g;x_r)$. □

Důsledek 2.8. *Nechť* $\Bbbk$ *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 f, g nemají společný faktor a přitom rovnice ze zadání mají nekonečně mnoho společných řešení. Nechť tato společná řešení mají nekonečně mnoho různých prvních souřadnic. Potom $\operatorname{Res}(f,g;y) \in \Bbbk[x]$ má nekonečně mnoho kořenů, a proto je nulový. To ale znamená, že f, g mají společný faktor. □

Příklad 2.9. Mají $f = xy - 1$, $g = x^2 + y^2 - 4$ společný faktor?

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

Příklad 2.10. Spočtěte společná řešení rovnic $x^2 + y^2 - 4 = 0$, $16x^2 + y^2 - 16 = 0$.

Řešení. Spočítáme $\operatorname{Res}(f,g;x) = -9(5y^2-16)^2$. Platí, že $\operatorname{Res}(f,g;x)$ 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 $\operatorname{Res}(f,g;y) = 9(5x^2-4)$, tj. $x = \pm\frac{2}{\sqrt{5}}$. Obecnější metodu, fungující pro více polynomů, probereme později. ◇

Příklad 2.11. 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, tj. to jsou takové horizontální přímky $y = y_0$, které se „dotýkají“ křivky $f(x,y) = 0$ (tato křivka je zrovna nesingulární). ◇

Věta 2.12 (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 $d = \deg f$, $e = \deg g$, tj. aby obsa-
? hovaly y^d, y^e s nenulovým koeficient. Toho lze dosáhnout podle důkazu věty o Noetherovské noramlizaci. Potom tyto souřadnice musí být kořeny rezultantu $\operatorname{Res}(f,g;y) \in \Bbbk[x]$. Zabývejme se nyní stupněm tohoto polynomu. Zjevně na pozici (j,i) příslušné matice je polynom stupně maximálně $j - i$ v případě $i \leq e$ a stupně maximálně $j - i + e$ v případě $i > e$. Protože druhá možnost nastává právě pro d voleb i, dostáváme pro každou permutaci σ stupeň odpovídajícího členu determinantu

$$\sum_{i \leq e} \sigma(i) - i + \sum_{i > e} \sigma(i) - i + e = de.$$

Zároveň je rezultant nenulový, protože f, g nemají společný faktor a proto může mít maximálně de 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 $\mathbb{k}[x]$ 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).

3. Lokalizace

Definice 3.1. *Lokální okruh* je okruh (komutativní s jedničkou) s jediným maximálním ideálem.

Věta 3.2. *Nechť A je okruh a $I \subsetneq A$ vlastní ideál. Potom I je jediný maximální ideál A, právě když $A \smallsetminus I$ obsahuje pouze jednotky.*

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

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

Věta 3.3 (nedělat). *Nechť A je okruh s maximálním ideálem $\mathfrak{m}$. Jestliže každý prvek $1+\mathfrak{m} = \{1 + x \mid x \in \mathfrak{m}\}$ je jednotka, pak A je lokální.*

Důkaz. Nechť $x \in A \smallsetminus \mathfrak{m}$. Ukážeme, že x je jednotka. Z maximality $\mathfrak{m}$ plyne, že $(x, \mathfrak{m}) = A$, tj. $xa + t = 1$ pro nějaké $t \in \mathfrak{m}$, $a \in A$. Proto $xa = 1 - t \in 1 + \mathfrak{m}$ je jednotka a tím pádem také x je jednotka. □

Definice 3.4. 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 S vzhledem k podmnožině S, a jeho třídy $[a, s] = \frac{a}{s}$. 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 3.5. *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.
- $S = A \setminus \mathfrak{p}$, 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.

Věta 3.6 (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 $x_1, \ldots, x_n \in N$ je množina generátorů. 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 $N = 0$. □

4. Noetherovské okruhy

Definice 4.1. Nechť A je okruh. Potom A-*modul* je komutativní grupa M společně s operací

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

splňující axiomy vektorového prostoru, tj.

$$\begin{aligned} 1x &= 1, & a(bx) &= (ab)x \\ (a+b)x &= ax + bx, & a(x+y) &= ax + ay. \end{aligned}$$

Definice 4.2. 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 4.3. *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 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 $M_0 \subsetneq M_1 \subsetneq \cdots$ 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 $M_n = M_{n+1}$, spor. □

Věta 4.4. *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 $L \subseteq M$ 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 4.5. *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 tedy i každý jeho kvocient. To jsou přesně konečně generované A-moduly. □

Věta 4.6. *Nechť A je Noetherovský okruh, který je podokruhem $A \subseteq B$. Pokud je B konečně generovaný jako A-modul, 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-podmodul). □

Příklad 4.7. Okruh $\mathbb{Z}$ je Noetherovský. Proto také $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\}$ je Noetherovský.

Věta 4.8. *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

$$\frac{a}{s} = \frac{b_1 a_1 + \cdots + b_k a_k}{s} = \frac{b_1}{s}\ \lambda(a_1) + \cdots + \frac{b_k}{s}\ \lambda(a_k).$$ □

Věta 4.9 (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

$$J = \{a \in A \mid \exists p \in I \colon p = ax^n + \mathrm{lot}\},$$

tj. ideál vedoucích koeficientů polynomů z I. Nechť $J = (a_1, \dots, a_k)$ a zvolme polynomy $p_i \in I$ s vedoucím koeficientem a_i, můžeme předpokládat, že mají všechny stupeň n. Množina $A_{<n}[x]$ polynomů stupně menšího než n je konečně generovaný A-modul a proto Noetherovský. Pišme $A_{<n}[x] \cap I = A\{q_1, \dots, q_l\}$. Potom je $I = (p_1, \dots, p_k, q_1, \dots, q_l)$: protože každý $p \in I$ stupně menšího než n leží v $(q_1, \dots, q_l)$, uvažme $p \in I$ stupně alespoň n. Potom $p = ax^m + \mathrm{lot}$, kde $a \in J$. Proto

$$p = (b_1 a_1 + \cdots + b_k a_k)x^m + \mathrm{lot} = b_1 x^{m-n} p_1 + \cdots + b_k x^{m-n} p_k + \mathrm{lot},$$

kde prvních k členů leží v $(p_1, \dots, p_k)$ a zbytek je menšího stupně a leží v $(p_1, \dots, p_k, q_1, \dots, q_l)$ podle indukčního předpokladu. □

prvně definice algebry atd.

Důsledek 4.10. *Nechť A je Noetherovský okruh. Pokud je B konečně generovaná A-algebra, tj. pokud $B = A[b_1, \dots, b_r]$, je také B Noetherovský okruh.*

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

Hilbertova věta o bázi dává naději, že bychom s ideály v okruhu polynomů $\Bbbk[x_1, \dots, x_r]$ 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 $\Bbbk[x_1, \dots, x_r]$ a různá uspořádání se hodí k různým účelům. My se spokojíme s tzv. lexikografickým uspořádáním:

$$x^\alpha = x_1^{\alpha_1} \cdots x_r^{\alpha_r} < x_1^{\beta_1} \cdots x_r^{\beta_r} = x^\beta,$$

právě když pro nějaké $i \geq 1$ platí $\alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i$. Vzhledem k tomu, že se jedná o lineární uspořádání, můžeme hovořit o vedoucím členu polynomu $f \in \Bbbk[x_1, \dots, x_r]$: 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 $I \subseteq \Bbbk[x_1, \dots, x_r]$ 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 4.11. *Nechť $I \subseteq \Bbbk[x_1, \dots, x_r]$ je ideál a $g_1, \dots, g_k \in I$. Jestliže $\mathrm{LT}\, I = (\mathrm{LM}\, g_1, \dots, \mathrm{LM}\, g_k)$, tak $I = (g_1, \dots, g_k)$. Množina prvků $g_1, \dots, g_k \in I$ s touto vlastností vždy existuje a nazývá se* Gröbnerova báze.

Důkaz. Předpokládejme sporem, že $f \in I \smallsetminus (g_1, \dots, g_k)$ je nejmenšího možného stupně. Protože $\operatorname{LM} f \in \operatorname{LT} I$ a jedná se o monom, musí být $\operatorname{LM} f = x^\alpha \operatorname{LM} g_i$. Potom

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

leží také v $I \smallsetminus (g_1, \dots, g_k)$ a je menšího stupně, neboť se vedoucí členy vyruší. To je spor s minimalitou $\deg f$.

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

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

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

a pokračujeme s testováním.

Poznámka. Řekneme, že Gröbnerova báze ideálu I je *redukovaná*, jestliže jsou všechny g_i normované a $\operatorname{LT} g_i$ 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.

4.1. Buchbergerův algoritmus

Algoritmus na hledání Gröbnerovy báze $I = (f_1, \dots, f_n)$ 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 $\operatorname{LM} f_i$, $\operatorname{LM} f_j$ a položíme

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

Poté tento polynom zredukujeme pomocí $f_1, \dots, f_n$ tak, že postupně odečítáme vhodné násobky f_k, abychom přesně zrušili vedoucí člen. Pokud dostaneme nenulový polynom, jehož vedoucí člen již není dělitelný žádným z f_k, přidáme jej k množině generátorů (tento může záviset na redukci, která není jednoznačná, protože není jasné jaký násobek kterého z f_k máme odečítat). Protože v každém kroku se zvětšuje $(\operatorname{LT} f_1, \dots, \operatorname{LT} f_n)$ a $\Bbbk[x_1, \dots, x_r]$ splňuje podmínku rostoucích řetězců, dospějeme po konečném počtu kroků do situace, kdy redukce všech S-polynomů jsou již nulové. Potom je naše množina generátorů Gröbnerovou bází: nechť $f = p_1 f_1 + \dots + p_n f_n \in I$ a předpokládejme, že v tomto vyjádření f je

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

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

- vedoucí členy se nevyruší, tj. $\operatorname{LM} f = \operatorname{LM}(p_{i_0} f_{i_0})$; pak $\operatorname{LM} f \in (\operatorname{LM} f_1, \dots, \operatorname{LM} f_n)$;

- vedoucí členy se vyruší; pak lze pro indexy $i \neq i_0$ s $\mathrm{LM}(p_i f_i)$ maximálním psát
$$p_i f_i - \frac{\mathrm{LC}(p_i f_i)}{\mathrm{LC}(p_{i_0} f_{i_0})} p_{i_0} f_{i_0} = q_i S(f_i, f_{i_0})$$
(S-polynom se získal jako *nejmenší* kombinace, ve které se ruší vedoucí členy). Podle konstrukce pak lze každý S-polynom $S(f_i, f_{i_0})$ nahradit kombinací f_j s menšími vedoucími členy; to dává spor s minimalitou.

Příklad 4.12. Spočtěte Gröbnerovu bázi $I = (f_1, f_2)$, kde $f_1 = x^3 - 2xy$, $f_2 = x^2y + x - 2y^2$.

Řešení. V prvním kroku
$$S(f_1, f_2) = yf_1 - xf_2 = -x^2 \qquad f_3 = x^2$$
a žádná redukce není potřeba. V dalším kroku je redukce $S(f_1, f_2) = -f_3$ nulová, dále
$$\begin{aligned} S(f_1, f_3) &= f_1 - xf_3 = -2xy & f_4 &= xy \\ S(f_2, f_3) &= f_2 - yf_3 = x - 2y^2 & f_5 &= x - 2y^2 \end{aligned}$$
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
$$\begin{aligned} S(f_3, f_4) &= yf_3 - xf_4 = 0 \\ S(f_3, f_5) &= f_3 - xf_5 = 2xy^2 \equiv 0 \\ S(f_4, f_5) &= f_4 - yf_5 = 2y^3 & f_6 &= y^3 \end{aligned}$$
(opět by bylo možné vypustit $f_3 = xf_5 + 2yf_4$). V posledním kroku
$$\begin{aligned} S(f_3, f_6) &= y^3 f_3 - x^2 f_6 = 0 \\ S(f_4, f_6) &= y^2 f_4 - xf_6 = 0 \\ S(f_5, f_6) &= y^3 f_5 - xf_6 = -2y^5 \equiv 0 \end{aligned}$$
Proto (f_4, f_5, f_6) je redukovaná Gröbnerova báze. $\diamond$

Příklad 4.13. 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 $f_1 = f_2 + f_3$, dále
$$S(f_2, f_3) = y^2 f_2 - x^2 f_3 = x^2y + y^4 - 2y^3 \equiv 0$$
a Gröbnerova báze je (f_2, f_3). Pokud bychom chtěli redukovanou, je ještě potřeba redukovat f_2, čímž dostaneme
$$f_2' = f_2 - f_3 = x^2 - y,$$
tedy $f_2' = f_1$. Proto redukovaná Gröbnerova báze je (f_1, f_3).

V dalším textu nám bude jasné, že $\Bbbk[x, y]/I$ nebo ještě lépe $\Bbbk[x, y]/\sqrt{I}$ souvisí s nulovou množinou $f_1 = 0$, $f_2 = 0$. Ta sestává za tří bodů $[0, 0]$, $[-1, 1]$, $[1, 1]$ a proto $\dim \Bbbk[x, y]/\sqrt{I} = 3$. Přitom $\dim \Bbbk[x, y]/I = 4$, 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). $\diamond$

5. Afinní variety

Odteď budeme předpokládat, že $\mathbb{k}$ je algebraicky uzavřené těleso. Budeme značit $\mathbb{A}^n$ množinu $\mathbb{k}^n$ chápanou jako afinní prostor nad $\mathbb{k}$, zatímco $\mathbb{k}^n$ budeme používat pro stejnou množinu chápanou jako vektorový prostor.

V následujícím bude hrát zásadní roli vztah mezi polynomy, tj. prvky $F \in \mathbb{k}[x_1, \dots, x_n]$ a polynomiálními funkcemi $f \colon \mathbb{A}^n \to \mathbb{k}$, $(p_1, \dots, p_n) \mapsto f(p_1, \dots, p_n)$. Zobecněním známe věty pro polynomy v jedné proměnné je následující tvrzení.

Tvrzení 5.1. *Je-li $\mathbb{k}$ nekonečné těleso (zejména je-li 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 $F \in \mathbb{k}[x_1, \dots, x_{n-1}][x_n]$ ve tvaru

$$F = G_d x_n^d + \cdots + G_1 x_n + G_0,$$

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

V dalším tak budeme volně přecházet mezi polynomy a polynomiálními funkcemi na afinním prostoru; také se jim říká *regulární funkce*.

Definice 5.2. *Afinní varieta* (přesněji *afinní uzavřená množina*) je množina řešení soustavy algebraických rovnic

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

kde $S \subseteq \mathbb{k}[x_1, \dots, x_n]$ 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 se tedy každou afinní varietu psát ve tvaru $V(I)$, kde I je ideál. Protože je každý ideál konečně generovaný, $I = (f_1, \dots, f_r)$, platí také $V(I) = V(f_1, \dots, f_r)$ a tedy každá afinní varietu lze tedy ve skutečnosti zadat konečným systémem polynomiálních rovnic.

Z teorie nadkvadrik víme, že každá nadkvadrika určuje svoji 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):

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

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

Lemma 5.3. *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 $X \subseteq VI(X)$ a rovnost nastává právě když X je afinní varieta,*
- *platí $S \subseteq IV(S)$ a rovnost nastává právě když S je ideál tvaru $I(X)$.*

Věta 5.4. *Zobrazení V zadává bijekci mezi ideály tvaru $I(X)$ a afinními varietami.*

Důkaz. Ukážeme, že na těchto podmnožinách jsou V a I vzájemně inverzní. Protože jsou tyto podmnožiny právě obrazy I a V, znamená to dokázat $IVI = I$, $VIV = V$. Důkazy jsou analogické, provedeme první. Platí $S \subseteq IV(S)$, a dosazením $S = I(X)$ dostáváme $I(X) \subseteq IVI(X)$. Naopak platí $X \subseteq VI(X)$ a aplikací I se inkluze obrátí, tj. $I(X) \supseteq IVI(X)$. □

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 5.5. *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 5.6. Každý prvoideál je radikálový.

Cvičení 5.7. Dokažte, že se vskutku jedná o ideál.

Příklad 5.8. 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 $\sqrt{(x^k)} = (x)$, $\sqrt{(x^2+1)} = (x^2+1)$.

Věta 5.9 (Hilbertova věta o nulách)**.** *Nechť $\Bbbk$ je algebraicky uzavřené těleso.*

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

Před vlastním důkaz si 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 5.10. *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

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

Lemma 5.11. *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. To je ale zároveň popis levé strany.

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 $gh(x) \neq 0$, 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 5.12. 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).

6. Ireducibilita

Definice 6.1. Afinní varieta 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 také afinní variety.

Příklad 6.2. $V(x_1x_2)$ je sjednocením osy x_1 a osy x_2, tedy $V(x_1x_2) = V(x_1) \cup V(x_2)$ a tedy není ireducibilní (je reducibilní).

Věta 6.3. *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 $V = V_1 \cup V_2$ a zvolme $g_1 \in I(V_1) \smallsetminus I(V)$, která je nula na V_1, ale nikoliv na V (platí $I(V_1) \supseteq I(V)$ a případná rovnost by dala $V_1 = VI(V_1) = VI(V) = V$). 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 $g_1, g_2 \notin I(V)$. □

Definice 6.4. Topologický prostor se nazývá *Noetherovský*, jestliže neexistuje nekonečná posloupnost

$$X_1 \supsetneq X_2 \supsetneq \cdots$$

uzavřených podmnožin.

Věta 6.5. *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 $\mathbb{k}[x_1, \ldots, x_n]$ (na afinních varietách je I injektivní). □

Cvičení 6.6. Každý Noetherovský topologický prostor je kompaktní (algebraičtí geometrové říkají kvazikompaktní, aby zdůraznili, že není Hausdorffův – někdy se kompaktním prostorem totiž rozumí kompaktní Hausdorffův).

Věta 6.7. *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 $V_i \nsubseteq V_j$ pro $i \neq j$ (říkáme, že je tento 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 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 $V_i = W_j$. □

7. Důkaz Hilbertovy věty o nulách

Je jednoduché ukázat, že $\mathfrak{m}_P$ je maximální ideál – je to totiž přesně jádro homomorfismu $\mathbb{k}[x_1, \ldots, x_n] \to \mathbb{k}$, $F \mapsto F(p_1, \ldots, p_n)$. 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 $\mathfrak{m}_P$.

Nechť J je libovolný maximální ideál. Potom $A = \mathbb{k}[x_1, \ldots, x_n]/J$ je rozšíření, které je konečně generované jako algebra, tj. A vznikne z $\mathbb{k}$ přidáním konečně mnoha prvků a následným uzavřením na sčítání a násobení.

Definice 7.1. 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 7.2 (o Noetherovské normalizaci)**.** *Nechť A je konečně generovaná algebra. Existuje podalgebra $B \subseteq A$ izomorfní $\mathbb{k}[t_1, \ldots, t_r]$ taková, že A je integrální nad B.*

Věta 7.3. *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 $b^{-1} \in B$. □

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

$$\pi \colon \Bbbk \subseteq \Bbbk[x_1, \ldots, x_n] \to \Bbbk[x_1, \ldots, x_n]/J = A$$

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

Druhá část je elementární: pokud je J vlastní ideál, pak je obsažem 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 f^k nuluje na $V(J)$ a nuluje se 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 $x_1, \ldots, x_n, t$:

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

Protože je však $f(x) = 0$ na $V(J)$, je tato varieta prázdná a podle druhé části Hilbertovy věty musí být $1 \in (J, f(x)t - 1)$ 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. Algebra $\Bbbk[x_1, \ldots, x_n, t]/(J, f(x)t - 1) = (\Bbbk[x_1, \ldots, x_n]/J)[t]/(f(x)t - 1)$ je přesně lokalizace $\Bbbk[x_1, \ldots, x_n]/J$ vzhledem k prvku $f(x)$. Tato lokalizace je podle Hilbertovy věty nulová, $1 = 0$, což podle definice znamená $f(x)^k = 0$.

Zbývá tak dokázat větu o Noetherovské normalizaci.

Důkaz Věty 7.2. 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 $f \neq 0$ leží v jeho jádře J a označme f_d jeho homogenní komponentu maximálního stupně. Potom $f_d \neq 0$ a existuje $P \in \Bbbk^n$ takový, že $f_d(P) \neq 0$. Změňme souřadnice na $\Bbbk^n$ tak, že $P = (0, \ldots, 0, 1)$. Nerovnost

$f_d(P) \neq 0$ pak znamená, že koeficient u $\widetilde{x}_n^d$ je nenulový, řekněme rovný jedné, tj. v okruhu $\Bbbk[\widetilde{x}_1, \dots, \widetilde{x}_{n-1}][\widetilde{x}_n]$ lze psát

$$f = \widetilde{x}_n^d + g_{d-1}(\widetilde{x}_1, \dots, \widetilde{x}_{n-1})\widetilde{x}_n^{d-1} + \dots + g_1(\widetilde{x}_1, \dots, \widetilde{x}_{n-1})\widetilde{x}_n + g_0(\widetilde{x}_1, \dots, \widetilde{x}_{n-1}) \in J.$$

Označíme-li $B = \Bbbk[\widetilde{a}_1, \dots, \widetilde{a}_{n-1}]$ podalgebru generovanou $\widetilde{a}_1, \dots, \widetilde{a}_{n-1}$, máme $A = B[\widetilde{a}_n]$ a $\widetilde{a}_n$ je kořenem normovaného polynomu s koeficienty v B.

K důkazu indukcí je tedy ještě potřeba ukázat: je-li A integrální nad B a B integrální nad C, pak také A je integrální nad C. To plyne z následujícího lemmatu. □

Lemma 7.4. *Nechť $B \subseteq A$ jsou konečně generované algebry. Potom A je integrální nad B, právě když je A konečný B-modul.*

Důkaz. Směr $\Rightarrow$ je zřejmý, neboť integrální rozšíření o jediný prvek $B[a]$ je volný B-modul s bází $\{1, a, \dots, a^{d-1}\}$.

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

$$(a_1, \dots, a_r)(aE - M) = 0.$$

Vynásobením maticí algebraických doplňků k $aE - M$ dostaneme

$$0 = (a_1, \dots, a_r)(aE - M)(aE - M)^a = (a_1, \dots, a_r)\det(aE - M).$$

Proto $a_i \det(aE - M) = 0$ a tedy

$$\det(aE - M) = 1 \det(aE - M) \in B\{a_1, \dots, a_r\} \det(aE - M) = 0.$$

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

8. 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 8.1. 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 8.2. Platí $\Bbbk[\mathbb{A}^n] \cong \Bbbk[x_1, \dots, x_n]/0 = \Bbbk[x_1, \dots, x_n]$.

Definice 8.3. Okruh A se nazývá *redukovaný*, jestliže pro $x \in A$ platí $x^n = 0 \Rightarrow x = 0$.

Lemma 8.4. *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 8.5. *Souřadnicá 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. □

Nechť nyní naopak 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 8.6. 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 8.7. *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 $G(F_1, \dots, F_m)$, který získáme dosazením polynomu $F_j \in \Bbbk[x_1, \dots, x_n]$ za každou proměnnou y_j vyskytující se v G. □

Definice 8.8. 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 8.9. Parabola je izomorfní přímce, $V(x_2 - x_1^2) \cong \mathbb{A}^1$. Konkrétní izomorfismus je například

$$(x_1, x_2) \mapsto x_1, \quad (t, t^2) \leftarrow\!\shortmid t.$$

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 8.10. *Izomorfní variety mají izomorfní souřadnicové algebry.*

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

Příklad 8.11. 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 obrazeme 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 zásadní následující tvrzení.

Tvrzení 8.12. *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

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

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

$$gf = g(f_1, \dots, f_m) = g(\varphi y_1, \dots, \varphi y_m),$$

tedy polynomiální funkce vzniklá dosazením φy_j za proměnnou y_j v polynomu G. Protože je však φ homomorfismus, 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 $\Bbbk[x_1, \ldots, x_n] \to A$. 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 $\Bbbk[V(J_A)] \cong A \xrightarrow{\varphi} B \cong \Bbbk[V(J_B)]$.)

9. Součin afinních variet

Věta 9.1. *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 $V = V(f_1, \ldots, f_r)$ a $W = V(g_1, \ldots, g_s)$, kde polynomy f_i píšeme v proměnných x_i a polynomy g_j v proměnných y_j. Tímto způsobem je lze interpretovat jako

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

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

Věta 9.2. *Pokud jsou obě V, W ireducibilní, je také $V \times W$ ireducibilní.*

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 pr_W je na ní izomorfismus, takže i obraz je uzavřený. $\square$

Zabývejme se nyní obrazem polynomiálního zobrazení. Ihned 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 n souřadnic. Přitom graf Γ_f je afinní varieta, $\Gamma_f = V(I(V), y_j - f_j(x))$.

Příklad 9.3. Popište obraz afinního 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 $\operatorname{Res}(t^2-1-x, t^3-t-y; t) = 0$. 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 $\operatorname{im} f = V(y^2 - x^2 - x^3)$. $\diamond$

Věta 9.4. *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 $I(\pi V) = I(V) \cap \Bbbk[y_1, \ldots, y_m]$.*

Nechť nyní $V = V(J)$. Protože je $I(\pi V) = \sqrt{J} \cap \Bbbk[y_1, \ldots, y_m]$ radikálem $J \cap \Bbbk[y_1, \ldots, y_m]$, lze psát $\overline{\pi V} = V(J \cap \Bbbk[y_1, \ldots, y_m])$. 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 $\Bbbk[y_1, \ldots, y_m]$ (proces dělení může používat pouze tyto prvky).

Příklad 9.5. Popište obraz afinního 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 přidáváme 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 9.6. Popište obraz afinního 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 $J = (-x, t - y)$ a opět nastávají dvě možnosti: pro $x \neq 0$ máme $J = (1)$ a pro $x = 0$ naopak $J = (t - y) \not\ni 1$ (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“.

10. 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, je počet průsečíků přesně de. Toto tvrzení není zdaleka elementární 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 $\Bbbk$. Budeme označovat $\mathbb{P}(V) = (V \smallsetminus \{0\})/{\sim}$, $u \sim v \Leftrightarrow \exists k \in \Bbbk \colon v = ku$, projektivní prostor vektorového prostoru V. Zejména $\mathbb{P}^n = \mathbb{P}(\Bbbk^{n+1})$. Značíme $(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n$ třídu zadanou vektorem $(x_0, x_1, \ldots, x_n)$ a mluvíme o *homogenních souřadnicích.* Pro každé $i = 0, 1, \ldots, n$ definujeme

$$U_i = \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n \mid x_i \neq 0\}$$
$$H_i = \{(x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n \mid x_i = 0\}$$

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 $f \in \Bbbk^d[x_0, \ldots, x_n]$ 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 10.1. *Projektivní varieta* je podmnožina $\mathbb{P}^n$ tvaru $V(S) = \bigcap_{f \in S} V(f)$, kde S je nějaká množina homogenních polynomů.

Příklad 10.2. Nadrovina $H_i = V(x_i)$ je projektivní varieta.

Opět dostáváme na $\mathbb{P}^n$ tzv. Zariského topologii, jejíž uzavřené množiny jsou právě projektivní variety.

Definice 10.3. *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 $1 \in A_0$.

Příklad 10.4. Okruh polynomů $A = \mathbb{k}[x_0, \dots, x_n] = \bigoplus_{d \geq 0} \mathbb{k}^d[x_0, \dots, x_n]$, kde

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

Definice 10.5. *Homogenní ideál* I v graduovaném okruhu A je ideál, pro který platí $I = \bigoplus_{d \geq 0}(A_d \cap I)$. Jinými slovy, pro každý prvek $f \in I$ s rozkladem $f = f_0 + \dots + f_d$ do komponent platí také $f_i \in I$.

Lemma 10.6. *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.*

Poznámka. Alternativní popis $V(f)$ pro f nehomogenní: jedná se o množinu těch bodů $P \in \mathbb{P}^n$ takových, že pro libovolný reprezentant $P = [x]$ platí $f(x) = 0$. Pišme $f = f_0 + \dots + f_d$ a zabývejme se tím, co se stane při změně reprezentanta, $f(tx) = f_0(x) + \dots + t^d f_d(x)$. Tento výraz je nulový pro *všechna* $t \in \mathbb{k}^\times$, právě když $f_0(x) = \dots = f_d(x) = 0$, tj. $V(f) = V(f_0, \dots, f_d)$.

Definujeme dále $I(X)$ jako ideál generovaný všemi homogenními polynomy f takovými, že $f|_X = 0$. Podle předchozí poznámky lze také ekvivalentně říct, že to je ideál všech polynomů nulujících se na X.

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

Věta 10.7 (projektivní věta o nulách)**.** *Nechť $\mathbb{k}$ je algebraicky uzavřené těleso. Potom pro homogenní ideál $J \subseteq \mathbb{k}[x_0, \dots, x_n]$ platí*

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

Důkaz. Uvažujme tzv. afinní kužel nad projektivní varietou $V(J) \subseteq \mathbb{P}^n$. Ten je definován jako vzor $V(J)$ při kanonické projekci $\pi \colon \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$, $\pi(x_0, \dots, x_n) = (x_0 : \dots : x_n)$. Vlastní homogenní ideál $J \subsetneq \mathbb{k}[x_0, \dots, x_n]$ zadává jednak projektivní varietu $V(J) \subseteq \mathbb{P}^n$ a jednak afinní varietu $V^{\mathrm{af}}(J) \subseteq \mathbb{A}^{n+1}$, přičemž platí

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

jedná se tedy o afinní kužel nad $V(J)$. Platí $V(J) = \emptyset$, právě když $V^{\mathrm{af}}(J) \subseteq \{0\} = V(x_0, \dots, x_n)$, tedy právě když $(x_0, \dots, x_n) \subseteq I(V^{\mathrm{af}}(J)) = \sqrt{J}$ podle afinní věty o nulách.

Z předchozí poznámky plyne $I(V(J)) = I(V^{\mathrm{af}}(J)) = \sqrt{J}$. $\square$

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

Věta 10.8. *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

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

Naopak,

$$j_0^{-1}(V^{\mathrm{af}}(f)) = \{(x_0 : \dots : x_n) \in \mathbb{P}^n \mid x_0^{\deg f} f(\tfrac{x_1}{x_0}, \dots, \tfrac{x_n}{x_0}) = 0\} = V(\widetilde{f}),$$

kde $\widetilde{f} = x_0^{\deg f} f(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0})$ je homogenní polynom. □

Důsledek 10.9. *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 a ireducibilními uzavřenými podmnožinami U_0 (tj. takových, které nelze napsat jako sjednocení vlastních uzavřených podmnožin). Inverzní zobrazení je dáno uzávěrem, $X \mapsto \overline{X}$, jak se snadno ověří – stačí si totiž uvědomit, že $V = (H_0 \cap V) \cup \overline{(U_0 \cap V)}$ a jelikož $V \not\subseteq H_0$, musí být díky ireducibilitě $V = \overline{U_0 \cap V}$. □

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

$$\overline{V^{\mathrm{af}}(f_1, \dots, f_r)} = V(\widetilde{f}_1, \dots, \widetilde{f}_r)$$

(toto vyžaduje algebraickou uzavřenost $\Bbbk$): pokud se pro $g \in \Bbbk[x_0, \dots, x_n]$ homogenní nuluje $g|_{x_0=1}$ na $V^{\mathrm{af}}(f_1, \dots, f_r)$, pak $g^k|_{x_0=1} = f_1h_1 + \dots + f_rh_r$, a proto $g^k \in (\widetilde{f}_1, \dots, \widetilde{f}_r)$.

Příklad 10.10. Pokud $C_0 = V^{\mathrm{af}}(x_2^2 - x_1(x_1 - 1)(x_1 - 2))$, pak projektivní rozšíření je $C = V(x_0x_2^2 - x_1(x_1 - x_0)(x_1 - 2x_0))$.

? ***Otázka.*** **Tady dokázat silnější verzi Bezoutovy věty?**

11. 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 11.1. 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 11.2. *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).

Definice 11.3. Zobrazení $f\colon V \to W$ mezi (kvazi)projektivními 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 $f = (f_0 : \cdots : f_m)$ na nějakém okolí bodu P ve V; zejména musí být alespoň jedno $f_j(P) \neq 0$.

Lemma 11.4. *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 $f = (f_0 : \cdots : f_m)$; 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 afinními prostory, 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 racionálního zobrazení. Budeme tedy zobrazením jako výše říkat *racionální* zobrazení, pokud nejsou nutně definované všude. Omezíme se pro jednoduchost na případ ireducibilní kvaziprojektivní variety.

Definice 11.5. *Racionální zobrazení* $f\colon V \dashrightarrow W$ mezi (kvazi)projektivními varietami je třída regulárních zobrazení $f'\colon V' \to W$, definovaných na otevřené husté podmnožině $V' \subseteq V$, vzhledem k relaci $f' \sim f'' \Leftrightarrow f' = f''$ na $V' \cap V''$.

Definiční obor f je množina všech bodů $P \in V$ takových, že existuje reprezentant f, který je na P definovaný. Také říkáme, že f je regulární v bodě P. Definiční obor značíme $\operatorname{dom} f$.

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 $(f_0 : \cdots : f_m)$; oba dva se hodí k různým účelům.

Zabývejme se nyní případem racionálních funkcí, 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, právě když platí $f_1 g_0 = g_1 f_0$ na nějaké otevřené husté podmnožině V a tedy i na celém V. Můžeme tedy algebraicky popsat racionální funkce jako racionální výrazy f_1/f_0, kde f_0, f_1 jsou homogenní polynomy téhož stupně a $f_0 \notin I(V)$, vzhledem k relaci $f_1/f_0 = g_0/g_1 \Leftrightarrow f_1 g_0 - g_1 f_0 \in I(V)$. Alternativně lze brát $f_0, f_1 \in \Bbbk[x_0, \ldots, x_n]/I(V)$ a uvažovat zlomky tvaru f_1/f_0 s čitatelem a jmenovatelem homogenním téhož stupně.

Racionální funkce na ireducibilní kvaziprojektivní varietě V tvoří 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 $\Bbbk(V) = \Bbbk(V_0)$, přičemž $\Bbbk(V_0)$ je podílové těleso souřadnicového okruhu $\Bbbk[V_0]$.

Věta 11.6. *Racionální funkce $f\colon V \dashrightarrow \Bbbk$ na afinní varietě V je regulární, právě když je polynomiální.*

Důkaz. Definujeme ideál jmenovatelů $D_f = \{h \in \Bbbk[V] \mid fh \in \Bbbk[V]\}$. Zjevně platí, že D_f obsahuje nulu a pak právě všechny funkce h, pro které existuje vyjádření $f = g/h$. Platí tedy $\operatorname{dom} f = V \smallsetminus V(D_f)$ a zejména je f regulární, právě když $V(D_f) = \emptyset$, tj. právě když $1 \in D_f$. To ale přesně znamená, že f má vyjádření ve tvaru $f = g/1$ a $f = g$ je polynomiální. □

Důsledek 11.7. *Racionální funkce $f\colon V \dashrightarrow \Bbbk$ na afinní varietě V definované na $V \smallsetminus V(h)$ jsou v bijekci s lokalizací $\Bbbk[V]_h$.*

Důkaz. Jedná se právě o regulární funkce na $V \smallsetminus V(h)$, což je afinní varieta $V(I(V), th - 1)$ se souřadnicovým okruhem $\Bbbk[V][t]/(th-1) = \Bbbk[V][h^{-1}] = \Bbbk[V]_h$.

Jinak $\operatorname{dom} f \supseteq V \smallsetminus V(h) \Leftrightarrow V(D_f) \subseteq V(h) \Leftrightarrow \sqrt{D_f} \ni h \Leftrightarrow f = g/h^k$. □

12. 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.

Příklad 12.1. 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 12.2. 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 12.3. *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 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 $\overline{\operatorname{im} g} = X$. □

Definice 12.4. Řekneme, že dominantní zobrazení $f\colon V \dashrightarrow W$ je *biracionální ekvivalence*, jestliž 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 ke kvaziafinním 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 $\mathrm{id}\colon V \dashrightarrow U$.

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, například $\Bbbk(\mathbb{P}^n) = \Bbbk(\mathbb{A}^n) = \Bbbk(x_1, \ldots, x_n)$.

Lemma 12.5. *Racionální zobrazení $f\colon V \dashrightarrow W$ je dominantní, právě když je $f^*\colon \Bbbk[W] \to \Bbbk(V)$ injektivní.*

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

Důkaz. 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 12.7. *Existuje kontravariantní ekvivalence kategorií*

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

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 K taková, že

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

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

Důsledek 12.8. *Dvě kvaziprojektivní variety V, W jsou biracionálně ekvivalentní, právě když $\Bbbk(V) \cong \Bbbk(W)$.*

Definice 12.9. Kvaziprojektivní varieta V se nazývá *racionální*, jestliže je biracionálně ekvivalentní $\mathbb{A}^m$ (ekvivalentně $\mathbb{P}^m$).

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

Příklad 12.10. Hyperbola je racionální. Uvažujme ji projektivně, tj. $H = V(y_1y_2 - y_0^2)$. Potom

$$\mathbb{P}^1 \to H, \quad (x_0 : x_1) \mapsto (x_0x_1 : x_1^2 : x_0^2)$$

(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 dokázat, že indukují izomorfismus $H_0 \cong \mathbb{A}^1 \smallsetminus \{0\}$. Toto je obecný fenomén.

Věta 12.11. *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'. □

13. Součin projektivních variet

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

$$s_{nm}\colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{n+m+1}, \quad ([v], [w]) \mapsto [v \otimes w].$$

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

Věta 13.1. *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

$$s_{nm}((x_0 : \cdots : x_n), (y_0 : \cdots : y_m)) = \begin{pmatrix} x_0y_0 : \cdots : x_0y_m \\ \vdots \qquad\qquad \vdots \\ x_ny_0 : \cdots : x_ny_m \end{pmatrix} = (\cdots : x_iy_y : \cdots),$$

tj. homogenní souřadnice z_{ij} je rovna x_iy_j (koeficient $\sum x_ie_i \otimes \sum y_j\widetilde{e}_j$ u $e_i \otimes \widetilde{e}_j$ je x_iy_j). Zjevně pro souřadnice obrazu platí $z_{ij}z_{kl} = z_{il}z_{jk}$. Nechť Z je varieta zadaná těmito rovnicemi, platí tedy $\Sigma_{nm} \subseteq Z$. Nechť naopak $R = (z_{ij}) \in Z$ a hledejme $P = (x_i) \in \mathbb{P}(V)$, $Q \in \mathbb{P}(W)$ tak, že $s_{nm}(P, Q) = R$. Alespoň jedna ze souřadnic R je nenulová, bez újmy na obecnosti budeme předpokládat, že to je $z_{00} = 1$. Potom musí být $x_0 \neq 0$ a $y_0 \neq 0$ a položíme tedy $x_0 = 1$, $y_0 = 1$. Potom musí být $z_{i0} = x_i$ a $z_{0j} = y_j$, takže jsme nuceni položit

$$P = (z_{00} : z_{10} : \cdots : z_{n0}), \quad Q = (z_{00} : z_{01} : \cdots : z_{0m}).$$

Stačí ověřit, že skutečně $R = s_{nm}(P, Q)$. Pravá strana má souřadnice $x_iy_j = z_{i0}z_{0j} = z_{ij}z_{00} = z_{ij}$. □

Z předchozího důkazu navíc vidíme, že obě projekce $\Sigma_{nm} \to \mathbb{P}^n$ a $\Sigma_{nm} \to \mathbb{P}^m$ jsou regulární, v prvním případě zadané

$$(\cdots : z_{ij} : \cdots) \mapsto (z_{00} : z_{10} : \cdots : z_{n0}) = (z_{0j} : z_{1j} : \cdots : z_{nj}).$$

Věta 13.2. *Nechť $V \subseteq \mathbb{P}^n$, $W \subseteq \mathbb{P}^M$ jsou projektivní variety. Potom $V \times W \subseteq \mathbb{P}^n \times \mathbb{P}^m \cong \Sigma_{nm}$ je také projektivní varieta. Jsou-li obě V, W ireducibilní, pak $V \times W$ je také ireducibilní.*

Důkaz. Nechť $V = V(f_1, \ldots, f_r)$, $W = V(g_1, \ldots, g_s)$ kde $\deg f_k = d_k$, $\deg g_l = e_l$. Pro bod $((x_0 : \cdots : x_n), (y_0 : \cdots : y_m))$ platí $f_k(x_0, \ldots, x_n) = 0$, právě když $f_k(x_0, \ldots, x_n)y_j^{d_k} = 0$ pro každé $j = 0, \ldots, m$. Přitom polynom $F_{kj} = f_ky_j^{d_k}$ je homogenní v součinech $x_iy_j = z_{ij}$ a budeme jej tak chápat. Analogicky dostaneme polynomy $G_{li} = g_lx_i^{e_l}$ a potom platí

$$V \times W = V(z_{ij}z_{kl} - z_{il}z_{jk}, F_{kj}, G_{li}).$$

Ireducibilita se dokáže stejně jako u afinních variet. □

Důsledek 13.3. *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 $\mathbb{A}^n$). □

Tvrzení 13.4. *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 $x_iy_j = x_jy_i$, tj. $z_{ij} = z_{ji}$.

Množina ze zadání je $(f, g)^{-1}(\Delta_W)$, kde $(f, g) \colon V \to W \times W$. □

Věta 13.5. *Projekce $\pi \colon \mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$ je uzavřená.*

Důkaz. Prvně dokůžeme následující tvrzení: Nechť $P \in \mathbb{P}^n$ je bod, pro jednoduchost budeme předpokládat $P = (0 : \dots : 0 : 1)$, a $X \subseteq \mathbb{P}^n$ projektivní varieta. Uvažujme pro $F, G \in I(X)$ homogenní stupňů d, e oba jako $F, G \in \Bbbk[x_0, \dots, x_{n-1}][x_n]$ stupňů d a e (tj. může se jednoduše stát, že vedoucí koeficient F je 0; to je přesně koeficient u ${x_n}^d$, takže to nastane, právě když $P \in V(F)$). Potom $V(\mathrm{Res}(F, G; x_n) \mid F, G \in I(X))$ je buď obraz X při projekci z P (pokud $P \notin X$) nebo celé $\mathbb{P}^{n-1}$ (pokud $P \in X$).

(Jednoduchý) důkaz spočívá v následujícím lemmatu: pro každou k-tici bodů $P_1, \dots, P_k \notin X$ existuje $F \in I(X)$ takový, že $P_1, \dots, P_k \notin V(F)$. Předně existuje polynom $F_i \in I(X)$ nenulový na P_i. Vynásobením vhodným polynomem G_i, nulovým na ostatních bodech, ale nenulovým na P_i, a sečtením dostaneme hledaný $F = F_1G_1 + \dots + F_kG_k$.

Další krok je uvážit zobrazení $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^{n-1} \times \mathbb{P}^m$, které je v první složce projekcí z libovolného bodu $P \in \mathbb{P}^n$ a ve druhé složce identita. Po n krocích dostaneme zobrazení $\mathbb{P}^n \times \mathbb{P}^m \to \mathbb{P}^m$. Přitom procedura z první části přesně v každém kroku zachovává obraz dané projektivní variety do druhé složky. □

Důkaz. Nechť $Z \subseteq \mathbb{P}^n \times \mathbb{P}^m$ je zadaná homogenními 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 $\Bbbk^d[x_0, \dots, x_n] \cap (g_1(-, Q), \dots, g_r(-, Q))$, což je vektorový prostor generovaný

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

To je vlastní podprostor $\Bbbk^d[x_0, \dots, x_n]$, právě když každých $D - 1$ polynomů $g_k(-, Q)x^\alpha$ je lineárně závislých, kde $D = \dim \Bbbk^d[x_0, \dots, x_n]$. 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 13.6. *Nechť X je projektivní varieta a Y kvaziprojektivní varieta. Potom projekce $\pi\colon X \times Y \to Y$ je uzavřená.*

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

Věta 13.7. *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 $X \times Y$. Podle předchozího důsledku je $\operatorname{im} f = \pi(\Gamma_f) \subseteq Y$ uzavřená podmnožina. □

Věta 13.8. *Každá regulární funkce $f\colon X \to \Bbbk$ na ireducibilní projektivní varietě X je konstantní.*

Důkaz. Uvažme složení $X \xrightarrow{f} \Bbbk \subseteq \mathbb{P}^1$, $P \mapsto (1 : f(P))$. Jedná se o regulární zobrazení a podle předchozí věty je jeho obraz uzavřený. Zároveň ale není roven $\mathbb{P}^1$, neboť je obsažen v $\mathbb{A}^1 = \Bbbk$, takže tímto obrazem musí být konečná podmnožina $\Bbbk$. 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 13.9. *Projektivní varieta je afinní (tj. je izomorfní nějaké uzavřené podmnožině afinního prostoru), 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. □

14. Veroneseho zobrazení

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

$$\mathbb{P}^{n+1} \to \mathbb{P}^D, \quad (x_0 : \cdots : x_n) \mapsto (\cdots : x^\alpha : \cdots)_{|\alpha|=d}.$$

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

Věta 14.1. *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 varieta.*

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

Věta 14.2. *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 nyní libovolné otevřené okolí $U \in P$ bodu $P \in X$ kvaziprojektivní variety X. Potom $X \smallsetminus U$ je projektivní varieta neobsahující P a existuje tedy homogenní polynom $f \in I(X \smallsetminus U) \smallsetminus I(P)$. Proto $P \in X_f = X \smallsetminus V(f) \subseteq U$ a tedy afinní otevřená okolí tvoří bázi okolí. □

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

15. Lokální vlastnosti variet

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

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

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 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.

16. 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

$$(\mathbb{K}^n)^k \supseteq V(k,n) \xrightarrow{\gamma} G(k,n)$$

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 16.1. *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 16.2. *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 $\pi : U \subseteq X \times Y$ bázová otevřená množina, tedy doplněk $U = (X \times Y) \smallsetminus V(g)$ nulové množiny nějakého polynomu $g = g(x, y)$. 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 lineární podmínka na koeficienty $g(x, -) \in K[y_0, \dots, y_m]$, které závisí polynomiálně na $x_0, \dots, x_n$. □

Uvažujme podmnožinu $\widehat{U} \subseteq V(k, n)$ danou k-ticemi $(v_1, \dots, v_k)$, jejichž projekce do $\mathbb{K}^k$ tvořeného prvními k souřadnicemi 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

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

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

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

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.

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

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

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

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

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.

Tvrzení 16.3. *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). $\square$

17. Dimenze

Definice 17.1. Řekneme, že projektivní varieta $X \subseteq \mathbb{P}^n$ má kodimenzi nejvýše k, jestliže každý k-rozměrný projektivní podprostor (zkráceně k-rovina) $\Lambda \subseteq \mathbb{P}^n$ protíná X. Samozřejmě pak X má kodimenzi právě k, jestliže navíc existuje $(k - 1)$-rovina disjunktní s X (tedy X nemá kodimenzi nejvýše $k + 1$). Dimenzí variety X pak nazveme číslo $d = n - k$.

Zabývejme se nyní $(k-1)$-rovinami v případě, že X má kodimenzi k. Podle definice existuje nějaká, která je disjunktní s X. Ukážeme nyní, že ve skutečnosti obecná $(k - 1)$-rovina bude s X disjunktní. Uvažujme tedy varietu incidence $\mathcal{C}_{k-1}(X)$. Ta je uzavřená a podle předchozího také vlastní, takže její komplement

$$\mathbb{G}(k - 1, n) \smallsetminus \mathcal{C}_{k-1}(X),$$

skládající se právě z $(k-1)$-rovin disjunktních s X, tvoří otevřenou neprázdnou, a tedy hustou, podmnožinu.

Lemma 17.2. *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 $\dim X_i \leq \dim X$. Předpokládejme, že je tato nerovnost striktní pro všechna i. Potom obecná k-rovina je disjunktní s každou X_i a tedy i s X. To je spor s tím, že kodimenze X je k. $\square$

Je-li Λ nyní k-rovina, obsahující nějakou "obecnou" $(k-1)$-rovinu, tedy takovou disjunktní s X. Potom $X \cap \Lambda$ musí být konečná, jelikož je disjunktní s projektivní nadrovinou a je tedy afinní. Ve skutečnosti opět platí, že množina všech k-rovin majících konečný průnik s X tvoří otevřenou neprázdnou podmnožinu. To je proto, že obecná $(k - 1)$-rovina je disjunktní s X a tedy obecná k-rovina Λ obsahuje $(k - 1)$-rovinu disjunktní s X. To ale znamená, že průnik $X \cap \Lambda \subseteq \Lambda$ musí být konečný, protože je disjunktní s nějakou nadplochou a je tedy afinní.

Ve skutečnosti platí, že počet průsečíků $X \cap \Lambda$ je pro obecnou k-rovinu maximální možný a roven stupni variety X.

Příklad 17.3. 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 $X = \mathbb{P}^n$.

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 $\operatorname{tr\,deg} \mathbb{K}(X)$ tělesa $\mathbb{K}(X)$ racionálních funkcí na X. Jedná se o maximální počet prvků $\mathbb{K}(X)$ algebraicky nezávislých nad $\mathbb{K}$. Jsou-li tyto prvky $a_1, \ldots, a_s$, je $\mathbb{K}(a_1, \ldots, a_s)$ izomorfní podílovému tělesu okruhu polynomů v s proměnných. Každý prvek $\mathbb{K}(X)$ je algebraický nad $\mathbb{K}(a_1, \ldots, a_s)$. Jelikož je $\mathbb{K}(X)$ konečně generované, je už rozšíření $\mathbb{K}(X) : \mathbb{K}(a_1, \ldots, a_s)$ konečné. Platí, že libovolný maximální systém algebraicky nezávislých prvků má stejný počet.

Tvrzení 17.4. *Platí* $\dim \pi(X) = \dim X$ *a* $\operatorname{tr\,deg} \mathbb{K}(\pi(X)) = \operatorname{tr\,deg} \mathbb{K}(X)$.

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 $\mathbb{K}(X)$ je generované $x_1/x_0, \ldots, x_n/x_0$, 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 $\mathbb{K}(X)$ jako rozšíření $\mathbb{K}(\pi(X))$. Jako takové je generované jediným prvkem x_n/x_0. Uvážme libovolný homogenní polynom $f \in I(X)$ stupně d, který je nulový na X, ale nikoliv na $P = (0 : \cdots : 0 : 1)$. To znamená, že jeho koeficient u x_n^d je nenulový a fakt, že $f/x_0^d = 0$ v $\mathbb{K}(X)$ vyjadřuje přesně, že prvek x_n/x_0 je algebraický nad $\mathbb{K}(\pi(X))$. Je tedy rozšíření $\mathbb{K}(X) : \mathbb{K}(\pi(X))$ konečné a proto se stupně transcendence rovnají. □

? ***Poznámka.* Tady by se asi hodilo říct, že obraz $\pi(X)$ je uzavřený, takže můžeme používat naši stávající definici dimenze.**

Důsledek 17.5. *Platí* $\dim X = \operatorname{tr\,deg} \mathbb{K}(X)$.

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

$$\operatorname{tr\,deg} \mathbb{K}(X) = \operatorname{tr\,deg} \mathbb{K}(x_1/x_0, \ldots, x_n/x_0) = n = \dim X.$$

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

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

podle předchozího tvrzení a indukčního předpokladu. □

Tvrzení 17.6. *Nechť $f : X \to Y$ je surjektivní obecně konečné zobrazení mezi ireducibilními kvaziprojektivními varietami a $X_0 \subsetneqq X$ vlastní podvarieta. Potom $\overline{f(X_0)} \subsetneqq Y$ je také vlastní podvarieta.*

Důkaz. Prvně můžeme Y nahradit libovolnou afinní otevřenou podmnožinou, například $Y_g = Y \smallsetminus V(g)$, a X příslušným vzorem $X_{gf} = X \smallsetminus V(gf)$, který je také afinní. Poté můžeme X nahradit grafem Γ_f, takže f je tím pádem zúžením projekce $\mathbb{A}^m \to \mathbb{A}^n$. Na závěr si uvědomme, že stačí dokázat tvrzení v případě $m = n + 1$, protože obecný případ je kompozicí takových projekcí. Jsme tedy v situaci, kdy

$$X \subseteq \mathbb{A}^{n+1}, \quad Y \subseteq \mathbb{A}^n \quad \text{a} \quad f(x_1, \ldots, x_{n+1}) = (x_1, \ldots, x_n).$$

Předpokládejme sporem, že $\overline{f(X_0)} = Y$. Potom $K(X_0)$ i $K(X)$ lze považovat za rozšíření $K(Y)$. Ukážeme prvně, že jsou to algebraická rozšíření: jelikož je f obecně konečné, existuje $h \in I(X)$, které je nenulové na nějakém bodu $f^{-1}(Y) \smallsetminus X$. Po vyjádření

$$h = a_0(x_1, \ldots, x_n)x_{n+1}^d + \cdots + a_d(x_1, \ldots, x_n)$$

je pak zřejmé, že nějaký koeficient $a_i \notin I(Y)$ a generátor $x_{n+1} \in K(X)$ je tedy algebraický nad $K(Y)$.

Zvolme minimální polynom $x_{n+1} \in K(X)$ nad $K(Y)$, po vynásobení vhodným nenulovým polynomem z $K[Y]$ můžeme dosáhnout toho, že je tento prvkem $K[Y][t] = K[f^{-1}(Y)]$, označme jej opět h. Jelikož platí $h(x_{n+1}) = 0$ i v $K(X_0)$ a h je ireducibilní, musí být h zároveň minimálním polynomem $x_{n+1} \in K(X_0)$ nad $K(Y)$. Nechť nyní $g \in K[f^{-1}(Y)]$ je libovolný nulový na X_0. Potom po vynásobení nějakým nenulovým $b \in K[Y]$ platí $h \mid bg$ díky minimalitě h. Je tedy $f^{-1}(V(b)) \cup V(g) \supseteq V(h) \supseteq X$. Jelikož je $I(X_0)$ generované konečně mnoha $g_1, \ldots, g_r$ dostáváme $f^{-1}(V(b_1) \cup \cdots \cup V(b_r)) \cup X_0 \supseteq X$. Proto $X_0 \supseteq X \smallsetminus (V(b_1) \cup \cdots \cup V(b_r)) = X_{b_1 \cdots b_r}$ je hustá v X. □

Důsledek 17.7. *Je-li $X_0 \subseteq X$ podvarieta projektivní variety X, která neobsahuje žádnou její komponentu, pak* $\dim X_0 < \dim X$.

Důkaz. Stačí se omezit na případ, kdy X je ireducibilní a tedy X_0 vlastní podvarieta. Připomeňme surjektivní obecně konečné zobrazení $\pi : X \to \mathbb{P}^d$ dané opakovanou projekcí z bodů. Podle předchozího tvrzení je $\pi(X_0) \subsetneqq \mathbb{P}^d$ a má tedy dimenzi

$$\dim X_0 = \dim \pi(X_0) < d = \dim X.$$ □

Věta 17.8. *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. □

Poznámka. V případě ireducibilní projektivní variety X předchozí věta 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 toto tvrzení platí také pro kvaziprojektivní variety.

Důsledek 17.9. *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 homogenní polynom, pak $X \subseteq V(f)$. Protože je X ireducibilní, leží v některé ireducibilní komponentě $V(f)$. Protože jsou obě ireducibilní a téže dimenze, musí být $X = V(f)$. □

Důsledek 17.10. *Každých n homogenních polynomů má společný nenulový kořen, tj. $\emptyset \neq V(f_1, \dots, f_n) \subseteq \mathbb{P}^n$.*

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 předchozího důsledku má totiž každý řetězec délku maximálně d. Podle předchozí věty pak 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 $K[X]$, která je definována jako "délka" d nejdelšího řetězce

$$0 = I_0 \subsetneqq \cdots \subsetneqq I_d \subsetneqq K[X]$$

prvoideálů v $K[X]$.

Tato definice má tu výhodu, že je vyjádřena v řeči variety samotné a nezávisí na jeho vložení do projektivního prostoru a je tedy zjevně invariantní vzhledem k izomorfismům[1].

Pomocí této charakterizace nyní dokážeme následující větu vhodnou pro počítání dimenzí.

Věta 17.11. *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 $Y_0 \subsetneqq Y$ je libovolná komponenta $Y \cap V(g)$, kde g není nulová na Y a položme $X_0 = f^{-1}(Y_0)$. Má-li Y_0 maximální dimenzi $\dim Y - 1$, dostáváme indukcí na $X_0 \to Y_0$, že

$$\dim X \geq \dim X_0 - 1 = \dim Y_0 + d - 1 = \dim Y + d.$$

Nechť naopak Y_0 je komponenta, jejíž vzor $X_0 = f^{-1}(Y_0)$ obsahuje komponentu $X \cap V(gf)$ maximální dimenze $\dim X - 1$. Potom

$$\dim X = \dim X_0 - 1 = \dim Y_0 + d - 1 \leq \dim Y + d.$$

□

[1] Ukážeme nyní, že je invariantní i vzhledem k biracionálním ekvivalencím. To je do jisté míry jasné u stupně transcendence, nedokázali jsme však, že ten je dobře definovaný. Nechť $\pi : X \to \mathbb{P}^d$ je nějaká obecně konečná projekce, kde X je ireducibilní projektivní varieta. Nechť $U \subseteq X$ je nějaká otevřená množina. Ukážeme, že $\dim U = \dim X$ (v definici pomocí délky řetězců). Zřejmě každý ostře rostoucí řetězec uzavřených ireducibilních podmnožin U zadává pomocí uzávěru ostře rostoucí řetězec uzavřených ireducibilních podmnožin X. Je tedy $\dim U \leq \dim X$. Pro opačnou implikaci stačí najít ireducibilní nadplochu $Y \subseteq X$, která nebude ležet v $X \smallsetminus U$ a použít indukci na $Y \cap U \subseteq Y$. Podle předchozího je $\pi(X \smallsetminus U)$ vlastní uzavřená množina. Zvolme v $\mathbb{P}^d$ libovolnou nadrovinu Λ neležící v $\pi(X \smallsetminus U)$ a nechť Y je libovolná komponenta $\pi^{-1}(\Lambda)$, která se zobrazí surjektivně na Λ. Potom $\pi : Y \to \Lambda$ je opět obecně konečná projekce a můžeme pokračovat indukcí.

Příklad 17.12. Spočítejme dimenzi Grassmannovy variety $G(k,n)$ elementárním způsobem. Uvažme zobrazení

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

s definičním oborem $V(k,n)$, který není projektivní, ale pouze kvaziprojektivní – chtělo by to všechno zobecnit, snad někdy příště. 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 $\dim G(k,n) = nk - k^2 = k(n-k)$.

Příklad 17.13. Každá projektivní varieta $X \subseteq \mathbb{P}^n$ je biracionálně ekvivalentní nadploše. Předpokládejme, že X má kodimenzi alespoň 2 a hledejme projekci

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

z nějakého bodu P tak, aby zúžení $\pi : X \to \pi(X)$ mělo v obecném fibru jediný prvek. Podle věty o obecně konečných zobrazeních je pak $\pi : X \to \pi(X)$ biracionální ekvivalence (na úrovni těles racionálních funkcí se jedná o rozšíření stupně jedna). Zabývejme se proto množinou všech přímek protínajících X. To je přesně $\mathcal{C}_1(X)$ a má dimenzi $d+n-1$, neboť varieta incidence má tuto dimenzi (projekce na X má fibry dimenze $n-1$) a projekce na $\mathcal{C}_1(X)$ má obecně konečné fibry.

Zabývejme se nyní podmnožinou $\mathcal{C}_1(X)$ těch přímek, které protínají X ve více jak jednom bodě. Uvažujme zobrazení $(X \times X) \smallsetminus \Delta \to \mathbb{G}(1,n)$ posílající dvojici bodů (x,y) na přímku $\overline{xy}$. Jeho obraz (přesněji řečeno uzávěr tohoto obrazu) má dimenzi nejvýše $2d < d+n-1$. Proto obecná přímka z $\mathcal{C}_1(X)$ protíná X v jediném bodě. Uvažujme nyní varietu dvojic (P,p), kde P je bod ležící na přímce p, která protíná X. Podmnožina těch dvojic (P,p), kde p protíná X v jediném bodě různém od P je podle předchozího otevřená a neprázdná. Libovolný bod P vyskytující se v nějaké takové dvojici pak bude splňovat, že projekce z něj bude po zúžení na X obecně injektivní.

Věta 17.14. *Nechť $f : X \to Y$ je 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

$$g : \Gamma_f \subseteq \mathbb{P}^n \times Y \longrightarrow Y.$$

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 kopmlement 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 $U = Y \setminus Y_n$ je otevřená.

Je-li nyní Y ireducibilní, tak zúžením na U dostáváme $f : f^{-1}(U) \to U$ splňující předpoklady předchozí věty. □

Zajímavým důsledkem je následující.

Důsledek 17.15. *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. Podle předpokladu 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. □

Poznámka. Shafarevich má kapitolku I.5.3 o konečných zobrazeních $f \colon X \to Y$ mezi afinními varietami X, Y. Ta jsou definována pomocí tak, že $\mathbb{k}[X]$ je intergrální nad $\mathbb{k}[Y]$ (ekvivalentně konečné). Potom má větu, že takové zobrazení musí být nutně surjektivní (využívá Nakayamovo lemma a nějakou algebru) s důsledkem, že každé konečné zobrazení je uzavřené. Dále ukáže lokálnost této podmínky a definuje ji obecně pro zobrazení mezi kvaziprojektivními varietami. Potom ukáže, že každé dominantní zobrazení obsahuje ve svém obraze nějakou neprázdnou otevřenou. Pak zkonstruuje konečnou projekci (viz výše) a zobecní to na nelineární „projekce“.

18. 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

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

značíme jej $\widetilde{X}$.

Tečný kužel variety X v bodě P_0 je afinní kužel na průniku tohoto blow-upu s rovinou $P = 0$ (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 $x \neq 0$, $t \neq 0$. Předpokládáme-li dále, že $X \neq \{P_0\}$, je to ekvivalentní $g(x, x) = 0$, 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 $f(x)_{\mathrm{in}}$. Vidíme tedy, že tečný kužel X v bodě $P_0 = 0$ je

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

Příklad 18.1. 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 proto tečný kužel má 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 $\widetilde{f}(x, \widetilde{x}) = f(x, tx) = t^d f(x)$, 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 18.2. 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 $((x, y), (\widetilde{x} : \widetilde{y})) \mapsto (x, \widetilde{y}/\widetilde{x})$). 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 $f = yf'$ 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}. Po konečném množství blow-upů pak bude tento polynom nižšího iniciálního stupně a po dalším konečném množství blow-upů pak dokonce lineární.

19. Tečný prostor

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

$$I_P^{(1)} = \{\mathrm{d}f(P) \mid f \in I\},$$

kde $\mathrm{d}f(P) = \frac{\partial f(P)}{\partial x_0}\,\mathrm{d}x_0 + \dots + \frac{\partial f(P)}{\partial x_n}\,\mathrm{d}x_n$ (a kde $\mathrm{d}x_i = x_i$ jakožto lineární forma na $\mathbb{k}^n$). 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

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

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

Zabývejme se nyní krátce tečným prostorem projektivních variet. Uvažujme zobrazení

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

V afinní mapě U_i se jedná o zobrazení $(x_0, \dots, x_n) \mapsto (x_0/x_i, \dots, \widehat{x_i/x_i}, \dots, x_n/x_i)$ a tedy jeho diferenciál ve $v = (v_0, \dots, v_n)$ je surjektivní s jádrem daným

$$(\mathrm{d}x_0\, v_i - \mathrm{d}x_i\, v_0)/{x_i}^2 = 0, \quad i = 0, \dots, \widehat{i}, \dots, n.$$

Řešením této soustavy jsou právě násobky v, tedy $\Bbbk^{n+1}/[v] \xrightarrow{\cong} T_{[v]}\mathbb{P}^n$, nezávisle na volbě afinní mapy. Pro f homogenní stupně d zjevně platí

$$d \cdot f = \tfrac{\partial f}{\partial x_0}\, x_0 + \dots + \tfrac{\partial f}{\partial x_n}\, x_n$$

a po dosazení bodu $[v] \in V(f)$ pak

$$0 = d \cdot f(v) = \tfrac{\partial f(v)}{\partial x_0}\, v_0 + \dots + \tfrac{\partial f(v)}{\partial x_n}\, v_n = \mathrm{d}f(v)v.$$

Zejména je tedy diferenciál $\mathrm{d}f(v)$ nulový na celé přímce $[v]$ a proto můžeme položit

$$T_{[v]}X = \bigcap_{f \in I(X)} \ker \mathrm{d}f(v)/[v],$$

případně pak jeho projektivní rozšíření, tj. projektivní podprostor $V(I(X)_{[v]}^{(1)})$.

Věta 19.1. *Množina nesingulárních bodů ireducibilní kvaziprojektivní variety tvoří neprázdnou otevřenou podmnožinu.*

Důsledek 19.2. *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 je d dimenze X. K tomu použijeme následující charakterizaci.

Tvrzení 19.3. *Tečný prostor $T_P X$ 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.*

Před důkazem tohoto tvrzení dokončeme důkaz věty. Z lokální charakterizace tečného prostoru plyne, že je invariantní vůči izomorfismům variet. Z otevřenosti množiny bodů, kde $\dim T_P X$ je minimální, pak plyne, že toto minimum je dokonce invariantní vzhledem k biracionálním ekvivalencím. 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. □

Vraťme se nyní k důkazu tvrzení.

Důkaz Tvrzení 19.3. Definujme prvně diferenciál polynomiální funkce $f \in \mathbb{K}[X]$ v bodě $P \in X$, $\mathrm{d}f(P)\colon T_P X \to \mathbb{K}$, jako zúžení diferenciálu libovolného rozšíření na polynomiální funkci na $\mathbb{A}^n$, tj. polynom. Jelikož se každé dvě takové rozšíření liší o prvek $I(X)$, jehož diferenciál je nulový na $T_P X$, je $\mathrm{d}f(P)$ dobře definovaný. 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

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

Máme tedy dobře definované zobrazení

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

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 $(x_i - x_i(P)) \in \mathfrak{m}_P$. Je-li tedy $\mathrm{d}f(P) = 0$, pak $f \in \mathfrak{m}_P^2$ a D_P je izomorfismus. $\square$

Poznámka. Taylorův polynom (a rozvoj) v regulárním bodě přes lokální parametry, lokální parametrizace (jakožto formální řada). Aplikace na biracionální invarianci dimenze ve smyslu délky nejdelšího řetězce ireducibilních podvariet. Definice stupně protínání dvou rovinných křivek v bodě.

20. Konečná zobrazení

Definice 20.1. Polynomiální zobrazení $f\colon X \to Y$ mezi afinními varietami se nazývá *konečné*, jestliže indukované zobrazení $f^*\colon \Bbbk[Y] \to \Bbbk[X]$ dělá z $\Bbbk[X]$ konečnou $\Bbbk[Y]$-algebru.

Lemma 20.2. *Zúžení konečného zobrazení $f\colon X \to Y$ na libovolnou afinní otevřenou podmnožinu $Y_h \subseteq Y$, tj. zobrazení $f\colon Y_f \to X_{hf}$, je opět konečné. Analogicky zúžení na libovolnou uzavřenou podmnožinu $Z \subseteq Y$ je konečné.*

Důkaz. Dokážeme první část, druhá je jednodušší. Zúžení ze znění lemmatu indukuje

$$f^*\colon \Bbbk[Y_h] = \Bbbk[Y]_h \longrightarrow \Bbbk[X]_{hf} = \Bbbk[X_{hf}].$$

Je-li $\Bbbk[Y]$-modul $\Bbbk[X]$ generován prvky $x_1, \ldots, x_n$, pak pro $g/(hf)^k \in \Bbbk[X]_{hf}$ platí

$$g/(hf)^k = (x_1 \cdot (h_1 f) + \cdots + x_n \cdot (h_n f))/(hf)^k = x_1 \cdot ((h_1/h^k) f) + \cdots + x_n \cdot ((h_n/h^k) f)$$

a $\Bbbk[X]_{hf}$ je tedy také generován $x_1, \ldots, x_n$. $\square$

Protože je $\Bbbk[X]$ konečná $\Bbbk[Y]$-algebra, je každý prvek integrální, zejména pak každá souřadnicová funkce x_i je kořenem

$$t^k + t^{k-1}(a_1 f) + \cdots + t(a_{k-1} f) + a_k f = 0,$$

kde $a_j \in \Bbbk[Y]$. Pro každou volbu $Q \in Y$ je tedy x_i kořenem normovaného číselného polynomu a existuje tedy pouze konečně mnoho bodů $P \in f^{-1}(Q)$. Obrácené tvrzení neplatí, například projekce $V(xy-1) \to \mathbb{A}^1$ má konečné fibry, ale na úrovni algeber indukuje zobrazení $\Bbbk[x] \mapsto \Bbbk[x, x^{-1}]$, které není konečnou algebrou.

Nakayamovo lemma je zásadní pomůckou pro důkazy s konečnými zobrazeními.

Věta 20.3. *Je-li zúžení regulárního zobrazení $f\colon X \to Y$ konečné na nějakém okolí každého bodu $Q \in Y$, pak f je konečné.*

Důkaz. Nechť $f^*\colon \Bbbk[Y_{h_i}] \to \Bbbk[X_{h_i f}]$ je konečná algebra, jako modul generovaná $g_{i1}, \ldots, g_{is} \in \Bbbk[X_{h_i f}]$. Po vynásobení vhodnou mocninou $h_i f$ lze docílit toho, že $g_{i1}, \ldots, g_{is}$ jsou regulární na celém X. Nechť $Y = Y_{h_1} \cup \cdots \cup Y_{h_r}$. Potom tvrdíme, že $\Bbbk[X]$ je jako $\Bbbk[Y]$-modul generovaná g_{ij}. Pro $g \in \Bbbk[X]$ platí $g{h_i}^{k_i} \in \Bbbk[Y][g_{i1}, \ldots, g_{is}]$. Protože však Y_{h_i} pokrývají Y, platí podle Hilbertovy věty o nulách $1 \in ({h_1}^{k_1}, \ldots, {h_r}^{k_r})$, tj.

$$g \in (g{h_1}^{k_1}, \ldots, g{h_r}^{k_r}) \subseteq \Bbbk[Y][g_{ij}]. \qquad \square$$

Definice 20.4. Řekneme, že regulární zobrazení $f\colon X \to Y$ mezi kvaziprojektivními varietami je *konečné*, jestliže existuje pokrytí Y afinními otevřenými množinami $U \subseteq Y$ takové, že $f\colon f^{-1}(U) \to U$ je konečné.

Věta 20.5. *Regulární zobrazení $f\colon X \to Y$ je izomorfismus, právě když je konečné, bijekce a diferenciál $\mathrm{d}f(P)$ je izomorfismus pro každé $P \in X$.*

Důkaz. Podle následujícího lemmatu stačí ukázat, že na úrovni lokálních okruhů indukuje f izomorfismus

$$f^*\colon \mathcal{O}_{Y;f(P)} \xrightarrow{\cong} \mathcal{O}_{X;P}.$$

Surjektivita $\mathrm{d}f(P)\colon \mathfrak{M}_{Y;f(P)}/\mathfrak{M}^2_{Y;f(P)} \xrightarrow{\cong} \mathfrak{M}_{X;P}/\mathfrak{M}^2_{X;P}$ v řeči $\mathcal{O}_{X;P}$-modulů znamená

$$\mathfrak{M}_{Y;f(P)}\mathcal{O}_{X;P} + \mathfrak{M}^2_{X;P} = \mathfrak{M}_{X;P}.$$

Podle Nakayamova lemmatu použitého na $\mathfrak{M}_{X;P}/\mathfrak{M}_{Y;f(P)}\mathcal{O}_{X;P}$ to pak znamená

$$\mathfrak{M}_{Y;f(P)}\mathcal{O}_{X;P} = \mathfrak{M}_{X;P}.$$

Nakonec se Nakayamovo lemma použije na $\mathcal{O}_{X;P}/\mathcal{O}_{Y;f(P)}$; předpoklady platí, protože

$$\mathfrak{M}_{Y;f(P)}\mathcal{O}_{X;P} + \mathcal{O}_{Y;f(P)} = \mathfrak{M}_{X;P} + \mathcal{O}_{Y;f(P)} = \mathcal{O}_{X;P}.$$

Dostáváme tak $\mathcal{O}_{X;P}/\mathcal{O}_{Y;f(P)} = 0$, tj. $f^*\colon \mathcal{O}_{Y;f(P)} \to \mathcal{O}_{X;P}$ je izomorfismus. $\square$

Jiná formulace Nakayamova lemmatu: N konečně generovaný, $N \otimes_A A/\mathfrak{m} = 0 \Rightarrow N = 0$

Lemma 20.6. *Regulární zobrazení $f\colon X \to Y$ je izomorfismus v nějakém okolí $P \in X$, právě když je indukované zobrazení $f^*\colon \mathcal{O}_{Y;f(P)} \to \mathcal{O}_{X;P}$ izomorfismus.*

Důkaz. Prvně nahraďme obě Y afinním otevřeným okolím $f(P)$ a poté X afinním otevřeným okolím P ležícím v jeho vzoru. Ukážeme nyní, že f^{-1} je regulární v okolí bodu $f(P)$.

Nechť $\Bbbk[X]$ je generovaný $x_1, \dots, x_n$. Podle předpokladu existují $y_1, \dots, y_n \in \mathcal{O}_{f(P)}$ tak, že $x_i = f^* y_i$. Nechť jsou tyto regulární na nějakém afinním otevřeném okolí $Y_h \ni P$. Potom $f^* \colon \Bbbk[Y_h] \to \Bbbk[X_{hf}]$ je surjektivní.

Injektivita se dokáže podobně. Nechť $(g_1, \dots, g_r)$ je jádro

$$f^* \colon \Bbbk[Y] \to \mathcal{O}_{X;P}.$$

Protože jsou obrazy g_j v $\mathcal{O}_{Y;f(P)}$ rovny nule (lokální zobrazení je injektivní), jsou všechna g_j nulová na nějakém okolí bodu $f(P)$. Na tomto okolí je injektivní i $f^* \colon \Bbbk[Y] \to \Bbbk[X]$.

Dohromady je pak f^* izomorfismus a tedy i f. Proto je f^{-1} regulární. □

Věta 20.7. *Konečné zobrazení $f \colon X \to Y$ je uzavřené.*

Důkaz. Nechť $Q \in Y$ neleží v obraze f. Potom podle Hilbertovy věty o nulách platí

$$f^*(\mathfrak{m}_Q)\Bbbk[X] = (f_1(x) - q_1, \dots, f_m(x) - q_m) = \Bbbk[X].$$

Podle důkazu Nakayamova lemmatu tedy existuje $h \in \mathfrak{m}_Q$ takové, že $f^*(1+h)\Bbbk[X] = 0$, tj. $(1+h)f = 0$ a $1 + h \in I(\operatorname{im} f)$. Protože je ale $h(Q) = 0$, je Y_{1+h} otevřené okolí Q, které je disjunktní s $\operatorname{im} f$. □

Důsledek 20.8. *Je-li $f \colon X \to Y$ libovolné regulární zobrazení takové, že $\overline{\operatorname{im} f} = Y$, pak $\operatorname{im} f$ obsahuje nějakou otevřenou hustou podmnožinu Y.*

Důkaz. Lze předpokládat, že Y je ireducibilní a X je afinní; dále lze X nahradit grafem Γ_f. Pak $X \subseteq \mathbb{A}^n \times Y$ je uzavřená podmnožina a f je projekce na druhou složku. V důkazu budeme neustále přecházet od Y k otevřeným neprázdným podmnožinám. Nechť (ℓ, Q_0) neleží v uzávěru $\overline{X} \subseteq \mathbb{P}^n \times Y$ a uvažme projekci $\mathbb{A}^n \times Y \to (\mathbb{A}^n/\ell) \times Y$. Ta je regulární a konečná nad $\{Q \in Y \mid (\ell, Q) \notin \overline{X}\} \ni Q_0$. Složení takovýchto projekcí je regulární a konečné zobrazení $\pi \colon X \to \mathbb{A}^d \times Y$. Protože již nelze vybrat projekci, musí být $\operatorname{im} \pi = \mathbb{A}^d \times Y$, takže $\operatorname{im} f = Y$. □

Věta 20.9. *Každá nesingulární projektivní varieta X dimenze d lze vložit do* $\mathbb{P}^{2d+1}$.

Důkaz. Důkaz spočívá v tom, že $X \subseteq \mathbb{P}^n$ postupně promítáme z bodů $P \notin X$. K tomu, aby zúžení projekce $\pi \colon X \to \pi(X)$ byl izomorfismus stačí, aby π bylo injektivní na X a mělo injektivní diferenciál.

Zabývejme se tedy podmnožinou

$$\{(P, Q, R) \mid Q,\ R \in X;\ Q \neq R;\ P,\ Q,\ R \text{ kolineární}\}.$$

Projekce na dvojici (Q, R) má zjevně fibry dimenze 1, takže má tato podmnožina dimenzi $2d + 1$. Podobně podmnožina

$$\{(P, Q) \mid Q \in X;\ P \in \mathbb{T}_Q X\}$$

má dimezni $2d$ (projekce na $Q \in X$ má fibry dimenze d). V obou případech pak projekce na P není surjektivní pokud $n > 2d + 1$, takže lze vhodnou projekci zvolit. □

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 jejic 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

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

má kořen $(x_0 : x_1)$. Snadným výpočtem se lze přesvědčit, že $\operatorname{Res}(f, g, x_2)$ je homogenní stupně $d \cdot e$. Platí totiž, že v matici zadávající $\operatorname{Res}(f, g, x_2)$ 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 $\operatorname{Res}(f, g; x_2)$ odpovídá nejvýše jednomu průsečíku. $\square$

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 $\operatorname{Res}(f, g, x_2)$. 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)

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

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

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

(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 $\operatorname{Res}(f, g, x_2)$.

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

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

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) ⇒ (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 homogenní prvek $f = a_1 f_1 + \dots + a_r f_r \in \bar{I}$ 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 druhou implikaci si stačí uvědomit, že to, zda $f \in \bar{I}$, závisí pouze na $I^{(d)}$, $d \gg 0$. □

Dejme nyní do souvislosti saturované ideály s projektivní větou o nulách. Platí, že zobrazení

$$\{\text{radikálové saturované ideály}\} \xrightarrow{V} \{\text{projektivní variety}\}$$

je bijekce (irelevantní ideál $\mathfrak{m}_0$ není saturovaný) a $V(I) = \emptyset$, právě když $1 \in \bar{I}$.

Nyní vysvětlíme, jaký geometrický objekt lze saturovanému ideálu přiřadit. Předně je to jeho množina 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 ideál I je ireducibilní, jestliže nelze napsat jako průnik dvou striktně větších ideálů. 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

$$I = I_1 \cap \dots \cap I_r$$

ireducibilních ideálů. Poznamenejme, že tento rozklad není jednoznačný v žádném smyslu. Řekneme, že ideál I je *primární*, jestliže

$$fg \in I \Longrightarrow (f \in I) \vee (g \in \sqrt{I}).$$

Tato vlastnost se dá interpretovat dvěma způsoby. Leží-li součin fg v I a $f \notin I$, pak $f \in \sqrt{I}$. Toto lze také interpretovat ekvivalentně v kvocientu S/I takto: každý dělitel nuly je nilpotentní. Pro nás bude v následujícím užitečnější její obrácení. Jestliže prvek S/I není nilpotentní, pak není dělitel nuly, tj. násobení tímto prvkem je injektivní zobrazení $S/I \to S/I$.

Myslím si, že pro homogenní ideál I, nestačí podmínku ověřovat pouze pro homogenní prvky f, g. Nicméně můžeme nadefinovat primární homogenní ideál jako ten, který výše uvedenou podmínku splňuje pouze pro f, g homogenní. To nám bude v následujícím postačovat.

Lemma 21.3. *Každý ireducibilní 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

$$(I : g^n) = \{h \in S \mid hg^n \in I\}$$

které zjevně tvoří neklesající posloupnost

$$(I : g) \subseteq (I : g^2) \subseteq \cdots .$$

Díky Noetherovskosti S musí pro nějaké n platit $(I : g^{n+1}) = (I : g^n)$. Jelikož chceme ukázat, že buď $g^n \in I$ nebo $f \in I$ stačí nám díky ireducibilitě I dokázat, že $(I+(f)) \cap (I+(g^n)) = I$. Nechť tedy h leží v tomto průniku (a můžeme předpokládat, že je homogenní). Máme

$$hg \in I + (fg) = I,$$

tedy při rozkladu $h = k + lg^n$ musí být $lg^{n+1} \in I$, což znamená $l \in (I : g^{n+1}) = (I : g^n)$ a proto $lg^n \in I$ a konečně $h \in I$. $\square$

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 $g \in \sqrt{I}$. $\square$

V dalším nás nebude zajímat rozklad na průnik ireducibilních ideálů, ale primárních ideálů. Platí, že $I \cap J$ je primární, pokud $\sqrt{I} = \sqrt{J}$ (který je pak roven $\sqrt{I \cap J}$):

$$fg \in I \cap J \Leftrightarrow ((f \in I) \vee (g \in \sqrt{I})) \wedge ((f \in J) \vee (g \in \sqrt{J})) \Leftrightarrow (f \in (I \cap J)) \vee (g \in \sqrt{I \cap J})$$

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

$$V(I) = V(I_1 \cap \cdots \cap I_r) = V(I_1) \cup \cdots \cup V(I_r).$$

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 $I^{(d)} \subseteq S^{(d)}$ má pro $d \gg 0$ konstantní kodimenzi, která je rovna dimenzi "afinního souřadnicového okruhu".*

[2] Nebudeme to dokazovat, jen uvedeme základní myšlenkou. Tou je charakterizovat tyto prvoideály alternativním způsobem jako ty, které se vyskytují mezi ideály $(I : f)$, $f \in S$.

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 d nalevo a polynomy stupně nejvýše d napravo jím indukovaný izomorfismus

$$\varphi_d : \mathbb{K}^{(d)}[x_0, x_1, \ldots, x_n] \xrightarrow{\cong} \mathbb{K}^{(\leq d)}[x_1, \ldots, x_n].$$

Vezmeme nyní kvocient podle obrazů ideálu I a dostaneme izomorfismus

$$\mathbb{K}^{(d)}[x_0, x_1, \ldots, x_n]/I^{(d)} \xrightarrow{\cong} \mathbb{K}^{(\leq d)}[x_1, \ldots, x_n]/\varphi_d(I^{(d)}).$$

Ukážeme nyní, že pravá strana je izomorfní "souřadnicovému okruhu" $\mathbb{K}[x_1, \ldots, x_n]/\varphi(I)$ pro $d \gg 0$. Podle projektivní věty o nulách $\mathfrak{m}_P = \sqrt{I}$, tj. $(x_1, \ldots, x_n)^k = (\mathfrak{m}_P)^k \subseteq I$ a proto $(\mathfrak{m}_0)^k \subseteq \varphi(I)$. Díky tomu je každý prvek $\mathbb{K}[x_1, \ldots, x_n]/\varphi(I)$ reprezentován polynomem stupně menšího než k. Je-li tedy $d \geq k - 1$ je přirozené zobrazení

$$\mathbb{K}^{(\leq d)}[x_1, \ldots, x_n]/\varphi_d(I^{(d)}) \longrightarrow \mathbb{K}[x_1, \ldots, x_n]/\varphi(I)$$

surjektivní. Potřebujeme dále ukázat, že pro $d \gg 0$ je

$$\varphi(I) \cap \mathbb{K}^{(\leq d)}[x_1, \ldots, x_n] = \varphi_d(I^{(d)}).$$

Přitom ale $(\mathfrak{m}_0)^k \cap \mathbb{K}^{(\leq d)}[x_1, \ldots, x_n] \subseteq \varphi_d(I^{(d)})$ vždy. Jelikož je $\varphi(I)/(\mathfrak{m}_0)^k$ konečně rozměrný vektorový prostor generovaný řekněmě $\varphi(g_1) + (\mathfrak{m}_0)^k, \ldots, \varphi(g_r) + (\mathfrak{m}_0)^k$, bude pro libovolné $d \geq \max\{\deg g_1, \ldots, \deg g_r\}$ platit, že $\varphi(I)$ je generovaný

$$(\varphi(g_1), \ldots, \varphi(g_r)) + (\mathfrak{m}_0)^k \subseteq \varphi(I^{(d)}). \qquad \square$$

Definujeme Hilbertovu funkci homogenního ideálu $I \subseteq \mathbb{K}[x_0, \ldots, x_n]$ jako

$$h_I(d) = \dim \mathbb{K}^{(d)}[x_0, \ldots, x_n]/I^{(d)}.$$

V následujícím ukážeme, že pro $d \gg 0$ je $h_I(d)$ polynom nad $\mathbb{Q}$ (a to sice tzv. numerický, tj. jeho hodnoty jsou celočíselné). Zatím jsme to ukázali pro ideál, jehož asociovaná varieta má jediný bod. Rozšíření na libovolné konečné množiny vyžaduje rozklad ideálu na ireducibilní komponenty. Je-li $I = I_1 \cap \cdots \cap I_r$, kde $V(I_k) = \{P_k\}$, tvrdíme, že pro $d \gg 0$ platí

$$h_I(d) = h_{I_1}(d) + \cdots + h_{I_r}(d).$$

Předpokládejme, že $r = 2$, 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, přičemž $I_1 + I_2 = S$, alespoň pro $d \gg 0$, neboť $V(I_1 + I_2) = V(I_1) \cap V(I_2) = \emptyset$ a tedy $\overline{I_1 + I_2} = S$. Ve výsledku $h_{I_1 \cap I_2}(d) = h_{I_1}(d) + h_{I_2}(d)$ pro $d \gg 0$.

Pro nás bude primární rozklad 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 na primární potom dává následující kritérium. Je-li $(f + I) \in S/I$ dělitel nuly, pak existuje $g \in S$ tak, že $fg \in I = I_1 \cap \cdots \cap I_r$ a tedy za předpokladu, že f neleží v žádném $\sqrt{I_j}$ dostáváme $g \in I_j$ pro všechna j, tedy $g \in I$.

Lemma 21.7. *Jestliže f není nulový na žádné ireducibilní komponentě I, pak $f + I \in S/I$ je nedělitel nuly.*

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 všech ireducibilních komponentách 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

$$h_I(k) = h_J(k) + \cdots + h_J(0).$$

Protože $V(I + (f)) = V(I) \cap V(f)$, je tato dimenze 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

$$\begin{aligned} h_I(k) &= c_{d-1}\underbrace{\left(\tbinom{k}{d-1} + \cdots + \tbinom{k_0+1}{d-1}\right)}_{\binom{k+1}{d}-\mathrm{const}} + \cdots + c_0\left(\tbinom{k}{0} + \cdots + \tbinom{k_0+1}{0}\right) + h_I(k_0) \\ &= c_{d-1}\tbinom{k+1}{d} + \cdots + c_0\tbinom{k+1}{1} + \mathrm{const} = \widetilde{c}_d\tbinom{k}{d} + \cdots + \widetilde{c}_1\tbinom{k}{1} + \widetilde{c}_0\tbinom{k}{0}. \end{aligned}$$

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. □

Příklad 21.9. Spočítejme stupeň ideálu (f). V případě, že f nemá násobné činitele v rozkladu na součin ireducibilních polynomů, tedy počítáme stupeň $I(V(f))$, tedy nadplochy $V(f)$. Postupujme stejně jako v předchozím důkazu pro $I = 0$, $J = (f)$, máme tedy

$$h_0(k) = \dim \mathbb{K}^{(k)}[x_0, \ldots, x_n] = \tbinom{k+n}{n}.$$

Z exaktní posloupnosti analogické té z důkazu, kde ale tentokrát f navyšuje stupeň o $\deg f$, dostáváme pro $k \gg 0$ vztah

$$\begin{aligned} h_{(f)}(k) &= h_0(k) - h_0(k - \deg f) = \tbinom{k+n}{n} - \tbinom{k+n-\deg f}{n} \\ &= \Big(k^n/n! + (n + \cdots + 1) \cdot k^{n-1}/n! + \mathrm{lot}\Big) - \\ &\qquad - \Big(k^n/n! + \big((n - \deg f) + \cdots + (1 - \deg f)\big) \cdot k^{n-1}/n! + \mathrm{lot}\Big) \\ &= n \deg f \cdot k^{n-1}/n! + \mathrm{lot} \\ &= \deg f \cdot k^{n-1}/(n-1)! + \mathrm{lot}. \end{aligned}$$

Je tedy stupeň ideálu (f) roven stupni polynomu f.

Věta 21.10 (Bezoutova). *Nechť $I \subseteq S$ je libovolný homogenní ideál a nechť $f \in S$ je homogenní polynom. Potom platí*

$$\deg(I + (f)) = \deg I \cdot \deg f$$

Důkaz. Využijeme exaktní posloupnost z důkazu předchozí věty, opět s posunem o $\deg f$. Označíme $J = I + (f)$ a dostáváme

$$\begin{aligned}
h_J(k) &= h_I(k) - h_I(k - \deg f) \\
&= \left(c_d k^d + c_{d-1} k^{d-1} + \mathrm{lot}\right) - \Big(\underbrace{c_d (k - \deg f)^d}_{c_d \cdot k^d - c_d d \deg f \cdot k^{d-1} + \mathrm{lot}} + \underbrace{c_{d-1}(k - \deg f)^{d-1}}_{c_{d-1} \cdot k^{d-1} + \mathrm{lot}} + \mathrm{lot}\Big) \\
&= c_d d \deg f \cdot k^{d-1} + \mathrm{lot} \\
&= \deg I / d! \cdot d \deg f \cdot k^{d-1} + \mathrm{lot} \\
&= \deg I \cdot \deg f \cdot k^{d-1}/(d-1)! + \mathrm{lot}
\end{aligned}$$

□

V případě, že je f lineární, je jeho stupeň 1 a je tedy počet průsečíků X s $V(f)$ roven stupni $\deg X$.

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. neexistuje $\operatorname{codim} X$ homogenních polynomů, které by generovaly $I(X)$. V našem případě je kodimenze dva a chceme tedy ukázat, že $I(X)$ není generovaný dvěma homogenními polynomy. Pokud by to byla pravda, musel by součin jejich stupňů být roven stupni X. Ten se jednoduše spočítá, že je tři. Ukážeme prvně, že $I(X)$ je roven ideálu

$$I = (x_0x_2 - x_1^2, x_0x_3 - x_1x_2, x_1x_3 - x_2^2).$$

Jako bázi $S^{(d)}/I(X)^{(d)}$ lze totiž zvolit jisté třídy monomů. Snadno se pak lze přesvědčit, že relace

$$x_0x_2 \sim x_1^2, \quad x_0x_3 \sim x_1x_2, \quad x_1x_3 \sim x_2^2$$

zachovávají součet indexů a naopak každá dvojice monomů se stejným součtem indexů je ekvivalentní. Je proto $h_I(k) = 3k+1$ a $\deg I = 3$. Jelikož $X = V(I)$ je jedinou komponentou I dimenze 1, musí být $\deg X = \deg I(X)$ nějaký dělitel 3, přičemž stupeň 1 má pouze projektivní podprostor a X není přímka.

Podle Bezoutovy věty by za předpokladu $I(X) = (f, g)$ musely mít polynomy f, g stupně 1 a 3, což by ale znamenalo, že X leží v rovině. Jednoduše se lze přesvědčit, že tomu tak není. 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, o kterém budeme uvažovat afinně. 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 $d = \dim V(I_1) = \dim V(I_2) > \dim V(I_1) \cap V(I_2)$ (nebo $V(I_1) \cap V(I_2) = \emptyset$). Potom platí* $\deg I = \deg I_1 + \deg I_2$.

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. Podle Hilbertovy věty o nulách platí $\sqrt{I_P} = \mathfrak{m}_P$ a tedy $(\mathfrak{m}_P)^k \subseteq I_P$ pro nějaké $k \gg 0$. Potom

$$I + (\mathfrak{m}_P)^k \subseteq I_P.$$

Pro druhou inkluzi si uvědomme, že

$$V\Big(\bigcap_{I_j \neq I_P} I_j + (\mathfrak{m}_P)^k\Big) = V\Big(\bigcap_{I_j \neq I_P} I_j\Big) \cap V((\mathfrak{m}_P)^k) = \emptyset$$

a podle Hilbertovy věty o nulách pak $\bigcap_{I_j \neq I_P} I_j + (\mathfrak{m}_P)^k = R$. Je-li $f \in I_P$, můžeme tedy psát $f = g + h$, kde $g \in \bigcap_{I_j \neq I_P} I_j$ a $h \in (\mathfrak{m}_P)^k$. Proto také $g = f - h \in I_P + (\mathfrak{m}_P)^k = I_P$ a dohromady $g \in I$. Proto platí také

$$I_P \subseteq I + (\mathfrak{m}_P)^k.$$

□

Poznamenejme, že jakmile $I + (\mathfrak{m}_P)^k = I + (\mathfrak{m}_P)^{k+1}$, je již tato společná hodnota rovna I_P. Toho lze využít pro výpočet I_P – postupně počítat $I, I + \mathfrak{m}_P, I + (\mathfrak{m}_P)^2, \ldots$ 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

$$I_P/(\mathfrak{m}_P)^k \subseteq R/(\mathfrak{m}_P)^k$$

většinou relativně snadno. Tato kodimenze je rovna dimenzi kvocientu R/I_P, tedy $\deg I_P$.

Řekneme, že dvě variety $X, Y \subseteq \mathbb{P}^n$ komplementární dimenze (tj. $\dim X + \dim Y = n$) se v bodě $P \in X \cap Y$ protínají transverzálně, jestliže $T_P X + T_P Y = T_P \mathbb{P}^n$.

Tvrzení 21.15. *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*

$$\deg(I(X) + I(Y))_P \geq n + 1 - \dim(T_P X + T_P Y).$$

Důkaz. Počítejme afinně s $P = 0$. Potom $I(X)$ obsahuje polynomy tvaru $f^{(1)} + \text{hot}$, kde $f^{(1)}$ je nulové na $T_0 X$ a podobně pro $I(Y)$. Pokud je tedy průnik transverzální, máme

$$x_1 + \text{hot}, \dots, x_n + \text{hot} \in I(X) + I(Y).$$

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 $T_P X + T_P Y$. Kodimenze tohoto ideálu je proto rovna té z tvrzení (jednička odpovídá absolutnímu členu). Kodimenze $(I(X) + I(Y))_P = I(X) + I(Y) + (\mathfrak{m}_0)^k$ 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 21.16. *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.

Věta 21.17 (Noetherovská normalizace)**.** *Je-li A konečně generovaná algebra nad $\mathbb{K}$, potom existuje polynomiální podalgebra $\mathbb{K}[x_1, \ldots, x_r] \subseteq A$ taková, že A je jejím konečným (integrálním) rozšířením. Ekvivalentně platí následující. Nechť X je afinní varieta. Potom existuje konečná projekce.*

Důkaz. Dokážeme geometrickou verzi. Uvažme projektivní rozšíření. Jednoduše lze ukázat, že v případě, že $X \subseteq \mathbb{A}^n$ je vlastní podvarieta, pak $\overline{X} \smallsetminus X \subseteq \mathbb{P}^n \smallsetminus \mathbb{A}^n \cong \mathbb{P}(\operatorname{dir} \mathbb{A}^n)$ je také vlastní (projektivní podvarieta). Zvolme libovolný směr $\ell \in \mathbb{P}(\operatorname{dir} \mathbb{A}^n)$ neležící v $\overline{X}$. Potom projekce ve směru ℓ je afinní zobrazení $\mathbb{A}^n \to \mathbb{A}^n/\ell$, jehož zúžení na X je konečné zobrazení $X \to Y$. Po konečném počtu kroků dospějeme ke konečnému zobrazení $X \to \mathbb{A}^d$, které indukuje kýžený injektivní homomorfismus algeber.

Nechť nyní $f \in \mathbb{K}[X]$ a reprezentujme jej pomocí homogenního polynomu stupně d na $\mathbb{K}^{n+1}$, který není nulový na bodu projekce $\ell = (0 : \cdots : 0 : 1)$. To znamená, že jeho koeficient u x_n^d je nenulový, řekněme, že je roven 1. To ale znamená, že $\mathbb{K}[X] = \mathbb{K}[Y][x_n]$ je generované prvkem x_n, který splňuje integrální polynom

$$f \in \mathbb{K}[x_0, \ldots, x_n] \cong \mathbb{K}[x_0, \ldots, x_{n-1}][t] \longrightarrow \mathbb{K}[Y][t].$$

Zbývá ukázat základní vlastnosti integrálních rozšíření: je-li B konečně generovaná nad A, pak je integrální, právě když je konečná a z toho plynoucí uzavřenost na kompozice. Základní ingredience je Cayleyho-Hamiltonova věta. □

** 22. Lokální parametry

Definice 22.1. Nechť X je kvaziprojektivní varieta dimenze d a $P \in X$ nesingulární bod. Řekneme, že $u_1, \ldots, u_d \in \mathcal{O}_P$ jsou *lokální parametry* v bodě P, jestliže $u_i \in \mathfrak{m}_P$ a tvoří bázi $\mathfrak{m}_P/\mathfrak{m}_P^2 = T_P^* X$.

Příklad 22.2. Na $\mathbb{A}^n$ jsou lokálními parametry v bodě P například $x_1 - p_1, \ldots, x_n - p_n$.

Lze zvolit okolí bodu P, na kterém jsou všechna u_i regulární.

Věta 22.3. *Nechť $u_1, \ldots, u_d$ jsou lokální parametry v bodě P takové, že jsou regulární na X a nechť $X_i = V(u_i)$. Potom X_i se protínají transverzálně v bodě P a zejména je P ireducibilní komponentou $X_1 \cap \cdots \cap X_d$.*

Důkaz. Podmínka je ekvivalentní tomu, že $\mathrm{d}u_1(P), \ldots, \mathrm{d}u_d(P)$ jsou lineárně nezávislé prvky $T_P^* X$. Jelikož je $u_i \in I(X_i)$, je $T_P X_i \subseteq \ker \mathrm{d}u_i(P)$. Zároveň má však X_i dimenzi alespoň $d-1$, takže musí nastat rovnost. Průnik $X_1 \cap \cdots \cap X_d$ má pak v bodě P dimenzi 0 a jedná se tedy o celou ireducibilní komponentu. □

Podle předchozí věty lze tedy volit okolí bodu P takové, že $X_i = V(u_i)$ se protínají v jediném bodě P a to navíc transverzálně.

Věta 22.4. *Lokální parametry v bodě P generují ideál $\mathfrak{m}_P \subseteq \mathcal{O}_P$.*

Důkaz. To plyne jednoduše z Nakayamova lemmatu ($N\mathfrak{m}_P = N$, N konečně generovaný $\Rightarrow N = 0$) – okruh $\mathcal{O}_P$ je Noetherovský a tedy $\mathfrak{m}_P$ je konečně generovaný; přitom $N = \mathfrak{m}_P/(u_1, \dots, u_d)$ splňuje $N\mathfrak{m}_P = N$ (tj. $\mathfrak{m}_P^2 \equiv \mathfrak{m}_P$ modulo $(u_1, \dots, u_d)$). □

Definice 22.5. Řekneme, že formální mocninná řada $\Phi = \sum_{i=0}^{\infty} F_i$ je *Taylorova řada* funkce $f \in \mathcal{O}_P$, jestliže pro každé $k \geq 0$ platí

$$f - \sum_{i=0}^{k} F_i(u_1, \dots, u_d) \in \mathfrak{m}_P^{k+1}.$$

Tato definice samozřejmě závisí na volbě lokálních parametrů.

Věta 22.6. *Nechť $u_1, \dots, u_d$ jsou lokální parametry v nesingulárním bodě $P \in X$. Potom každá funkce $f \in \mathcal{O}_P$ má jedinou Taylorovu řadu Φ. Přiřazení $f \mapsto \Phi$ je injektivní homomorfismus $\mathcal{O}_P \to \Bbbk[\![x_1, \dots, x_d]\!]$.*

Důkaz. Existence je relativně jednoduchá. Stačí induktivně zkonstruovat součet $F_0 + \cdots + F_k$. Podle předpokladu $f - (F_0 + \cdots + F_k)(u_1, \dots, u_d) \in \mathfrak{m}_P^{k+1}$, takže v $\mathfrak{m}_P^{k+1}$ existuje vyjádření tvaru

$$f - (F_0 + \cdots + F_k)(u_1, \dots, u_d) = \sum_{|\alpha|=k+1} g_\alpha u^\alpha,$$

kde $g_\alpha \in \mathcal{O}_P$. Pišme $g_\alpha = g_\alpha(P) + h_\alpha$, pak platí $h_\alpha \in \mathfrak{m}_P$, takže platí

$$f - (F_0 + \cdots + F_k)(u_1, \dots, u_d) \equiv \sum_{|\alpha|=k+1} g_\alpha(P) u^\alpha. \qquad (\operatorname{mod} \mathfrak{m}_P^{k+2})$$

Stačí tedy položit $F_{k+1} = \sum g_\alpha(P) x^\alpha$.

Pro jednoznačnost stačí ukázat, že každá Taylorova řada nulové funkce je nulová. Nechť tedy $\Phi = \sum F_i$ je Taylorova řada nulové funkce, podle indukčního předpokladu již víme, že má nulovou část do dimenze k, tedy

$$F_{k+1}(u_1, \dots, u_d) \in \mathfrak{m}_P^{k+2}.$$

Pokud budeme sporem předpokládat, že $F_{k+1} \neq 0$, můžeme vhodnou lineární změnou souřadnic docílit toho, že F_{k+1} má koeficient u x_d^{k+1} rovný jedné, tj. $F_{k+1} = x_d^{k+1} + x_d^k G_1 + \cdots + G_{k+1}$, kde $G_i \in \Bbbk_i[x_1, \dots, x_{d-1}]$. Po dosazení $u_1, \dots, u_d$ dostaneme

$$F_{k+1}(u_1, \dots, u_d) = u_d^{k+1} + u_d^k G_1(u_1, \dots, u_{d-1}) + \cdots + G_{k+1}(u_1, \dots, u_{d-1}).$$

Zároveň však tento výraz leží v $\mathfrak{m}_P^{k+2}$ a lze jej tedy vyjádřit jako

$$F_{k+1}(u_1, \dots, u_d) \in g u_d^{k+2} + (u_1, \dots u_{d-1})\mathfrak{m}_P^{k+1},$$

kde $g \in \mathcal{O}_P$. Odečtením pak $(1 - g u_d) u_d^{k+1} \in (u_1, \dots, u_{d-1})$. Přitom $1 - g u_d \in \mathcal{O}_P$ je jednotka, takže také $u_d^{k+1} \in (u_1, \dots, u_{d-1})$. Zejména

$$V(u_1, \dots, u_{d-1}) \subseteq V(u_d),$$

což je spor s transverzalitou.

Jelikož je přiřazení $f \mapsto \Phi$ zřejmě homomorfismus okruhů, stačí se zabývat jeho jádrem, tj. funkcí $f \in \mathcal{O}_P$ s nulovou Taylorovou řadu, tj. $f \in \bigcap_{k \geq 0} \mathfrak{m}_P^k = I$. Protože je I konečně generovaný a platí $I\mathfrak{m}_P = I$, podle Nakayamova lemmatu je $I = 0$. □

Věta 22.7. *Ireducibilní podvarieta $Y \subseteq X$ kodimenze 1 má v okolí každého nesingulárního bodu $P \in X$ lokální rovnici $f \in \mathcal{O}_P$, tj. existuje okolí $U \ni P$ takové, že f je regulární na U, a že $(f) \subseteq \mathcal{O}(U)$ je přesně ideál funkcí nulových na $U \cap Y$.*

Tato věta plyne z následující věty.

? ***Poznámka.*** **Doplnit důkaz.**

Věta 22.8. *Lokální okruh $\mathcal{O}_P$ nesingulárního bodu $P \in X$ je obor s jednoznačným rozkladem.*

Tato věta plyne ze stejné vlastnosti pro $\Bbbk[\![x_1, \dots, x_d]\!]$ a algebraického lemmatu o podokruzích UFD.

? ***Poznámka.*** **Doplnit důkaz.**

Věta 22.9. *Nechť $f \colon X \to \mathbb{P}^m$ je racionální zobrazení z nesingulární kvaziprojektivní variety. Potom množina bodů, kde f není definovaná, má kodimenzi alespoň 2.*

Důkaz. V okolí $U \ni P$ pišme $f = (f_0 : \cdots : f_m)$, přičemž můžeme předpokládat, že $f_0, \dots, f_m$ jsou regulární na U a jako prvky $\mathcal{O}_P$ nemají společný faktor (využíváme, že $\mathcal{O}_P$ je UFD). Pokud by $V(f_0, \dots, f_m)$ obsahovalo nějakou ireducibilní komponentu kodimenze 1, pak lokálně $V(f_0, \dots, f_m) \supseteq V(g)$ a tedy $g \mid f_i$, spor. □

Důsledek 22.10. *Racionální zobrazení z nesingulární křivky do projektivního prostoru je regulární.*

Důsledek 22.11. *Biracionální ekvivalence mezi nesingulárními křivkami je izomorfismus.*

$**$ **Věta 22.12.** *Nechť $Y \subseteq X$ je podvarieta a $P \in Y$ je nesingulární bod obou X, Y. Potom lze zvolit lokální parametry $u_1, \dots, u_n$ na X v bodě P tak, že v nějakém okolí $U \ni P$ je $(u_1, \dots, u_m)$ přesně ideál funkcí nulových na $U \cap Y$; navíc $u_{m+1}, \dots, u_n$ jsou lokální parametry na Y v bodě P.*

? ***Poznámka.*** **Doplnit důkaz.**

? ***Poznámka.*** **Zajímavé cvičení: Nechť pro hladkou ireducibilní afinní varietu $V = V(F_1, \dots, F_r)$ kodimenze r jsou diferenciály $\mathrm{d}F_1(P), \dots, \mathrm{d}F_r(P)$ lineárně nezávislé v každém bodě $P \in V$. Dokažte, že $I(V) = (F_1, \dots, F_r)$. Aplikujte na Plückerovy relace pro Grassmannovu varietu.**

? ***Poznámka.*** **Normalizace křivek = odstranění singularit. Vložení hladkých d-rozměrných projektivních variet do $\mathbb{P}^{2d+1}$. Větvení, počet vzorů $f^{-1}(y)$ konečného zobrazení do *normální* variety je roven stupni rozšíření (ještě je potřeba nějaká separabilnost rozšíření); vztah k nakrytím. Divizory na hladkých varietách, zejména křivkách, Bezoutova věta, průsečíková čísla.**