Úvod do algebraické geometrie

Typeset by $\mathcal{AMS}$-TEX

1. Přehled lineární a komutativní algebry

Definice 1.1. Buď $R \equiv (R, +, \cdot, 0, 1)$ netriviální komutativní okruh s jednotkou. Prvek $r \in R$ se nazývá *dělitel (divisor) nuly*, pokud existuje $0 \neq r' \in R$ tak, že $r \cdot r' = 0$. ($r = 0$ je vždy dělitelem nuly.)

Pokud okruh R neobsahuje dělitele nuly, nazýváme ho *oborem integrity*.

Příklad 1.2. Každý nilpotentní prvek, tj. prvek $r \in R$ takový, že $(\exists n \in \mathbb{N})\ r^n = 0$, je dělitelem nuly.

Definice 1.3. Nechť $r, s \in R$, $r \neq 0 \neq s$. Řekneme, že r je dělitel s (píšeme $r|s$), pokud $(\exists r' \in R)\ r \cdot r' = s$.

Prvek $r \in R$ je *invertibilní element (jednotka)*, pokud $(\exists s \in R)\ r \cdot s = 1$. Množinu (podokruh) všech jednotek okruhu R značíme R^*.

Příklad 1.4. Pro okruh $R = \mathbb{Z}$ je $R^* = \{1, -1\}$.

Definice 1.5. Dva prvky r, $s \in R$ jsou *asociované*, pokud $(\exists s' \in R^*)\ r = s' \cdot s$. Dělitel prvku $r \in R$, $r \neq 0$, který je asociován s prvkem r, se nazývá *nevlastní dělitel* prvku r.

Prvek $r \in R$, $r \neq 0$, který má pouze nevlastní dělitele a sám není invertibilní (tj. $r \notin R^*$), nazýváme *prvočinitelem* (*nerozložitelným, irreducibilním prvkem*).

Definice 1.6. R je *okruh s jednoznačným rozkladem* (*UFD, unique factorization domain*), pokud

- R je obor integrity,
- $(\forall r \in R)\ 0 \neq r \notin R^* \Rightarrow (\exists m \in \mathbb{N})$ ($\exists$ prvočinitelé $r_1, \ldots, r_m$) $r = r_1 \cdot \ldots \cdot r_m$,
- rozklad z předchozího bodu je určen jednoznačně, tj. pokud $r = r_1 \cdot \ldots \cdot r_m = s_1 \cdot \ldots \cdot s_n$, pak $m = n$ a $(\exists \pi \in S_m)$ tak, že r_i je asociován s $s_{\pi(i)}$ $(\forall i \leq m)$.

Příklad 1.7. Každé těleso je okruhem s jednoznačným rozkladem na prvočinitele.

Definice 1.8. Nechť jsou R, S netriviální komutativní okruhy s jednotkami. Zobrazení $\rho : R \to S$ je *homomorfismus* (píšeme $\rho \in \mathrm{Hom}(R, S)$), pokud

- $(\forall r_1, r_2 \in R)\ \rho(r_1 + r_2) = \rho(r_1) + \rho(r_2)$,
- $(\forall r_1, r_2 \in R)\ \rho(r_1 \cdot r_2) = \rho(r_1) \cdot \rho(r_2)$,
- $\rho(1_R) = 1_S$.

Řekneme, že R je *A-algebra*, je-li na ní definováno zobrazení $\rho_R \in \mathrm{Hom}(A, \mathrm{End}(R))$, kde $(\forall r \in R,\ \forall a \in A)$

$$a \mapsto (r \mapsto \rho_R(a)(r)),$$
$$a \cdot r := \rho_R(a)(r),$$

a navíc $(\forall a \in A,\ \forall r_1, r_2 \in R)\ a \cdot (r_1 r_2) = (a \cdot r_1) r_2 = r_1 (a \cdot r_2)$.

Tedy, z definic, platí $(\forall a, a_1, a_2 \in A,\ \forall r, r_1, r_2 \in R)$:

$$a \cdot (r_1 + r_2) = a \cdot r_1 + a \cdot r_2,$$
$$(a_1 + a_2) \cdot r = a_1 \cdot r + a_2 \cdot r,$$
$$(a_1 a_2) \cdot r = a_1 \cdot (a_2 \cdot r).$$

Zobrazení $\varphi : R \to S$, kde R, S jsou A-algebry, je *homomorfismem A-algeber*, je-li diagram

$$\begin{tikzcd} & A \arrow[dl, "\rho_R"'] \arrow[dr, "\rho_S"] & \\ R \arrow[rr, "\varphi"] & & S \end{tikzcd}$$

komutativní $\big($tj. $(\forall a \in A)\ (\forall r \in R)\ \varphi(\rho_R(a) \cdot r) = \rho_S(a) \cdot \varphi(r)\big)$. Množinu všech homomorfismů A-algeber R a S označíme $\mathrm{Hom}_A(R, S)$.

Podokruh R' A-algebry R nazveme *A-podalgebrou*, jestliže

$$(\forall a \in A)\ (\forall r \in R')\ a \cdot r \in R',$$

přičemž podokruh R' A-algebry R nemusí být A-podalgebrou!

Definice 1.9. $I \subset R$, $I \neq \emptyset$, je *ideálem*, pokud

- $r_1, r_2 \in I \Rightarrow r_1 + r_2 \in I$,
- $r \in R$, $r' \in I \Rightarrow r \cdot r' \in I$.

Příklad 1.10. $R = \mathbb{Z}$, $I = \langle 14 \rangle$, tj. $r \in I \Leftrightarrow (\exists a \in \mathbb{Z})\ r = 14a$.

Pro A-algebru R a ideál v ní je vše obsaženo v druhém bodu předchozí definice (podmnožina I A-algebry je ideálem, právě když je ideálem v okruhu R bez struktury A-algebry). Můžeme se tedy omezit na ideály v okruzích.

Ideál $I \subset R$ se nazývá *vlastním ideálem*, pokud $I \neq R$. I je *maximálním ideálem*, pokud neexistuje vlastní ideál $I' \subset R$ takový, že $I \subsetneq I'$.

Příklad 1.11. $R = \mathbb{Z}$, $I = \langle 14 \rangle$ není maximální ideál, $I' = \langle 2 \rangle \neq \mathbb{Z}$ a přitom $I \subsetneq I'$.

Z Zornova lemmatu plyne, že každý ideál v okruhu R je obsažen v nějakém maximálním ideálu. (Alespoň v jednom: např. $\langle 14 \rangle \subset \langle 2 \rangle$ a $\langle 14 \rangle \subset \langle 7 \rangle$.)

Je-li $\{I_\alpha\}_{\alpha \in M}$ systém ideálů, pak $\bigcap_{\alpha \in M} I_\alpha$ je ideálem (průnik zde uvažujeme v množinovém smyslu). Je-li M podmnožina okruhu R, pak *ideálem generovaným* M nazveme ideál okruhu R, který je průnikem všech ideálů obsahujících množinu M. Značíme jej $\langle M \rangle$, resp. $\langle r_1, \ldots, r_k \rangle$, pokud je M generovaná prvky $r_1, \ldots, r_k$.

Každý prvek $r \in \langle r_1, \ldots, r_k \rangle$ lze vyjádřit ve tvaru $r = \sum_{i=1}^{k} s_i r_i$, kde $s_i \in R$ $(\forall i)$.

Ideál I je *konečně generovaný*, pokud existují $k \in \mathbb{N}$, $r_1, \ldots, r_k \in R$ tak, že $I = \langle r_1, \ldots, r_k \rangle$. Ideál I se nazývá *hlavní ideál*, pokud $(\exists r \in R)\ I = \langle r \rangle$.

Příklad 1.12. Nulový ideál $\{0\} = \langle 0 \rangle$ a celý okruh $R = \langle 1 \rangle$ jsou hlavní ideály.

Okruh, jehož každý ideál je konečně generovaný, se nazývá *noetherovský*. Okruh, jehož každý ideál je hlavní, se nazývá *okruh hlavních ideálů* (pokud je navíc oborem integrity, jedná se o *obor integrity hlavních ideálů* (*PID, principial ideal domain*)).

Zřejmě je každý okruh hlavních ideálů noetherovský.

Ideál I v okruhu R se nazývá *prvoideál*, pokud

$$r_1 \notin I,\ r_2 \notin I \Rightarrow r_1 \cdot r_2 \notin I,$$

tj. pokud pro $r_1 \cdot r_2 \in I$ je buď $r_1 \in I$ nebo $r_2 \in I$.

Věta 1.13. *Každý maximální ideál je prvoideál.*

Věta 1.14. *Nechť R je okruh s jednoznačným rozkladem na prvočinitele. Pak hlavní ideál $\langle i \rangle$ je prvoideálem, právě když prvek $i \in R$ je buď invertibilní nebo je prvočinitelem.*

Buď I ideál v okruhu R. Definujeme

$$\sqrt{I} := \{r \in R;\ (\exists n \in \mathbb{N})\ r^n \in I\}.$$

Podmnožina $\sqrt{I}$ je ideál nazývající se *radikál ideálu* I.

Radikál nulového ideálu $\{0\}$ (tj. množina všech nilpotentních prvků v R) se nazývá *nilradikál* okruhu R.

I je *radikálový ideál*, právě když $\sqrt{I} = I$. Každý prvoideál je zřejmě radikálovým ideálem. Radikál libovolného ideálu je radikálovým ideálem.

Věta 1.15. *Buď R libovolný okruh a buď $I \subset R$ libovolný ideál. Průnik všech prvoideálů okruhu R obsahujících ideál I je roven radikálu ideálu I, tj.*

$$\sqrt{I} = \bigcap \{I';\ I \subset I' \ \ \&\ \ I' \text{je prvoideál}\}.$$

Speciálně je průnik všech prvoideálů roven nilradikálu okruhu R.

Věta 1.16. *Buď R noetherovský okruh a buď $I \subset R$ radikálový ideál. Pak existuje $k \in \mathbb{N}$ a prvoideály $I_1, \dots, I_k$ tak, že*

- *$I = I_1 \cap \dots \cap I_k$,*
- *pro žádné dva indexy i, j, $1 \leq i, j \leq k$, neplatí $I_i \subset I_j$.*

Příslušné prvoideály $I_1, \dots, I_k$ jsou určeny jednoznačně (až na permutaci).

Operace na ideálech.

Buď $\{I_\gamma\}_{\gamma \in A}$ systém ideálů v okruhu R. Množina všech konečných součtů $r_1 + \dots + r_k$, $r_i \in I_i$ pro $1 \leq i \leq k$, je tzv. *součtem ideálů* systému $\{I_\gamma\}_{\gamma\in A}$ a značí se $\sum_{\gamma \in A} I_\gamma$. Tato množina je opět ideálem.

Pokud $\sharp A = n < \infty$, označujeme součet symbolem $I_1 + \dots + I_n$.

Součinem ideálů I_1, I_2 okruhu R se nazývá ideál generovaný množinou $\{r_1 \cdot r_2;\ r_1 \in I_1,\ r_2 \in I_2\}$, značíme jej $I_1 \cdot I_2$.

Je-li $I \subset R$ ideál, definujeme $I^1 := I$ a indukcí $I^n := I \cdot I^{n-1}$ pro $n \geq 2$. I^n se nazývá *n-tá mocnina ideálu I*.

Příklad 1.17. $R := \mathbb{Z}$.

$$\begin{aligned}
\langle m \rangle + \langle n \rangle &= \langle m, n \rangle = \langle \gcd(m, n) \rangle, \\
\langle m \rangle \langle n \rangle &= \langle mn \rangle, \\
\langle m \rangle \supset \langle n \rangle &\Leftrightarrow m | n.
\end{aligned}$$

Buď R okruh, $I \subset R$ ideál. Na R definujme relaci ekvivalence $\sim$:

$$r_1 \sim r_2 \Leftrightarrow r_1 - r_2 \in I$$

a označme R/I množinu tříd této ekvivalence. Pro r_1, $r_2 \in R$ označme $[r_1]$, $[r_2]$ příslušné třídy v R/I (tj. $r_1 \in [r_1] \in R/I$, podobně r_2). Nezávisle na výběru reprezentantů můžeme definovat

$$\begin{aligned}
[r_1] + [r_2] &= [r_1 + r_2], \\
[r_1] \cdot [r_2] &= [r_1 \cdot r_2],
\end{aligned}$$

tedy R/I je okruh, tzv. *faktorokruh* okruhu R podle I. Máme přirozenou projekci

$$\begin{aligned}
&R \to R/I, \\
&r \mapsto r + I = [r].
\end{aligned}$$

Věta 1.18. *Buď R okruh, $I \subset R$ ideál.*

- *Faktorokruh R/I je oborem integrity, právě když I je prvoideál.*
- *R/I je tělesem, právě když I je maximální ideál.*

Důkaz druhé části.
$\Leftarrow$: Předpokládejme, že I je maximální ideál. Nechť $x \in R \setminus I$. Pak ideál $I + \langle x \rangle$ je roven R. Tedy existují $u \in I$, $y \in R$ tak, že $1_R = u + xy$. Odtud $[x][y] = 1_{R/I}$, neboli $[x]$ je invertibilní v R/I. Protože x bylo voleno libovolně, dokázali jsme, že R/I je těleso (v němž $0_{R/I} = [I]$, $1_{R/I} = [1]$).
$\Rightarrow$: Předpokládejme, že R/I je těleso, $J \supsetneq I$ ideál. Zvolme $x \in J \setminus I$. Protože $[x]$ je invertibilní v R/I, existují $y \in R$, $u \in I$ tak, že $xy = 1_R + u$. Máme $1_R = xy - u \in J$, tj. $J = R$ a I je maximální ideál. $\square$

Důsledek 1.19. *Každý maximální ideál je prvoideál.*

Věta 1.20. *Je-li R noetherovský okruh a $I \subset R$ ideál, pak R/I je rovněž noetherovský okruh.*

Mějme R-algebry A, B. $A \otimes_R B$ má strukturu R-modulu (a také R-algebry): pro $r \in R$, a, $c \in A$, b, $d \in B$ je

$$r \cdot (a \otimes b) = ra \otimes b = a \otimes rb,$$
$$(a \otimes b) \cdot (c \otimes d) = (ac \otimes bd).$$

Nechť $I_A \subset A$, $I_B \subset B$ jsou ideály, $\pi_A : A \to A/I_A$, $\pi_B : B \to B/I_B$ přirozené projekce. Pak $I_A \otimes_R B$ a $A \otimes_R I_B$ jsou ideály v R-modulu $A \otimes_R B$.

Věta 1.21. *Jádro homomorfismu R-modulů $\pi_1 \otimes_R \pi_2 : A \otimes_R B \to A/I_A \otimes_R B/I_B$ je*

$$\operatorname{Ker}(\pi_1 \otimes_R \pi_2) \cong I_A \otimes_R B + A \otimes_R I_B$$

jakožto R-modul v $A \otimes_R B$.

2. Gradované okruhy a homogenní ideály

Nechť R je A-algebra. Nechť $R_0, R_1, R_2, \dots \subset R$ jsou A-podmoduly takové, že pro každé $r \in R$ existuje jediná posloupnost $(r_0, r_1, \dots)$ taková, že

$$r_i \in R_i \;\;\&\;\; \{i;\; r_i \neq 0\} \text{ je konečná } \;\;\&\;\; r = \sum_{i=0}^{\infty} r_i.$$

Předpokládejme, že pro libovolná $i, j \in \mathbb{N}$ a pro libovolné prvky $r \in R_i$, $r' \in R_j$ je $r \cdot r' \in R_{i+j}$. Pak R má strukturu $\mathbb{Z}$-gradované A-algebry. Pokud $A = \mathbb{Z}$, jedná se o $\mathbb{Z}$-gradovaný okruh. Pak $R = \bigoplus_{i=0}^{\infty} R_i$ přičemž prvky patřící do R_i nazýváme *i-homogenní*.

Pro $r = \sum_{i=1}^{\infty} r_i$, se r_i nazývá *i-tá homogenní komponenta* prvku $r \in R$.

Věta 2.1. *Buď R gradovaný okruh, který je jako obyčejný okruh UFD. Pokud $r \in R$ je homogenní prvek a $r = r_1 \cdot \ldots \cdot r_n$ rozklad na prvočinitele, jsou všechny prvky r_i, $i = 1, \dots, n$, homogenní.*

Definice 2.2. $I \subset R$, kde R je gradovaný okruh, je *homogenní ideál*, má-li vlastnost:

$$\text{pro } r \in I, \text{ kde } r = \sum_{i=0}^{\infty} r_i \text{ je rozklad na homogenní komponenty, platí } r_i \in I \; (\forall i).$$

Věta 2.3. *Buď $I \subset R$ homogenní ideál. Pokud I je konečně generovaný, pak existuje konečný počet homogenních prvků $r_1, \dots, r_k \in R$ tak, že $I = \langle r_1, \dots, r_k \rangle$. Je-li homogenní ideál I hlavním ideálem, existuje homogenní $r \in R$ tak, že $I = \langle r \rangle$.*

Věta 2.4. *Buď I homogenní ideál v gradovaném okruhu R. I je prvoideál, právě když*

$$(\forall r, r' \in R)\; (r, r' \text{ homogenní } \;\&\; r \notin I \;\&\; r' \notin I) \Rightarrow r \cdot r' \notin I.$$

Věta 2.5. *Buď R gradovaný okruh.*
(1) Je-li $I \subset R$ homogenní ideál, je $\sqrt{I}$ také homogenní ideál.
(2) Je-li $\{I_\gamma\}_{\gamma \in \Gamma}$ systém homogenních ideálů v R, pak $\bigcap_{\gamma \in \Gamma} I_\gamma$, $\sum_{\gamma \in \Gamma} I_\gamma$ jsou také homogenní ideály.
(3) Jsou-li I_1, I_2 homogenní ideály, pak $I_1 I_2$ je homogenní ideál.

Věta 2.6. *Buď R gradovaný okruh a $I \subset R$ ideál. Průnik všech homogenních prvoideálů okruhu R obsahujících I je roven $\sqrt{I}$.*

Nechť pro $R = \bigoplus_{i=0}^{\infty} R_i$ je $I \subset R$ homogenní ideál. Nechť $\widetilde{R_i}$ je obraz homogenní komponenty R_i při epimorfismu $\pi : R \to R/I$. Tedy na R/I máme strukturu gradovaného okruhu (prvek $\alpha \in R/I$ je homogenní stupně i, právě když existuje $r \in R$ tak, že $\pi(r) = \alpha$ a r je stupně i).

3. Lokální okruhy a podílové okruhy

Definice 3.1. R se nazývá *lokální okruh*, pokud v něm existuje právě jeden maximální ideál. Označme tento ideál I_R.

I_R obsahuje právě všechny neinvertibilní prvky okruhu R.

Definice 3.2. Homomorfismus $\rho : R \to S$ lokálního okruhu R do lokálního okruhu S se nazývá *lokální homomorfismus*, pokud $\rho^{-1}[I_S] = I_R$.

Definice 3.3. Neprázdná podmnožina $D \subset R$ se nazývá *multiplikativní množinou*, pokud

- $(d_1 \in D \;\; \& \;\; d_2 \in D) \Rightarrow d_1 \cdot d_2 \in D$,
- $1_R \in D$.

Buď $D \subset R$ multiplikativní množina. Definujme relaci ekvivalence $\sim$ na $D \times R$:

$$(d, r) \sim (d', r') \Leftrightarrow (\exists \widetilde{d} \in D) \; \widetilde{d}(rd' - dr') = 0.$$

Položme $R_D := D \times R / \sim$ (množina tříd ekvivalence $\sim$), třídu prvku (d, r) označme $\frac{r}{d}$.

Nechť α_1, $\alpha_2 \in R_D$, $(d_1, r_1) \in \alpha_1$, $(d_2, r_2) \in \alpha_2$. Můžeme definovat

$$\alpha_1 + \alpha_2 := \frac{r_1 d_2 + d_1 r_2}{d_1 d_2},$$
$$\alpha_1 \cdot \alpha_2 := \frac{r_1 r_2}{d_1 d_2}.$$

Lemma 3.4. *Takto definované operace nezávisí na výběru reprezentantů $(d_1, r_1) \in \alpha_1$, $(d_2, r_2) \in \alpha_2$. Navíc množina R_D tvoří komutativní okruh s jednotkou.*

Důkaz. Nechť (d_1, r_1), $(d_1', r_1') \in \alpha_1$, $(d_2, r_2) \in \alpha_2$. Z definice: $(d_1, r_1)(d_2, r_2) = (d_1 d_2, r_1 r_2)$, $(d_1', r_1')(d_2, r_2) = (d_1' d_2, r_1' r_2)$. Protože $(d_1, r_1) \sim (d_1', r_1')$, lze volit $\widetilde{d} \in D$ tak, že $\widetilde{d}(r_1 d_1' - d_1 r_1') = 0$. Odtud a z komutativity okruhu

$$0 = \widetilde{d}(r_1 d_1' - d_1 r_1') d_2 r_2 = \widetilde{d}(d_1 d_2 r_1' r_2 - r_1 r_2 d_1' d_2).$$

Tedy $(d_1 d_2, r_1 r_2) \sim (d_1' d_2, r_1' r_2)$.

Obdobně v ostatních případech. $\square$

R_D se nazývá *podílový okruh* okruhu R vzhledem k multiplikativní množině $D \subset R$. Máme přirozený homomorfismus

$$\lambda_D : R \to R_D,$$
$$r \mapsto \frac{r}{1}.$$

Věta 3.5. *Buď $\rho : R \to S$ homomorfismus okruhů, $D \subset R$ multiplikativní množina. Nechť $(\forall d \in D)$ je $\rho(d)$ invertibilní prvek v S (tj. $\rho(d) \in S^*$). Pak existuje jediný homomorfismus $\widetilde{\rho} : R_D \to S$ tak, že diagram*

$$\begin{tikzcd} R \arrow[rr, "\lambda_D"] \arrow[dr, "\rho"'] & & R_D \arrow[dl, "\widetilde{\rho}"] \\ & S & \end{tikzcd}$$

komutuje.

Pro libovolný okruh R a prvoideál $I \subsetneq R$, je $D = R \setminus I$ multiplikativní množina (obor integrity na třídách). Pak R_D se značí R_I a nazývá se *lokalizací okruhu* R podle prvoideálu I. Okruh R_I je lokální.

Maximální ideál I_{R_I} obsahuje prvky tvaru $\frac{r}{d}$, kde $r \in I$, $d \in D = R \setminus I$. $\lambda_I : R \to R_I$ je příslušný přirozený homomorfismus.

Předpokládejme, že R je obor integrity (nemá dělitele nuly). Pak $\langle 0 \rangle \subset R$ je prvoideál. Lokalizace R_0 je tzv. *podílové těleso* okruhu R. Přirozený homomorfismus $R \to R_0$, $r \mapsto \frac{r}{1}$, je v tomto případě monomorfismem.

Pro obor integrity R a multiplikativní množinu $D \subset R$ existuje přirozené zobrazení

$$\begin{aligned} &R_D \to R_0, \\ (d,r) \in \alpha \mapsto \ &\text{třída obsahující třídu } \alpha \text{ (a tedy } (d,r)). \end{aligned}$$

Tato definice opět nezávisí na volbě reprezentantů.

Dalším speciálním typem multiplikativní množiny je $D_r = \{1\} \cup \{r^n;\ n \in \mathbb{N}\}$ pro libovolný vybraný prvek $r \in R$ (značíme $\lambda_r : R \to R_{D_r}$).

Je-li $\rho : R \to S$ homomorfismus okruhů a $I_s \subset S$ prvoideál, pak $\lambda_r \rho : R \to S_{I_s}$ zobrazuje každý prvek $r \notin \rho^{-1}[I_s]$ na invertibilní prvek v S_{I_s}.

4. Nulstellensatz, homogenní verze. Stupeň transcendence těles

Poznámka 4.1. Lze si představit těleso $\mathbb{C}$, ale výsledky platí pro libovolné algebraicky uzavřené těleso charakteristiky 0.

Buď A okruh, $\gamma = (\gamma_1, \dots, \gamma_n) \in (\mathbb{N}_0)^n$ multiindex, $|\gamma| = \sum_{i=1}^n \gamma_i$, $t = (t_1, \dots, t_n)$, $t^\gamma = t_1^{\gamma_1} \dots t_n^{\gamma_n}$.

Výraz $\sum_{|\gamma| \le k} c_\gamma t^\gamma$ je polynom (v n proměnných) stupně k, pokud existuje $c_\gamma \neq 0$, $|\gamma| = k$. Píšeme $\mathrm{st}(f) = k$.

Pro $a = (a_1, \dots, a_n) \in A^n = \underbrace{A \times \dots \times A}_{n-\text{krát}}$ buď $f(a) = \sum_{|\gamma| \le k} c_\gamma a^\gamma$, tedy $f : A^n \to A$.

Tvrzení 4.2. *Prostor polynomů je algebrou nad okruhem A.*

Důkaz. Nechť $f = \sum c_\gamma t^\gamma$, $g = \sum d_\gamma t^\gamma$. Pak

$$
\begin{aligned}
f + g &= \sum (c_\gamma + d_\gamma) t^\gamma, \\
f \cdot g &= \sum_{\gamma, \alpha} (c_\alpha + d_{\gamma - \alpha}) t^\gamma,
\end{aligned}
$$

kde $\gamma - \alpha = (\gamma_1 - \alpha_1, \dots, \gamma_n - \alpha_n)$. Navíc platí:

$$
\begin{aligned}
\mathrm{st}(f + g) &= \max(\mathrm{st}(f), \mathrm{st}(g)), \\
\mathrm{st}(f \cdot g) &= \mathrm{st}(f) + \mathrm{st}(g). \quad \square
\end{aligned}
$$

$A[t] \equiv A[t_1, \dots, t_n]$ je okruh (algebra nad A) s přirozeným monomorfismem

$$
\begin{aligned}
A &\to A[t_1, \dots, t_n], \\
a &\mapsto f = a,
\end{aligned}
$$

který definuje kanonickou strukturu A-algebry.

Pro libovolnou A-algebru R a $r \in R^n$ definujme homomorfismus

$$
\begin{aligned}
A[t_1, \dots, t_n] &\to R, \\
\sum_\alpha c_\alpha t^\alpha &\mapsto \sum_\alpha c_\alpha r^\alpha = \sum_\alpha c_\alpha r_1^{\alpha_1} \dots r_n^{\alpha_n}.
\end{aligned}
$$

Polynom $f = \sum_{|\gamma| = k} c_\gamma t^\gamma$ je tzv. *homogenní polynom stupně k*. Výraz $t^\gamma \equiv t_1^{\gamma_1} \dots t_n^{\gamma_n}$ se nazývá *monom.* Homogenní polynomy stupně k tvoří spolu s nulovým polynomem A-podmodul označovaný $A[t_1, \dots, t_n]^k$. Pro $k \in \mathbb{N}$ tyto podmoduly generují strukturu gradované algebry na $A[t_1, \dots, t_n]$.

Věta 4.3. *Je-li A okruh s jednoznačným rozkladem na prvočinitele (UFD), pak $A[t_1, \dots, t_n]$ je rovněž UFD.*

V situaci z předchozí věty nazveme $f \in A$, který je prvočinitelem, *irreducibilním (nerozložitelným) polynomem.*

Okruh $\mathbb{C}[t_1, \dots, t_n]$ je noetherovský, neboť platí následující

Hilbertova věta o bázi, 4.4. *Je-li A noetherovský okruh, pak $A[t_1,\dots,t_n]$ je rovněž noetherovský okruh.*

Konkrétně pro těleso T je $T[t_1,\dots,t_n]$ noetherovský okruh.

Buď A okruh s jednoznačným rozkladem na prvočinitele, $f, g \in A[t]$,

$$\begin{aligned} f(t) &= c_0 + c_1 t + \dots + c_r t^r, \\ g(t) &= d_0 + d_1 t + \dots + d_s t^s, \end{aligned}$$

$c_r \neq 0 \neq d_s$, $\mathrm{st}(f) = r \geq 1$, $\mathrm{st}(g) = s \geq 1$. *Resultant polynomů* f, g, je prvek A tvaru

$$R(f,g) = \begin{vmatrix} c_0 & c_1 & \dots & c_r & 0 & \dots & 0 \\ 0 & c_0 & & & c_r & & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \dots & 0 & c_0 & c_1 & \dots & c_r \\ d_0 & d_1 & \dots & d_s & 0 & \dots & 0 \\ 0 & d_0 & & & d_s & & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \dots & 0 & d_0 & d_1 & \dots & d_s \end{vmatrix} \begin{array}{l} \left.\vphantom{\begin{matrix}c\\c\\ \vdots\\c\end{matrix}}\right\} s \text{ řádků}, \\ \left.\vphantom{\begin{matrix}c\\c\\ \vdots\\c\end{matrix}}\right\} r \text{ řádků}. \end{array}$$

Věta 4.5. *Buď A UFD. Polynomy f, g nad A mají společného prvočinitele, právě když $R(f,g) = 0$.*

f, $g \in A[t_1,\dots,t_n] = A[t_1,\dots,t_{n-1}][t_n]$, tj. jedná se o polynomy v proměnné t_n s hodnotami v $A[t_1,\dots,t_{n-1}]$. Vyšetřujeme případ, kdy f, g mají společného prvočinitele obsahujícího t_n.

Nechť

$$\begin{aligned} f &= f_0 + f_1 t_n + \dots + f_r t_n^r, \\ g &= g_0 + g_1 t_n + \dots + g_s t_n^s, \end{aligned}$$

$f_r, g_s \neq 0$, $f_0,\dots,f_r,g_0,\dots,g_s \in A[t_1,\dots,t_{n-1}]$. Tedy pro $R(f,g) \in A[t_1,\dots,t_{n-1}]$ mají f a g společného prvočinitele, právě když $R(f,g) = 0$ (= triviální polynom v $A[t_1,\dots,t_{n-1}]$).

Podobně pro homogenní případ: nechť F, $G \in A[t_0,\dots,t_n]$ jsou homogenní polynomy, $\mathrm{st}(F) = r$, $\mathrm{st}(G) = s$,

$$\begin{aligned} F &= F_0 + F_1 t_n + \dots + F_r t_n^r, \\ G &= G_0 + G_1 t_n + \dots + G_s t_n^s, \end{aligned}$$

$F_0,\dots,F_r,G_0,\dots,G_s \in A[t_0,\dots,t_{n-1}]$ (nikoli však homogenní).

Z předchozího: F, G mají společného prvočinitele polynomického v t_n, právě když $R(F,G) = 0$.

Z homogenity navíc plyne

Věta 4.6. *Resultant $R(f,g)$ je buď nulový polynom nebo je to homogenní polynom stupně $s \cdot t$.*

Poznámka 4.7. Připomeňme, že průnik maximálních ideálů okruhu $\mathbb{C}[t_1,\dots,t_n]$ obsahujících ideál $I \subset \mathbb{C}[t_1,\dots,t_n]$ je roven radikálu $\sqrt{I}$ ideálu I. Podobný výsledek platí pro homogenní verzi.

Věta 4.8 (Hilbertův Nulstellensatz). *Nechť* $f_1, \dots, f_k \in \mathbb{C}[t_1, \dots, t_n]$ *a nechť je splněno: pokud pro nějaké* $a \in \mathbb{C}^n$ *platí* $f_1(a) = \cdots = f_k(a) = 0$, *pak také* $f(a) = 0$.

Potom existuje $m \in \mathbb{N}$ *a polynomy* $g_1, \dots, g_k \in \mathbb{C}[t_1, \dots, t_n]$ *tak, že*

$$f^m = g_1 f_1 + \cdots + g_k f_k.$$

Poznámka 4.9. Hilbertova věta o nulách nese podstatnou informaci o souhře dvou faktorů: algebraických vlastností ideálu na straně jedné a jeho geometrických (tj. spektrálních) vlastností (tzn. množiny bodů, kterou anihilují) na straně druhé.

Věta 4.10 (Hilbertův Nulstellensatz – homogenní verze). *Nechť jsou* $F_1, \dots, F_k \in \mathbb{C}[t_0, \dots, t_n]$ *homogenní polynomy takové, že existuje alespoň jeden bod* $\widetilde{a} \in \mathbb{C}^{n+1}$, $\widetilde{a} \neq 0$ *tak, že* $F_1(\widetilde{a}) = \cdots = F_k(\widetilde{a}) = 0$. *Předpokládejme, že platí: pokud pro nějaké* $a \in \mathbb{C}^{n+1}$ *je* $F_1(a) = \cdots = F_k(a) = 0$, *pak také* $F(a) = 0$.

Potom existuje $m \in \mathbb{N}$ *a homogenní polynomy* $G_1, \dots, G_k \in \mathbb{C}[t_0, \dots, t_n]$ *tak, že*

$$F^m = G_1 F_1 + \cdots + G_k F_k.$$

Několik poznámek k faktorizaci v $A[t]$.

Je-li A těleso, je $A[t]$ PID (tj. UFD).

Základní věta algebry, 4.11. *Buď* $f \in \mathbb{C}[t]$ *polynom stupně* ≥ 1. *Pak existuje právě jedno* $c \in \mathbb{C}$, $c \neq 0$, *a čísla* $a_1, \dots, a_n \in \mathbb{C}$ *určená jednoznačně až na pořadí tak, že* $f(t) = c \cdot (t - a_1) \dots (t - a_n)$.

Věta platí nejen pro $\mathbb{C}$, ale pro libovolné algebraicky uzavřené těleso charakteristiky 0.

Poznámka 4.12. Číslo $a \in \mathbb{C}$ je alespoň dvojnásobným kořenem tehdy a jen tehdy když

$$R(f, f') = 0, \text{ kde } f' = \frac{df}{dt}.$$

Věta 4.13. *Buď* $F \in \mathbb{C}[t_0, t_1]$ *homogenní polynom stupně* ≥ 1. *Pak existují homogenní polynomy* $c_1 t_0 + d_1 t_1, \dots, c_k t_0 + d_k t_1$ *stupně* 1 *určené jednoznačně až na pořadí a na násobky* $\lambda \in \mathbb{C}^\times$ *tak, že*

$$F(t_0, t_1) = (c_1 t_0 + d_1 t_1) \dots (c_k t_0 + d_k t_1).$$

Kořen pro homogenní polynom:

$$(a, b) \sim (a', b') \Leftrightarrow (\exists \lambda \in \mathbb{C}^\times)\ (a, b) = (\lambda a', \lambda b').$$

Třídy $(a : b)$ (tj. prvky $\mathbb{P}^1/_{\mathbb{C}}$) jsou dle definice kořeny polynomu.

Tělesa.

Motiv: stupeň transcendence rozšíření (algebraický) je roven Krullově dimenzi okruhu (geometrické).

Definice 4.14. Těleso K je *algebraicky uzavřené*, pokud pro každý polynom $f \in K[t]$ stupně ≥ 1 existují a jsou určeny jednoznačně prvky $c \in K$, $a_1, \dots, a_k \in K$ tak, že
$$f(t) = c \cdot (t - a_1) \dots (t - a_k).$$

Základní věta algebry říká, že $\mathbb{C}$ je algebraicky uzavřené těleso.

Jsou-li K, L tělesa, $K \subset L$, pak K je *podtělesem* L (a L je *nadtělesem (rozšířením)* tělesa K). L má strukturu K-algebry (ta je konečně generovaná, právě když $|[L : K]| < \infty$).

Buď $f \in K[t] \subset L[t]$ polynom, $\mathrm{st}(f) \geq 1$. Prvek $a \in L$ je *kořen polynomu* f, pokud $f(a) = 0$.

Prvek $a \in L$ je *algebraický nad* K, pokud existuje polynom $f \in K[t]$ tak, že $f(a) = 0$. Prvek $a \in L$, ktery není algebraický, se nazývá *transcendentní (nad K)*. Je-li každý prvek $a \in L$ algebraický nad K, je [L:K] *algebraické rozšíření* K.

Buď $M \subset L$ podmnožina. M je *algebraicky nezávislá* nad K, platí-li
$$(\forall n \in \mathbb{N})\ (\forall f \in K[t_1, \dots, t_n])\ (\forall a_1, \dots, a_n \in M)$$
$$\big((\forall i, j = 1, \dots, n,\ i \neq j)\ a_i \neq a_j\ \ \&\ \ f(a_1, \dots, a_n) = 0\big)\ \Rightarrow f = 0.$$

Buď $M \subset L$ maximální taková množina (vzhledem k inkluzi). Pak $\sharp M$ se nazývá *stupněm transcendence* $[L : K]$ (značí se $\mathrm{sttr}_{\mathrm{K}}(\mathrm{L})$).

Je-li M nekonečná, je $\mathrm{sttr}_K(L) = \infty$, navíc $\mathrm{sttr}_K(L)$ nezávisí na volbě $M \subset L$.

5. Afinní uzavřené množiny

Poznámka 5.1. Následující úvahy provádíme pro těleso $\mathbb{C}$, ale téměř vždy je možné je zobecnit pro algebraicky uzavřená tělesa (někdy platí za předpokladu, že se jedná o těleso charakteristiky 0).

Komplexní afinní prostor dimenze n označme $A_n \equiv A_n/\mathbb{C}$ (občas budeme také pracovat s $A_n/\mathbb{R}$). $R = \mathbb{C}[t_1, \dots, t_n]$ buď algebra polynomů o n proměnných nad $\mathbb{C}$.

Pro podmnožinu $S \subset \mathbb{C}[t]$ položme

$$V(S) := \{a \in A_n;\ (\forall f \in S)\ f(a) = 0\},$$

tj. $V(S) \subset A_n$ je množina všech společných nulových bodů všech polynomů z S.

Definice 5.2. Množiny tvaru $V(S)$, kde $S \subset \mathbb{C}[t]$, se nazývají *afinní uzavřené množiny* v A_n (též se používá název uzavřené množiny). Množinu všech uzavřených podmnožin A_n označíme $\mathcal{C}_n$.

Poznámka 5.3. Pro ideál $\langle S\rangle \subset \mathbb{C}[t]$ generovaný množinou S platí $V(\langle S\rangle) = V(S)$. Má tedy smysl studovat přímo ty podmnožiny, které jsou ideály (speciálního typu, viz dále).

Hilbertova věta o bázi (z předchozí kapitoly) říká, že pro každý ideál $S \subset \mathbb{C}[t]$ najdeme $k \in \mathbb{N}$, $f_1, \dots, f_k \in S \subset \mathbb{C}[t]$ tak, že

$$(\forall f \in S)\ (\exists g_i \in \mathbb{C}[t])\ f = \sum_{i=1}^{k} g_i f_i.$$

Jinak zapsáno, $V(S) = V([f_1, \dots, f_k])$. Každá uzavřená množina je tedy určena konečným počtem polynomů, neboli rovnicemi $f_1 = 0, \dots, f_k = 0$.

Příklady 5.4.
1. $S = \langle f\rangle$, kde $f(t_1, \dots, t_n) = \sum_{i=1}^n c_i t_i + c$ je polynom stupně 1. Pak $V(S)$ je nadrovina v A_n.
2. $S = \langle f\rangle$, kde $f = \sum_{i,j} c_{i,j} t_i t_j + \sum c_n t_n + c$ je polynom stupně 2. Pak $V(S)$ je kvadrika v A_n.
3. $S = \langle f_1, \dots, f_n\rangle$, kde $f_k(t_1, \dots, t_n) = t_k - a_k$, $k = 1, \dots, n$. Pak $V(S)$ je jediný bod $a = (a_1, \dots, a_n)$.

Věta 5.5. *Jsou-li S_1, $S_2 \subset \mathbb{C}[t]$ dva ideály, pak platí*

(1) $S_1 \subset S_2 \Rightarrow V(S_1) \supset V(S_2)$,
(2) $V(S_1) \cup V(S_2) = V(S_1 \cap S_2) = V(S_1 \cdot S_2)$,
(3) *je-li $\{S_\gamma\}_{\gamma\in\Gamma}$ libovolná množina ideálů z $\mathbb{C}[t]$, pak platí*

$$\bigcap_{\gamma\in\Gamma} V(S_\gamma) = V\Big(\sum_{\gamma\in\Gamma} S_\gamma\Big).$$

Důkaz. (1) Zřejmé z definice.

(2) Protože $S_1 \cdot S_2 \subset S_1 \cap S_2$, je dle (1) $V(S_1 \cap S_2) \subset V(S_1 \cdot S_2)$. Buď $a \in V(S_1) \cup V(S_2)$, volme např. $a \in V(S_1)$. Pokud $f \in S_1 \cap S_2$, je $f \in S_1$ (samozřejmě také $f \in S_2$), tj. $f(a) = 0$, neboli

$$V(S_1) \cup V(S_2) \subset V(S_1 \cap S_2) \subset V(S_1 \cdot S_2).$$

Buď nyní $a \in V(S_1 \cdot S_2)$ a předpokládejme, že $a \notin V(S_1)$, tj. existuje polynom $f \in S_1$ tak, že $f(a) \neq 0$. Vezměme libovolné $g \in S_2$. Je zřejmě $f \cdot g \in S_1 \cdot S_2$, a tedy $(f \cdot g)(a) = f(a) \cdot g(a) = 0$. Protože $\mathbb{C}[t]$ je oborem integrity (viz předchozí lekci) a $f(a) \neq 0$, je $g(a) = 0$. Protože jsme $g \in S_2$ volili libovolně, dostáváme $a \in V(S_2)$. Tedy

$$V(S_1 \cdot S_2) \subset V(S_1) \cup V(S_2).$$

To spolu s předchozí inkluzí:

$$V(S_1) \cup V(S_2) \subset V(S_1 \cap S_2) \subset V(S_1 \cdot S_2) \subset V(S_1) \cup V(S_2)$$

dokazuje (2).

(3) Pro každé $\alpha \in \Gamma$ je $S_\alpha \subset \sum_{\gamma \in \Gamma} S_\gamma$. Podle (1) je pak $V(\sum_{\gamma \in \Gamma} S_\gamma) \subset V(S_\alpha)$. Odtud (protože $\alpha \in \Gamma$ bylo libovolné)

$$V\Big(\sum_{\gamma \in \Gamma} S_\gamma\Big) \subset \bigcap_{\gamma \in \Gamma} V(S_\gamma).$$

Dokažme opačnou inkluzi. Buď $a \in \bigcap_{\gamma \in \Gamma} V(S_\gamma)$ a uvažujme libovolný polynom $f \in \sum_{\gamma \in \Gamma} S_\gamma$. Existují tedy $k \in \mathbb{N}$, $\gamma_1, \ldots, \gamma_k \in \Gamma$ tak, že $f = f_{\gamma_1} + \cdots + f_{\gamma_k}$, přičemž $f_{\gamma_i} \in S_{\gamma_i}$, $i = 1, \ldots, k$. Pak $f(a) = f_{\gamma_1}(a) + \cdots + f_{\gamma_k}(a) = 0$. Jinak zapsáno,

$$\bigcap_{\gamma \in \Gamma} V(S_\gamma) \subset V\Big(\sum_{\gamma \in \Gamma} S_\gamma\Big). \quad \square$$

Vlastnosti množiny $\mathcal{C}_n$.

$\{0\} \in \mathcal{C}_n$, neboť $\{0\} = V(\langle \mathbb{C}[t] \rangle)$.

$A_n \in \mathcal{C}_n$, neboť $A_n = V(\langle 0 \rangle)$.

Z (2) předchozí věty vyplývá, že $X,\, X' \in \mathcal{C}_n \Rightarrow X \cup X' \in \mathcal{C}_n$ (příslušný ideál je roven $S \cap S'$, kde $S,\, S'$ jsou ideály odpovídající $X,\, X'$).

Z (3) plyne, že $\big((\forall \gamma \in \Gamma)\ X_\gamma \in \mathcal{C}_n\big) \Rightarrow \bigcap_{\gamma \in \Gamma} X_\gamma \in \mathcal{C}_n$.

Toto jsou nutné podmínky k zadání (předpisu) topologie pomocí uzavřených množin. Tato topologie se nazývá *Zariského topologií* (množina uzavřená v Zariského topologii je dána definicí uzavřené afinní množiny v A_n). Otevřené množiny jsou právě doplňky uzavřených. (Zariského topologie indukuje topologii na každé podmnožině A_n – nejčastěji uvažujeme uzavřené podmnožiny.)

Poznámka 5.6. Nevýhodou Zariského topologie je, že všechny otevřené množiny mají dimenzi n, jsou tedy "příliš velké". Může nastat situace, že prostor není v této topologii Hausdorffův (tedy neexistuje dostatečně mnoho "malých" otevřených množin separujících body).

Buď $X \subset A_n$ uzavřená množina. Definujme $I(X) \subset \mathbb{C}[t]$ předpisem

$$I(X) := \{f \in \mathbb{C}[t];\ (\forall a \in X)\ f(a) = 0\}.$$

Zřejmě je $I(X) \subset \mathbb{C}[t]$ ideál.

Definice 5.7. $I(X)$ se nazývá *ideál asociovaný* s uzavřenou množinou X.

Pokud pro ideál $S \subset \mathbb{C}[t]$ platí $X = V(S)$, je $S \subset I(V(S))$. Rovnost zde obecně neplatí.

Příklad 5.8. $X = V(S) \subset A_2$, kde $S \subset \mathbb{C}[t_1, t_2]$ je ideál generovaný $f(t_1, t_2) = t_1^2$. Příslušnou uzavřenou množinou je přímka $t_1 = 0$. Polynom $g = t_1$ se na X anuluje (tj. $g \in I(V(S))$). Avšak $g \notin S$, tedy $S \subsetneq I(V(S))$.

Problém. Pro které ideály $S \subset \mathbb{C}[t]$ je $S = I(V(S))$?

Pozorování 5.9. $I(V(S))$ je radikálový ideál, neboť pokud $(\exists n \in \mathbb{N})\ f^n \in I(V(S))$ (tj. f^n se anuluje $I(V(S))$), pak f se anuluje na $V(S)$ $\big(f \in I(V(S))\big)$. To vyplývá z faktu, že $\mathbb{C}[t]$ je obor integrity: kdyby $f(a) \neq 0$ pro nějaké $a \in V(S)$, pak též $f^n(a) \neq 0$.

V minulé lekci diskutovaný Hilbertův Nulstellensatz v této řeči dává:

$$I(V(S)) = \sqrt{S} \ (= \text{ radikál ideálu } S),$$

tedy příslušná podmínka není jen nutná, ale i postačující. Shrneme:

Věta 5.10. *Pro každý ideál $S \subset \mathbb{C}[t]$ platí:*

- $S \subset I(V(S))$,
- $I(V(S)) = \sqrt{S}$.

Přitom $S = I(V(S))$, právě když S je radikálový ideál.

Věta 5.11. *Buď $S \subset \mathbb{C}[t]$ ideál. Pak uzavřená množina $V(S)$ je prázdná, právě když $S = \mathbb{C}[t]$.*

Důkaz. $\Leftarrow$: $S = \mathbb{C}[t]$, pak $V(S) = \{0\}$ (neboť např. prvky ze základního tělesa $\mathbb{C}$ se nikde neanulují).

$\Rightarrow$: Předpokládejme, že $V(S) = \{0\}$. Pak dle předchozí věty: $\sqrt{S} = I(V(S)) = I(\{0\}) = \mathbb{C}[t]$. Tedy pro každý konstantní polynom $a \in \mathbb{C}[t]$ je $a \in \sqrt{S}$ (např. pro $a = 1 \in \sqrt{S}$ je $1 \in S$), a tedy $S = \mathbb{C}[t]$. $\square$

Poznámka 5.12. Uzavřená množina $V(S)$ určená ideálem $S \subsetneq \mathbb{C}[t]$ je neprázdná.

Poznámka 5.13. Předchozí věty jsou zobecněním základní věty algebry pro $\mathbb{C}[t_0]$. Je-li $f \in \mathbb{C}[t_0]$ nekonstantní polynom, pak $\langle f \rangle \neq \mathbb{C}[t_0]$, a tudíž $V(\langle f \rangle) \neq 0$ (tato množina je dána přesně kořeny polynomu f).

Pokud je $X \subset A_n$ uzavřená, je $X = V(I(X))$, neboť

- $X \subset V(I(X))$ je zřejmá inkluze,
- pro $X = V(S)$, kde $S \subset \mathbb{C}[t]$ je ideál, plyne z $S \subset I(V(S))$ inkluze $V(S) \supset V(I(V(S)))$, což je $X \supset V(I(X))$.

Shrňme:

Věta 5.14. *Zobrazení $S \mapsto V(S)$ je bijektivní zobrazení množiny všech radikálových ideálů v $\mathbb{C}[t]$ na množinu všech uzavřených podmnožin A_n.*

Důkaz. Zobrazení $X \mapsto I(X)$ je inverzí k $S \mapsto V(S)$. $\square$

6. Reducibilita a irreducibilita

Definice 6.1. Uzavřená množina $X \subset A_n$ se nazývá *rozložitelná* (*reducibilní*), pokud existují uzavřené množiny X_1, $X_2 \subset A_n$ tak, že

- $X = X_1 \cup X_2$,
- $X_1 \neq X \neq X_2$

(tj. $X \subset A_n$ je rozložitelná, právě když je sjednocením vlastních uzavřených podmnožin).

Uzavřená množina, která není rozložitelná, se nazývá *nerozložitelná* (*irreducibilní*).

Věta 6.2. *Uzavřená množina X je nerozložitelná, právě když je $I(X) \subset \mathbb{C}[t]$ prvoideál.*

Důkaz. $\Rightarrow$: Dokazujeme nepřímo: nechť existují f_1, $f_2 \in \mathbb{C}[t]$ tak, že $f_1 \notin I(X)$, $f_2 \notin I(X)$, $f_1 f_2 \in I(X)$ (tj. $I(X)$ není prvoideál). Množiny $Y_1 = V(\langle f_1 \rangle)$, $Y_2 = V(\langle f_2 \rangle)$ jsou uzavřené, tudíž jsou uzavřené i množiny $X_1 = X \cap Y_1$, $X_2 = X \cap Y_2$. Protože $f_1 f_2 \in I(X)$, platí $f_1(a) f_2(a) = 0$ ($\forall a \in X$), tj. buď $a \in X_1$ nebo $a \in X_2$. Z libovolnosti $a \in X$ plyne, že $X = X_1 \cup X_2$. Protože $f_1 \notin I(X_1)$, existuje $a \in X$ tak, že $f_1(a) \neq 0$, neboli $X_1 \neq X$. Podobně $X_2 \neq X$. Protože $X = X_1 \cup X_2$, ukázali jsme reducibilitu X.

$\Leftarrow$: Předpokládejme, že je X reducibilní, $X = X_1 \cup X_2$, X_1, X_2 uzavřené, přičemž $X_1 \neq X \neq X_2$. Inkluze $X_1 \subsetneq X$, ($X_2 \subsetneq X$) dávají (viz předchozí lekce)

$$I(X_1) \supsetneq I(X) \; \big(I(X_2) \supsetneq I(X)\big).$$

Jinak řečeno, existuje polynom $f_1 \in I(X_1)$ ($f_2 \in I(X_2)$) tak, že $f_1 \notin I(X)$ ($f_2 \notin I(X)$). Protože $X = X_1 \cup X_2$, musí být $f_1 f_2 \in I(X)$. Ideál $I(X)$ tedy není prvoideálem. $\square$

Postup při rozkládání uzavřené množiny $X \subset A_n$.

Lemma 6.3. *Každá uzavřená $X \subset A_n$ je konečným sjednocením nerozložitelných uzavřených množin.*

Důkaz. Předpokládejme pro spor, že $X \subset A_n$ není konečně rozložitelná. Speciálně není rozložitelná, tedy existují uzavřené X_1, $X_2 \subset A_n$ tak, že $X = X_1 \cup X_2$, $X_1 \neq X \neq X_2$. Vyberme z $\{X_1, X_2\}$ konečně nerozložitelnou množinu, označme ji $Y^{(1)}$. Množina $Y^{(1)}$ není (konečně) rozložitelná, tj. existují uzavřené množina $Y_1^{(1)}$, $Y_2^{(1)}$ tak, že $Y(1) = Y_1^{(1)} \cup Y_2^{(1)}$, $Y_1^{(1)} \neq Y^{(1)} \neq Y_2^{(1)}$. Podobně alespoň jedna z množin $Y_1^{(1)}$, $Y_2^{(1)}$ není (konečně) rozložitelná a pokračujeme tak v předchozím procesu. Finálně máme nekonečnou posloupnost uzavřených množin

$$X = Y^{(0)} \supsetneq Y^{(1)} \supsetneq Y^{(2)} \supsetneq \dots,$$

tedy

$$I(X) = I\big(Y^{(0)}\big) \subsetneq I\big(Y^{(1)}\big) \subsetneq I\big(Y^{(2)}\big) \subsetneq \dots,$$

což je ve sporu s noetherovskostí okruhu $\mathbb{C}[t]$. $\square$

Dokázali jsme existenci $k \in \mathbb{N}$ takového, že $X = X_1 \cup X_2 \cup \dots \cup X_k$ pro X, $X_1, \dots X_k \subset A_n$ uzavřené.

Lemma 6.4. *Buď $X \subset A_n$ uzavřená. Pak existuje $k \in \mathbb{N}$ a uzavřené množiny $X_1, \dots, X_k \subset A_n$ tak, že $X = X_1 \cup \dots \cup X_k$, přičemž pro žádnou dvojici $1 \le i, j \le k$, $i \ne j$, neplatí $X_i \subset X_j$. Množiny $X_1, \dots, X_k$ jsou určeny jednoznačně až na pořadí.*

Důkaz. Buď $X = X'_1 \cup \dots \cup X'_{k'}$, kde $X'_1, \dots, X'_{k'}$ jsou nerozložitelné a pro žádnou dvojici $1 \le r, s \le k'$, $r \ne s$, neplatí $X'_s \subset X'_r$.

Uvažujme libovolný index $r \le k'$, ukážeme, že $(\exists i \le k)\ X'_r \subset X_i$ (sporem). Předpokládejme, že $(\forall j \le k)\ X'_r \not\subset X_j$. Protože $X'_r \not\subset X_1$, musí být $X'_r \subset \bigcup_{j=2}^k X_j$. (Pokud by $X'_r \not\subset \bigcup_{j=2}^k X_j$, bylo by $X'_r = (X'_r \cap X_1) \cup (X'_r \cap \bigcup_{j=2}^k X_j)$, přičemž $X'_r \cap X_1 \ne X'_r$, $X'_r \cap \bigcup_{j=2}^k X_j \ne X'_r$, což je spor s nerozložitelností X'_r.) Podobně indukcí $X'_r \subset \bigcup_{j=3}^k X_j$, $\dots$, $X'_r \subset \bigcup_{j=k}^k X_j = X_k$ ve sporu s předpokladem $X'_r \not\subset X_j$ $(\forall j \le k)$.

Pro dané $1 \le r \le k'$ tedy existuje $1 \le i \le k$ tak, že $X'_r \subset X_i$. Podobně existuje $1 \le s \le k'$ tak, že $X_i \subset X'_s$, tedy $X'_r \subset X_i \subset X'_s$. Protože $X'_r \not\subset X'_s$, pokud $r \ne s$, je $r = s$ a $X'_r = X_i$. Induktivním postupem dostáváme $k = k'$ a $(\exists \pi \in S_k)$ $X_i = X'_{\pi(i)}$ $(\forall i = 1, \dots, k)$. $\square$

Poznámka 6.5. Rozkladu $X = X_1 \cup \dots \cup X_k$ z předchozího lemmatu se říká *rozklad na komponenty* $X_1, \dots, X_k$.

Definice 6.6. Nerozložitelnou uzavřenou množinu $X \subset A_n$ nazveme *varietou* (popř. *afinní varietou*).

Příklad 6.7. Buď $n = 3$, uvažujme okruh $\mathbb{C}[t_1, t_2, t_3]$ a ideál $I = \langle f_1, f_2 \rangle$, kde

$$f_1(t_1, t_2, t_3) = t_2 - t_1^2,$$
$$f_2(t_1, t_2, t_3) = t_3 - t_1^3.$$

Ukážeme, že $X = V(I)$ je varieta (někdy se nazývá *twistovaná kubika*). To nastane dle definic tehdy a jen tehdy, je-li I prvoideál. Protože je každý prvoideál radikálovým ideálem, bude platit $I(V(I)) = I$.

Studujme homomorfismus

$$h : \mathbb{C}[t_1, t_2, t_3] \to \mathbb{C}[t_1],$$

definovaný na generátorech okruhu:

$$t_1 \mapsto t_1,$$
$$t_2 \mapsto t_1^2,$$
$$t_3 \mapsto t_1^3.$$

h je epimorfismus, $\mathbb{C}[t_1]$ je obor integrity, tedy I je prvoideál. Ukažme, že $\mathrm{Ker}(h) = I$. Platí $\mathbb{C}[t_1, t_2, t_3] \cong I \oplus \mathbb{C}[t_1]$, neboť $\forall f \in \mathbb{C}[t_1, t_2, t_3]$ je $f = f_1 + f_2$, kde $f_1 \in I$, $f_2 \in \mathbb{C}[t_1]$ (máme

$$\mathbb{C}[t_1] \hookrightarrow \mathbb{C}[t_1, t_2, t_3],$$
$$\sum_i a_i t_1^i \mapsto \sum_i a_i t_1^i t_2^0 t_3^0).$$

Navíc platí implikace $f \in I \cap \mathbb{C}[t_1] \Rightarrow h(f) = 0$, tedy $\mathrm{Ker}(h) = I$.

Příklad 6.8. A_n je varieta, neboť $I(A_n) = \{0\}$ a $\{0\} \subset \mathbb{C}[t_1, \dots, t_n]$ je prvoideál.

Rozklad na komponenty je v řeči ideálů vyjádřen následující větou.

Věta 6.9. *Buď $X = X_1 \cup \dots \cup X_k$ rozklad uzavřené množiny X na komponenty. Pak*

$$I(X) = I(X_1) \cap \dots \cap I(X_k),$$

přičemž všechny $I(X_i)$, $1 \le i \le k$, jsou prvoideály a pro žádné $1 \le i, j \le k$, $i \ne j$, neplatí $I(X_i) \subset I(X_j)$.

Důkaz. Plyne z výše uvedených vět. $\square$

Speciální typ předchozích úvah.

Definice 6.10. Uzavřenou množinu $X \subset A_n$ nazýváme *nadplochou* v A_n, pokud existuje netriviální hlavní ideál $I \subset \mathbb{C}[t]$ (tj. $\{0\} \ne I \ne \mathbb{C}[t]$) tak, že $X = V(I)$.

Věta 6.11. *Buď $X = V(\langle f \rangle)$ nadplocha v A_n, buď $f = f_1^{r_1} \dots f_k^{r_k}$ ($k \in \mathbb{N}$) rozklad $f \in \mathbb{C}[t]$ na prvočinitele. Definujme $\widetilde{f} := f_1 \dots f_k$. Pak $I(X) = \langle \widetilde{f} \rangle$.*

Důkaz. Víme, že pro $I = \langle f \rangle$ je $I(V(\langle I \rangle)) = \sqrt{I} = \sqrt{\langle f \rangle}$. Protože $\widetilde{f}^{r_1 + \dots + r_k} \in \langle f \rangle$, je $\widetilde{f} \in I(X)$, tj. $\langle \widetilde{f} \rangle \subset I(X)$. Obrácená inkluze: buď $g \in I(X)$, pak existuje $n \in \mathbb{N}$ tak, že $g^n \in \langle f \rangle$. Je tedy $(\forall 1 \le i \le k)$ $f_i | g^n$, a protože polynomy f_i jsou nerozložitelné, je $f_i | g_i$. Platnost $(\forall i)$ $f_i | g_i$ je ekvivalentní $g \in \langle \widetilde{f} \rangle = \langle f_1, \dots, f_k \rangle$.

Obě inkluze pak dávají $I(X) = \langle \widetilde{f} \rangle$. $\square$

Uvažujme $\mathbb{C}$-izomorfismus

$$A_m \times A_n \to A_{m+n},$$
$$\big((a_1, \dots, a_m), (b_1, \dots, b_n)\big) \mapsto (a_1, \dots, a_m, b_1, \dots, b_n).$$

Máme vnoření na podokruhy (tj. $\mathbb{C}$-podalgebry):

$$\mathbb{C}[t], \mathbb{C}[u] \hookrightarrow \mathbb{C}[t, u].$$

Pokud $f \in \mathbb{C}[t] \subset \mathbb{C}[t, u]$ a $(a, b) \in A_m \times A_n = A_{m+n}$, má smysl psát $f(a, b)$ (samozřejmě $f(a, b) = f(a)$). Podobně pro $g \in \mathbb{C}[u] \subset \mathbb{C}[t, u]$ $(g(a, b) = g(b))$.

Je-li $S \subset \mathbb{C}[t]$ ideál, pak S^{in} označíme ideál generovaný obrazem množiny S při přirozeném vnoření $\mathbb{C}[t] \hookrightarrow \mathbb{C}[t, u]$.

Věta 6.12. *Nechť jsou $X \subset A_m$, $Y \subset A_n$ uzavřené množiny. Pak $X \times Y \subset A_{m+n}$ je uzavřená.*

Důkaz. Dokážeme, že $X \times Y = V(I(X)^{in} + I(Y)^{in})$. Pro $(a, b) \in X \times Y$ a $f \in I(X)$, $g \in I(Y)$ je $f(a, b) = f(a) = 0$, $g(a, b) = g(b) = 0$. $I(X) \cong I(X)^{in} \subset \mathbb{C}[u, v]$, $I(Y) \cong I(Y)^{in} \subset \mathbb{C}[u, v]$, platí tedy zřejmě $X \times Y \subset V(I(X)^{in} + I(Y)^{in})$.

Naopak: buď $(a, b) \in V(I(X)^{in} + I(Y)^{in})$. Pak pro libovolné $f \in I(X)$ (resp. $g \in I(Y)$) je $f(a) = f(a, b) = 0$ $(g(b) = g(a, b) = 0)$, tj. $a \in X$ $(b \in Y)$. Odtud $X \times Y = V(I(X)^{in} + I(Y)^{in})$, tedy $X \times Y$ je uzavřená množina. $\square$

Věta 6.13. *Jsou-li $X \subset A_m$, $Y \subset A_n$ nerozložitelné uzavřené množiny, pak množina $X \times Y$ je rovněž nerozložitelná.*

Důkaz. Je třeba ukázat, že $I(X \times Y)$ je prvoideál v $\mathbb{C}[t,u]$. Uvažujme f, $g \in \mathbb{C}[t,u]$ takové, že $fg \in I(X \times Y)$. Pak platí $(\forall a \in X)\ f(a,u) \cdot g(a,u) \in I(Y)$ (dle předchozí věty), tedy buď $f(a,u) \in I(Y)$ nebo $g(a,u) \in I(Y)$. Definujme

$$X_1 := \{a \in X;\ f(a,u) \in I(Y)\},$$
$$X_2 := \{a \in X;\ g(a,u) \in I(Y)\}.$$

Platí: $X_1 \cup X_2 = X$. Ukážeme, že obě množiny jsou uzavřené. Je

$$X_1 = \bigcap_{b \in Y} V(\langle f(t,b) \rangle) \cap X,$$

a protože $\bigcap_{b \in Y} V(\langle f(t,b)\rangle) = V\big(\sum_{b \in Y} V(\langle f(t,b)\rangle)\big)$ je uzavřená, je $X_1 \subset X$ rovněž uzavřená. Podobně pro X_2.

Množina X je nerozložitelná, a tedy buď $X = X_1$ nebo $X = X_2$. V prvním případě je $f \in I(X \times Y)$, v druhém případě $g \in I(X \times Y)$. Dokázali jsme:

$$f \cdot g \in I(X \times Y) \Rightarrow \big(f \in I(X \times Y) \vee g \in I(X \times Y)\big),$$

tedy $I(X \times Y)$ je prvoideál. $\square$

7. Regulární funkce na afinních uzavřených množinách

Definice 7.1. Buď $X \subset A_n$ uzavřená. Funkce $f' : X \to \mathbb{C}$ se nazývá *regulární funkcí* na X, pokud existuje polynom $f \in \mathbb{C}[t] \equiv \mathbb{C}[A_n]$ tak, že $(\forall a \in X)\ f'(a) = f(a)$.

Poznámka 7.2. Zobrazení $f' \mapsto f$ není jednoznačné. Pokud $h \in I(X)$, pak $g = f + h$ určuje tutéž třídu f' jako f (a vice versa).

Věta 7.3. *Množina $\mathbb{C}[X]$ všech regulárních funkcí na uzavřené množině $X \subset A_n$ tvoří $\mathbb{C}$-algebru. Zobrazení $h : \mathbb{C}[t] \to \mathbb{C}[X]$ definované předpisem $(hf)(a) := f(a)$ $(a \in X)$ je homomorfismus algebry $\mathbb{C}[t]$ na algebru $\mathbb{C}[X]$, přičemž $\mathrm{Ker}(h) \cong I(X)$, tedy h indukuje izomorfismus $\mathbb{C}$-algeber: $\mathbb{C}[X] \cong \mathbb{C}[t]/I(X)$.*

Navíc je $\mathbb{C}[X]$ noetherovský okruh.

Důkaz. Snadné užití definic a předchozích výsledků. $\square$

Příklad 7.4. Mějme $X = \{a\} \subset A_n$. Zobrazení

$$\begin{aligned} \mathbb{C}[X] &\to \mathbb{C}, \\ r &\mapsto r(a), \end{aligned}$$

je izomorfismem $\mathbb{C}[X] \cong \mathbb{C}$.

Příklad 7.5. $X := A_n$. Zřejmě $\mathbb{C}[X] \cong \mathbb{C}[t]$.

Příklad 7.6. Buď $X \subset A_2/_{\mathbb{C}}$ nadplocha (křivka). $I := \langle f(t_1, t_2) \rangle = \langle t_1 t_2 - 1 \rangle$. Množina $X \cap A_2/_{\mathbb{R}}$ je hyperbola. Dokážeme, že polynom $t_1 t_2 - 1$ je irreducibilní.

Předpokládejme, že $t_1 t_2 - 1 = p_1 \cdot p_2$, kde p_1, p_2 jsou nekonstantní polynomy. Pokud $p_1 = a_2 t_2 + a_1 t_1 + a_0$, $p_2 = b_2 t_2 + b_1 t_1 + b_0$, je $a_1 b_1 = 0 = a_2 b_2$, tzn. nastává jeden z následujících případů:

(1) $a_1 = 0 = a_2$,
(2) $a_1 = 0 = b_2$,
(3) $a_2 = 0 = b_1$,
(4) $b_1 = 0 = b_2$.

Případy (1) a (4) nemohou nastat (polynom p_1 nebo p_2 by byl konstantní). Uvažujme případ (2): $t_1 t_2 - 1 = (a_1 t_1 + a_0)(b_2 t_2 + b_0)$, kde $a_1 \neq 0$, $b_2 \neq 0$. Odtud $a_1 b_0 = 0 = a_0 b_2$, a tedy $a_0 = 0 = b_0$ ve sporu s $a_0 b_0 = -1$. Podobně dokážeme, že nenastane případ (3). Tedy polynom $t_1 t_2 - 1$ je nerozložitelný, tj. $\langle t_1 t_2 - 1 \rangle$ je prvoideál a platí

$$\sqrt{t_1 t_2 - 1} = t_1 t_2 - 1,$$

jde tedy o radikálový ideál.

Dle předchozí věty $\mathbb{C}[X] \cong \mathbb{C}[t_1, t_2]/\langle t_1 t_2 - 1 \rangle$.

Poznámka 7.7. Regulární funkce $f = t_1$ je invertibilní funkcí na X.

Věta 7.8. *Nechť $X \subset A_m$, $Y \subset A_n$ jsou uzavřené množiny. Potom jsou $\mathbb{C}$-algebry $\mathbb{C}[X \times Y]$ a $\mathbb{C}[X] \otimes \mathbb{C}[Y]$ izomorfní.*

Důkaz. Formule

$$\big(\widetilde{h}(f, g)\big)(a, b) := f(a) g(b),\ f \in \mathbb{C}[X],\ g \in \mathbb{C}[Y],$$

definuje bilineární zobrazení $\widetilde{h} : \mathbb{C}[X] \times \mathbb{C}[Y] \to \mathbb{C}[X \times Y]$ vektorových prostorů nad $\mathbb{C}$. Dle definice tenzorového součinu $\widetilde{h}$ indukuje lineární zobrazení komplexních vektorových prostorů

$$\begin{aligned} &h : \mathbb{C}[X] \otimes \mathbb{C}[Y] \to \mathbb{C}[X \times Y], \\ &\big(h(f \otimes g)\big)(a, b) = f(a)g(b). \end{aligned}$$

Pak

$$\begin{aligned} \Big(h\big((f_1 \otimes g_1)(f_2 \otimes g_2)\big)\Big)(a, b) &= \big(h(f_1 f_2 \otimes g_1 g_2)\big)(a, b) \\ &= f_1(a) f_2(a) g_1(b) g_2(b) \\ &= \big(h(f_1 \otimes g_1)\big)(a, b)\big(h(f_2 \otimes g_2)\big)(a, b) \\ &= \big(h(f_1 \otimes g_1) h(f_2 \otimes g_2)\big)(a, b), \end{aligned}$$

tedy h je homomorfismus algeber. Je to epimorfismus, neboť funkce na $X \times Y$ jsou určeny polynomy v proměnných $\{t, u\} = \{t_1, \ldots, t_m, u_1, \ldots, u_n\}$.

Ukážeme, že h je monomorfismem. Buď $x \in \mathbb{C}[X] \otimes \mathbb{C}[Y]$ tak, že $h(x) = 0$. Prvek x má tvar $\sum_{i,j=1}^{k,l} c_{i,j} f_i \otimes g_j$, kde f_i $(i \in \mathbb{N})$ a g_j $(j \in \mathbb{N})$ jsou lineárně nezávislé prvky $\mathbb{C}[X]$, resp. $\mathbb{C}[Y]$. Pro libovolné $a \in X$, $b \in Y$ je $h(x)(a, b) = 0$, tedy

$$\begin{aligned} \sum_{i,j=1}^{k,l} c_{i,j} f_i(a) g_j(b) = 0, \\ \sum_{i=1}^{k} \left(\sum_{j=1}^{l} c_{i,j} g_j(b) \right) f_i = 0. \end{aligned}$$

Lineární nezávislost $f_1, \ldots, f_k$ dává

$$\sum_{j=1}^{l} c_{i,j} g_j(b) = 0 \ (\forall 1 \le i \le k) \ (\forall b \in Y),$$

odtud $\sum_{j=1}^{l} c_{i,j} g_j = 0$, a protože g_j jsou lineárně nezávislé, je $c_{i,j} = 0$ $(\forall i, j)$. Tedy $x = 0$. $\square$

Poznámka 7.9. Jako důsledek této věty lze ukázat, že pro uzavřené množiny $X \subset A_m$, $Y \subset A_n$ platí

$$I(X \times Y) = \big(I(X) \otimes \mathbb{C}[t] + \mathbb{C}[u] \otimes I(Y)\big),$$

kde $I(X) \otimes \mathbb{C}[t]$ a $\mathbb{C}[u] \otimes I(Y)$ chápeme jako ideály v $\mathbb{C}[u] \otimes \mathbb{C}[t] \cong \mathbb{C}[u, t]$.

Definice 7.10. Mějme uzavřené množiny $X \subset A_m$, $Y \subset A_n$. Zobrazení $\Phi : X \to Y$ se nazývá *regulární*, jestliže existují regulární funkce $r_1, \ldots, r_n \in \mathbb{C}[X]$ takové, že $(\forall a \in X)$ $\Phi(a) = \big(r_1(a), \ldots, r_n(a)\big)$.

Příklad 7.11. Každá regulární funkce $r : X \to \mathbb{C}$ je regulárním zobrazením X do $Y = A_1 \equiv \mathbb{C}$.

Příklad 7.12. Každé afinní zobrazení $\Phi : X = A_m \to Y = A_n$ je regulárním zobrazením, neboť $\Phi(a) = (\Phi_1(a), \dots, \Phi_n(a))$, kde $(\forall 1 \leq i \leq n)$ Φ_i je lineární funkce (např. tedy $id : X \to X$ je regulární zobrazení).

Příklad 7.13. Buď $X \subset A_n$ určená $I(X) = \langle t_1 t_2 - 1 \rangle$. Pro $Y = A_1$ definujme $\Phi : X \to Y$ předpisem $\Phi(a_1, a_2) := a_1$. Označíme-li $r = t_1$ regulární funkci na X, platí $\Phi(a_1, a_2) = r(a_1, a_2)$, tedy zobrazení Φ je regulární.

Příklad 7.14. Buď $X \subset A_n$ křivka, $I(X) = \langle t_2 - t_1^2 \rangle$. Pro $Y = A_1$ definujme $\Phi : X \to Y$ předpisem $\Phi(a_1, a_2) := a_1$. Jde opět o regulární zobrazení.

Příklad 7.15. Pro $X = A_1$ buď $Y \subset A_2$ křivka $t_2^2 - t_1^3 = 0$. Definujme zobrazení $\Phi(a) := (a^2, a^3)$. Protože $r_1(a) = a^2$, $r_2(a) = a^3$ jsou polynomy na X, je Φ regulární zobrazení.

Každé regulární zobrazení $\Phi : X \to Y$ uzavřených množin $X \subset A_m$, $Y \subset A_n$ indukuje homomorfismus

$$\begin{aligned} &\Phi^* : \mathbb{C}[Y] \to \mathbb{C}[X], \\ &\quad \Phi^*(s) := s \circ \Phi \ (\forall s \in \mathbb{C}[Y]), \end{aligned}$$

neboť pro $\Phi(a) = (r_1(a), \dots, r_n(a))$, kde $r_1, \dots, r_n$ jsou polynomy z $\mathbb{C}[t_1, \dots, t_m]$, je $r_1, \dots, r_n \in \mathbb{C}[X]$. Pro polynom (tedy regulární funkci na Y) $s \in \mathbb{C}[Y]$ je

$$(s \circ \Phi)(a) = s(\Phi(a)) = s(r_1(a), \dots, r_n(a)),$$

tj. funkce $s \circ \Phi$ je určena polynomem $s(r_1, \dots, r_n) \in \mathbb{C}[t_1, \dots, t_n]$, je tedy regulární.

Věta 7.16. *Nechť jsou $X \subset A_m$, $Y \subset A_n$ uzavřené množiny, $\rho : \mathbb{C}[Y] \to \mathbb{C}[X]$ libovolný homomorfismus algeber. Pak existuje jediné regulární zobrazení $\Phi : X \to Y$ tak, že $\Phi^* = \rho$.*

Důkaz. Nechť jsou $s_1, \dots, s_n$ regulární funkce na Y určené polynomy $u_1, \dots, u_n \in \mathbb{C}[u]$. Definujme $r_i := \rho(s_i)$ $(\forall 1 \leq i \leq n)$ a regulární zobrazení $\Phi : X \to A_n$ předpisem $\Phi(a) := (r_1(a), \dots, r_n(a))$. Ukážeme, že $(\forall a \in X)$ $\Phi(a) \in Y$. Buď tedy $g \in I(Y)$ libovolný polynom, $a \in X$. Je pak

$$\begin{aligned} g(\Phi(a)) = g(r_1(a), \dots, r_n(a)) = (g(r_1, \dots, r_n))(a) = \\ = (g(\rho s_1, \dots, \rho s_n))(a) = (\rho(g(s_1, \dots, s_n)))(a) = (\rho\emptyset)(a) = 0, \end{aligned}$$

neboť ρ je homomorfismus algeber a g je polynom (tedy $[\rho, g] = 0$). Dále $(\forall b \in Y)$ je $\big(g(s_1, \dots, s_n)\big)(b) = g(s_1(b), \dots, s_n(b)) = g(b_1, \dots, b_n) = 0$, tj. $g(s_1, \dots, s_n) = 0$ $(\forall g \in I(X))$.

Dokázali jsme tak, že $\Phi(a) \in Y$.

Buď $s \in \mathbb{C}[Y]$ libovolná regulární funkce, $g \in \mathbb{C}[u]$ polynom generující s. Pro každé $b \in Y$ platí:

$$\big(g(s_1, \dots, s_n)\big)(b) = g(s_1(b), \dots, s_n(b)) = g(b_1, \dots, b_n) = s(b),$$

neboli $g(s_1, \dots, s_n) = s$. Potom

$$\begin{aligned} \big(\Phi^*(s)\big)(a) = s(\Phi(a)) = s(r_1(a), \dots, r_n(a)) = \\ = g(r_1(a), \dots, r_n(a)) = (g(r_1, \dots, r_n))(a) = (g(\rho s_1, \dots, \rho s_n))(a) = \\ = (\rho(g(s_1, \dots, s_n)))(a) = (\rho(s))(a), \end{aligned}$$

tj. $\Phi^* = \rho$.

Ukážeme jednoznačnost regulárního zobrazení Φ. Předpokládejme, že Φ, Φ' : $X \to Y$ jsou dvě regulární zobrazení, $\Phi^* = \Phi'^* = \rho$. Nechť

$$\Phi(a) = (r_1(a), \dots, r_n(a)),$$
$$\Phi'(a) = (r'_1(a), \dots, r'_n(a)),$$

kde $r_1, \dots, r_n, r'_1, \dots, r'_n \in \mathbb{C}[X]$. Pak $(\forall 1 \leq i \leq n)$

$$\big(\Phi^*(s_i)\big)(a) = s_i(\Phi(a)) = s_i(r_1(a), \dots, r_n(a)) = r_i(a),$$
$$\big(\Phi'^*(s_i)\big)(a) = s_i(\Phi'(a)) = s_i(r'_1(a), \dots, r'_n(a)) = r'_i(a).$$

Protože však $\Phi^* = \Phi'^*$, je $r_i = r'_i$ $(\forall 1 \leq i \leq n)$, a tedy $\Phi = \Phi'$. $\square$

Podobně se dokáže

Věta 7.17. *Nechť jsou $X \subset A_m$, $Y \subset A_n$, $Z \subset A_k$ uzavřené množiny, $\Phi : X \to Y$, $\Psi : Y \to Z$ regulární zobrazení. Pak $\Psi \circ \Phi : X \to Z$ je regulární zobrazení a $(\Psi \circ \Phi)^* = \Phi^* \circ \Psi^*$.*

Definice 7.18. Mějme uzavřené množiny $X \subset A_m$, $Y \subset A_n$. Regulární zobrazení $\Phi : X \to Y$ je *izomorfismus*, pokud existuje regulární zobrazení $\Psi : Y \to X$ takové, že $\Psi \circ \Phi = id_X$ a $\Phi \circ \Psi = id_Y$.

Příklad 7.19. Připomeňme příklad $I(X) = \langle t_2 - t_1^2 \rangle$ v A_2, $Y = A_1$ a regulární zobrazení

$$\Phi : X \to Y,$$
$$(a_1, a_2) \mapsto a_1.$$

Inverzní zobrazení

$$\Psi : Y \to X,$$
$$a \mapsto (a, a^2),$$

je zřejmě regulární, tedy Φ je izomorfismus.

(Důkaz, že se jedná o inverzi:

$$\Psi \circ \Phi : (a_1, a_2) \mapsto a_1 \mapsto (a_1, a_1^2) = (a_1, a_2),$$
$$\Phi \circ \Psi : a \mapsto (a, a^2) \mapsto a.)$$

Příklad 7.20. Regulární zobrazení

$$\Phi : A_1 \to A_2,$$
$$a \mapsto (a^2, a^3),$$

není izomorfismus. Předpokládejme, že existuje inverzní regulární zobrazení Ψ : $Y \to A_1$ existuje. Pak najdeme polynom $f \in \mathbb{C}[t_1, t_2]$ takový, že $\Psi(b) = f(b)$ $(\forall b \in Y)$. Platí tedy:

$$a = \Psi \circ \Phi(a) = \Psi(a^2, a^3) = f(a^2, a^3) \ (\forall a \in A_1).$$

Takový polynom v proměnných a^2, a^3 neexistuje – spor. Inverzní zobrazení tedy není regulární (v příští lekci najdeme racionální zobrazení Ψ inverzní k Φ).

8. Racionální funkce na afinních varietách

Buď $X \subset A_n/_{\mathbb{C}}$ varieta. Víme, že algebra regulárních funkcí $\mathbb{C}[X]$ je oborem integrity, lze tedy vytvořit podílové těleso. Označme ho $\mathbb{C}(X)$.

Definice 8.1. Těleso $\mathbb{C}(X)$ nazýváme *tělesem racionálních funkcí na varietě* X. Jeho prvky se nazývají *racionální funkce na varietě* X.

Poznámka 8.2. Regulární funkce jsou zobrazení $X \to \mathbb{C}$, racionální funkce pak zobrazení $X \to \mathbb{P}^1/_{\mathbb{C}}$. Prvek $f \in \mathbb{C}$ je třída ekvivalence $(r, s) \in \mathbb{C}[X] \times \mathbb{C}[X]$, kterou zapisujeme ve tvaru $f = \frac{r}{s}$.

Alternativní konstrukce $\mathbb{C}(X)$.

$I(X) \subset \mathbb{C}[t]$ je prvoideál (X je varieta); lokalizujme $\mathbb{C}[t]$ vzhledem k ideálu $I(X)$. Výsledkem je algebra $O_X := \mathbb{C}[t]_{I(X)}$, jejíž prvky jsou třídy ekvivalence dvojic (f, g), kde f, $g \in \mathbb{C}[t]$, $g \notin I(X)$. Připomeňme, že $(f_1, g_1) \sim (f_2, g_2)$, právě když $f_1g_2 - f_2g_1 \in I(X)$.

V lokální algebře O_X existuje jediný maximální ideál I_X – ten je generován všemi prvky $\frac{f}{g} \in O_X$ takovými, že $f \in I(X)$. Definujme přirozený homomorfismus algeber $h : O_X \to \mathbb{C}(X)$ následovně. Buď $\xi \in O_X$, $\xi = \frac{f}{g}$, f, $g \in \mathbb{C}[t]$, $g \notin I(X)$. Nechť jsou r, $s \in \mathbb{C}[X]$ regulární funkce určené polynomy f, g. Definujme $h(\xi) := \frac{r}{s}$ (protože $g \notin I(X)$, je $s \neq 0$).

Tento předpis nezávisí na volbě prvků tříd ekvivalence: pokud $\frac{f}{g} = \xi = \frac{f'}{g'}$, je $(f, g) \sim (f', g')$, neboť $fg' - f'g \in I(X)$. Označíme-li r', s' třídy určené f', g', je $r' = f' \mod I(X)$, $s' = g' \mod I(X)$, a tedy $rs' - r's = 0$, tj. $\frac{r}{s} = \frac{r'}{s'}$, tudíž $h(\xi)$ nezávisí na výběru reprezentanta.

Zřejmě

- h je homorfismus algeber,
- pokud $\xi \in I_X$, je $h(\xi) = 0$ (pokud $f \in I(X)$, je $r = 0$),
- h je epimorfismus.

Ukážeme, že $\mathrm{Ker}(h) = I_X$: buď $\xi \in O_X$ takové, že $h(\xi) = 0$. Tj. $h(\xi) = \frac{0}{a}$, kde 0 a a jsou regulární funkce (s hodnotou 0, resp. a, všude); rovnost $\frac{r}{s} = \frac{0}{a}$ dává $r \cdot a - 0 \cdot s = 0$, tedy $r = 0$, tzn. $f \in I(X)$ a $\xi = \frac{f}{g} \in I_X$. Je tedy $\mathrm{Ker}(h) = I_X$. Shrneme:

Věta 8.3. *Homomorfismus algeber $h : O_X \to \mathbb{C}(X)$ indukuje izomorfismus $\widetilde{h} : O_X/I_X \to \mathbb{C}(X)$.*

V dalším budeme pomocí $\widetilde{h}$ tyto (faktor)algebry ztotožňovat.

Buď $\alpha \in \mathbb{C}(X)$ racionální funkce, $\alpha = \frac{r}{s}$, kde r, $s \in \mathbb{C}[X]$, nechť $a \in X$. Pokud $s(a) \neq 0$, definujeme hodnotu racionální funkce α v bodě $a \in X$: $\alpha(a) := \frac{r(a)}{s(a)}$. Tato hodnota je dobře definována , neboť pokud $\alpha = \frac{r'}{s'}$, $s'(a) \neq 0$, plyne z $rs' - r's = 0$ rovnost $r(a)s'(a) - r'(a)s(a) = 0$, a tedy $\frac{r(a)}{s'(a)} = \alpha(a) = \frac{r'(a)}{s(a)}$.

Definice 8.4. Buď $\alpha \in \mathbb{C}(X)$ racionální funkce. Řekneme, že $a \in X$ je *regulárním bodem* racionální funkce α, pokud

$$\big(\exists r, s \in \mathbb{C}[X]\big)\ \alpha = \frac{r}{s}\ \ \&\ \ s(a) \neq 0.$$

Je-li $a \in X$ regulární bod racionální funkce α, $\alpha(a)$ je hodnota racionální funkce α v bodě a. Množina všech regulárních bodů je definiční obor funkce α; značíme jej D_α.

Věta 8.5. *Buď $\alpha \in \mathbb{C}(X)$ racionální funkce. Pak D_α je neprázdná, otevřená a hustá podmnožina variety X (v Zariského topologii).*

Důkaz. Nechť $\alpha = \frac{r}{s}$, r, $s \in \mathbb{C}[X]$. Protože $s \neq 0$, existuje alespoň jeden bod $a \in X$ takový, že $s(a) \neq 0$. Bod a je tedy regulárním bodem funkce $\alpha \in \mathbb{C}(X)$, tedy $D_\alpha \neq \emptyset$.

Předpokládejme, že $\alpha = \frac{r_\gamma}{s_\gamma}$, $\gamma \in \Gamma$, jsou všechna možná vyjádření racionální funkce α. Pak

$$X \setminus D_\alpha = \bigcap_{\gamma \in \Gamma} \{a \in X;\ s_\gamma(a) = 0\}$$

platí díky předchozí definici.

Je-li f_γ polynom generující regulární funkci s_γ, pak platí

$$\{a \in X;\ s_\gamma(a) = 0\} = X \cap \{a \in A_n;\ f_\gamma(a) = 0\},$$

tedy je $\{a \in X;\ s_\gamma(a) = 0\}$ uzavřená množina. $X \setminus D_\alpha$ je rovněž uzavřená, tedy D_α je otevřená podmnožina variety X.

Hustotní argument je obsahem následujícího lemmatu. $\square$

Lemma 8.6. *Buď $X \subset A_n$ varieta, $U \subset X$ neprázdná otevřená množina. Pak U je hustá v X.*

Důkaz. Buď $F = X \setminus U$, $\overline{U}$ uzávěr U v X v Zariského topologii. Množiny F, $\overline{U}$ jsou uzavřené v X, X je uzavřená v A_n, tedy F i $\overline{U}$ jsou uzavřené v A_n. Buď $f \in I(\overline{U})$ libovolný polynom. U je neprázdná, tedy existuje $a \in U$ tak, že $a \notin F$. Existuje $g \in I(F)$ takový, že $g(a) \neq 0$. Protože $\overline{U} \cup F = X$, je $f \cdot g \in I(X)$. Protože $g \notin I(X)$, $(g(a) \neq 0)$ a $I(X)$ je prvoideál (X je varieta), je $f \in I(X)$. Je tedy $I(\overline{U}) \subset I(X)$, odtud $X \subset \overline{U}$, tedy $\overline{U} = X$. $\square$

Poznámka 8.7. Zdůrazněme znovu, že pokud X není irreducibilní, $\mathbb{C}[X]$ není obor integrity, a tudíž nelze vytvořit podílové těleso $\mathbb{C}(X)$.

Příklady racionálních funkcí.

(1) $X = A_n$, racionální funkce na A_n je podíl dvou polynomů $\frac{f}{g}$, f, $g \in A_n$.

(2) Buď $X \subset A_n$ varieta. Přirozená inkluze $\mathbb{C}[X] \hookrightarrow \mathbb{C}(X)$ říká, že každá regulární funkce $\alpha \in \mathbb{C}[X]$ je též racionální. Tedy $D_\alpha = X$.

(3) Uvažujme křivku $X \subset A_n$, $I(X) = t_1^2 + t_2^2 - 1$. (X je varieta.) Pro r, $s \in \mathbb{C}[X]$ vyberme $r = 1 - t_2$, $s = t_1$. Pokud $a \in X$ je prvek různý od $(0, -1)$, $(0, 1)$, je $s(a) \neq 0$ a $a \in X$ je regulárním bodem racionální funkce $\alpha = \frac{r}{s}$. Bod $(0, -1)$ není regulárním bodem. (Kdyby jím byl, existovaly by r', $s' \in \mathbb{C}[X]$ tak, že $\alpha = \frac{r'}{s'}$ a $s'(0, -1) \neq 0$. Pak by ovšem $rs' - r's = 0$, odkud $r(0, -1) = 0$ – spor, neboť z definice $r(0, -1) = (1 - t_2)(0, -1) = 2$.)

Bod $(0, 1)$ však regulárním bodem je. Vezměme regulární funkci $r_1 = 1 + t_2$; platí $rr_1 = (1 - t_1)(1 + t_1) = 1 - t_1^2 = t_2^2 = s^2$. Pak $\alpha = \frac{r}{s} = \frac{rr_1}{sr_1} = \frac{s^2}{sr_1} = \frac{s}{r_1}$, a α je regulární v bodě $(0, 1)$, neboť $r_1(0, 1) = 2$. Je tedy $D_\alpha = X \setminus \{(0, -1)\}$.

Nechť jsou α, β racionální funkce na X, $c \in \mathbb{C}$. Je-li $a \in X$ regulárním bodem funkce α, pak je regulárním bodem funkce $c\alpha$, kde $c\alpha(a) = c \cdot \alpha(a)$. Je-li a regulárním bodem funkcí α, β, je též regulárním bodem funkcí $\alpha + \beta$ a $\alpha \cdot \beta$. Je-li a regulárním bodem funkce α a $\alpha(a) \neq 0$, je také regulárním bodem funkce $\frac{1}{\alpha}$, přičemž $\left(\frac{1}{\alpha}\right)(a) = \frac{1}{\alpha(a)}$. Je $D_{c\alpha} \supset D_\alpha$ ($D_{c\alpha} = D_\alpha$, je-li $c \neq 0$), $D_{\alpha+\beta} \supset D_\alpha \cap D_\beta$, $D_{\alpha \cdot \beta} \supset D_\alpha \cap D_\beta$, $D_{\frac{1}{\alpha}} \supset D_\alpha \setminus \{a \in X;\ \alpha(a) = 0\}$, tyto inkluze mohou být vlastní.

Jsou-li $\alpha_1, \dots, \alpha_k \in \mathbb{C}(X)$ a je-li $f \in \mathbb{C}[t_1, \dots, t_k]$, pak zřejmě $f(\alpha_1, \dots, \alpha_k)$ je racionální funkce na X, kde $f(\alpha_1, \dots, \alpha_k)(a) = f\big(\alpha_1(a), \dots, \alpha_k(a)\big)$ $(\forall a \in D_{\alpha_1} \cap \dots \cap D_{\alpha_k})$ a $D_{f(\alpha_1,\dots,\alpha_k)} \supset D_{\alpha_1} \cap \dots \cap D_{\alpha_k}$.

Které racionální funkce na X jsou regulární v každém $a \in X$?

Lemma 8.8. *Buď $X \subset A$ uzavřená, $s_1, \dots, s_m \in \mathbb{C}[X]$. Předpokládejme, že neexistuje $a \in X$ tak, aby $s_1(a) = \dots = s_m(a) = 0$. Pak $\langle s_1, \dots, s_m \rangle = \mathbb{C}[X]$.*

Důkaz. Nechť $f_1, \dots, f_m \in \mathbb{C}[t]$, $f_1 = s_1 \mod I(X)$, $\dots$, $f_m = s_m \mod I(X)$. Nechť polynomy $h_1, \dots, h_l \in \mathbb{C}[t]$ generují ideál $I(X)$. Zřejmě neexistuje $a \in A_n$ tak, že $f_1(a) = \dots = f_m(a) = h_1(a) = \dots = h_l(a) = 0$, neboť kdyby takový prvek $a \in A_n$ existoval, bylo by $a \in X$ a navíc by platilo $s_1(a) = \dots = s_m(a) = 0$. Je tedy $\langle f_1, \dots, f_m, h_1, \dots, h_l \rangle = \mathbb{C}[t]$, a tedy $\langle s_1, \dots, s_m \rangle = \mathbb{C}[X]$. $\square$

Věta 8.9. *Buď $X \subset A_n$ varieta, $\alpha \in \mathbb{C}(X)$ racionální funkce. Nechť je každé $a \in X$ regulárním bodem funkce α, tj. $D_\alpha = X$. Pak $\alpha \in \mathbb{C}[X]$, tj. α je regulární funkce na X.*

Důkaz. Buď $a \in X$ libovolný prvek; α je regulární v a, tj. existují $r_a, s_a \in \mathbb{C}[X]$ tak, že $\alpha = \frac{r_a}{s_a}$, $s_a(a) \neq 0$. Vyšetřeme v $\mathbb{C}[X]$ ideál $I_R \subset \mathbb{C}[X]$ generovaný regulárními funkcemi s_a, $a \in X$. Protože $\mathbb{C}[X]$ je noetherovská algebra, ideál S je konečně generovaný, tj. existují $a_1, \dots, a_m \in X$ tak, že $I_R = \langle s_{a_1}, \dots, s_{a_m} \rangle$. Nyní neexistuje bod $a \in X$ tak, aby $s_{a_1}(a) = \dots = s_{a_m}(a) = 0$ (kdyby takový bod existoval, platilo by $(\forall s \in I_R)$ $s(a) = 0$, speciálně $s_a(a) = 0$ – spor). Podle předchozího lemmatu je tedy $I_R = \mathbb{C}[X]$, tj. $1 \in \langle s_{a_1}, \dots, s_{a_m} \rangle$, a existují regulární funkce $f_1, \dots, f_m \in \mathbb{C}[X] \subset \mathbb{C}(X)$ takové, že $1 = \sum_{i=1}^m f_i s_{a_i}$. Z toho plyne

$$\alpha = \alpha \sum_{i=1}^m f_i s_{a_i} = \sum_{i=1}^m \alpha f_i s_{a_i} = \sum_{i=1}^m \frac{r_{a_i}}{s_{a_i}} f_i s_{a_i} = \sum_{i=1}^m f_i r_{a_i},$$

tj. $\alpha \in \mathbb{C}[X]$. $\square$

Kdy je dané těleso K, které je rozšířením tělesa $\mathbb{C}$, izomorfní tělesu racionálních funkcí na nějaké varietě?

Věta 8.10. *Buď K těleso, které je rozšířením tělesa $\mathbb{C}$. Pak existuje $X \subset A_n$ $(n \in \mathbb{N})$ tak, že $K \cong \mathbb{C}(X)$, právě když $[K : \mathbb{C}] < \infty$ (tj. K je konečným rozšířením tělesa $\mathbb{C}$).*

Důkaz. $\Rightarrow$: Je-li X uzavřená množina, je $\mathbb{C}[X]$ konečně generováno. Pokud je X varieta (tj. existuje $\mathbb{C}(X)$), je těleso $\mathbb{C}[X]$ konečně generované nad $\mathbb{C}$.

$\Leftarrow$: Předpokládejme, že je dáno rozšíření K, $[K : \mathbb{C}] < \infty$. Označme $k_1, \dots, k_n \in K$ generátory K nad $\mathbb{C}$. $\mathbb{C}[k_1, \dots, k_n]$ je podalgebra generovaná prvky $k_1, \dots, k_n$; tato podalgebra splňuje podmínky věty..........., tj. existuje uzavřená podmnožina $X \subset A_n/\mathbb{C}$ s vlastností

$$\mathbb{C}[k_1, \dots, k_n] \cong \mathbb{C}[X].$$

$\mathbb{C}[k_1, \dots, k_n]$ je jakožto podalgebra v tělese oborem integrity, množina X je tedy varietou.

$$K \cong \text{ podtělesu tělesa } \mathbb{C}[k_1, \dots, k_n] \cong \text{ podtělesu tělesa } \mathbb{C}[X] = \mathbb{C}(X). \quad \square$$

9. Biracionální zobrazení, biracionální izomorfismus

Definice 9.1. Buď $X \subset A_m$ varieta, $Y \subset A_n$ uzavřená množina. Zobrazení $\varphi : X \to Y$ se nazývá *racionální zobrazení*, pokud existují racionální funkce $\alpha_1, \dots, \alpha_n \in \mathbb{C}(X)$ tak, že

(i) $D_\varphi = D_{\alpha_1} \cap \dots \cap D_{\alpha_n}$,
(ii) $(\forall a \in D_\varphi)\ \varphi(a) = \big(\alpha_1(a), \dots, \alpha_k(a)\big)$.

Poznámka 9.2. Zopakujme, že racionální zobrazení nemusí být definováno na celé varietě X (tzn. $D_\varphi \subsetneq X$).

Pro varietu $X \subset A_m$ a neprázdné otevřené množiny $U_1, \dots, U_n \subset X$ je $U_1 \cap \dots \cap U_n$ hustá otevřená podmnožina X. Pak ihned z předchozí definice plyne

Věta 9.3. *Buď $\varphi : X \to Y$ racionální zobrazení. Pak $D_\varphi \subset X$ je neprázdná hustá otevřená podmnožina. Je-li $D_\varphi = X$, je $\varphi \in \mathbb{C}[X]$ regulární zobrazení.*

Příklady racionálních zobrazení.

Příklad 9.4. Pro $\alpha \in \mathbb{C}(X)$ definujme $\varphi : X \to A_1$ tak, že $D_\varphi = D_\alpha$ a $(\forall a \in D_\varphi)$ $\varphi(a) = \alpha(a)$. Z definice plyne, že φ je racionální zobrazení. Tedy každá racionální funkce je racionálním zobrazením do A_1.

Příklad 9.5. Připomeňme příklad křivky $X \subset A_2$ dané rovnicí $t_1 t_2 - 1 = 0$ s regulárním zobrazením $\Phi : X \to A_1$, $\Phi(a_1, a_2) = a_1$.

Platí: $D_{\Phi^{-1}} = A_1 \setminus \{0\}$, pro každé $a \in D_{\Phi^{-1}}$ je $\Phi^{-1}(a) = \big(a, \frac{1}{a}\big)$, přičemž bylo ukázáno, že zobrazení není regulární. Ukážeme však, že Φ^{-1} je racionální (A_1 je varieta). Buď $r \in \mathbb{C}[A_1]$ regulární funkce určená polynomem $t \in \mathbb{C}[t]$. Pro $\alpha_1 = r$, $\alpha_2 = \frac{1}{r}$ je $D_{\alpha_1} = A_1$, $D_{\alpha_2} = A_1 \setminus \{0\}$, tj. $D_\alpha = D_{\alpha_1} \cap D_{\alpha_2} = A_1 \setminus \{0\} = D_{\Phi^{-1}}$. Pro každé $a \in D_{\Phi^{-1}}$ je

$$\big(\alpha_1(a), \alpha_2(a)\big) = \Big(r(a), \frac{1}{r(a)}\Big) = \Big(a, \frac{1}{a}\Big) = \Phi^{-1}(a)$$

a Φ^{-1} je racionální zobrazení.

Příklad 9.6. Připomeňme příklad křivky $Y \subset A_2$ dané rovnicí $t_2^2 - t_1^3 = 0$ s regulárním zobrazením

$$\begin{aligned} A_1 &\to Y, \\ a &\mapsto \big(a^2, a^3\big). \end{aligned}$$

Inverzní zobrazení splňuje $D_{\Phi^{-1}} = Y$, kde

$$\begin{aligned} \Phi^{-1}(a_1, a_2) &= \frac{a_2}{a_1} \text{ pro } (a_1, a_2) \in Y,\ (a_1, a_2) \neq (0,0), \\ \Phi^{-1}(0,0) &= 0. \end{aligned}$$

Dále jsme ukázali, že zobrazení Φ^{-1} není regulární. Není ani racionální, neboť jeho definiční obor $D_{\Phi^{-1}}$ je celá varieta Y, a tedy Φ^{-1} by muselo být regulární.

Definujme zobrazení $\Psi(a_1, a_2) = \Phi^{-1}(a_1, a_2)$ s $D_\Psi = Y \setminus \{(0,0)\}$. Ukážeme, že Ψ je racionální. Mějme funkce r, $s \in \mathbb{C}[Y]$ určené polynomy t_1, $t_2 \in \mathbb{C}[t_1, t_2]$ a položme $\alpha = \frac{r}{s}$. Je patrné, že každý prvek $(a_1, a_2) \in Y$, $(a_1, a_2) \neq (0,0)$, je regulárním bodem funkce α. Ukážeme sporem, že $(a_1, a_2) = (0, 0)$ není regulárním bodem funkce α.

Předpokládejme, že $(0, 0)$ je regulárním bodem racionální funkce α. Tj. existují r', $s' \in \mathbb{C}[Y]$ tak, že $rs' - r's = 0$ a $s'(0, 0) \neq 0$. Pro f, $g \in \mathbb{C}[t_1, t_2]$, $r' = f \mod I(Y)$, $s' = g \mod I(Y)$, je

$$t_2 g(t_1, t_2) - t_1 f(t_1, t_2) \in I(Y).$$

Protože $\forall t \in A_1$ je $\left(t^2, t^3\right) = \Phi(t) \in Y$, je

$$t^3 g(t^2, t^3) - t^2 f(t^2, t^3) = 0,$$

tj. $tg(t^2, t^3) = f(t^2, t^3)$. Vidíme, že f nemůže mít absolutní člen, tj. $f = f(t^2, t^3)$ obsahuje monomy stupně alespoň 2. Polynom $g \in \mathbb{C}[t_1, t_2]$ má nulový člen, neboť $g(0, 0) = s'(0, 0) \neq 0$. Polynom $tg(t^2, t^3)$ má nenulový lineární člen, tj. rovnost $tg(t^2, t^3) = f(t^2, t^3)$ nemůže platit, což je spor.

Je tedy $D_\alpha = D_\Psi$. Pro libovolné $(a_1, a_2) \neq (0, 0)$ $((a_1, a_2) \in D_\alpha)$ je

$$\alpha(a_1, a_2) = \frac{r(a_1, a_2)}{s(a_1, a_2)} = \frac{a_2}{a_1} = \Phi^{-1}(a_1, a_2).$$

Problém. Buď $\varphi : X \to Y$ racionální zobrazení. Jsou potom racionální funkce $\alpha_1, \ldots, \alpha_n \in \mathbb{C}(X)$ takové, že $D_\varphi = D_{\alpha_1} \cap \cdots \cap D_{\alpha_n}$, $\varphi(a) = (\alpha_1(a), \ldots, \alpha_n(a))$ $(\forall a \in D_\varphi)$, určeny jednoznačně? Zhruba řečeno, je odpověď stejná jako v případě regulárních funkcí, tedy: ano.

Lemma 9.7. *Nechť je α, $\alpha' \in \mathbb{C}(X)$, $X \subset A_m$. Buď $U \subset D_\alpha \cap D_{\alpha'}$ neprázná otevřená podmnožina (tedy hustá v Zariského topologii) taková, že $(\forall a \in U)$ $\alpha(a) = \alpha'(a)$. Pak $\alpha = \alpha'$.*

Důkaz. Pro $\beta = \alpha - \alpha'$ je $\beta(a) = 0$ $(\forall a \in U)$. Lze psát $\beta = \frac{r}{s}$, kde r, $s \in \mathbb{C}[X]$, $s \neq 0$. Množina $F := \{a \in X;\ s(a) = 0\}$ je uzavřená v X, neboť pro libovolný $g \in \mathbb{C}[t]$, $s = g \mod I(X)$, platí $F = \{a \in A_m;\ f(a) = 0\} \cap X$. Množina $V := X \setminus F$ je otevřená v X a, protože $s \neq 0$, je $V \neq \emptyset$. Je tedy také $W = U \cap V$ otevřená neprázdná (a tedy hustá) podmnožina X.

Pro každé $a \in W \subset X$ je $\frac{r(a)}{s(a)} = 0$, a tedy $r(a) = 0$. Označme $G := \{a \in X;\ r(a) = 0\}$. Podobně jako F je i G uzavřená v X, navíc (z definice) $W \subset G$. Odtud $X = \overline{W} \subset \overline{G} = G \subset X$, tedy $G = X$, tedy $r(a) = 0$ $(\forall a \in X)$. Odtud $r = 0$, to znamená $\beta = 0$ a $\alpha = \alpha'$. $\square$

Věta 9.8. *Buď $\varphi : X \to Y$ racionální zobrazení a $\alpha_1, \ldots, \alpha_n$, $\alpha'_1, \ldots, \alpha'_n \in \mathbb{C}(X)$ takové, že*

$$D_\varphi = D_{\alpha_1} \cap \cdots \cap D_{\alpha_n} = D_{\alpha'_1} \cap \cdots \cap D_{\alpha'_n}$$

a $(\forall a \in D_\varphi)$ platí

$$\varphi(a) = \big(\alpha_1(a), \ldots, \alpha_n(a)\big) = \big(\alpha'_1(a), \ldots, \alpha'_n(a)\big).$$

Pak $\alpha_i = \alpha'_i$ $(\forall i \in \{1, \ldots, n\})$.

Důkaz. Buď $1 \leq i \leq n$. Pro každé $a \in D_\varphi \subset D_{\alpha_i} \cap D_{\alpha'_i}$ platí $\alpha_i(a) = \alpha'_i(a)$. Přitom množina D_φ je neprázdná otevřená. Užitím předchozího lemmatu je $\alpha_i = \alpha'_i$. $\square$

Tyto (jednoznačně určené) racionální funkce $\alpha_1, \ldots, \alpha_n \in \mathbb{C}(X)$ nazýváme *složkami racionálního zobrazení* $\varphi : X \to Y$.

Problém. Buď $X \subset A_m$, $\varphi : X \to A_n$ racionální zobrazení. Je-li dána uzavřená podmnožina $Y \subset A_n$, lze zjistit, zda obraz $\varphi[X] \subset Y$ $(\subset A_n)$?

Věta 9.9. *Buď $X \subset A_m$, $\varphi : X \to A_n$ racionální zobrazení se složkami $\alpha_1, \dots, \alpha_n$. Pak φ zobrazuje X do uzavřené množiny $Y \subset A_n$, právě když $\forall f \in I(Y) \subset \mathbb{C}[A_n]$ platí $f(\alpha_1, \dots, \alpha_n) = 0$.*

Důkaz. $\Rightarrow$: Nechť $\varphi : X \to Y$ a $f \in I(Y)$ je libovolný polynom. Pak pro každé $a \in D_\varphi$ platí $f\big(\alpha_1(a), \dots, \alpha_n(a)\big) = f\big(\alpha_1, \dots, \alpha_n\big)(a) = 0$. Hodnoty nulové racionální funkce a racionální funkce $f\big(\alpha_1, \dots, \alpha_n\big)$ jsou stejné na neprázdné otevřené (a tedy husté) podmnožině $D_\varphi \subset X$. Podle výše dokázaného lemmatu platí $f\big(\alpha_1, \dots, \alpha_n\big) = 0$.

$\Leftarrow$: Předpokládejme, že pro každé $f \in I(Y)$ platí $f\big(\alpha_1, \dots, \alpha_n\big) = 0$. Pak $\forall a \in D_\varphi$

$$f\big(\alpha_1(a), \dots, \alpha_n(a)\big) = f\big(\alpha_1, \dots, \alpha_n\big)(a) = 0,$$

tedy φ je zobrazení z X do Y. $\square$

Předpokládejme, že $\varphi : X \to Y$, kde $Y \subset A_n$ je varieta. Podobně jako jsme definovali homomorfismus algeber $\Phi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$, $f \mapsto f \circ \Phi$, budeme definovat pro racionální zobrazení homomorfismus těles $\varphi^* : \mathbb{C}(Y) \to \mathbb{C}(X)$.

Protože homomorfismy těles jsou vždy monomorfismy, jsou možnosti pro φ indukující φ^* omezenější (např. problémy nastávají již v případě, kdy $\Phi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ není monomorfismem, a nedá se tudíž rozšířit na homomorfismus $\varphi^* : \mathbb{C}(Y) \to \mathbb{C}(X)$).

Uvažujme regulární funkci $r \in \mathbb{C}[Y]$, $\varphi^*(r) \in \mathbb{C}(X)$. Nechť jsou $\alpha_1, \dots, \alpha_n$ složky racionálního zobrazení φ a $f \in \mathbb{C}[t_1, \dots, t_n]$ polynom generující regulární funkci $r \in \mathbb{C}[Y]$ (tj. $r = f \mod I(Y)$, $Y \subset A_n$). Pak definujeme

$$\varphi^*(r) = f(\alpha_1, \dots, \alpha_n).$$

Tato volba zřejmě nezávisí na výběru polynomu $f \in \mathbb{C}[t_1, \dots, t_n]$, neboť pro $g \in \mathbb{C}[t_1, \dots, t_n]$, $g = r \mod I(Y)$, je $h = g - f \in I(Y)$ a platí $h(\alpha_1, \dots, \alpha_n) = 0$. Dostáváme tedy

$$g(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n) + h(\alpha_1, \dots, \alpha_n) = f(\alpha_1, \dots, \alpha_n).$$

Platí

$$D_{\varphi^*(r)} \supset D_\varphi$$

(pozor – srovnáváme definiční obor racionální funkce na X, tj. $\varphi^*(r)$, s definičním oborem racionálního zobrazení $\varphi : X \to Y$).

Příklad 9.10. Buď $X \subset A_2$ křivka $I(X) = t_2^2 - t_1^3 - t_1^2$. Uvažujme racionální funkci $\alpha = \frac{r}{s} = \frac{t_2}{t_1}$. Racionální funkce dává racionální zobrazení $\varphi = \alpha : X \to A_1$. Je $D_\varphi = D_\alpha = X \setminus \{(0,0)\}$. Buď $r' = t^2$ regulární funkce na A_1 $(r' \in \mathbb{C}[t])$. Pak

$$\varphi^*(r') = \alpha^2 = \left(\frac{r}{s}\right)^2 = \frac{r^2}{s^2} = \frac{s^2 + s^3}{s^2} = s + 1$$

(na X platí $r^2 = s^2 + s^3$).

Zřejmě $D_{\varphi^*(r')} = X$, je tedy $D_{\varphi^*(r')} \supsetneq D_\varphi$.

Definice 9.11. Buď $Y \subset A_n$ varieta. Pro $\alpha \in \mathbb{C}(Y)$ definujme racionální funkci $\varphi^*(\alpha) \in \mathbb{C}(X)$ předpisem

$$\varphi^*(\alpha) := \frac{\varphi^*(r)}{\varphi^*(s)},$$

kde $\alpha = \frac{r}{s}$, r, $s \in \mathbb{C}[Y]$. $\varphi^*(r)$, $\varphi^*(s)$ jsou racionální funkce, tedy podíl chápeme v tělese $\mathbb{C}(X)$.

Poznámka 9.12. Příslušný podíl má smysl, pokud $\varphi^*(s) \neq 0$. Chceme definovat $\varphi^*(\alpha)$ pro všechna $\alpha \in \mathbb{C}(Y)$. Je nutné se omezit na taková zobrazení $\varphi : X \to Y$, pro něž $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}(X)$ je monomorfismus. Tato zobrazení specifikuje následující věta.

Věta 9.13. *Buď $X \subset A_m$ varieta, $Y \subset A_n$ uzavřená množina, $\varphi : X \to Y$ racionální zobrazení. Pak zobrazení $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}(X)$ je monomorfismus, právě když obor hodnot R_φ je hustá podmnožina Y (v Zariského topologii).*

Důkaz. $\Rightarrow$: Předpokládejme, že φ^* je monomorfismus a uvažujme uzávěr $\overline{R_\varphi}$. Buď $f \in I(\overline{R_\varphi})$ libovolný polynom. Pak $(\forall a \in D_\varphi)$ $f\big(\alpha_1(a), \ldots, \alpha_n(a)\big) = 0$, a tedy $f(\alpha_1, \ldots, \alpha_n) = 0$. Označme $r = f \mod I(Y)$, $r \in \mathbb{C}[Y]$, pak $f(\alpha_1, \ldots, \alpha_n) = 0$, ekvivalentně $\varphi^*(r) = 0$. Protože φ^* je monomorfismus, je $r = 0$, a tedy $f \in I(Y)$. Dokázali jsme inkluzi $I(\overline{R_\varphi}) \subset I(Y)$, odkud $\overline{R_\varphi} \supset Y$. Protože ale $\overline{R_\varphi} \subset Y$, platí $\overline{R_\varphi} = Y$, tzn. R_φ je hustá v Y.

$\Leftarrow$: Předpokládejme, že R_φ je hustá v Y. Buď $r \in \mathbb{C}[Y]$ taková, že $\varphi^*(r) = 0$. Přepišme rovnost v ekvivalentním tvaru jako $f(\alpha_1, \ldots, \alpha_n) = 0$, kde $r = f \mod I(Y)$ ($f \in \mathbb{C}[A_n]$ je libovolná). Je $f\big(\alpha_1(a), \ldots, \alpha_n(a)\big) = 0$ ($a \in D_\varphi$), čili $f(b) = 0$ $(\forall b \in R_\varphi)$. To dává $V(\langle f \rangle) \supset R_\varphi$, a protože $V(\langle \varphi \rangle)$ je uzavřená, platí též $V(\langle f \rangle) \supset \overline{R_\varphi} = X$. Je tedy $f \subset I(Y)$, tj. $r = 0$. $\square$

Je-li $\overline{R_\varphi} = Y$, pak homomorfismus $\varphi^* : \mathbb{C}[Y] \to C(X)$ je monomorfismem, a tedy $\frac{\varphi^*(r)}{\varphi^*(s)}$ je definováno pro každé $\alpha = \frac{r}{s} \in \mathbb{C}(Y)$. Navíc, pokud $\frac{r}{s} = \frac{r'}{s'}$, je $rs' - r's = 0$, odtud $\varphi^*(r)\varphi^*(s') - \varphi^*(r')\varphi^*(s) = 0$, neboli

$$\frac{\varphi^*(r)}{\varphi^*(s)} = \frac{\varphi^*(r')}{\varphi^*(s')}.$$

Definice 9.14. Nechť jsou $X \subset A_m$, $Y \subset A_n$ variety, $\varphi : X \to Y$ racionální zobrazení, R_φ je hustá v Y. Definujeme $\varphi^* : \mathbb{C}[Y] \to \mathbb{C}(X)$ předpisem $\varphi^*\big(\frac{r}{s}\big) = \frac{\varphi^*(r)}{\varphi^*(s)}$. Z definice plyne, že $D_{\varphi^*(\alpha)} = \varphi^{-1} D_\alpha$.

Poznámka 9.15. Homomorfismus těles $\varphi : T_1 \to T_2$ je monomorfismus, neboť $\varphi(0) = 0$. Pokud $\exists \alpha \neq 0$ tak, že $\varphi(\alpha) = 0$, pak

$$\varphi(\alpha^n) = \varphi^n(\alpha),$$
$$\varphi(\alpha^{-n}) = \big(\varphi(\alpha^{-1})\big)^n = \Big(\frac{1}{\varphi(\alpha)}\Big)^n.$$

Pro $\alpha > 1$, $n \to \infty$, je $\varphi(\alpha^{-n}) \to \varphi(0) = 0$, avšak $\Big(\frac{1}{\varphi(\alpha)}\Big)^n \to \infty$, což je spor. Pro $\alpha < 1$ je postup analogický. Tedy neexistuje $\alpha \neq 0$ tak, aby $\varphi(\alpha) = 0$, tj. φ je monomorfismus.

Věta 9.16. *Nechť jsou $X \subset A_m$ a $Y \subset A_n$ variety a $\rho : \mathbb{C}(Y) \to \mathbb{C}(X)$ libovolný homomorfismus těles. Pak existuje jediné racionální zobrazení $\varphi : X \to Y$ takové, že $\varphi^* = \rho$.*

Důkaz. Mějme regulární funkce $r_1, \dots, r_n$ na Y určené polynomy $u_1, \dots, u_n \in \mathbb{C}[t_1, \dots, t_n]$. Definujme $\alpha_1 = \rho(r_1)$, $\dots$, $\alpha_n = \rho(r_n)$ (je $\mathbb{C}[Y] \subset \mathbb{C}(Y)$) a buď $\varphi : X \to A_n$ racionální zobrazení se složkami $\alpha_1, \dots, \alpha_n$.

Ukažme, že φ zobrazuje X do Y. Buď $f \in I(Y)$. Z vlastnosti homomorfismu plyne, že

$$f(\alpha_1, \dots, \alpha_n) = f(\rho(r_1), \dots, \rho(r_n)) = \rho(f(r_1, \dots, r_n)).$$

Platí $f(r_1, \dots, r_n) = 0$, neboť $(\forall a \equiv (a_1, \dots, a_n) \in Y)$,

$$f(r_1, \dots, r_n)(a) = f(r_1(a), \dots, r_n(a)) = f(a_1, \dots, a_n) = f(a) = 0.$$

Podle věty .... zobrazuje f X do Y (je $f(\alpha_1, \dots, \alpha_n) = 0$). Ukažme dále, že obraz R_φ racionálního zobrazení φ je hustý v Y. Buď $g \in I(\overline{R_\varphi})$ libovolný. Pak pro každé $a \in D_\varphi$ je $g(\varphi(a)) = 0$, tj. $g(\alpha_1(a), \dots, \alpha_n(a)) = \big(g(\alpha_1, \dots, \alpha_n)\big)(a) = 0$. S použitím lemmatu .... odtud plyne, že $g(\alpha_1, \dots, \alpha_n) = 0$. Tedy

$$0 = g(\alpha_1, \dots, \alpha_n) = g(\rho(r_1), \dots, \rho(r_n)) = \rho(g(r_1, \dots, r_n)).$$

Protože ρ je monomorfismus těles, platí $g(r_1, \dots, r_n) = 0$. Pro každé $a \in Y$ je

$$g(a) = g(a_1, \dots, a_n) = g(r_1(a), \dots, r_n(a)) = \big(g(r_1, \dots, r_n)\big)(a) = 0,$$

tj. $g \in I(Y)$, a tedy $I(\overline{R_\varphi}) \subset I(Y)$. Duálně $\overline{R_\varphi} \supset Y$, tedy $\overline{R_\varphi} = Y$. Z definice homomorfismu φ^* plyne:

$$\begin{aligned} \varphi^*(r_1) &= \alpha_1, \\ &\vdots \\ \varphi^*(r_n) &= \alpha_n. \end{aligned}$$

Buď dále $\alpha = \frac{r}{s} \in \mathbb{C}(Y)$, r, $s \in \mathbb{C}[Y]$.

$$\begin{aligned} \mathbb{C}[u_1, \dots, u_n] &\ni f = r \mod I(Y), \\ \mathbb{C}[u_1, \dots, u_n] &\ni g = s \mod I(Y), \end{aligned}$$

tj. pro $u_i = r_i \mod I(Y)$ je $r = f(r_1, \dots, r_n)$, $s = g(r_1, \dots, r_n)$. Pak

$$\begin{aligned} \varphi^*(\alpha) &= \frac{\varphi^*(r)}{\varphi^*(s)} = \frac{\varphi^*(f(r_1, \dots, r_n))}{\varphi^*(g(r_1, \dots, r_n))} = \frac{f\big(\varphi^*(r_1), \dots, \varphi^*(r_n)\big)}{g\big(\varphi^*(r_1), \dots, \varphi^*(r_n)\big)} = \\ &= \frac{f(\alpha_1, \dots, \alpha_n)}{g(\alpha_1, \dots, \alpha_n)} = \frac{f(\rho(r_1), \dots, \rho(r_n))}{g(\rho(r_1), \dots, \rho(r_n))} = \frac{\rho\big(f(r_1, \dots, r_n)\big)}{\rho\big(g(r_1, \dots, r_n)\big)} = \frac{\rho(r)}{\rho(s)} = \rho(\alpha), \end{aligned}$$

tj. $\varphi^* = \rho$.

Pro dvě racionální zobrazení φ, $\psi : X \to Y$ splňující $\varphi^* = \rho = \psi^*$ platí: pokud $\varphi = (\alpha_1, \dots, \alpha_n)$, $\psi = (\beta_1, \dots, \beta_n)$, pak $(\forall 1 \le i \le n)$ $\alpha_i = \varphi^*(r_i) = \rho r_i = \psi^*(r_i) = \beta_i$. Je tedy $\varphi = \psi$. $\square$

Věta 9.17. *Buď $X \subset A_m$ varieta, $Y \subset A_n$ uzavřená množina, $\varphi : X \to Y$ racionální zobrazení. Pak zobrazení $\varphi : D_\varphi \to Y$ je spojité (na D_φ i na Y uvažujeme Zariského topologii).*

Důkaz. Stačí dokázat, že $\varphi : D_\varphi \to A_n$ je spojité (v Zariského topologii na A_n). Kritériem spojitosti bude to, že vzor uzavřené množiny je uzavřená množina. Buď $Z \subset A_n$ uzavřená. Ukážeme, že její vzor $\varphi^{-1}(Z)$ je uzavřená podmnožina D_φ.

Nechť $Z = V(S)$, $S = \langle f_1, \dots, f_k\rangle \subset \mathbb{C}[u_1, \dots, u_k]$ je ideál. Pak $V(S) = \bigcap_{i=1}^k V\langle f_i\rangle$ $(k < \infty)$ a stačí ukázat, že $(\forall 1 \le i \le k)$ $\varphi^{-1}(V\{f_i\})$ je uzavřená v D_φ. Buď $f \in \mathbb{C}[u_1, \dots, u_n]$ polynom. Ukažme, že $\varphi^{-1}(V\langle f\rangle)$ je uzavřená v D_φ. Nechť $\varphi = (\alpha_1, \dots, \alpha_n)$, pak pro $a \in D_\varphi$ platí

$$a \in \varphi^{-1}(V\langle f\rangle) \Leftrightarrow \big(\alpha_1(a), \dots, \alpha_n(a)\big) \in (V\langle f\rangle)$$
$$\Leftrightarrow f\big(\alpha_1(a), \dots, \alpha_n(a)\big) = 0 \Leftrightarrow \big(f(\alpha_1, \dots, \alpha_n)\big)(a) = 0.$$

Poznamenejme, že $f(\alpha_1, \dots, \alpha_n)$ je racionální funkce na X. Množina $\varphi^{-1}(V\langle f\rangle)$ je uzavřená, právě když $\forall \alpha \in \mathbb{C}(X)$ je $\{a \in D_\alpha;\ \alpha(a) = 0\}$ uzavřená podmnožina D_φ $\big($označíme-li $\alpha \equiv f(\alpha_1, \dots, \alpha_n)$, jelikož $D_\alpha \supset D_\varphi$, je $\varphi^{-1}(V\langle f\rangle) = \{a \in D_\alpha;\ \alpha(a) = 0\} \cap D_\varphi$ uzavřená v $D_\varphi\big)$.

Pro každé $a \in D_\alpha$ vyberme r_a, $s_a \in \mathbb{C}[X]$ tak, že $\alpha = \frac{r_a}{s_a}$, $s_a(a) \neq 0$. Buď $T \subset \mathbb{C}[X]$ ideál generovaný funkcemi s_a pro $a \in D_\alpha$. Pak existují $a^{(1)}, \dots, a^{(l)} \in D_\alpha$ tak, že $T = (s_{a^{(1)}}, \dots, s_{a^{(l)}})$, přičemž (dle věty.....) pro žádné $a \in D_\alpha$ neplatí $s_{a^{(1)}}(a) = \dots = s_{a^{(l)}}(a) = 0$. Navíc $\{a \in X;\ \alpha(a) = 0\} = \{a \in D_\alpha;\ r_{a^{(1)}}(a) = \dots = r_{a^{(l)}}(a) = 0\}$. Je-li

$$g_1 = r_1 \mod I(X),$$
$$\vdots$$
$$g_l = r_l \mod I(X),$$

$g_1, \dots, g_l \in \mathbb{C}[t_1, \dots, t_n]$, pak

$$\{a \in D_\alpha;\ \alpha(a) = 0\} = \{a \in D_\alpha;\ g_1(a) = \dots = g_l(a) = 0\},$$

tj. $\{a \in D_\alpha;\ \alpha(a) = 0\}$ je uzavřená množina (podmnožina D_α). $\square$

Skládání racionálních zobrazení.

Nechť jsou $X \subset A_m$, $Y \subset A_n$ variety, $Z \subset A_p$ uzavřená množina. Mějme racionální zobrazení $\varphi : X \to Y$, $\psi : Y \to Z$. Složené zobrazení X do Z značíme $\psi \circ \varphi$. Protože $D_{\psi\circ\varphi} = \varphi^{-1}(D_\psi)$, je $D_{\psi\circ\varphi}$ otevřená podmnožina D_φ (může být i prázdná!).

Složení racionálních zobrazení nemusí být racionálním zobrazením, např.

Příklad 9.18. Nechť $X = Y = Z = A_1$, $\varphi : X \to Y$, $\psi : Y \to Z$, $\varphi = \frac{1}{t}$, $\psi = \frac{1}{u}$, je pak

$$D_\varphi = R_\varphi = D_\psi = R_\psi = A_1 \setminus \{0\},$$
$$D_{\psi\circ\varphi} = R_{\psi\circ\varphi} = A_1 \setminus \{0\},$$

$(\psi \circ \varphi)(a) = a$ $(\forall a \in A_1 \setminus \{0\})$.

Je-li r regulární (a tudíž racionální) funkce na X určená polynomem $r = t$, je $(\psi \circ \varphi)(a) = r(a)$ $(\forall a \in A_1 \setminus \{0\})$. Pak dle lemmatu..... je $\psi \circ \varphi = r$ na A_1, tj. $D_{\psi\circ\varphi} = D_r = A_1$, což je spor. Tedy $\psi \circ \varphi$ není racionální funkcí.

Shrnutí strategie s uvedením relevantních výsledků.

Předpokládejme, že $D_{\psi\circ\varphi}$ je neprázdná množina. Hledejme racionální zobrazení $\alpha : X \to Z$ takové, že

(i) $D_\alpha \supset D_{\psi\circ\varphi}$,
(ii) $(\forall a \in D_{\psi\circ\varphi})\ \alpha(a) = (\psi \circ \varphi)(a)$.

Takové zobrazení existuje právě jedno, neboť platí

Lemma 9.19. *Nechť jsou Y_0, $Y \subset A_n$ variety, $Y_0 \subset Y$. Buď $\beta \in \mathbb{C}(Y)$ racionální funkce, $D_\beta \cap Y_0 \neq \emptyset$. Pak existuje jediná racionální funkce $\beta_0 \in \mathbb{C}(Y_0)$ taková, že*

(i) $D_{\beta_0} \supset D_\beta \cap Y_0$,
(ii) $(\forall b \in D_\beta \cap Y_0)\ \beta_0(b) = \beta(b)$.

Definice 9.20. Nechť jsou $X \subset A_m$, $Y \subset A_n$ variety. Racionální zobrazení $\varphi : X \to Y$ se nazývá *biracionální izomorfismus*, pokud existuje racionální zobrazení $\psi : Y \to X$ tak, že

(i) $\varphi^{-1}(D_\psi) \neq \emptyset$, $\psi^{-1}(D_\varphi) \neq \emptyset$,
(ii) $\psi \circ \varphi = \mathrm{id}_X$, $\varphi \circ \psi = \mathrm{id}_Y$.

Základní charakteristika biracionálního izomorfismu dává následující větu.

Věta 9.21. *Nechť jsou $X \subset A_m$, $Y \subset A_n$ variety, $\varphi : X \to Y$ racionální zobrazení. Pak φ je biracionální izomorfismus, právě když platí*

(i) $\overline{R_\varphi} = Y$,
(ii) $\varphi^* : \mathbb{C}(Y) \to \mathbb{C}(X)$ *je izomorfismem těles.*

Důkaz. (Nástin některých vlastností): Pokud φ je biracionální izomorfismus, existuje $\psi : Y \to X$ takové, že pro $a \in D_{\psi\circ\varphi}$ (resp. $b \in D_{\varphi\circ\psi}$) je $(\psi \circ \varphi)(a) = a$ (resp. $(\varphi \circ \psi)(b) = b$). Tyto rovnosti říkají ($\varphi : D_{\psi\circ\varphi} \to D_{\varphi\circ\psi}$, resp. $\psi : D_{\varphi\circ\psi} \to D_{\psi\circ\varphi}$ je zobrazení do), že $\varphi/_{D_{\psi\circ\varphi}}$ a $\psi/_{D_{\varphi\circ\psi}}$ jsou navzájem inverzní zobrazení, tj. $(\psi \circ \varphi)(D_{\psi\circ\varphi}) = D_{\psi\circ\varphi}$, a tedy $\varphi(D_{\psi\circ\varphi}) = \psi^{-1}(D_{\psi\circ\varphi})$. Lze pak psát $R_\varphi \supset \varphi(D_{\psi\circ\varphi}) = \psi^{-1}(\varphi^{-1}(D_\psi)) \supset D_{\varphi\circ\psi} = \psi^{-1}(D_\varphi)$. Množina $\psi^{-1}(D_\varphi)$ je neprázdná (dle předpokladu) a je otevřenou podmnožinou Y. Pak ovšem

$$\overline{R_\varphi} \supset \overline{\psi^{-1}(D_\varphi)} = Y,$$

tj. $\overline{R_\varphi} = Y$. Analogicky se ukáže, že $\overline{R_\psi} = X$.

Vlastnost (ii), resp. obrácená implikace, se dokáže obdobně. □

Definice 9.22. Variety $X \subset A_m$, $Y \subset A_n$ jsou *biracionálně izomorfní*, pokud existuje biracionální izomorfismus $\varphi : X \to Y$.

Věta 9.23. *Variety $X \subset A_m$, $Y \subset A_n$ jsou biracionálně izomorfní, právě když existuje izomorfismus těles $\mathbb{C}(X) \to \mathbb{C}(Y)$.*

Příklad 9.24. Zpět ke křivce $X \subset A_2$. Máme $I(X) = \langle t_1t_2 - 1\rangle$ a regulární zobrazení

$$\Phi : X \to Y = A_1,$$
$$(a_1, a_2) \mapsto a_1.$$

$I(X)$ je prvoideál, tzn. X je varieta. Bylo ukázáno, že inverzní zobrazení Φ^{-1} je racionální. Vidíme, že

$$\Phi^{-1}(D_{\Phi^{-1}}) = X \neq \emptyset,$$
$$((\Phi^{-1})^{-1})(D_{\Phi}) = A_1 \setminus \{0\} \neq \emptyset,$$

a tedy existují $\Phi \circ \Phi^{-1}$ a $\Phi^{-1} \circ \Phi$ a pro tato složení platí:

$$\Phi \circ \Phi^{-1}(b) = b \ (\forall b \in A_1 \setminus \{0\}),$$
$$\Phi^{-1} \circ \Phi(a) = a \ (\forall a \in X).$$

(Zde jsou $\Phi \circ \Phi^{-1}$ a $\Phi^{-1} \circ \Phi$ chápána jako racionální zobrazení zkonstruovaná v tomto paragrafu.)

Ukázali jsme, že $\Phi^{-1} \circ \Phi = \mathrm{id}_X$, $\Phi \circ \Phi^{-1} = \mathrm{id}_Y$, a tedy regulární zobrazení je biracionálním izomorfismem.

10. Projektivní uzavřené množiny

Nechť $f \in \mathbb{C}[t_0, \dots, t_n]$, $\mathbf{a} \in \mathcal{P}_n/_{\mathbb{C}}$. Obecně $f(\mathbf{a})$ nemá smysl, neboť f může nabývat různých hodnot pro různé reprezentanty třídy $\mathbf{a}$: pokud $a \in \mathbf{a}$, pak také $\lambda a \in \mathbf{a}$ a může nastat $f(a) \neq f(\lambda a)$ ($f(\lambda a) = \lambda^k f(a)$ pro homogenní polynom stupně k a $\lambda \in \mathbb{C}^\times$).

Definice 10.1. Buď $f \in \mathbb{C}[t] := \mathbb{C}[t_0, \dots, t_n]$, $\mathbf{a} \in \mathcal{P}_n$. Polynom f *se anuluje v bodě* $\mathbf{a}$ (píšeme $f(\mathbf{a}) = 0$), pokud $(\forall a \in \mathbf{a})\ f(a) = 0$.

Buď $f \in \mathbb{C}[t]$ polynom stupně k, $f = \sum_{i=0}^k F_i$, kde F_i je homogenní polynom stupně i (nebo nulový polynom). Tento rozklad je určen jednoznačně; F_i je i-tá homogenní komponenta polynomu f.

Věta 10.2. *Polynom f se anuluje v $\mathbf{a} \in \mathcal{P}_n$, právě když se každá jeho homogenní komponenta anuluje v bodě $\mathbf{a}$.*

Důkaz. $\Leftarrow$: Je-li $F_i(a) = 0$ pro každé $i = 0, \dots, k$, je zřejmě $f(a) = 0$.

$\Rightarrow$: Je-li $f(\mathbf{a}) = 0$, zvolme $a \in \mathbf{a}$. Tedy $0 = f(a) = \sum_{i=0}^k F_i(a)$. Pro každé $\forall \lambda \in \mathbb{C}^\times$ je

$$0 = f(\lambda a) = \sum_{i=0}^k F_i(\lambda a) = \sum_{i=0}^k \lambda^i F_i(a).$$

Polynom $\sum_{i=0}^k F_i(a) x^i$ má nekonečně mnoho kořenů (každé $\lambda \in \mathbb{C}^\times$ je kořenem), tedy je to nulový polynom, tzn. každý z jeho koeficientů $F_i(a)$ je nulový ($\forall i = 0, \dots, k$, $\forall a \in \mathbf{a}$). Odtud $F_i(\mathbf{a}) = 0$ ($\forall i = 0, \dots, k$). $\square$

Pro $S \subset \mathbb{C}[t_0, \dots, t_n]$ definujeme

$$V(S) = \{\mathbf{a} \in \mathcal{P}_n;\ (\forall f \in S)\ f(\mathbf{a}) = 0\}.$$

Definice 10.3. Množiny tvaru $V(S)$, $S \subset \mathbb{C}[t]$, budeme nazývat *projektivními uzavřenými množinami* v $\mathbb{P}_n$. Množinu všech uzavřených množin v $\mathbb{P}_n$ označíme $\widetilde{\mathcal{C}_n}$.

Buď $\bar{S} \subset \mathbb{C}[t]$ podmnožina daná rozšířením S o všechny homogenní komponenty prvků z S. Předchozí věta pak říká, že $V(S) = V(\bar{S})$. Dále $V(\langle \bar{S} \rangle) = V(S)$, kde $\langle \bar{S} \rangle$ je ideál v $\mathbb{C}[t]$ generovaný podmnožinou $\bar{S}$. Lze nahlédnout, že $\langle \bar{S} \rangle$ je homogenní ideál, tj. s každým prvkem obsahuje všechny jeho homogenní komponenty. V dalším se omezíme na homogenní ideály $\langle S \rangle$.

Dle homogenní verze Hilbertovy věty existuje konečný počet homogenních polynomů $F_1, \dots, F_k \in \langle S \rangle$ generujících homogenní ideál $\langle S \rangle \subset \mathbb{C}[t]$, $V(\langle S \rangle) = V(\langle F_1, \dots, F_k \rangle)$. Jinak řečeno, projektivní uzavřená množina $V(\langle S \rangle)$ je určena rovnicemi $F_1 = 0, \dots, F_k = 0$.

Příklad 10.4. Nechť $S = \langle F \rangle$ a $F(t_0, \dots, t_n) = \sum_{i=0}^n c_i t_i$ je homogenní polynom stupně 1. $V(\langle S \rangle)$ je nadrovina v $\mathbb{P}_n$.

Příklad 10.5. Buď $n = 3$ a $S = \langle F_1, F_2, F_3 \rangle$,

$$\begin{aligned} F_1(t_0, t_1, t_2, t_3) &= t_1 t_3 - t_2^2, \\ F_2(t_0, t_1, t_2, t_3) &= t_0 t_2 - t_1^2, \\ F_3(t_0, t_1, t_2, t_3) &= t_0 t_3 - t_1 t_2. \end{aligned}$$

Uzavřená množina $V(\langle S\rangle)$ je křivkou v $\mathbb{P}_3$.

Mnoho pojmů se v příslušné modifikaci přenáší z afinního do projektivního případu. Zastavme se u pojmů, kde překlad není přímočarý. Prvním z nich je analogie izomorfismu $A_m \times A_n \xrightarrow{\simeq} A_{m+n}$, kterému se v projektivním případě $\mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_{(m+1)(n+1)-1}$ říká *Segreho zobrazení.*

Je

$$\mathcal{P}_{(m+1)(n+1)-1} \subset \mathbb{C}^{(m+1)(n+1)} \xrightarrow{\simeq} \mathrm{Mat}_{\mathbb{C}}(m+1, n+1),$$

$$(a_0, \dots, a_{mn+m+n}) \mapsto \begin{pmatrix} a_0 & a_1 & \dots & a_n \\ a_{n+1} & a_{n+2} & \dots & a_{2n+1} \\ \vdots & & \ddots & \vdots \\ a_{mn+m} & a_{mn+m+1} & \dots & a_{mn+m+n} \end{pmatrix}.$$

Pak definujeme

$$\sigma : \mathbb{C}^{m+1} \times \mathbb{C}^{n+1} \xrightarrow{\simeq} \mathbb{C}^{(m+1)(n+1)},$$

$$\sigma\big(a, b\big) = \begin{pmatrix} a_0 b_0 & a_0 b_1 & \dots & a_0 b_{n+1} \\ a_1 b_0 & a_1 b_1 & \dots & a_1 b_{n+1} \\ \vdots & & \ddots & \vdots \\ a_{m+1} b_0 & a_{m+1} b_1 & \dots & a_{m+1} b_{n+1} \end{pmatrix} =: C = (c_{i,j}).$$

Nechť $\mathbf{a} \in (a_0, a_1, \dots, a_{m+1})$, $\mathbf{b} \in (b_0, b_1, \dots, b_{n+1})$. Jsou-li $\mathbf{a} \in \mathcal{P}_m$, $\mathbf{b} \in \mathcal{P}_n$ dva body a je-li $a \in \mathbf{a}$, $b \in \mathbf{b}$, pak definujeme $s(\mathbf{a}, \mathbf{b}) \in \mathcal{P}_{(m+1)(n+1)-1}$ jako jediný bod takový, že $\sigma(a, b) \in s(\mathbf{a}, \mathbf{b})$. Tato definice nezávisí na volbě reprezentantů $\big($tj. $\sigma(\lambda a, \mu b) = (\lambda\mu)\sigma(a, b)\big)$, neboli $s : \mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_{(m+1)(n+1)-1}$ je korektně definované tzv. Segreho zobrazení.

Poznámka 10.6. Topologie na kartézském součinu $\mathcal{P}_m \times \mathcal{P}_n$ je dána uzavřenými množinami generovanými bihomogenními polynomy (stupně (k, l))

$$F(t, u) := \sum_{\substack{k_0 + \dots + k_m = k \\ l_0 + \dots + l_n = l}} C_{k_0, \dots, k_m, l_0, \dots, l_n} t_0^{k_0} \dots t_m^{k_m} u_0^{l_0} \dots u_n^{l_n}.$$

Každý polynom $F \in \mathbb{C}[t, u]$ lze zapsat ve tvaru součtu bihomogenních polynomů (tzv. *bihomogenních komponent*).

$F \in \mathbb{C}[t, u]$ se anuluje v $(\mathbf{a}, \mathbf{b}) \in \mathcal{P}_m \times \mathcal{P}_n$ $(F(\mathbf{a}, \mathbf{b}) = 0)$, pokud $f(a, b) = 0$ $(\forall a \in \mathbf{a}, \forall b \in \mathbf{b})$. Množiny tvaru $V(S) = \{(\mathbf{a}, \mathbf{b}) \in \mathcal{P}_m \times \mathcal{P}_n;\ (\forall F \in S)\ F(\mathbf{a}, \mathbf{b}) = 0\}$ jsou tedy uzavřené pomnožiny $\mathcal{P}_m \times \mathcal{P}_n$.

Bez důkazu uvedeme následující větu.

Věta 10.7. *Segreho zobrazení $s : \mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_{(m+1)(n+1)-1}$ je homeomorfismem topologického prostoru $\mathcal{P}_m \times \mathcal{P}_n$ na uzavřenou podmnožinu $M \subset \mathcal{P}_{(m+1)(n+1)-1}$ (s topologií podprostoru $\mathcal{P}_{(m+1)(n+1)-1}$) tvaru $M = V(S)$, kde $S \subset \mathbb{C}[c_{i,j};\ 0 \le i \le m, 0 \le j \le n]$ je ideál generovaný polynomy $F_{i,j,k,l}$, $0 \le i, k \le m$, $0 \le j, l \le n$,*

$$F_{i,j,k,l}(C) = c_{i,j} c_{k,l} - c_{i,l} c_{k,j}.$$

Přitom jeho základní vlastnosti jsou:

(i) *Jsou-li $M_1 \subset \mathcal{P}_m$, $M_2 \subset \mathcal{P}_n$ uzavřené množiny, pak*

$$s(M_1 \times M_2) \subset \mathcal{P}_{(m+1)(n+1)-1}$$

je uzavřená množina.

(ii) *Jsou-li $M_1 \subset \mathcal{P}_m$, $M_2 \subset \mathcal{P}_n$ nerozložitelné uzavřené množiny, pak uzavřená množina $s(M_1 \times M_2) \subset \mathcal{P}_{(m+1)(n+1)-1}$ je rovněž nerozložitelná.*

Důsledkem těchto dvou vlastností je např. to, že $M \subset \mathcal{P}_{(m+1)(n+1)-1}$ (z předchozí věty) je varieta ($\mathcal{P}_n$ je uzavřená nerozložitelná množina v $\mathbb{P}_n$, totéž pro $\mathcal{P}_m$).

Věta 10.8. *Buď $p_2 : \mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_n$ projekce. Pak p_2 je uzavřené spojité zobrazení.*

Důkaz. Dokážeme spojitost zobrazení p_2: pro každou uzavřenou $M \subset \mathcal{P}_n$ je $p_2^{-1}(M) \subset \mathcal{P}_m \times \mathcal{P}_n$ uzavřená. Nechť jsou $G_1, \dots, G_n \in \mathbb{C}[u]$ homogenní polynomy takové, že $M = V\big(\langle G_1, \dots, G_r\rangle\big)$. Při ztotožnění s bihomogenními polynomy v $\mathbb{C}[t, u]$:

$$\begin{aligned} \mathbb{C}[u] &\to \mathbb{C}[t, u], \\ G_i &\mapsto \hat{G}_i \ (i = 1, \dots, r) \end{aligned}$$

(polynom stupně k přejde na polynom stupně $(0, k)$) je $p_2^{-1}(M) = V\big(\langle \hat{G}_1, \dots, \hat{G}_r\rangle\big)$, tzn. množina $p_2^{-1}(M)$ je uzavřená.

Ukážeme, že zobrazení p_2 je uzavřené: pro každou uzavřenou množinu $N \subset \mathcal{P}_m \times \mathcal{P}_n$ je množina $p_2(N) \subset \mathcal{P}_n$ uzavřená. Nechť jsou tedy $F_1, \dots, F_r \in \mathbb{C}[t, u]$ bihomogenní polynomy takové, že $N = V\big(\langle F_1, \dots, F_r\rangle\big)$. Pak platí ekvivalence

$$\begin{aligned} \mathbf{b} \notin p_2(N) &\Leftrightarrow V\big(\langle F_1(t, b), \dots, F_r(t, b)\rangle\big) = \{\emptyset\} \ (\forall b \in \mathbf{b}) \\ &\Leftrightarrow (\exists k \in \mathbb{N}) \ \langle t_0, \dots, t_m\rangle^k \subset \langle F_1(t, b), \dots, F_r(t, b)\rangle \ (\forall b \in \mathbf{b}). \end{aligned}$$

V poslední ekvivalenci jsme využili tvrzení: Buď I_k k-tá mocnina $\langle t_0, \dots, t_n\rangle^k$ ideálu $\langle t_0, \dots, t_n\rangle \subset \mathbb{C}[t]$. Pak uzavřená množina $V(S)$ je prázdná, právě když $S \supset I_k$ pro nějaké $k \in \mathbb{N}$.

Připomeňme, že podmnožina prostoru $\mathcal{P}_n$ je otevřená (uzavřená), právě když je otevřený (uzavřený) její vzor vzhledem k přirozené projekci $\pi : A_{n+1}^0 \to \mathcal{P}_n$, kde $A_{n+1}^0 = A_{n+1} \setminus \{(0, \dots, 0)\}$ se Zariského topologií podprostoru prostoru A_{n+1}.

Stačí tedy ukázat, že $(\forall k \in \mathbb{N})$ je množina

$$U_k := \big\{b \in A_{k+1}^0;\ \langle t_0, \dots, t_m\rangle^k \subset \langle F_1(t, b), \dots, F_r(t, b)\rangle\big\}$$

otevřená.

Označme (k_i, l_i) bistupeň F_i. Je $\langle t_0, \dots, t_m\rangle^k \subset \langle F_1(t, b), \dots, F_r(t, b)\rangle$, právě když pro každý homogenní polynom $F \in \mathbb{C}[t]$ existují polynomy $g_1, \dots, g_r \in \mathbb{C}[t]$ takové, že $F(t) = \sum_{i=1}^r g_i(t) F(t, b)$. Pak existuje dokonce posloupnost $G_i(t) \in \mathbb{C}[t]_{k-k_i}$ ($\mathbb{C}[t]_j$ je j-tá homogenní komponenta algebry $\mathbb{C}[t]$) takové, že $F(t) = \sum_{i=1}^r G_i(t) F_i(t, b)$. Definujme homomorfismus vektorových prostorů

$$\sigma(b) : \mathbb{C}[t]_{k-k_1} \oplus \dots \oplus \mathbb{C}[t]_{k-k_r} \to \mathbb{C}[t]_k$$

předpisem

$$\big(\sigma(b)\big)(G_1(t), \dots, G_r(t)) = \sum_{i=1}^r G_i(t) F_i(t, b).$$

Předchozí inkluze platí, právě když je $\sigma(b)$ epimorfismus. Jinak řečeno,

$$U_k = \big\{b \in A_{n+1}^0;\ \sigma(b) \text{ je epimorfismus}\big\}.$$

V každém z prostorů $\mathbb{C}[t]_k$, $\mathbb{C}[t]_{k-k_i}$ $(i = 1, \dots, r)$ uvažujeme bazi tvořenou monomy $t^\alpha = t_0^{\alpha_0} \dots t_n^{\alpha_n}$, kde $n = |k - k_i|$. Píšeme-li

$$F_i(t,u) = \sum_{|\alpha(i)|=k_i} F_{\alpha(i)}(u) t^{\alpha(i)}, \; F_{\alpha_i} \in \mathbb{C}[u],$$

lze snadno sestavit matici homomorfismu $\sigma(b)$ vzhledem k bazím t^α. (Pro $t^\alpha \in \mathbb{C}[t]_{k-k_i}$ je $\big(\sigma(b)\big)(t^\alpha) = \sum_{|\alpha(i)|=k_i} F_{\alpha(i)}(b) t^{\alpha(i)+\alpha}$.)

Homomorfismus $\sigma(b)$ je epimorfismem, právě když je alespoň jeden subdeterminant řádu $\dim \mathbb{C}[t]_k$ příslušné matice nenulový. Každý z těchto determinantů je homogenním polynomem vzhledem k $b_0, \dots, b_n$ (= složky bodu b). Přesněji, ke každému subdeterminantu $D(b)$ řádu $\dim \mathbb{C}[t]_k$ matice homomorfismu $\sigma(b)$ existuje $h \in \mathbb{C}[u]$ tak, že $D(b) = h(b)$. Tato rovnost platí pro všechna $b \in A^0_{n+1}$, neboli množina $\{b \in A^0_{n+1};\ D(b) \neq 0\}$ je otevřená v Zariského topologii. Protože U_k je sjednocením množin tohoto tvaru příslušných každému subdeterminantu řádu $\dim \mathbb{C}[t]_k$, znamená to, že U je otevřená. $\square$

Důsledek 10.9. *Jsou-li $M_1 \subset \mathcal{P}_m$, $M_2 \subset \mathcal{P}_n$ uzavřené množiny, $\pi_2 : M_1 \times M_2 \to M_2$ projekce, pak π_2 je spojité uzavřené zobrazení.*

Důkaz. π_2 je restrikcí p_2 na $M_1 \times M_2$. $\square$

Poznámka 10.10. Analogické tvrzení platí pro projekci $p_1 : \mathcal{P}_m \times \mathcal{P}_n \to \mathcal{P}_m$ na první složku.

11. Lokální vlastnosti algebraických variet

Motivace. Buď $M \subset \mathbb{P}_n$ projektivní varieta a $a \in M$ bod. Vlastnost variety M vztahující se k $a \in M$ nazveme *lokální vlastností variety M v bodě a*, pokud je tato vlastnost určena již těmi body variety M, které leží v okolí bodu a (ve smyslu Zariského topologie). Protože pro každé $a \in M$ existuje otevřené okolí U, takové, že $U = M \setminus Z_i$ (pro $0 \leq i \leq n$), kde $M \cap U \subset A_n \subset \mathbb{P}_n$, můžeme se omezit na podvariety afinních prostorů.

V dalším budeme budeme popisovat lokální okruh v daném bodě.

Pro afinní varietu $X \subset A_n$, $a \in X$, definujme

$$\mathcal{O}_{a,X} := \{\alpha \in \mathbb{C}(X);\ \alpha \text{ je regulární v bodě } a \in X\}.$$

Věta 11.1. *$\mathcal{O}_{a,X}$ je podokruh v $\mathbb{C}(X)$. $\mathcal{O}_{a,x}$ obsahuje jediný maximální ideál*

$$M_{a,X} = \{\alpha \in \mathcal{O}_{a,X};\ \alpha(a) = 0\}.$$

Důkaz. Vlastnosti podokruhu jsou zřejmé, je rovněž snadné nahlédnout, že $M_{a,X}$ je ideál v $\mathcal{O}_{a,X}$. Ukažme, že je maximální.

Buď $I \subsetneq \mathcal{O}_{a,X}$ vlastní ideál a předpokládejme, že existuje $\alpha \in I$, $\alpha(a) \neq 0$. Pak lze psát $\alpha = \frac{r}{s}$, $r(a) \neq 0$, $s(a) \neq 0$. Je tedy $\frac{s}{r} \in \mathcal{O}_{a,X}$ a tudíž $1 = \frac{s}{r} \cdot \frac{r}{s} \in I$, což znamená $I = \mathcal{O}_{a,X}$ – spor. Každý vlastní ideál $I \subsetneq \mathcal{O}_{a,X}$ je tedy obsažen v $M_{a,X}$, tj. $M_{a,X}$ je jediný maximální ideál. $\square$

Definice 11.2. Okruh $\mathcal{O}_{a,X}$ nazýváme *lokálním okruhem variety X* v bodě $a \in X$.

Poznámka 11.3. Samozřejmě je $\mathcal{O}_{a,X} \subset \mathbb{C}(X)$ podalgebrou a $M_{a,X}$ je jediný maximální ideál této podalgebry. Ve standardní terminologii je $\mathcal{O}_{a,X}$ nazýván *lokálním okruhem.*

Lokální vlastnost $\mathcal{O}_{a,X}$ plyne z následujícího výsledku.

Definice 11.4. Buď $U \subset X$ otevřená množina, f komplexní funkce definovaná na U (tj. $f : U \to \mathbb{C}$). Řekneme, že f je *regulární racionální funkcí na U*, pokud pro každé $a \in U$ existuje otevřené okolí $V \subset U$ bodu a a r, $s \in \mathbb{C}[X]$ tak, že $f(b) = \frac{r(b)}{s(b)}$ $(\forall b \in V)$.

Věta 11.5. *Buď f regulární racionální funkce definovaná na $U \subset X$. Pak je f na U spojitá.*

($f : U \to \mathbb{C} = A_1/_{\mathbb{C}}$; na U i A_1 uvažujeme Zariského topologii.)

Důkaz. Ukážeme, že pro každou uzavřenou $Y \subset \mathbb{C}$ je $f^{-1}(Y) \subset U$ uzavřená v U. Je-li $Y = \emptyset$ nebo $Y = \mathbb{C}$, je závěr zřejmý. Ostatní uzavřené množiny jsou konečné. Je $f^{-1}(\{b_1, \ldots, b_k\}) = \bigcup_{i=1}^{k} f^{-1}(b_i)$, tedy stačí dokázat, že pro každé $b \in \mathbb{C}$ je $f^{-1}(b)$ uzavřená podmnožina U (neboli $U \setminus f^{-1}(b)$ je otevřená podmnožina U).

Buď $a \in U$ libovolný bod. Pak existuje otevřené okolí $V_a \subset U$ bodu a a r_a, $s_a \in \mathbb{C}[X]$ takové, že

$$(\forall a' \in V_a)\ f(a') = \frac{r_a(a')}{s_a(a')}.$$

Nechť regulární funkce r_a, s_a jsou určeny polynomy g_a, $h_a \in \mathbb{C}[t_1, \ldots, t_n]$. Pak

$$\big(U \setminus f^{-1}(b)\big) \cap V_a = \big\{a' \in A_n;\ g_a(a') - bh_a(a') \neq 0\big\} \cap V_a,$$

což je otevřená podmnožina U. Je pak $U \setminus f^{-1}(b)$ otevřená podmnožina U. $\square$

Regulární funkce na afinní varietě X jsou zřejmě regulárními racionálními funkcemi na X a podle poslední věty jsou na X spojité. Podobně racionální funkce $\alpha \in \mathbb{C}(X)$ je regulární racionální funkcí na svém definičním oboru D_α a dle předchozí věty je rovněž spojitá na X.

Buď $a \in X$. Uvažujme dvojice (U, f), kde

- U je otevřená podmnožina X, $a \in U$,
- f je regulární racionální funkce na U,

s relací ekvivalence

$$(U_1, f_1) \sim (U_2, f_2) \Leftrightarrow (\forall b \in U_1 \cap U_2)\ f_1(b) = f_2(b).$$

Lemma 11.6. *$\sim$ je relací ekvivalence.*

Důkaz. Reflexivita a symetrie je zřejmá.

Dokážeme tranzitivitu. Nechť jsou (U_1, f_1), (U_2, f_2), (U_3, f_3) dvojice takové, že $(U_1, f_1) \sim (U_2, f_2)$ a $(U_2, f_2) \sim (U_3, f_3)$, neboli $f_1(b) = f_2(b)$ $(\forall b \in U_1 \cap U_2)$, $f_2(b) = f_3(b)$ $(\forall b \in U_2 \cap U_3)$. Odtud $f_1(b) = f_3(b)$ $(\forall b \in U_1 \cap U_2 \cap U_3)$. Množina $U_1 \cap U_2 \cap U_3$ je otevřená a neprázdná ($a \in U_1$, $a \in U_2$, $a \in U_3 \Rightarrow a \in U_1 \cap U_2 \cap U_3$), tedy je hustá v X a speciálně v $U_1 \cap U_3$. Regulární racionální funkce f_1 a f_3 jsou spojité na otevřené podmnožině $U_1 \cap U_3$ a jsou si rovny na její husté otevřené podmnožině $U_1 \cap U_2 \cap U_3$, tedy $f_1 = f_3$ na $U_1 \cap U_3$. $\square$

Definice 11.7. Třídu ekvivalence dvojice (U, f) nazýváme *germem (zárodkem)* regulární racionální funkce f v bodě $a \in U$.

Množinu germů označíme $\widetilde{\mathcal{O}_a}$. Lze na ní zavést strukturu okruhu: pokud σ_1, $\sigma_2 \in \widetilde{\mathcal{O}_a}$ a $(U_1, f_1) \in \sigma_1$, $(U_2, f_2) \in \sigma_2$ jsou libovolní reprezentanti σ_1, σ_2, definujeme $\sigma_1 + \sigma_2$ jako třídu obsahující $(U_1 \cap U_2, f_1 + f_2)$, $\sigma_1 \cdot \sigma_2$ jako třídu obsahující $(U_1 \cap U_2, f_1 \cdot f_2)$.

Podobným argumentem jako v předchozím lemmatu zdůvodníme, že definice $\sigma_1 + \sigma_2$, $\sigma_1 \cdot \sigma_2$ nezávisí na volbě prvků v třídách a že $\widetilde{\mathcal{O}_a}$ je okruh.

Věta 11.8. *Okruhy $\mathcal{O}_a$ a $\widetilde{\mathcal{O}_a}$ jsou izomorfní.*

Důkaz. Je-li $\alpha \in \mathcal{O}_a$, pak $a \in D_\alpha$ a lze definovat

$$\rho(\alpha) := [(D_\alpha, \alpha)],$$

kde $[(D_\alpha, \alpha)]$ značí třídu určenou prvkem (D_α, α).

Máme tedy zobrazení $\rho : \mathcal{O}_a \to \widetilde{\mathcal{O}_a}$, které je očividně homomorfismem okruhů. Je-li $\rho(\alpha) = 0$, znamená to, že $\alpha(b) = 0$ $(\forall b \in V)$, kde $V \subset U$ je nějaké otevřené okolí bodu a. Z lemmatu popisujícího jednoznačnost racionální funkce na varietě pak plyne, že $\alpha = 0$, tj. ρ je monomorfismus.

Buď $[(U, f)] \in \widetilde{\mathcal{O}_a}$ libovolný prvek. Existuje otevřené okolí V bodu a a r, $s \in \mathbb{C}[X]$ tak, že $(\forall b \in V)$ $f(b) = \frac{r(b)}{s(b)}$. Uvažujme $\alpha = \frac{r}{s} \in \mathcal{O}_a$. Je $(U, f) \sim (V, \alpha)$, $(V, \alpha) \sim (D_\alpha, \alpha)$, odkud $(U, f) \sim (D_\alpha, \alpha)$, což znamená, že $\rho(\alpha) = [(U, f)]$. Tedy ρ je epimorfismus. $\square$

Konečně slíbené tvrzení:

Věta 11.9. *Okruh $\mathcal{O}_a$ je izomorfní s lokalizací okruhu $\mathbb{C}[X]$ vzhledem k prvoideálu $I_a = \{s \in \mathbb{C}[X];\ s(a) = 0\}$.*

Důkaz. Označme $D_a = \mathbb{C}[X] \backslash I_a$ a definujme zobrazení $\sigma : \mathbb{C}[X]/_{I_a} \to \mathcal{O}_a$ takto: Je-li $[(r,s)] \in \mathbb{C}[X]_{I_a}$ třída určená dvojicí $(r,s) \in \mathbb{C}[X] \times D_a$, definujeme $\sigma\big([(r,s)]\big) = \frac{r}{s}$ (snadno se nahlédne nezávislost $\sigma\big([(r,s)]\big)$ na výběru reprezentanta ve třídě $[(r,s)]$ a to, že σ je homomorfismus okruhů).

Pokud $\sigma\big([(r,s)]\big) = 0$, je $r = 0$, čili $[(r,s)]$ je nulový prvek v $\mathbb{C}[X]_{I_a}$ a σ je monomorfismus.

Je-li $\alpha \in \mathcal{O}_a$, lze psát $\alpha = \frac{r}{s}$, kde $s(a) \neq 0$. Pak $\sigma\big([(r,s)]\big) = \alpha$, což dokazuje, že σ je epimorfismus. $\square$

Příklad 11.10. $X = A_n$, $a \in A_n$. Každá racionální funkce $\alpha \in \mathbb{C}(A_n)$ má tvar $\alpha = \frac{f}{g}$, $f, g \in \mathbb{C}[t_1, \ldots, t_n]$, přičemž $g \not\equiv 0$. Zřejmě $\alpha \in \mathcal{O}_{a,A_n} \Leftrightarrow g(a) \neq 0$.

Věta 11.11. $\bigcup_{a\in X} \mathcal{O}_a = \mathbb{C}(X)$, $\bigcap_{a\in X} \mathcal{O}_a = \mathbb{C}[X]$.

Důkaz. Z definice lokálního okruhu $\mathcal{O}_a$ plyne, že $\bigcup_{a\in X} \mathcal{O}_a \subset \mathbb{C}(X)$. Každá racionální funkce je (z konstrukce) regulární alespoň v jednom bodě $a \in X$. Odtud $\mathbb{C}(X) \subset \bigcup_{a\in X} \mathcal{O}_a$.

Je-li $\alpha \in \bigcap_{a\in X} \mathcal{O}_a$, znamená to, že α je racionální funkce, regulární v každém bodě prostoru X; je pak $\alpha \in \mathbb{C}[X]$. Inkluze $\mathbb{C}[X] \subset \bigcap_{a\in X} \mathcal{O}_a$ je zřejmá. $\square$

Protože $\mathcal{O}_a \subset \mathbb{C}(X)$ jakožto podokruh v tělese, je oborem integrity.

Věta 11.12. *Podílové těleso $\mathcal{F}_a$ oboru integrity $\mathcal{O}_a$ je izomorfní s tělesem $\mathbb{C}(X)$.*

Důkaz. Buď $\alpha \in \mathcal{F}_a$ třída určená dvojicí (r,s). Potom definujeme $\rho(\alpha) \in \mathbb{C}(X)$ předpisem $\rho(\alpha) = \frac{r}{s}$. Opět se lze přesvědčit, že ρ nezávisí na výběru reprezentanta třídy α a že

$$\rho : \mathcal{F}_a \to \mathbb{C}(X)$$

je homomorfismus (a tedy monomorfismus, neboť se jedná o homomorfismus těles).

Buď $\alpha \in \mathbb{C}(X)$ libovolný prvek a pišme $\alpha = \frac{r}{s}$. Je-li t třída určená dvojicí (r,s), pak zřejmě $\rho(t) = \alpha$; ρ je tedy epimorfismus. $\square$

12. Schémata

Mnoho pojmů v této sekci je zobecněním (přímým, ale technicky komplikovaným) pojmu algebraické variety. Výklad proto zúžíme jen na nejnutnější soubor definic a výsledků.

Topologický prostor Spec(R).

Pro uzavřenou afinní množinu $X \subset A_n$, $a \in X$, označme

$$I_a = \{f \in \mathbb{C}[X];\ f(a) = 0\}$$

ideál v $\mathbb{C}[X]$.

Věta 12.1. *Maximální ideály v algebře $\mathbb{C}[X]$ jsou právě všechny ideály tvaru I_a, $a \in X$.*

Důkaz. $\Leftarrow$: Buď $a \in X$ libovolný bod; snadno dokážeme, že ideál I_a je maximální. Zobrazení $\rho_a : \mathbb{C}[X] \to \mathbb{C}$ definované předpisem $\rho_a(f) = f(a)$ je epimorfismem algeber, $\mathrm{Ker}(\rho_a) \cong I_a$, $\mathrm{Im}(\rho_a) \cong \mathbb{C}$. Je tedy $\mathbb{C}[X]/_{I_a} \cong \mathbb{C}$, tj. faktoralgebra $\mathbb{C}[X]/_{I_a}$ je tělesem, a tedy I_a je maximální ideálem.

$\Rightarrow$: Buď $I \subset \mathbb{C}[X]$ maximální ideál. Uvažujme epimorfismus $m : \mathbb{C}[t] \to \mathbb{C}[X]$. Protože ideál $m^{-1}(I)$ nesplývá s $\mathbb{C}[t]$, existuje alespoň jeden bod $a \in A_n$ takový, že $f(a) = 0$ $(\forall f \in m^{-1}(I))$. Protože však platí inkluze ideálů $m^{-1}(I) \supset I(X)$, je $a \in X \subset A_n$. Je-li $r \in \mathbb{C}[X]$ regulární funkce a $f \in \mathbb{C}[t]$ polynom reprezentující regulární funkce, je $f = m^{-1}(r)$, a tudíž pro $r \in I$ je $0 = r(a) = f(a)$ (je $a \in X$). Finálně dostáváme $I \subset I_a$, a protože I je maximální ideál, je $I = I_a$. $\square$

Maximální ideál pro $X = A_n/_{\mathbb{C}}$, $\mathbf{a} \equiv (a_1, \dots, a_n)$, je (např. využitím Taylorovy věty)

$$I_a = \langle t_1 - a_1, t_2 - a_2, \dots, t_n - a_n \rangle.$$

Předchozí věta říká, že zobrazení $a \leftrightarrow I_a$ je bijekce mezi

- afinními uzavřenými množinami $X \subset A_n$,
- množinami maximálních ideálů $I_a \subset \mathbb{C}[X]$.

Uvažujme libovolný komutativní okruh R s jednotkou. Zkusme vyšetřit, jakožto analog předchozího případu, množinu všech maximálních ideálů okruhu R. Označme ji Specm(R) a nazývejme *spektrem maximálních ideálů okruhu* R. Narazíme však na následující technické problémy.

Každé regulární zobrazení $\Phi : X \to X'$ dvou afinních uzavřených variet indukuje homomorfismus $\Phi^* : \mathbb{C}[X'] \to \mathbb{C}[X]$. Analogicky bychom chtěli zavést ke každému homomorfismu $\rho : R' \to R$ indukované zobrazení $\rho^* : \mathrm{Specm}(R) \to \mathrm{Specm}(R')$ maximálních spekter. Přirozená volba $m \subset R \to \rho^{-1}(m) \subset R'$ však nemusí dát maximální ideál $\rho^{-1}(m)$ (dá pouze prvoideál).

Příklad 12.2. Vnoření $\rho : \mathbb{Z} \hookrightarrow \mathbb{Q}$ dává $\langle 0 \rangle \subset \mathbb{Z} = \rho^{-1}(\langle 0 \rangle)$, $\langle 0 \rangle \subset \mathbb{Z}$ však není maximální ideál v $\mathbb{Z}$.

Poznámka 12.3. Problém je v tom, že je nemožné zrekonstruovat prostřednictvím maximálních ideálů a znalosti $\Phi^* : \mathbb{C}[X'] \to \mathbb{C}[X]$ regulární zobrazení $\Phi : X \to X'$.

Platí: je-li $\beta \subset R$ prvoideál, je $m^{-1}(\beta) \subset R'$ také prvoideál. Přirozeně se nabízí uvažovat množinu všech prvoideálů okruhu R. Označme ji Spec(R) (přičemž R jakožto ideál v R nepatří do Spec(R)). Uvidíme, že z prvoideálů okruhů R, R' lze regulární zobrazení Φ již zrekonstruovat. Nejdříve však definujeme strukturu svazku a okruhovaného prostoru.

Definice 12.4. *Předsvazkem* $\mathcal{F}$ abelovských grup na topologickém prostoru X nazýváme přiřazení (pro každou otevřenou množinu $U \subset X$)

$$U \mapsto \mathcal{F}(U),$$

kde $\mathcal{F}(U)$ je abelovská grupa a pro každou dvojici U, V otevřených podmnožin X takových, že $U \supset V$ máme homomorfismus abelovských grup $\rho^U_V : \mathcal{F}(U) \to \mathcal{F}(V)$, pro který platí:

(i) $\mathcal{F}(\emptyset)$ je triviální (jednoprvková) abelovská grupa,
(ii) $\rho^U_U = \mathrm{id}_U : \mathcal{F}(U) \to \mathcal{F}(U)$ (pro každou otevřenou $U \subset X$),
(iii) $\rho^U_V \circ \rho^V_W = \rho^U_W$ (pro všechny otevřené množiny U, V, $W \subset X$ takové, že $U \supset V \supset W$).

Prvky $\mathcal{F}(U)$ se nazývají *řezy předsvazku* $\mathcal{F}$ *nad* $U \subset X$. Je-li $s \in \mathcal{F}(U)$, $V \subset U$ a $s' = \rho^U_V(s)$, nazýváme s' *restrikcí* s *na* V.

Poznámka 12.5. Podobně lze definovat předsvazky okruhů, modulů atp.

Definice 12.6. Předsvazek $\mathcal{F}$ na topologickém prostoru X se nazývá *svazkem*, pokud platí

(iv) je-li $U \subset X$ otevřená množina, $\{V_i\}_{i\in I}$ otevřené pokrytí U, $s \in \mathcal{F}(U)$ takový prvek, že $\rho^U_{V_i}(s) = 0$ $(\forall i \in I)$, pak $s = 0$ v $\mathcal{F}(U)$,
(v) pro každou otevřenou množinu $U \subset X$, pro každé otevřené pokrytí $\{V_i\}_{i\in I}$ množiny U existují $s_i \in \mathcal{F}(V_i)$ $(\forall i \in I)$ tak, že $s_i|_{V_i\cap V_j} = s_j|_{V_i \cap V_j}$ $(\forall i, j \in I \times I)$.

Z poslední vlastnosti plyne jednoznačnost určení prvku $s \in \mathcal{F}(U)$.

Definice 12.7. *Stéblem předsvazku* $\mathcal{F}$ v bodě $p \in X$ nazýváme direktní limitu

$$\mathcal{F}_p := \lim_{\overrightarrow{U}} \{\mathcal{F}(U);\ U \text{ je otevřená množina v } X,\ p \in U\}.$$

Ekvivalentně je $\mathcal{F}_p$ třída ekvivalence $\sim$ dvojic (U, s), kde

- $U \subset X$ je otevřená množina, $p \in U$,
- $s \in \mathcal{F}(U)$;

$(U, s) \sim (U', s')$, právě když existuje otevřená množina $V \subset X$, $V \subset U \cap U'$ tak, že:

- $p \in U$,
- $s|_V = s'|_V$.

Stéblo předsvazku $\mathcal{F}$ Abelových grup je Abelova grupa. $\mathcal{F}_p$ se nazývá *grupa germů řezů* $\mathcal{F}$ *v* $p \in X$. Je-li $U \subset X$ otevřená množina, $p \in U$, pak přiřazení

$$\mathcal{F}(U) \ni s \mapsto \text{ třída ekvivalence } (U, s) \text{ v } \mathcal{F}_p$$

je homomorfismus abelovských grup; značíme ho ρ^U_p.

Morfismem $\varphi : \mathcal{F}_1 \to \mathcal{F}_2$ dvou předsvazků na X se nazývá systém homomorfismů abelovských grup

$$\{\varphi(U) : \mathcal{F}_1(U) \to \mathcal{F}_2(U)\}$$

takový, že pro každé dvě otevřené množiny U, $V \subset X$, $U \supset V$, platí

$$\rho'^U_V \varphi(U) = \varphi(V)\rho^U_V$$

(tj. diagram

$$\begin{tikzcd} U \arrow[r, "\varphi(U)"] \arrow[d, "\rho"'] & U \arrow[d, "\rho'"] \\ V \arrow[r, "\varphi(V)"] & V \end{tikzcd}$$

je komutativní).

Morfismus předsvazků, ke kterému existuje inverzní morfismus, se nazývá *izomorfismem.*

Každý morfismus předsvazků $\varphi : \mathcal{F} \to \mathcal{F}'$ určuje homomorfismus stébel $\varphi_p : \mathcal{F}_p \to \mathcal{F}'_p$ $(\forall p \in X)$.

Definice 12.8. *Okruhovaným prostorem* nazýváme dvojici $(X, \mathcal{O}_X)$, kde X je topologický prostor a $\mathcal{O}_X$ je svazek okruhů na X. $\mathcal{O}_X$ je označován jako *strukturální svazek* $(X, \mathcal{O}_X)$.

Morfismem okruhovaných prostorů

$$(\varphi, \psi) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

nazýváme dvojici sestávající ze spojitého zobrazení $\varphi : X \to Y$ a homomorfismu svazků $\psi : \mathcal{O}_Y \to \varphi_* \mathcal{O}_X$. $\big((\varphi_* \mathcal{O}_X)(U) = \mathcal{O}_X(\varphi^{-1}(U))$ pro otevřenou množinu $U \subset Y.\big)$

Morfismus (φ, ψ) se nazývá *izomorfismem*, pokud $\varphi : X \to Y$ je homeomorfismus topologických prostorů a $\psi : \mathcal{O}_Y \to \varphi_* \mathcal{O}_X$ je izomorfismus svazků.

Okruhovaný prostor se nazývá *lokálně okruhovaný*, pokud $\mathcal{O}_{p,X}$ je lokálním okruhem pro každé $p \in X$. Definici lokálního morfismu si jistě čtenář doplní.

Poznámka 12.9. Obecně není pravda, že morfismus svazků je indukován (podkladovým) zobrazením topologických prostorů.

Na množině $\mathrm{Spec}(R)$ zavedeme topologii. Buď $\beta \subset R$ ideál. Symbolem $\mathcal{M}(\beta)$ označíme množinu všech prvoideálů v R obsahujících ideál β. Platí

Věta 12.10. *Nechť jsou $\beta_1, \beta_2 \subset R$ ideály. Pak*

(i) $\mathcal{M}(\beta_1) \subset \mathcal{M}(\beta_2) \Leftrightarrow \sqrt{\beta_1} \supset \sqrt{\beta_2}$,
(ii) $\mathcal{M}(\beta_1) \cup \mathcal{M}(\beta_2) = \mathcal{M}(\beta_1 \beta_2)$,
(iii) *pro libovolný soubor $\{\beta_\gamma\}_{\gamma \in \Gamma}$ ideálů okruhu R je*

$$\bigcap_{\gamma \in \Gamma} \mathcal{M}(\beta_\gamma) = \mathcal{M}\Big(\sum_{\gamma \in \Gamma} \beta_\gamma\Big).$$

Důkaz. Jednoduchý, viz literatura. □

Je $\mathcal{M}(R) = \{0\}$, $\mathcal{M}(\langle 0 \rangle) = \mathrm{Spec}(R)$. Z předchozí věty vidíme, že systém podmnožin $\mathrm{Spec}(R)$ tvaru $\mathcal{M}(\beta)$ splňuje axiomy topologie na $\mathrm{Spec}(R) = X$ zadané pomocí systému uzavřených množin.

Buď $r \in R$ libovolný prvek. Označme $D(r)$ množinu všech prvoideálů ze $Spec(R)$ neobsahujících prvek r. $D(r)$ je otevřená množina, neboť $D(r) = \mathrm{Spec}(R) \setminus \mathcal{M}(\langle r \rangle)$. Lze ukázat, že množiny tvaru $D(r)$ tvoří bazi (otevřených množin) topologie prostoru $\mathrm{Spec}(R)$.

Věta 12.11. *Topologický prostor* Spec(R) *je kvazikompaktní.*

Věta 12.12. *Buď* $\beta \in \operatorname{Spec}(R)$. *Pak* $\overline{\beta} = \mathcal{M}(\beta)$, *tudíž uzavřený podprostor* β *je homeomorfní s topologickým prostorem* Spec(R/β). *Navíc bod* β *je uzavřený, právě když je* β *maximální ideál.*

Definice 12.13. Buď X topologický prostor. Bod $q \in X$ se nazývá *specializací bodu* $p \in X$, pokud $q \in \overline{\{p\}}$ ($\overline{\{p\}}$ značí uzávěr v topologii diskutované v této sekci). Bod $p \in X$ se nazývá *obecným bodem prostoru* X, pokud $\overline{\{p\}} = X$.

Věta 12.14. *Topologický prostor* Spec(R) *obsahuje obecný bod, právě když nilradikál okruhu* R *je prvoideálem. Je-li nilradikál* R *prvoideálem, je jediným obecným bodem topologického prostoru* Spec(R) *bod určený radikálem.*

Příslušné důkazy lze nalézt v citované literatuře.

13. Vnoření (realizace) algebraických variet v komplexních projektivních prostorech

Kompaktní hladká varieta dimenze n je vnořitelná do prostoru $\mathbb{R}^{2n+1}$, ale obecně neexistuje analogické (holomorfní) vnoření do $\mathbb{C}^N$.

Hledáme vnoření do $\mathbb{CP}^N$. (Chow dokázal, že komplexní algebraická varieta je vnořitelná do prostoru $\mathbb{CP}^N$.)

Tedy řešíme soustavu homogenních algebraických rovnic:

$$(*)\qquad \begin{aligned} f_1(z_0,\dots,z_N) &= 0\\ &\vdots\\ f_M(z_0,\dots,z_N) &= 0. \end{aligned}$$

Polynomy $f_1,\dots,f_M$ generují prvoideál I_X v okruhu polynomů $\mathbb{C}[z_0,\dots,z_N]$. Hodnost Jacobiho matice

$$\begin{pmatrix} \frac{\partial f_1}{\partial z_0} & \cdots & \frac{\partial f_1}{\partial z_N}\\ \vdots & & \vdots\\ \frac{\partial f_M}{\partial z_0} & \cdots & \frac{\partial f_M}{\partial z_N} \end{pmatrix}$$

označme R. Tato hodnota nezávisí na volbě $a_0,\dots,a_N$ splňujících soustavu rovnic (*). Dimenze variety je pak $N-R$.

Nutnou (nikoli postačující) podmínkou vnořitelnosti X do $\mathbb{CP}^N$ je

$$\dim X = \text{ stupeň transcendence tělesa } \mathcal{M}(X) \text{ meromorfních funkcí do } \mathbb{C}.$$

Navíc jsou pro komplexní nerozložitelné algebraické variety následující tělesa izomorfní:

- těleso meromorfních funkcí s hodnotami v $\mathbb{C}$,
- těleso $R(X)$ racionálních funkcí na X.

$R(X)$ je generováno zlomky tvaru $\frac{P_k(z_0,\dots,z_k)}{Q_k(z_0,\dots,z_k)}$, kde P_k, Q_k jsou homogenní polynomy stejného stupně.

Tvrzení 13.1. *Každá kompaktní komplexní varieta dimenze* 1 *je izomorfní projektivní algebraické komplexní varietě (hladké algebraické křivce).*

Důkaz. Tvrzení dokážeme pro komplexní tory $X \cong \mathbb{C}/\Lambda$. Chceme najít (nekonstantní) zobrazení $f : X \hookrightarrow \mathbb{CP}^N$, kde $N \in \mathbb{N}$.

Označme $\mathbb{P}^N/\mathbb{C}$ množinu přímek v $\mathbb{C}^{N+1}$. Je $\dim_{\mathbb{C}}\left(\mathbb{P}^N/\mathbb{C}\right) = N$. Položme $U_i := \{(z_0,\dots,z_N);\ z_i \neq 0\}$. Pak přiřazení

$$(z_0,\dots,z_N) \mapsto \left(\frac{z_0}{z_i},\dots,\frac{z_{i-1}}{z_i},\frac{z_{i+1}}{z_i},\dots,\frac{z_N}{z_i}\right)$$

definuje izomorfismus $U_i \cong \mathbb{C}^N$.

Máme holomorfní funkce $f_0,\dots,f_N$ dané složením $\mathbb{C} \to \mathbb{C}/\Lambda \hookrightarrow \mathbb{CP}^N$. Tyto funkce nemusí být periodické, avšak platí

$$f_i(z+\lambda) = e_\lambda(z) f_i(z)\ (\forall i \in \{0,\dots,N\},\ \lambda \in \Lambda),$$

kde $e_\lambda \in \mathcal{O}^*(\mathbb{C})$ jsou holomorfní invertibilní funkce na $\mathbb{C}$.

Definice 13.2. Holomorfní funkce $f : \mathbb{C} \to \mathbb{C}$ se nazývá *θ-funkcí mřížky* Λ, pokud pro každý prvek $\lambda \in \Lambda$ existuje invertibilní holomorfní funkce $e_\lambda(z)$ tak, že

$$f(z+\lambda) = e_\lambda(z) f(z) \ (\forall z \in \mathbb{C}).$$

Množina $\{e_\lambda(z)\}_{\lambda \in \Lambda}$ se nazývá *θ-faktorem* funkce $f : \mathbb{C} \to \mathbb{C}$.

Příklad 13.3. $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, $\tau \in \mathcal{H} := \{x + iy;\ y > 0,\ x, y \in \mathbb{R}\}$.

Položme

$$\Theta(z,\tau) = \sum_{n \in \mathbb{Z}} \mathrm{e}^{i\pi(n^2\tau + 2zn)}.$$

Lemma 13.4. *Θ je holomorfní funkce na $\mathbb{C}$.*

Důkaz. Ukážeme, že řada $\sum_{n\in\mathbb{Z}} \mathrm{e}^{i\pi(n^2\tau+2zn)}$ konverguje stejnoměrně na každé omezené podmnožině $\mathbb{C}$. Pak

$$\bar\partial\Theta = \bar\partial\left(\sum_{n\in\mathbb{Z}} \mathrm{e}^{i\pi(n^2\tau+2zn)}\right) = \sum_{n\in\mathbb{Z}} \left(\bar\partial \mathrm{e}^{i\pi(n^2\tau+2zn)}\right) = \sum 0 = 0,$$

tj. Θ je holomorfní funkcí.

Buď $M \subset \mathbb{C}$ omezená množina, nechť $(\forall z \in M)$ $|\mathrm{Im}(z)| < K$. Pak

$$\sum_{n\in\mathbb{Z}} \left|\mathrm{e}^{i\pi(n^2\tau+2zn)}\right| \le \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2 \mathrm{Im}(\tau)} \mathrm{e}^{2\pi cn}$$

a $\mathrm{e}^{-\pi n^2\mathrm{Im}(\tau)}\mathrm{e}^{2\pi cn} = \mathrm{e}^{-(\pi n\mathrm{Im}(\tau) - 2\pi c)n}$, tedy pro $n \ge n_0$ je $\pi n \mathrm{Im}(\tau) > 2\pi c$. Odtud

$$\sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n^2\mathrm{Im}(\tau)}\mathrm{e}^{2\pi cn} < \sum_{n\in\mathbb{Z}} \mathrm{e}^{-\pi n(n-n_0)\mathrm{Im}(\tau)}$$

a tato řada konverguje $(\mathrm{Im}(\tau) > 0)$. $\square$

Je Θ θ-funkcí?

- Zřejmě je periodická: $\Theta(z,\tau) = \Theta(z+m,\tau)$, $m \in \mathbb{Z}$.
- $\Theta(z+\tau,\tau) = \sum_{n\in\mathbb{Z}} \mathrm{e}^{i\pi(n^2\tau+2zn+2\tau n)} = \sum_{n\in\mathbb{Z}} \mathrm{e}^{i\pi\left((n+1)^2\tau + 2z(n+1) - \tau - 2z\right)} =$ $= \mathrm{e}^{i\pi(-\tau-2z)} \sum_{n\in\mathbb{Z}} \mathrm{e}^{i\pi\left((n+1)^2\tau+2z(n+1)\right)} = \mathrm{e}^{-i\pi(\tau+2z)}\Theta(z,\tau)$.

Obecně: pro $\lambda = m + n\tau \in \Lambda$ je

$$\Theta(z+m+n\tau,\tau) = \mathrm{e}^{-i\pi(n^2\tau+2nz)}\Theta(z,\tau),$$

kde $e_{m+n\tau}(z) := \mathrm{e}^{-i\pi(n^2\tau+2nz)}$ je *θ-faktor*, $\Theta(z,\tau)$ je Riemannova θ-funkce.

Obecná forma θ-funkcí.

θ-faktor splňuje:

$$e_{\lambda+\lambda'}(z) = e_\lambda(z+\lambda')e_{\lambda'}(z),$$

neboť

$$f(z+\lambda+\lambda') = e_{\lambda+\lambda'}(z)f(z) = e_\lambda(z+\lambda')f(z+\lambda') = e_\lambda(z+\lambda')e_{\lambda'}(z)f(z).$$

Pokud $\varphi \in \mathcal{O}^*(\mathbb{C})$, je φf také θ-funkcí s faktorem

$$e'_\lambda(z) = e_\lambda(z)\varphi(z+\lambda)\varphi^{-1}(z), \tag{*}$$

neboť $(f\varphi)(z+\lambda) = e'_\lambda(z)(f\varphi)(z)$.

Definice 13.5. Množina holomorfních invertibilních funkcí $\{e_\lambda\}_{\lambda\in\Lambda}$ splňující

$$e_{\lambda+\lambda'}(z) = e_\lambda(z+\lambda')e_{\lambda'}(z)$$

se nazývá *θ-faktor* mřížky Λ. Dva θ-faktory $\{e_\lambda\}_{\lambda\in\Lambda}$, $\{e'_\lambda\}_{\lambda\in\Lambda}$ jsou *ekvivalentní* (píšeme $\{e_\lambda\}_{\lambda\in\Lambda} \sim \{e'_\lambda\}_{\lambda\in\Lambda}$), pokud

- (*) platí pro některou funkci $\varphi \in \mathcal{O}^*(\mathbb{C})$,
- $e'_\lambda = e_\lambda \circ T$, kde T je translace $z \mapsto z + a$ určená prvkem $a \in \mathbb{C}$.

Buď $T_\theta(e_\lambda, \Lambda)$ podprostor θ-funkcí daného typu prostoru $\mathcal{O}(\mathbb{C})$. Platí

$$f, g \in T_\theta(e_\lambda, \Lambda) \Rightarrow \frac{f}{g} \in \mathcal{M}(\mathbb{C}/\Lambda)$$

(meromorfní funkce na $\mathbb{C}/\Lambda$ je periodická).

Pokud $\{e_\lambda\}_{\lambda\in\Lambda} \sim \{e'_\lambda\}_{\lambda\in\Lambda}$, platí $T_\theta(e_\lambda, \Lambda) \cong T_\theta(e'_\lambda, \Lambda)$.

Bez důkazu uvedeme následující

Tvrzení 13.6. *Lze nalézt* $\varphi \in \mathcal{O}^*(\mathbb{C})$ *tak, že* $\log\big(e_\lambda(z)\varphi(z+\lambda)\varphi^{-1}(z)\big)$ *je lineární holomorfní funkcí, tj.* $e'_\lambda(z) = \mathrm{e}^{-2\pi i(a_\lambda z + b_\lambda)}$, *kde* a_λ, $b_\lambda \in \mathbb{C}$.

Nahradíme: $f_z \to f_z \mathrm{e}^{2\pi i\left(\frac{1}{2}a_1 z^2 + \left(b_i - \frac{a_1}{2}\right)z\right)}$, budeme předpokládat, že $a_1 = 0 = b_1$. Speciálně

$$\begin{aligned} f(z+1) &= f(z),\\ f(z+\tau) &= \mathrm{e}^{-2\pi i(az+b)}f(z). \end{aligned}$$

Potom

$$\begin{aligned} f(z+\tau+1) &= f\big((z+\tau)+1\big) = f(z+\tau) = \mathrm{e}^{-2\pi i(az+b)}f(z)\\ &= f\big((z+1)+\tau\big) = \mathrm{e}^{-2\pi i\left(a(z+1)+b\right)}f(z) = \mathrm{e}^{-2\pi i a}\mathrm{e}^{-2\pi i(az+b)}f(z), \end{aligned}$$

odtud $\mathrm{e}^{-2\pi i a} = 1$, tedy $a = k \in \mathbb{Z}$. Rozvoj ve Fourierovu řadu $f(z) = \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{2\pi i n z}$, $c_n \in \mathbb{C}$, a dosazení $z \to z + \tau$ dává:

$$\begin{aligned} f(z+\tau) &= \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{2\pi i n\tau}\mathrm{e}^{2\pi i n z} = \mathrm{e}^{-2\pi i(kz+b)}f(z)\\ &= \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{-2\pi i b}\mathrm{e}^{2\pi i(n-k)z} = \sum_{n\in\mathbb{Z}} c_{n+k}\mathrm{e}^{-2\pi i b}\mathrm{e}^{2\pi i n z}, \end{aligned}$$

tedy $c_{n+k} = c_n \mathrm{e}^{2\pi i(n\tau+b)}$.

Pokud $k = 0$, dostáváme $c_n = 0$ pro každé $n \in \mathbb{Z}$ s výjimkou nejvýš jediného: označme ho N. $N\tau + b \in \mathbb{Z}$, $f(z) = c_N \mathrm{e}^{2\pi i N z}$.

Buď $k \neq 0$; postupujeme rekurzí. Předpokládejme, že $k < 0$. Nechť $c_N \neq 0$ pro nějaké $N \in \mathbb{N}$. Pak $|c_{N-k}| = |c_N \mathrm{e}^{-2\pi i(N\tau+b)}|$, a tedy c_{N-sk} roste exponenciálně pro $\mathbb{N} \ni s \to \infty$ ($\mathrm{Im}(\tau) > 0$). Fourierova řada diverguje.

Nechť $c_N \neq 0$ pro některé $N \in -\mathbb{N}$. Ze vztahu $c_n = \mathrm{e}^{-2\pi i(n\tau+b)}c_{n+k}$ ($k < 0$) dostáváme, že $|c_{N+sk}|$ diverguje pro $1 \leq s \to \infty$.

Předpokládejme, že $k>0$. Pak

$$\begin{aligned} f\left(z+\frac{\tau}{2}-\frac{b}{k}+1\right) &= f\left(z+\frac{\tau}{2}-\frac{b}{k}\right),\\ f\left(z+\frac{\tau}{2}-\frac{b}{k}+\tau\right) &= \mathrm{e}^{-2\pi i\left(k\left(z+\frac{\tau}{2}-\frac{b}{k}\right)+b\right)} f\left(z+\frac{\tau}{2}-\frac{b}{k}\right)\\ &= \mathrm{e}^{-2\pi i\left(kz+k\cdot\frac{\tau}{2}\right)} f\left(z+\frac{\tau}{2}-\frac{b}{k}\right). \end{aligned}$$

Předpokládejme, že $b=\frac{k\tau}{2}$, $s\in\{0,\dots,k-1\}$. Pak

$$c_{s+rk}=\mathrm{e}^{\pi i\left[\frac{(s+rk)^2\tau}{k}\right]}c_s$$

je explicitní řešení rekurentní relace (modulo faktor $\mathrm{e}^{\frac{\pi i s^2}{k}}$ skrytý v prvním členu c_s, $s\in\{0,\dots,k-1\}$).

Ukázali jsme, že každou funkci $f(z)$ s θ-faktorem

$$(**)\qquad e_{m+n\tau}=\mathrm{e}^{-2\pi i k\left(nz+\frac{n^2}{2}\right)}$$

lze psát ve tvaru

$$f(z)=\sum_{s=0}^{k-1}c_s\Theta_s(z,\tau)_k,$$

kde

$$\begin{aligned}\Theta_s(z,\tau)_k &= \sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[\frac{(s+rk)^2\tau}{k}\right]}\mathrm{e}^{2\pi i z[s+rk]}\\ &= \sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[\left(\frac{s}{k}+r\right)^2 rk+2kz\left(\frac{s}{k}+r\right)\right]},\quad s=0,\dots,k-1.\end{aligned}$$

Jednoznačnost Fourierových koeficientů holomorfních funkcí a fakt, že funkce $\Theta_s(z)_k$ jsou lineárně nezávislé, implikují, že $\{\Theta_s(z,\tau)\}_{s\in\mathbb{Z}_k}$ je bazí prostoru θ-funkcí s θ-faktorem (**).

Shrnutí. *Každý θ-faktor je ekvivalentní θ-faktoru tvaru*

$$e_{m+n\tau}(z)=\mathrm{e}^{-2\pi i\left(nkz+\frac{n^2}{2}k\tau\right)}.$$

Prostor $\mathcal{T}h(k,\Lambda_\tau)$ θ-funkcí s θ-faktorem uvedeného tvaru je nulový pro $k<0$.

Pro $k=0$ sestává z konstantních funkcí.

Pro $k>0$ je $\dim_{\mathbb{C}}\mathcal{T}h(k,\Lambda_\tau)=k$ a prostor je generován funkcemi $\Theta_s(z,\tau)_k$, $s=0,\dots,k-1$.

Protože

$$\mathrm{e}^{-2\pi i\left(nkz+\frac{n^2}{2}k\tau\right)}\cdot\mathrm{e}^{-2\pi i\left(nk'z+\frac{n^2}{2}k'\tau\right)}=\mathrm{e}^{-2\pi i\left(n(k+k')z+\frac{n^2}{2}(k+k')\tau\right)},$$

platí

$$\left(f\in\mathcal{T}h(\{e_\lambda\}_{\lambda\in\Lambda},\Lambda)\ \&\ g\in\mathcal{T}h(\{e'_\lambda\}_{\lambda\in\Lambda},\Lambda)\right)\Rightarrow fg\in\mathcal{T}h(\{e_\lambda e'_\lambda\}_{\lambda\in\Lambda},\Lambda).$$

Pro $k=1$ máme
$$\Theta_0(z,\tau)_1=\Theta(z,\tau).$$

Zobecnění. θ-funkce s racionálními parametry:
$$\vartheta_{a,b}(z,\tau):=\sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[(a+r)^2\tau+2(z+b)(a+r)\right]},\ a,b\in\mathbb{Q}.$$

Platí
$$\Theta_s(z,\tau)_k=\vartheta_{\frac{s}{k},0}(kz,k\tau).$$

Klasické Jacobiho θ-funkce se definují:
$$\begin{aligned}
\Theta_1(z,\tau)&:=\vartheta_{\frac12,\frac12}(z,\tau)=i\sum_{r\in\frac12+\mathbb{Z}}(-1)^{r-1}\mathrm{e}^{2\pi izr}\mathrm{e}^{2\pi i\tau\frac{r^2}{2}},\\
\Theta_2(z,\tau)&:=\vartheta_{\frac12,0}(z,\tau)=\sum_{r\in\frac12+\mathbb{Z}}\mathrm{e}^{2\pi izr}\mathrm{e}^{2\pi i\tau\frac{r^2}{2}},\\
\Theta_3(z,\tau)&:=\vartheta_{0,0}(z,\tau)=\sum_{r\in\mathbb{Z}}\mathrm{e}^{2\pi izr}\mathrm{e}^{2\pi i\tau\frac{r^2}{2}},\\
\Theta_4(z,\tau)&:=\vartheta_{0,\frac12}(z,\tau)=\sum_{r\in\mathbb{Z}}(-1)^r\mathrm{e}^{2\pi izr}\mathrm{e}^{2\pi i\tau\frac{r^2}{2}}.
\end{aligned}$$

Vlastnosti funkcí $\vartheta_{a,b}$ s racionálními koeficienty.

$$\begin{aligned}
\vartheta_{a,b}(z,\tau)&=\mathrm{e}^{2\pi i(b-b')a}\vartheta_{a',b'}(z,\tau),\ \text{pokud } a'-a,\ b'-b\in\mathbb{Z},\\
\vartheta_{a,b}(z+1,\tau)&=\sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[(a+r)^2\tau+2(z+b)(a+r)+2(a+r)\right]}=\mathrm{e}^{2\pi ia}\vartheta_{a,b}(z,\tau),\\
\vartheta_{a,b}(z+\tau,\tau)&=\sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[(a+r)^2\tau+2(z+b)(a+r)+2\tau(a+r)\right]}=\mathrm{e}^{2\pi ib}\mathrm{e}^{i\pi(-\tau-2z)}\vartheta_{a,b}(z,\tau).
\end{aligned}$$

Každá funkce $\vartheta_{a,b}(z,\tau)$ se získá z funkce $\Theta(z,\tau)$ pomocí
- translace v proměnné z,
- násobení faktorem, který se nikde neanuluje:

$$\begin{aligned}
\Theta(z+b+a\tau,\tau)&=\sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[r^2\tau+2(z+b+a\tau)r\right]}=\\
&=\sum_{r\in\mathbb{Z}}\mathrm{e}^{\pi i\left[(a+r)^2\tau+2(z+b)(r+a)-a^2\tau-2(z+b)a\right]}=\mathrm{e}^{-i\pi\left(a^2\tau+2(z+b)a\right)}\vartheta_{a,b}(z,\tau)
\end{aligned}$$

nebo
$$\vartheta_{a,b}(z,\tau)=\mathrm{e}^{i\pi\left(a^2\tau+2(z+b)a\right)}\vartheta_{0,0}(z+b+a\tau,\tau).$$

Definice 13.7.
$$\mathcal{T}h(k,\Lambda_\tau)_{a,b}:=\left\{f\in\mathcal{O}/_{\mathbb{C}}(\mathbb{C});\ f(z+m+n\tau)=\mathrm{e}^{-2\pi i(-ma+nb)}\mathrm{e}^{-2k\pi i\left(nz+\frac{n^2}{2}\tau\right)}f(z)\right\}$$

buď množina všech θ-funkcí řádu k s racionálními koeficienty a, b.

Máme bilineární zobrazení

$$\mathcal{T}h(k,\Lambda_\tau)_{a,b} \times \mathcal{T}h(k',\Lambda_\tau)_{a',b'} \to \mathcal{T}h(k+k',\Lambda_\tau)_{a+a',b+b'}.$$

Pro každé $f \in \mathcal{T}h(k,\Lambda_\tau)$ je

$$\mathrm{e}^{i\pi[a^2\tau+2(z+a)b]} f\Big(z+\frac{b+a\tau}{k}\Big) \in \mathcal{T}h(k,\Lambda_\tau)_{a,b},$$

tedy

$$\mathcal{T}h(k,\Lambda_\tau) \cong \mathcal{T}h(k,\Lambda_\tau)_{a,b}.$$

Podobně

$$\mathcal{T}h(k,\Lambda_\tau)_{a,b} \cong \mathcal{T}h(k,\Lambda_\tau)_{a',b'},$$

pokud $a'-a,\ b-b' \in \mathbb{Z}$.

Použití θ-funkcí na vnoření $\mathbb{C}/\Lambda_\tau \to \mathbb{CP}^*$.

Lemma 13.8. *Buď $0 \neq f \in \mathcal{T}h(k,\Lambda)$. Pak f má právě k nulových bodů v $\mathbb{C}$ mod Λ, včetně násobností.*

Důkaz. Známý výsledek z teorie funkcí jedné komplexní proměnné tvrdí, že pro meromorfní funkci na otevřené množině $D \subset \mathbb{C}$ a pro kompaktní množinu $K \subset D$ takovou, že $\Gamma := \partial K$ je orientovaná Jordanova křivka, platí:

$$\text{"počet nulových bodů včetně násobností"} - \text{"počet pólů včetně násobností"} = \frac{1}{2\pi}\oint_\Gamma d\log(f(z))dz.$$

Zde předpokládáme, že $f(z)$ nemá nuly ani póly na Γ. – Toho lze v našem případě dosáhnout vhodnou translací fundamentálního paralelogramu mřížky Γ:

$$\Pi \mapsto z_0 + \Pi,$$

$K = \Pi$, neobsahujícího nulové body $\vartheta_{ab}(z,\tau)$. Tuto operaci lze realizovat, neboť množina nul holomorfní funkce na $\mathbb{C}$ je diskrétní, tj. množina nul na libovolné kompaktní množině $K \subset \mathbb{C}$ je konečná.

Mějme

$$f(z+m+n\tau) = \mathrm{e}^{-i\pi k\left(\frac{n^2}{2}\tau+2nz\right)} f(z).$$

Odtud

$$\begin{aligned} Z &= \frac{1}{2\pi i}\int_\Gamma d\log f(z) = \\ &= \frac{1}{2\pi i}\int_{\vec{\varepsilon}}^{\vec{\varepsilon}+1}\big(d\log f(z,\tau) - d\log f(z+\tau,\tau)\big) - \frac{1}{2\pi i}\int_{\vec{\varepsilon}}^{\vec{\varepsilon}+\tau}\big(d\log f(z) - d\log f(z+\tau,\tau)\big) = \\ &= \frac{1}{2\pi i}\int_{\vec{\varepsilon}}^{\vec{\varepsilon}+1} d\big(\pi i k(2z+\tau)\big) = k. \end{aligned}$$

Tedy nuly tvoří k-orbity vzhledem k Λ. $\square$

Lemma 13.9. *Nuly funkce $\vartheta_{a,b}(z,\tau)$ v $\mathbb{C}$ jsou body*

$$z = \left(a + \frac{1}{2}\right)\tau + \left(b + \frac{1}{2}\right) + \Lambda.$$

Důkaz. Užitím vztahu

$$\vartheta_{a,b}(z,\tau) = \mathrm{e}^{i\pi\left(a^2\tau + 2(z+b)a\right)}\vartheta_{0,0}(z + b + a\tau, \tau)$$

dostáváme (lineární transformace $z \to b + a\tau + z$ posouvá nuly)

$$\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau) = \mathrm{e}^{i\pi\left(\frac{1}{4}\tau + 2(z+\frac{1}{2})\frac{1}{2}\right)}\vartheta_{0,0}\Big(z + \frac{1}{2} + \frac{1}{2}\tau, \tau\Big).$$

Funkce $\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau)$ má nulový bod na mřížce Λ, tedy stačí dokázat lichost funkce $\vartheta_{a,b}(z,\tau)$ vzhledem k proměnné z.

$$\begin{aligned}\vartheta_{a,b}(-z,\tau) = \sum_{r\in\mathbb{Z}} \mathrm{e}^{i\pi\left[(a+r)^2\tau + 2(-z+b)(a+r)\right]} &= \sum_{r\in\mathbb{Z}} \mathrm{e}^{i\pi\left[(-a-r)^2\tau + 2(z-b)(-a-r)\right]} = \\ &= \sum_{r\in\mathbb{Z}} \mathrm{e}^{i\pi\left[(-a+r)^2\tau + 2(z-b)(-a+r)\right]} = \vartheta_{-a,-b}(z,\tau).\end{aligned}$$

Pro $(a,b) = \left(\frac{1}{2},\frac{1}{2}\right)$ máme

$$\vartheta_{\frac{1}{2},\frac{1}{2}}(-z,\tau) = \vartheta_{-\frac{1}{2},-\frac{1}{2}}(z,\tau) = \mathrm{e}^{i\pi}\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau) = -\vartheta_{\frac{1}{2},\frac{1}{2}}(z,\tau)$$

(aplikovali jsme vztah $\vartheta_{a,b}(z,\tau) = \mathrm{e}^{2\pi i(b-b')a}\vartheta_{a',b'}(z,\tau)$ pro $a' - a,\ b' - b \in \mathbb{Z}$), tedy funkce je lichá. $\square$

Lemma 13.10. *Množina nulových bodů funkce $\Theta_s(z,\tau)_k$ je*

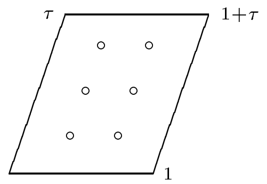
$$\left\{\left(\frac{s}{k} + \frac{1}{2}\right)\tau + \frac{1}{2k} + \frac{i}{k} + \Lambda;\ i = 0,\dots,k-1\right\}.$$

Důkaz. Užitím vztahu $\Theta_s(z,\tau)_k = \vartheta_{\frac{s}{k},0}(kz, k\tau)$ z předchozího lemmatu plyne: je-li z nulovým bodem funkce Θ_s, pak kz je nulovým bodem funkce $\vartheta_{\frac{s}{k},0}(z,k\tau)$. Tedy

$$kz = \left(\frac{s}{k} + \frac{1}{2}\right)k\tau + \frac{1}{2} + \mathbb{Z} + \mathbb{Z}k\tau$$

a

$$z = \left(\frac{s}{k} + \frac{1}{2}\right)\tau + \frac{1}{2k} + \frac{1}{k}\mathbb{Z} + \mathbb{Z}\tau.$$



$\square$

Věta 13.11. *Pro každé $k \geq 1$ formule*

$$z \mapsto \big(\Theta_0(z,\tau)_k, \dots, \Theta_{k-1}(z,\tau)_k\big)$$

definuje holomorfní zobrazení

$$\Phi_k : E_\tau := \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \to \mathbb{CP}^{k-1}.$$

Je-li $k \geq 3$, je zobrazení Φ_k holomorfní vnoření (tj. je injektivní a v každém bodě z má nenulovou derivaci).

Důkaz. Zobrazení Φ_k je dobře definováno: pro $s \in \{0, \dots, k-1\}$ funkce $\Theta_s(z,\tau)_k$ odpovídají stejnému θ-faktoru. Tedy pro z a $z + \lambda$, kde $\lambda \in \Lambda$, je na pravé straně stejný prvek projektivního prostoru $\mathbb{CP}^{k-1}$.

Z předchozího lemmatu víme, že se funkce Θ_s, $s \in \{0, \dots, k-1\}$, neanulují ve stejných bodech.

Definované zobrazení je holomorfní, neboť θ-funkce jsou holomorfní. Podobně se dokáže jeho injektivita. $\square$

Základní literatura

- Griffiths P., Harris J.: *Principles of Algebraic Geometry*, 1994 J. Willey & Sons Publ.
- Hartstorne R.: *Algebraic Geometry*, Graduated Texts in Math. **52**, 1997 Springer Verlag.
- Shafarevich I. R.: *Basic Algebraic Geometry*, 1974 Springer Verlag.