Algebraická geometrie

geometrická část

Aleš Drápal

Kapitola 1

Uzávěrové operátory a Zariského topologie

Definice 1.1 (Uzávěrový systém)**.** Ať X je nějaká množina a ať $\mathcal{S}$ je systém jejích podmnožin. Pak $\mathcal{S}$ nazveme *uzávěrovým systémem*, jestliže:

(i) $X \in \mathcal{S}$

(ii) Jsou-li $A_i \in \mathcal{S}, i \in I$, pak $\bigcap(A_i; i \in I) \in \mathcal{S}$

Typický příklad: $\mathcal{S}$ je systém všech konvexních podmnožin roviny (obecně $\mathbb{R}^n$).
V algebře se přirozeně vyskytuje mnoho uzávěrových systémů - podgrupy, podokruhy, ideály a další.

Definice 1.2 (Uzávěrový operátor)**.** S každým uzávěrovým systémem je přirozeně spjat *uzávěrový operátor*. Označme ho $\mathcal{C}l_{\mathcal{S}}$. Pro stručnost ať $\mathcal{C} = \mathcal{C}l_{\mathcal{S}}$. Pak $\mathcal{C} : \mathcal{P}(X) \to \mathcal{S}$, kde $\mathcal{P}(X)$ je potenční množina, tedy množina všech podmnožin množiny X. Definujeme $\mathcal{C}(B) = \bigcap(A \in \mathcal{S}, A \supseteq B)$. Z definice uzávěrového systému plyne, že $\mathcal{C}(B)$ vskutku leží v $\mathcal{S}$. Volněji řečeno, $\mathcal{C}(B)$ je nejmenší prvek $\mathcal{S}$, který obsakuje množinu $B \subseteq X$.

Snadno nahlédnete, že platí:

(UO1) $\mathcal{C}\mathcal{C}(B) = \mathcal{C}(B)$ (idempotence)

(UO2) $\emptyset \subseteq B_1 \subseteq B_2 \subseteq X \implies \mathcal{C}(B_1) \subseteq \mathcal{C}(B_2)$ (monotonie)

(UO3) $B \subseteq \mathcal{C}(B)$ (extensionalita)

Lemma 1.1 (Charakterizace uzávěrových operátorů)**.** *Ať $\mathcal{C} : \mathcal{P}(X) \to \mathcal{P}(X)$ je zobrazení, které splňuje **(UO1)–(UO3)**. Potom $\mathcal{S} = \{B \subseteq X; \mathcal{C}(B) = B\}$ tvoří uzávěrový systém. Přitom platí $\mathcal{C} = \mathcal{C}l_{\mathcal{S}}$.*

Důkaz. Triviální □

V některých situacích je snažší nebo přirozenější definovat uzávěrový operátor než uzávěrový systém. Příklady:

1. Ať K je těleso. Pro každé $B \subseteq K$ sestrojme nejprve těleso F generované množinou B a pak položme $\mathcal{C}l(B) = \{a \in K;\ a$ je algebraické nad $F\}$.

2. Ať R je okruh. Pro každé $B \subseteq R$ sestrojme nejprve podokruh S generovaný množinou B a pak položme $\mathcal{C}l(B) = \{a \in R,;\ a$ je celistvé nad $S\}$.

Pozn. Těleso i okruh budou vždy znamenat těleso komutativní a okruh komutativní.

Otázka k zamyšlení - Jak vypadá uzávěrový systém příslušný operátorům $\mathcal{C}l$ v příkladech 1. a 2.?

Některé uzávěrové operátory mohou mít navíc ještě vlastnost:

(UO4) $\mathcal{C}(B_1 \cup B_2 \cup \cdots \cup B_k) = \mathcal{C}(B_1) \cup \mathcal{C}(B_2) \cup \cdots \cup \mathcal{C}(B_k)$

Taková vlastnost není samozřejmá. Například ji nemá systém všech podprostorů lineárního prostoru nebo systém všech konvexních podmnožin.

Lemma 1.2. *Ať $\mathcal{S}$ je uzávěrový systém, $\mathcal{C} = \mathcal{C}l_{\mathcal{S}}$. Pak $\mathcal{C}$ splňuje **(UO4)**, právě když S splňuje:*

(iii) Jsou–li $A_i \in \mathcal{S}, 1 \leq i \leq k$, pak $A_1 \cup \cdots \cup A_k \in \mathcal{S}$ (Uzavřenost na konečná sjednocení)

Důkaz. **(UO4)** $\Longrightarrow$ (iii): Využijeme, že $A \in \mathcal{S} \iff \mathcal{C}(A) = A$. Jest $A_1 \cup \cdots \cup A_k = \mathcal{C}(A_1) \cup \cdots \cup \mathcal{C}(A_k) = \mathcal{C}(A_1 \cup \cdots \cup A_k)$.
(iii) $\Longrightarrow$ **(UO4)**: Jistě $\mathcal{C}(B_1 \cup \cdots \cup B_k) \supseteq \mathcal{C}(B_i), 1 \leq i \leq k$.
$\mathcal{C}(B_1 \cup \cdots \cup B_k) \subseteq \mathcal{C}(B_1) \cup \cdots \cup \mathcal{C}(B_k)$ plyne z toho, že $\mathcal{C}(B_1) \cup \cdots \cup \mathcal{C}(B_k) \in \mathcal{S}$ dle (iii). □

Definice 1.3 (Topologie uzavřených množin)**.** Uzávěrový systém S se nazývá *topologií uzavřených množin*, jestliže splňuje (i), (ii), (iii) a (iv): $\emptyset \in \mathcal{S}$.

Topologie může být zadána uzavřenými nebo otevřenými množinami na základě vztahu $U \subseteq X$ otevřená $\iff X \setminus U$ uzavřená.

Definice 1.4 (Topologie otevřených množin)**.** *Topologie otevřených množin* na X je tedy systém $\mathcal{U}$, že

- $\emptyset \in \mathcal{U}$;
- $X \in \mathcal{U}$;
- $\bigcup(U_i, i \in I) \in \mathcal{U}$, pokud $U_i \in \mathcal{U}\ \forall i \in I$;
- $U_1 \cap \cdots \cap U_k \in \mathcal{U}$, pokud $U_1, \ldots, U_k \in U$.

Některé uzávěrové systémy vznikají z Galoisovy korespondence.

Definice 1.5 (Galoisova korespondence)**.** Ať X a Y jsou množiny. Ať $\mathcal{A} : \mathcal{P}(X) \to \mathcal{P}(Y)$ a $\mathcal{B} : \mathcal{P}(Y) \to \mathcal{P}(X)$. Pak $(\mathcal{A}, \mathcal{B})$ nazveme *Galoisovou korespondencí*, platí–li:

(i) $\emptyset \in A_1 \subseteq A_2 \in X \implies \mathcal{A}(A_1) \supseteq \mathcal{A}(A_2)$
$\emptyset \in B_1 \subseteq B_2 \in Y \implies \mathcal{B}(B_1) \supseteq \mathcal{B}(B_2)$;

(ii) $\mathcal{BA}(A) \supseteq A$ pro $\forall A \in X$
$\mathcal{AB}(B) \supseteq B$ pro $\forall B \in Y$.

Lemma 1.3. *Ať $(\mathcal{A}, \mathcal{B})$ je Galoisova korespondence. Potom $\mathcal{BA}$ i $\mathcal{AB}$ jsou uzávěrové operátory. Navíc platí $\mathcal{BAB} = \mathcal{B}$ a $\mathcal{ABA} = \mathcal{A}$*

Důkaz. Monotonie $\mathcal{BA}$ plyne z dvojího použití (1). Extensionalita je shodná s podmínkou (2), pro idempotenci stačí ukázat rovnost $\mathcal{ABA} = \mathcal{A}$. Inkluzi $\mathcal{BA}(A) \supseteq A$ dostaneme z (2), takže z (1) plyne $\mathcal{ABA}(A) \subseteq \mathcal{A}(A)$. Pokud v (2) píšeme $\mathcal{A}(A)$ na místě B, obdržíme $\mathcal{ABA}(A) \supseteq \mathcal{A}(A)$. □

Dodatek k Lemma 1.3. Ať $\mathcal{Y} = \{\mathcal{A}(A); A \subseteq X\}$ a $\mathcal{X} = \{\mathcal{B}(B); B \subseteq Y\}$. Potom $\mathcal{A}$ a $\mathcal{B}$ poskytují vzájemně inverzní bijekce množin $\mathcal{X}$ a $\mathcal{Y}$.

Důkaz. To je přímý důsledek vztahů $\mathcal{BAB} = \mathcal{B}$ a $\mathcal{ABA} = \mathcal{A}$. □

Uvažujme nyní těleso K a přirozené číslo $n \geq 1$. Budeme uvažovat okruh $K[x_1, \ldots, x_n]$. Protože seznam $x_1, \ldots, x_n$ se často opakuje, je zvykem psát pouze $K[x]$. Tedy $K[x] = K[x_1, \ldots, x_n]$, kde n se rozumí z kontextu.

Další důležitou množinou bude $\mathbb{A}^n = \bar{K} \times \cdots \times \bar{K}$. Použitím $\mathbb{A}$ odkazuji na afinní prostor. $\bar{K}$ znamená algebraický uzávěr. V algebraické geometrii je zvykem pro každé těleso L, $K \subseteq L \subseteq \bar{K}$ psát $\mathbb{A}^n(L)$ ve významu $\underbrace{L \times \cdots \times L}_{n-krát}$.
$\mathbb{A}^n(L)$ se nazývá množinou *L–racionálních bodů*.

Pro $S \subseteq \mathbb{A}^n$ položme $\mathbb{I}(S) = \{f \in K[x]; \forall a \in S \text{ je } f(a) = 0\}$. Pro $M \subseteq K[x]$ položme $\mathbb{V}(M) = \{a \in \mathbb{A}^n; \forall f \in M \text{ je } f(a) = 0\}$. Symbolicky $\mathbb{A}^n \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftharpoons}} K[x]$

Lemma 1.4. $(\mathbb{I}, \mathbb{V})$ *je Galoisova korespondence.*

Důkaz. Jistě $\emptyset \subseteq S_1 \subseteq S_2 \subseteq \mathbb{A}^n \implies \mathbb{I}(S_1) \supseteq \mathbb{I}(S_2)$, neboť „polynom, který se nuluje na větší množině, se nuluje i na menší“. Podobně $\emptyset \subseteq M_1 \subseteq M_2 \subseteq K[x] \implies \mathbb{V}(M_1) \supseteq \mathbb{V}(M_2)$, neboť „nula většího počtu polynomů je společnou nulou i menšího počtu polynomů“.
Je-li $a \in S$, tak pro $\forall f \in \mathbb{I}(S)$ je $f(a) = 0$, takže $S \subseteq \mathbb{V}\mathbb{I}(S)$. Je-li $f \in M$, tak pro $\forall a \in \mathbb{V}(M)$ je $f(a) = 0$, tedy $M \subseteq \mathbb{I}\mathbb{V}(M)$. □

Definice 1.6 (Algebraické množiny)**.** Množina $S \in \mathbb{A}^n$ se nazývá *algebraická* (případně afinní algebraická), pokud $S = \mathbb{V}(M)$ pro nějaké $M \subseteq K[x]$.

Lemma 1.5. *Platí*

(i) Ať $S_i \subseteq \mathbb{A}^n, i \in I$. Pak $\bigcap_{i\in I} \mathbb{I}(S_i) = \mathbb{I}(\bigcup_{i\in I} S_i)$

(ii) Ať $M_i \in K[x], i \in I$. Pak $\bigcap_{i\in I} \mathbb{V}(M_i) = \mathbb{V}(\bigcup_{i\in I} M_i)$.

Důkaz. Zřejmé. □

Poznámka:
Je-li R okruh a $M \in R$, je zvykem (M) chápat jako ideál generovaný M.
Pokud $M = \{f_1, \ldots, f_k\}$, píšeme místo (M) též $(f_1, \ldots, f_k)$.

Lemma 1.6. $\mathbb{I}(S)$ *je ideál* $K[x]$ *a* $\mathbb{V}(M) = \mathbb{V}((M))$.

Důkaz. Ať $f(a) = 0$ a ať $g \in K[x]$. Pak $(g \cdot f)(a) = g(a) \cdot f(a) = 0$. Je-li též $g(a) = 0$, je $(f + g)(a) = 0$. Proto je $\mathbb{I}(S)$ vždy ideál. Stejná úvaha vede na rovnost $\mathbb{V}((M)) = \mathbb{V}(M)$, neboť $(M) = \{\sum_{i=1}^{k} g_i f_i; f_i \in M \text{ a } g_i \in K[x]\}$. To znamená, že (M) lze získat postupným přidáváním součtů $f_1 + f_2$ a násobků gf. □

Lemma 1.5(i) říká, že ideál $\mathbb{I}(S_1 \cup \cdots \cup S_k)$ je roven ideálu $\mathbb{I}(S_1) \cup \cdots \cup \mathbb{I}(S_k)$. Pro algebraickou geometrii větší roli než průnik ideálů hraje jejich součin. Připomeňme, že pro $I_1, \ldots, I_k$ ideály je

$$I_1 \cdots I_k = \{f_1 \cdots f_k; \forall 1 \leq j \leq k \, f_j \in I_j\}$$

Přitom $I_1 \cdots I_k \subseteq I_1 \cap \cdots \cap I_k$ *(viz KO)*. Máme tedy:

Důsledek 1.7. $\mathbb{I}(S_1 \cup \cdots \cup S_k) \supseteq \mathbb{I}(S_1) \cdots \mathbb{I}(S_k)$.

Lemma 1.8. *Ať $I_1, \ldots, I_k$ jsou ideály v $K[x]$.*
Potom $\mathbb{V}(I_1 \cdots I_k) = \mathbb{V}(I_1) \cup \cdots \cup \mathbb{V}(I_k)$.

Důkaz. Inkluze $\supseteq$ plyne z $I_1 \cdots I_k \subseteq I_j$. Ať $a \in \mathbb{V}(I_1 \cdots I_k) \overset{1.6}{=} \mathbb{V}(\{f_1 \cdots f_k; f_j \in I_j\})$. Předpokládejme, že $a \notin \mathbb{V}(I_1) \cup \cdots \cup \mathbb{V}(I_{k-1})$. Pak existují $f_1 \in I_1, \ldots, f_{k-1} \in I_{k-1}$, že $f_j(a) \neq 0$ pro každé $0 \leq j \leq k-1$. Předpokládejme, že pro všechna $f_k \in I_k$ je $0 = \underbrace{f_1(a) \cdots f_{k-1}(a)}_{\neq 0} f_k(a)$. Tedy $f_k(a) = 0$ a $a \in \mathbb{V}(I_k)$. □

Pro každé $a_1 \in \bar{K}$ se definuje *minimální polynom* $m_{a_1} \in K[x]$ *(viz KO)*. Je-li $a_1 \in \bar{K}$, je $m_{a_1} = x_1 - a_1$. Pokud m_{a_1} chápeme jako polynom v jiné proměnné než x_1, píšeme $m_{a_1}(x_2)$ apod.

Lemma 1.9. *Ať $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$.*
Potom $\mathbb{I}(a) \subseteq (m_{a_1}(x_1), \ldots, m_{a_n}(x_n) \subsetneq K[x]$.

Důkaz. Chceme ukázat, že každé $m_{a_j}(x_j)$ se nuluje na $\{a\}$. To je ovšem zřejmé, neboť $m_{a_j}(a_j) = 0$. Uvažujme nyní homomorfismus okruhů $\pi : K[x] \to K[x_1]$, který nuluje $x_2, \ldots, x_n$. Tedy

$$\pi(\sum_{i_1 \cdots i_n} \lambda_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n}) = \sum_{i_1 \cdots i_n} \lambda_{i_1 \cdots i_n} x_1^{i_1}$$

Jinak řečeno, zobrazuji ideál generovaný $m_{a_1}(x_1), \ldots, m_{a_n}(x_n)$ na $m_{a_1} K[x_1]$ (hlavní ideál), což je vlastní podmnožina $K[x_1]$. Proto platí i inkluze v lemmatu. □

Důsledek 1.10. $\mathbb{V}(K[x]) = \emptyset$

Důkaz. Z $a \in \mathbb{V}(K[x])$ plyne $\mathbb{I}(a) \supseteq \mathbb{IV}(K[x]) = K[x]$ - spor! □

Lemma 1.11. *Ať $\mathcal{C}$ je uzávěrový operátor na X.*
Potom $\{S \subseteq X; \mathcal{C}(S) = S\}$ je topologií uzavřených množin, je-li $\mathcal{C}(\emptyset) = \emptyset$ a pro všechna $S_1, S_2 \subseteq X$ platí $\mathcal{C}(S_1 \cup S_2) \subseteq \mathcal{C}(S_1) \cup \mathcal{C}(S_2)$.

Důkaz. Z $S_1 \cup S_2 \supseteq S_1$ a $S_1 \cup S_2 \supseteq S_2$ plyne $\mathcal{C}(S_1 \cup S_2) \supseteq \mathcal{C}(S_1)$ a $\mathcal{C}(S_1 \cup S_2) \supseteq \mathcal{C}(S_2)$. Je tedy $\mathcal{C}(S_1 \cup S_2) \supseteq \mathcal{C}(S_1) \cup \mathcal{C}(S_2)$, takže $\mathcal{C}(S_1 \cup S_2) = \mathcal{C}(S_1) \cup \mathcal{C}(S_2)$. Zbytek z Lemmatu 1.2 a za ním následující pasáže. □

Tvrzení 1.12 (O algebraických množinách)**.** *Množina $S \subseteq \mathbb{A}^n$ je algebraická, pokud $\mathbb{VI}(S) = S$. Platí, že $S \subseteq \mathbb{A}^n$ je algebraická, pokud $S = \mathbb{V}(I)$ pro nějaký ideál I. Všechny algebraické množiny tvoří topologii uzavřených množin, kde uzávěrový operátor je roven $\mathbb{VI}$.*

Důkaz. S je algebraická $\overset{def.}{\Leftrightarrow}$ $S = \mathbb{V}(M)$ pro nějaké $M \subseteq K[x]$. Je-li $S = \mathbb{V}(M)$, tak $S = \mathbb{VIV}(M) = \mathbb{VI}(S)$ a $\mathbb{I}(S)$ je ideál. Dle 1.10 je $\mathbb{V}(K[x]) = \emptyset$, takže $\mathbb{VI}(\emptyset) = \mathbb{V}(K[x]) = \emptyset$. Dle 1.7 je $\mathbb{I}(S_1 \cup S_2) \supseteq \mathbb{I}(S_1) \cdot \mathbb{I}(S_2)$, takže $\mathbb{VI}(S_1 \cup S_2) \subseteq \mathbb{V}(\mathbb{I}(S_1) \cdot \mathbb{I}(S_2)) \overset{1.8}{=} \mathbb{VI}(S_1) \cup \mathbb{VI}(S_2)$. □

Definice 1.7 (Afinní uzávěr a Zariského topologie)**.** Zobrazení $\mathbb{VI}(S)$ se nazývá *afinním uzávěrem* S.
Topologie určená $\mathbb{VI}(S)$ se nazývá *Zariského topologie* (afinních algebraických množin).

Definice 1.8 (Ireducibilní množiny)**.** Algebraická množina S se nazývá *ireducibilní*, pokud S je neprázdná a nelze ji vyjádřit jako sjednocení vlastních algebraických podmnožin. Tedy $S = S_1 \cup S_2 \implies S_1 = S$ nebo $S_2 = S$.

Pozn.: Připomeňme, že z Dodatku k lemmatu 1.3 plyne
$S_1 \subsetneq S_2 \implies \mathbb{I}(S_1) \supsetneq \mathbb{I}(S_2)$, kdykoliv S_1 a S_2 jsou algebraické.

Lemma 1.13. *Neexistuje nekonečná posloupnost $S_1, S_2, \ldots$ algebraických množin taková, že $S_1 \supsetneq S_2 \supsetneq \ldots$.*

Důkaz. Ať existuje. Pak $\mathbb{I}(S_1) \subsetneq \mathbb{I}(S_2) \subsetneq \ldots$, což je ve sporu s faktem, že $K[x]$ je noetherovský *(viz KO).* □

Lemma 1.14. *Každou neprázdnou algebraickou množinu S lze vyjádřit jako sjednocení ireducibilních algebraických množin.*

Důkaz. Budujme binární strom takový, že

- kořen je roven S
- koncové vrcholy (listy) jsou ireducibilní algebraické množiny
- ostatní vrcholy jsou tvaru $T = T_1 \cup T_2, T_1 \neq T, T_2 \neq T$ algebraické

Strom musí být konečný, neboť v nekonečném by bylo možné najít větev s nekonečnou posloupností ostře klesajících algebraických množin. □

Tvrzení 1.15. *Algebraická množina S je ireducibilní, právě když $\mathbb{I}(S)$ je prvoideál $K[x]$.*

Důkaz. Ať $\mathbb{I}(S)$ není prvoideál. Pak existují ideály $J_1 \supsetneq \mathbb{I}(S), J_2 \supsetneq \mathbb{I}(S)$, že $J_1 J_2 \subseteq \mathbb{I}(S)$ *(viz KO)*. Odsud plyne $\mathbb{V}(J_1) = \mathbb{V}(\mathbb{I}\mathbb{V}(J_1)) \subsetneq \mathbb{V}\mathbb{I}(S) = S$ a $\mathbb{V}(J_2) \subsetneq S$. To znamená, že $S = \mathbb{V}\mathbb{I}(S) = \mathbb{V}(J_1 J_2) = \mathbb{V}(J_1) \cup \mathbb{V}(J_2)$ je sjednocením dvou vlastních algebraických podmnožin. Ať S není ireducibilní, tedy $S = S_1 \cup S_2$, kde $S_1 \subsetneq$ a $S_2 \subsetneq S$. Pak $\mathbb{I}(S_1) \supsetneq \mathbb{I}(S), \mathbb{V}(S_2) \supsetneq \mathbb{I}(S)$ a $\mathbb{I}(S) = \mathbb{I}(S_1 \cup S_2) \overset{1.7}{\supseteq} \mathbb{I}(S_1)\mathbb{I}(S_2)$. □

Definice 1.9 (Ireducibilní rozklad)**.** Buď $S \subseteq \mathbb{A}^n$ algebraická množina. Vyjádření $S = S_1 \cup \cdots \cup S_k$ nazveme jejím *ireducibilním rozkladem*, pokud každá S_i je ireducibilní algebraická a jejím vynecháním vznikne vlastní podmnožina S.

Tvrzení 1.16. *Každá algebraická množina má právě jedno ireducibilní vyjádření (rozklad).*

Důkaz. Ať $S = S_1 \cup \cdots \cup S_k = T_1 \cup \cdots \cup T_l$ jsou dvě taková vyjádření. Pak $\forall i \in \{1, \ldots, k\}$ platí $\mathbb{I}(S_i) \supseteq \mathbb{I}(S) \supseteq \mathbb{I}(T_1) \cdots \mathbb{I}(T_l)$. Protože $\mathbb{I}(S_i)$ je prvoideál, musí existovat $j \in \{1, \ldots l\}$, že $\mathbb{I}(S_i) \supseteq \mathbb{I}(T_j)$. Označme (nějaké) takové j jako $\sigma(i)$. Je tedy $S_i \subseteq T_{\sigma(i)}$. Analogicky $\exists \tau : \{1, \ldots l\} \to \{1, \ldots, k\}$, že $T_j \subseteq S_{\tau(j)}$. Tedy $S_i \subseteq T_{\sigma(i)} \subseteq S_{i'}$, kde $i' = \tau\sigma(i)$. Z $i' \neq i$ by vyplynulo, že S_i lze vypustit. Je tedy $i = \tau\sigma(i)$ a podobně $j = \sigma\tau(j)$. Proto $k = l$ a σ a τ jsou vzájemně inverzní permutace, přičemž z $S_i \subseteq T_{\sigma(i)} \subseteq S_i$ plyne $S_i = T_{\sigma(i)}$. □

Definice 1.10 (Radikály a radikálové ideály)**.** Připomeňme, že $\sqrt{I} = \{a \in R; \exists k \geq 1, \text{ že } a^k \in I\}$ se nazývá *radikál* ideálu I v okruhu R.
Platí, že $\sqrt{I} = \bigcap(P \in \text{ Spec } R; P \supseteq I)$, kde Spec R označuje množinu všech prvoideálů v R. Máme $\sqrt{P} = P$ pro každé $P \in$ Spec R a $\sqrt{I} \supseteq I$ pro každý ideál I. Ideály, které splňují $\sqrt{I} = I$ se nazývají *radikálové*. Operátor $M \mapsto \sqrt{(M)}$ je uzávěrový operátor na R.

Naším cílem nyní bude ukázat, že radikálové ideály v $K[x]$ se shodují s ideály, které lze vyjádřit jako $\mathbb{I}(S), S \subseteq \mathbb{A}^n$. K tomu nám poslouží Hilbertova věta o nulách, jež uvedený fakt tvrdí pro případ $K = \bar{K}$.

Hilbertova věta o nulách: Ať K je algebraicky uzavřené těleso. Maximální ideály $K[x]$ jsou právě všechny ideály tvaru:
$M(a_1,\dots,a_n) = (x_1 - a_n,\dots,x_n - a_n)$, kde $a = (a_1,\dots,a_n) \in \mathbb{A}^n$. Pro každý vlastní ideál $I \subsetneq K[x]$ platí, že $\mathbb{IV}(I) = \sqrt{I} = \bigcup(M(a); a \in \mathbb{V}(I))$.

Přechod od $\bar{K}$ ke K vyžaduje jistou drobnou algebraickou přípravu. Jsou-li $R \subseteq S$ okruhy a I je ideál R, pak

$$IS = \{\sum_{i=1}^{k} a_i s_i; a_i \in I \,\&\, s_i \in I, 1 \le i \le k\}$$

je ideál S. Je to nejmenší ideál, který obsahuje I.

Lemma 1.17. *Ať $K \subseteq L$ jsou tělesa a ať I je ideál $K[x]$. Položme $J = IL[x]$. Pak $I = J \cap K[x]$.*

Důkaz. Je zřejmé, že $I \subseteq J \cap K[x]$.
Pro důkaz opačné inkluze stačí ověřit, že kdykoliv $g \in K[x]$ lze vyjádřit jako $\sum_{i=1}^{k} a_i s_i$, kde $a_1,\dots,a_k \in I \,\&\, s_1,\dots,s_k \in L[x]$, tak $\exists t_1,\dots,t_k \in K[x]$, že $\sum a_i s_i = \sum a_i t_i$. Pak je totiž každé $a_i s_i$ prvkem I, takže i $g \in I$.
Vyložíme, že existenci t_i lze odvodit ze základních fakt lineární algebry. Lze jistě zvolit $N \ge 0$, že $g = \sum g_{j_1,\dots,j_n} x_1^{j_1} \cdots x_n^{j_n}$, $a_i = \sum a_{i_{j_1,\dots,j_n}} x_1^{j_1} \cdots x_n^{j_n}$ a $s_i = \sum s_{i_{j_1,\dots,j_n}} x_1^{j_1} \cdots x_n^{j_n}$, kde $0 \le j_1 + \cdots + j_n \le N \,\&\, 1 \le i \le k$.
Máme $a_{i_{j_1,\dots,j_n}} \in K$, $g_{j_1,\dots,j_n} \in K \,\&\, s_{i_{j_1,\dots,j_n}} \in L$. Definujme $b_{i_{j_1,\dots,j_n}} \in L$ tak, že $s_i a_i = \sum b_{i_{j_1,\dots,j_n}} x_1^{j_1} \cdots x_n^{j_n}$. Volbu N lze provézt tak, že $0 \le j_1 + \cdots + j_n \le N$. Rovnost $g = \sum a_i s_i$ pak znamená, $\forall j_1 \ge 0,\dots,j_n \ge 0$, $\sum j_k \le N$ musí být $b_{1_{j_1,\dots,j_n}} + \cdots + b_{k_{j_1,\dots,j_n}} = g_{j_1,\dots,j_n}$.
Jest $b_{i_{j_1,\dots,j_n}} = \sum a_{i_{j'_1,\dots,j'_n}} s_{i_{j''_1,\dots,j''_n}}$, kde $j'_k + j''_k = j_k$. Jestliže za každé $b_{i_{j_1,\dots,j_n}}$ dosadíme

$$\sum_{j'_k + j''_k = j_k} a_{i_{j'_1,\dots,j'_n}} s_{i_{j''_1,\dots,j''_n}},$$

tak se uvedené rovnosti dají chápat jako systém lineárních rovnic s koeficienty $a_{i_{j'_1,\dots,j'_n}} \in K$ a neznámými $x_{i_{j''_1,\dots,j''_n}} = s_{i_{j''_1,\dots,j''_n}}$. Pravá strana je tvořena prvky K. Hodnost matice, která je tvořena prvky K, se nezmění, chápeme-li ji jako matici nad L. Má-li pak soustava řešení v L $(x_{i_{j''_1,\dots,j''_n}} = s_{i_{j''_1,\dots,j''_n}})$, musí mít i řešení v $K(x_{i_{j''_1,\dots,j''_n}} = t_{i_{j''_1,\dots,j''_n}})$. □

Tvrzení 1.18. *Ať $I \subseteq K[x]$ je ideál. Potom $\mathbb{IV}(I) = \sqrt{I}$.*

Důkaz. Použijeme Hilbertovu větu o nulách. Potřebujeme dát do souvislosti Galoisovu korespondenci $(\mathbb{I}, \mathbb{V})$, která se vztahuje k $\mathbb{A}^n$ a $K[x]$, a obdobně definovanou Galoisovu korespondenci $(\underline{\mathbb{I}}, \underline{\mathbb{V}})$, která se vztahuje k $\mathbb{A}^n$ a $\bar{K}[x]$. Podle lemmatu 1.6 je $\underline{\mathbb{V}}(I) = \underline{\mathbb{V}}(I\bar{K}[x])$. Z definice operátoru $\mathbb{V}$ máme $\underline{\mathbb{V}}(I) = \mathbb{V}(I)$. Z definice operátoru $\mathbb{I}$ plyne, že $\mathbb{I}\mathbb{V}(I) = \underline{\mathbb{I}}\mathbb{V}(I) \cap K[x]$. Položme $J = I\bar{K}[x]$. Podle Hilbertovy věty o nulách je $\underline{\mathbb{I}}\mathbb{V}(I) = \underline{\mathbb{V}}(J) = \sqrt{J} = \{f \in \bar{K}[x]; f^m \in J \text{ pro nějaké } m \geq 1\}$. Tedy $f \in K[x]$ leží v $\sqrt{J}$ právě když $f^m \in J \cap K[x]$ pro nějaké $m \geq 1$. Ovšem podle lemmatu 1.17 je $J \cap K[x] = I$. Tedy $f \in K[x]$ padne do $\sqrt{J}$ právě když $f \in \sqrt{I}$. Proto $\mathbb{I}\mathbb{V}(I) = \sqrt{J} \cap K[x] = \sqrt{I}$. □

Uzávěrový operátor $\mathbb{V}\mathbb{I}$ posílá každou podmnožinu $\mathbb{A}^n$ na nejmenší ji obsahující algebraickou množinu. Na druhou stranu uzávěrový operátor $\mathbb{I}\mathbb{V}$ posílá každou podmnožinu $K[x]$ na nejmenší radikálový ideál, který ji obsahuje. Operátor $\mathbb{I}$ a $\mathbb{V}$ tedy poskytují vzájemně jednoznačnou korespondenci mezi algebraickými množinami a radikálovými ideály.
Operátor $\mathbb{V}\mathbb{I}$ je současně uzávěrovým operátorem Zariského topologie na $\mathbb{A}^n$ (její struktura závisí na volbě K). Algebraická množina je ireducibilní, není-li ji možno vyjádřit jako sjednocení vlastních algebraických podmnožin. Ireducibilní algebraické množiny tedy odpovídají prvoideálům (každý prvoideál je zjevně radikálovým ideálem). Výše uvedená fakta budeme v dalším považovat za samozřejmá.

Kapitola 2

Afinní variety a topologie

Ať K je těleso a ať $\mathbb{A}^n$ je jemu příslušný afinní prostor. Připomeňme, že algebraická množina $V \subseteq \mathbb{A}^n$ je ireducibilní, je-li $\mathbb{I}(V)$ prvoideál $K[x]$. Jako synonymum k označení ireducibilní algebraické množiny budeme používat slovo *varieta*, či přesněji sousloví *afinní varieta* (časem se seznámíme i s projektivními varietami). Poznamenejme, že v různých jiných kontextech se pod varietou rozumí i jiné typy objektů, a to i uvnitř algebraické geometrie. Prvoideály jsou v našem pojetí vždy vlastními ideály. Proto je varieta vždy množinou neprázdnou.

Definice 2.1 (Souřadnicové okruhy)**.** *Souřadnicovým okruhem* algebraické množiny S se rozumí okruh $K[x]/\mathbb{I}(S)$. Značí se $K[S]$.

Lemma 2.1. *Neprázdná algebraická množina S je varietou právě tehdy, když $K[S]$ je oborem integrity.*

Důkaz. To je přímý důsledek faktu, že pro ideál I okruhu R platí, že R/I je obor integrity právě když I je prvoideál. □

Definice 2.2 (Funkční tělesa)**.** Je-li V varieta, tak se podílové těleso okruhu $K[V]$ nazývá *funkční těleso* variety V. Značí se $K(V)$.
Buď nyní V varieta s bodem $\alpha = (\alpha_1, \ldots, \alpha_n) \in V$. Každý prvek $K(V)$ lze zapsat jako $\frac{f+\mathbb{I}(V)}{g+\mathbb{I}(V)}$. Říkáme, že $\frac{f}{g}$ *representuje* tento prvek.

Každé $\gamma \in K(V)$ může mít samozřejmě více representací. Víme, že $\frac{f_1+\mathbb{I}(V)}{g_1+\mathbb{I}(V)} = \frac{f_2+\mathbb{I}(V)}{g_2+\mathbb{I}(V)}$ právě když $f_1 g_2 - f_2 g_1 \in \mathbb{I}(V)$.
Pro $\alpha \in V$ definujeme $O_\alpha = \{\gamma \in K(V); \exists f, g \in K[x], \text{že } \gamma = \frac{f+\mathbb{I}(V)}{g+\mathbb{I}(V)}, g(\alpha) \neq 0\}$. Zřejmě je O_α podokruhem $K(V)$.

Lemma 2.2. *Ať $\gamma \in O_\alpha$ je representováno $\frac{f_1}{g_1}$ i $\frac{f_2}{g_2}$, kde $g_1(\alpha) \neq 0, g_2(\alpha) \neq 0$. Pak $f_1(\alpha) = 0 \iff f_2(\alpha) = 0$.*

Důkaz. Označme $h = f_1 g_2 - g_2 f_1 \in \mathbb{I}(V)$. Tedy $h(\alpha) = 0$, takže $f_1(\alpha) \underbrace{g_2(\alpha)}_{\neq 0} = f_2(\alpha) \underbrace{g_1(\alpha)}_{\neq 0}$. □

Pozn: $M_\alpha \subseteq O_\alpha$ definuji jako $\{\gamma \in O_\alpha$; je-li γ representováno $\frac{f}{g}, g(\alpha) \neq 0$, tak $f(\alpha) = 0\}$. Z L2.2 snadno plyne, že M_α je ideálem O_α.

Lemma 2.3. *O_α je lokální okruh a M_α je jeho (jediný) maximální ideál.*

Důkaz. Ověříme, že $O_\alpha \setminus M_\alpha = O_\alpha^*$. Jistě $O_\alpha \setminus M_\alpha \supseteq O_\alpha^*$. Ať $\gamma \in O_\alpha \setminus M_\alpha$ je representováno f/g, kde $g(\alpha) \neq 0$. Pak $f(\alpha) \neq 0$ dle L2.2. To znamená, že O_α obsahuje i γ^{-1}, neboť γ^{-1} je representováno g/f. □

Definice 2.3 (Polynomiální zobrazení)**.** Ať $f : V \to W$ je zobrazení, kde $V \subseteq \mathbb{A}^n$ a $W \subseteq \mathbb{A}^m$ jsou variety. Toto zobrazení nazveme *polynomiální*, jestliže existují polynomy $f_1, \ldots, f_m \in K[x]$ takové, že pro každé $\alpha = (\alpha_1, \ldots, \alpha_n) \in V$ je $f(x) = (f_1(\alpha), \ldots, f_m(\alpha)) \in W$.

Poznámky:
• Identické zobrazení $V \to V$ je jistě *polynomiální*, protože za $f_1, \ldots, f_n$ lze zvolit polynomy $x_1, \ldots, x_n$.
• Je-li $f : V \to W, g : W \to Z$, kde $V \subseteq \mathbb{A}^n, W \subseteq \mathbb{A}^m, Z \subseteq \mathbb{A}^k$, přičemž f je určeno $(f_1, \ldots, f_m)$ a g je určeno $(g_1, \ldots, g_k)$, máme $(g \cdot f)(\alpha) = g(f_1(\alpha), \ldots, f_m(\alpha)) = (g_1(f_1(\alpha), \ldots, f_m(\alpha)), \ldots, g_k(f_1(\alpha), \ldots, f_m(\alpha)))$, což lze vyjádřit jako $(h_1(\alpha), \ldots, h_k(\alpha))$, kde

$$h_j(\alpha_1, \ldots, \alpha_n) = h_j(\alpha) = g_j(f_1(\alpha), \ldots, f_m(\alpha))$$

Vidíme, že složení polynomiálních zobrazení je opět polynomiální.

Definice 2.4 (Morfismy)**.** O polynomiálních zobrazeních $f : V \to W$ se mluví také jako o (afinních) *morfismech* variet V a W.
Dvě variety V a W nazveme *izomorfní*, jestliže existují polynomiální zobrazení $f : V \to W$ a $g : W \to V$ takové, že $gf = \mathrm{id}_V$ a $fg = \mathrm{id}_W$.

Později ukážeme, že V je izomorfní W právě když $K[V] \cong K[W]$.

Lemma 2.4. *Ať $f : V \to W$ a $g : V \to W$ jsou polynomiální zobrazení variet V a W, přičemž f je určeno $(f_1, \ldots, f_m)$ a g je určeno $(g_1, \ldots, g_m)$. Pak $\forall \alpha \in V$ je $f(\alpha) = g(\alpha) \iff f_i - g_i \in \mathbb{I}(V)$ pro každé $i \in \{1, \ldots, m\}$.*

Důkaz. Podmínku $f_i - g_i \in \mathbb{I}(V)$ lze vyjádřit také tak, že $f_i(\alpha) = g_i(\alpha)$ pro každé $\alpha \in V$. Zbytek je jasný. □

Vedle polynomiálních zobrazení má smysl uvažovat i racionální zobrazení $(r_1, \ldots, r_m) : V \to W$, kde $r_i = s_i/t_i$ pro $s_i, t_i \in K[x]$. Je-li $r'_i = s'_i/t'_i$ jiná sada racionálních zobrazení, tak ve zobecněném lemmatu 2.4 by na pravé straně mohla stát podmínka $s_i t'_i - s'_i t_i \in \mathbb{I}(V)$. Ovšek jak formulovat levou stranu? Problém je nejen v tom, že r_i a r'_i nemusí být definovány ve všech bodech V, ale i v tom, že nulové body t_i a t'_i se mohou velmi lišit. Cílem dalšího výkladu bude ukázat, že problém vážný vlastně není, neboť za uvedených podmínek bude množina bodů V, na které jsou všechna t_i i t'_i nenulová, hustou podmnožinou V v Zariského topologii.

Poznámky k topologii: Buď Y podmnožina topologického prostoru X. O $S \subseteq Y$ řekneme, že je otevřená v Y, je-li $S = Y \cap U$ pro nějakou otevřenou podmnožinu prostoru X. Podobně vztahem $S = Y \cap F$, $F \subseteq X$ uzavřená, definujeme množiny uzavřené v Y. Je snadné ověřit, že tímto lze na Y definovat topologii (říkáme jí *indukovaná*, nebo též zděděná).
Je-li Y otevřená množina v X, jsou indukovanými otevřenými množinami právě všechny otevřené podmnožiny X obsažené v Y. Podobně, je-li Y uzavřená, jsou indukovanými uzavřenými množinami právě všechny uzavřené podmnožiny X obsažené v Y. To je zřejmé.
V topologickém prostoru X se množina D nazývá hustá, je-li její uzávěr roven X.

Lemma 2.5. *Množina $D \subseteq X$ je hustá, právě když $X \setminus D$ neobsahuje žádnou neprázdnou otevřenou množinu.*

Důkaz. Označme F uzávěr D. Ať $U \subseteq X \setminus D$ je otevřená. Je-li $U \neq \emptyset$, je $F \subseteq X \setminus U$, neboť $D \subseteq X \setminus U$, přičemž $X \setminus U$ je uzavřená. Z $U \neq \emptyset$ plyne $F \neq X$. Je-li $F \neq X$, je $X \setminus F$ neprázdná otevřená množina v $X \setminus D$. □

Lemma 2.6. *Ať U a D jsou husté podmnožiny topologického prostoru X. Je-li U otevřená množina, je množina $U \cap D$ hustá.*

Důkaz. Ať V je otevřená taková, že $V \cap (U \cap D) = \emptyset$. Pak je $V \cap U$ otevřená a splňuje $(V \cap U) \cap D = \emptyset$. Podle L2.5 musí být $V \cap U = \emptyset$. Dalšími aplikacemi téhož lemmatu dostáváme $V = \emptyset$, takže $U \cap D$ musí být hustá. □

Varieta V má indukovanou Zariského topologii. Jejími uzavřenými množi nami $F \subseteq V$ jsou uzavřené (tedy algebraické) množiny Zariského K–topologie $\mathbb{A}^n$. Definice variety říká, že z $V = F_1 \cup F_2$, kde obě F_i jsou uzavřené, vyplývá, že $V = F_1$ nebo $V = F_2$.

Tvrzení 2.7. *Každá neprázdná otevřená podmnožina variety V je hustá.*

Důkaz. Ať $U_1 \subseteq V$ je otevřená a neprázdná. Ať $U_2 \subseteq V$ je také otevřená a ať $U_2 \cap U_1 = \emptyset$. Podle L2.5 stačí ukázat, že $U_2 = \emptyset$. Položme $F_i = V \setminus U_i, i \in \{1,2\}$. Z $U_1 \cap U_2 = \emptyset$ plyne $V = F_1 \cup F_2$. Z $U_1 \neq \emptyset$ plyne $F_1 \subsetneq V$. Protože V je varieta, dostáváme $F_2 = V$, takže $U_2 = \emptyset$. □

Pro každé $f \in K[x]$ je $D_f = \{\alpha \in \mathbb{A}^n; f(\alpha) \neq 0\}$ otevřenou množinou, neboť $D_f = \mathbb{A}^n \setminus \mathbb{V}(f)$.

Tvrzení 2.8. *(i) Pro každou algebraickou množinu $S \subseteq \mathbb{A}^n$ existuje $k \geq 1$ a $f_1, \ldots, f_k \in K[x]$ takové, že $S = \mathbb{V}(f_1, \ldots, f_k)$.*

(ii) Pro každou otevřenou množinu $U \subseteq \mathbb{A}^n$ existuje $k \geq 1$ a $f_1, \ldots, f_k \in K[x]$, že $U = D_{f_1} \cup \cdots \cup D_{f_k}$.

Důkaz. Ať $S = \mathbb{V}(I)$, kde I je ideál. Okruh $K[x]$ je noetherovský, a proto je I generován konečnou množinou $\{f_1, \ldots, f_k\}$. Podle L1.6 je $S = \mathbb{V}(f_1, \ldots, f_k) = \mathbb{V}(f_1) \cap \cdots \cap \mathbb{V}(f_k)$. Jistě $D_{f_i} = \mathbb{A}^n \setminus \mathbb{V}(f_i)$, odkud $\mathbb{A}^n \setminus S = D_{f_1} \cup \cdots \cup D_{f_k}$. Každou otevřenou množinu lze vyjádřit jako $\mathbb{A}^n \setminus S$ kde S je algebraická. □

Varieta V má zděděnou topologii, a proto její otevřené množiny jsou tvaru $(D_{f_1} \cap V) \cup \cdots \cup (D_{f_k} \cap V)$.

Tvrzení 2.9. *Ať pro $i \in \{1,2\}$ jsou $f_i, g_i \in K[x]$ taková, že $g_i \notin \mathbb{I}(V)$. Pak je $U = D_{g_1} \cap D_{g_2} \cap V$ otevřená hustá podmnožina V. Ať $D \subseteq U$ je nějaká hustá podmnožina V. Potom*

$$\frac{f_1(\alpha)}{g_1(\alpha)} = \frac{f_2(\alpha)}{g_2(\alpha)} \text{ pro všechna } \alpha \in D \iff \frac{f_1 + \mathbb{I}(V)}{g_1 + \mathbb{I}(V)} = \frac{f_2 + \mathbb{I}(V)}{g_2 + \mathbb{I}(V)}.$$

Důkaz. Z $g_i \notin \mathbb{I}(V)$ plyne, že $U_i = D_{g_i} \cap V$ je neprázdná otevřená podmnožina V. Z L2.6 a L2.7 víme, že $U = U_1 \cap U_2$ je otevřená a hustá. Uvažme nyní $h = f_1 g_2 - f_2 g_1$. Stačí ukázat, že $h \in \mathbb{I}(V)$ právě když $h(\alpha) = 0$ pro každé $\alpha \in D$. Přímá implikace je triviální. Pro opačnou implikaci stačí nahlédnout, že $D_h \cap V = \emptyset$. To ovšem plyne z L2.5, neboť předpokládáme, že $D_h \cap D = \emptyset$. □

Poznámky:
• Z definice tělesa plyne, že každé $\gamma \in K(V)$ lze representovat zkomkem f/g tak, že $g \notin \mathbb{I}(V)$. Z tvrzení 2.9 vyplývá, že dvě racionální lomené funkce $f_i(x)/g_i(x)$ se shodují na husté podmnožině V právě když f_i/g_i representují týž prvek $K(V)$. Proto můžeme prvky $K(V)$ označit za *racionální funkce* $V \to K$.
• Pro $\gamma \in K(V)$ označme $D_{(\gamma)}$ sjednocení všech množin $D_g \cap V$ takových, že $g \notin \mathbb{I}(V)$ a že existuje nějaké $f \in K[x]$, pro které f/g representuje γ. Množina $D_{(\gamma)}$ je sjednocením hustých otevřených množin, a proto je hustou otevřenou podmnožinou V. Pro každé $\alpha \in D_{(\gamma)}$ existuje f/g representující γ takové, že $g(\alpha) \neq 0$. Proto můžeme právem $D_{(\gamma)}$ nazvat *definičním oborem* racionální funkce γ.
• Ať X a Y jsou topologické prostory. Zobrazení $f : X \to Y$ nazveme *spojité*, je-li $f^{-1}(U)$ otevřená podmnožina X, kdykoliv je $U \subseteq Y$ otevřená. Pokud $U = U_1 \cup \cdots \cup U_k$, kde U_i jsou otevřené, tak zjevně stačí ověřit otevřenost každé $f^{-1}(U_i)$, neboť $f^{-1}(U) = f^{-1}(U_1) \cup \cdots \cup f^{-1}(U_k)$.

Uvažme lomené racionální funkce $f_j(x)/g_j(x), 1 \leq j \leq m$ a položme $\varphi = (\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)})$. Pak φ lze považovat za zobrazení $D_{(\varphi)} \to \mathbb{A}^m$, kde $D_{(\varphi)} = D_{g_1} \cap \cdots \cap D_{g_m}$ je otevřená podmnožina $\mathbb{A}^n$.

Lemma 2.10. *Zobrazení $\varphi : D_{(\varphi)} \to \mathbb{A}^m$ je spojité.*

Důkaz. Ať $h \in K[x_1, \ldots, x_m]$. Podle bodu (ii) tvrzení 2.8 stačí, že $\varphi^{-1}(D_h)$ je otevřená podmnožina $\mathbb{A}^n$. Pro $\alpha \in D_\varphi$ lze $h\varphi(\alpha)$ zapsat jako $\frac{p(\alpha)}{q(\alpha)}$, kde $p, q \in K[x]$ a $q(\alpha) = g_1^{e_1}(x) \cdots g_m^{e_m}(x)$, pro nějaké $e_1 \geq 1, \ldots, e_m \geq 1$. Vidíme, že $\alpha \in \varphi^{-1}(D_h) \iff \varphi(\alpha) \in D_h \iff h\varphi(\alpha) \neq 0 \iff p(\alpha) \neq 0 \iff \alpha \in D_p$ pro každé $\alpha \in D_\varphi$. Tudíž $\varphi^{-1}(D_h) = D_p \cap D_{(\varphi)}$ je otevřená. □

Definice 2.5 (Racionální zobrazení)**.** *Racionálním zobrazením* z variety $V \subseteq \mathbb{A}^n$ do variety $W \subseteq \mathbb{A}^m$ nazveme každou m-tici $(\gamma_1, \ldots, \gamma_m)$ racionálních funkcí $\gamma_1, \ldots, \gamma_m \in K(V)$ takových, že pro každé $\alpha \in D_{(\varphi_1)} \cap \cdots \cap D_{(\varphi_m)} = D_{(r)}$ je $(\gamma_1(\alpha), \ldots, \gamma_m(\alpha)) \in W$. Množina $D_{(r)}$ je podle lemmatu 2.6 hustou otevřenou podmnožinou V. Lze ji považovat za definiční obor racionálního zobrazení r.

Definice 2.6 (Representace racionálních zobrazení)**.** Pokud $\frac{f_j}{g_j}, g_j \notin \mathbb{I}(V)$ representují $\gamma_j, 1 \leq j \leq m$, tak m–tici $\varphi = (\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)})$ nazýváme *representací* r. Je zřejmé, že $D_{(r)}$ je sjednocením všech hustých otevřených množin $D_{(\varphi)} \cap V$ takových, že φ representuje r.

Množina $D_{(\varphi)} \cap V$ je hustá otevřená, neboť každá z množin $D_{g_j} \cap V$ je hustá otevřená.

Lemma 2.11. *Ať φ representuje racionální zobrazení r z V do W. Označme ψ zúžení φ na $D_{(\varphi)} \cap V$. Pak $\psi : D_{(\varphi)} \cap V \to W$ a $r : D_{(r)} \to W$ jsou spojitá zobrazení.*

Důkaz. Ať $U \subseteq \mathbb{A}^n$ je otevřená. Pak $\psi^{-1}(U \cap V) = \varphi^{-1}(U) \cap V$, což je podle lemmatu 2.10 otevřená množina ve V. Proto je ψ spojité. Místo ψ pišme $\tilde{\varphi}$. Ať φ probíhá všechny representace r. Pak je $r^{-1}(U \cap W)$ sjednocením všech $\tilde{\varphi}(U \cap W)$, a proto je to množina otevřená. Tudíž i r je spojité. □

Lemma 2.12. *Nechť $V \subseteq \mathbb{A}^n$ a $W \subseteq \mathbb{A}^m$ jsou variety a ať $D \subseteq V$ je hustá. Ať $\varphi = (\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)})$ je takové, že $f_j, g_j \in K[x], 1 \leq j \leq m$, že $D \subseteq D_{(\varphi)}$ a že $\varphi(\alpha) \in W$ pro každé $\alpha \in D$. Ať γ_j je racionální funkce representovaná f_j/g_j. Potom $r = (\gamma_1, \ldots, \gamma_m)$ je racionální zobrazení z variety V do variety W.*

Důkaz.
Ať f'_j/g'_j je nějaká representace $\gamma_j, g'_j \notin \mathbb{I}(V)$. Položme $\varphi' = (\frac{f'_1(x)}{g'_1(x)}, \ldots, \frac{f'_m(x)}{g'_m(x)})$ a $D' = D \cap D_{(\varphi')}$. Chceme ověřit, že $\varphi'(\alpha) \in W$ pro každé $\alpha \in D_{(\varphi')} \cap V$. Mějme $W = \mathbb{V}(h_1, \ldots, h_k)$, kde $h_s \in K[x_1, \ldots, x_m], 1 \leq s \leq m$. Cílem tedy je ukázat, že $h\varphi'(\alpha) = 0$ pro každé $h = h_s$ a každé $\alpha \; in D_{(\varphi')} \cap V$. Přitom $h\varphi'(\alpha) = 0 \iff \varphi'(\alpha) \notin D_h \iff \alpha \notin (\varphi')^{-1}(D_h)$. Předpokládáme, že $\varphi^{-1}(D_h) \cap D = \emptyset$. Zobrazení φ a φ' se na $D_{(\varphi')} \cap D_{(\varphi')} \supseteq D'$ shodují, takže je i $(\varphi')^{-1}(D_h) \cap D' = ((\varphi')^{-1}(D_h) \cap V) \cap D' = \emptyset$. Podle lemmatu 2.6 je množina $D' = D \cap D_{(\varphi')}$ hustá podmnožina V. Proto podle lemmatu 2.5 musí být množina $(\varphi')^{-1}(D_h) \cap V$ prázdná, neboť podle lemmatu 2.10 je otevřená. Tudíž $\alpha \notin (\varphi')^{-1}(D_h)$ pro každé $\alpha \in V$. □

Uvažme nyní zobrazení $\varphi = (\frac{f_1(x)}{g_1(x)}, \ldots, \frac{f_m(x)}{g_m(x)}) : D_{(\varphi)} \to \mathbb{A}^m$ a $\psi = (\frac{h_1(x_1,\ldots,x_m)}{k_1(x_1,\ldots,x_m)}, \ldots, \frac{h_l(x_1,\ldots,x_m)}{k_l(x_1,\ldots,x_m)}) : D_{(\psi)} \to \mathbb{A}^l$.
Pak můžeme uvažovat složené zobrazení $\psi \circ \varphi : \varphi^{-1}(D_{(\psi)}) \to \mathbb{A}^l$. Za $x_1, \ldots, x_m$ dosazujeme $f_1(x)/g_1(x), \ldots, f_m(x)/g_m(x)$. Vzniklé obrazy lze jistě upravit tak, že pro každé $\alpha \in \varphi^{-1}(D_{(\psi)}$ je $(\psi \circ \varphi)(\alpha) = (\frac{p_1(\alpha)}{q_1(\alpha)}, \ldots, \frac{p_l(\alpha)}{q_l(\alpha}$), kde $p_r, q_r \in K[x], 1 \leq r \leq l$. Položme $\mu = (\frac{p_1(\alpha)}{q_1(\alpha)}, \ldots, \frac{p_l(\alpha)}{q_l(\alpha}$). Pak je $\varphi^{-1}(D_{(\psi)}) \subseteq D_{(\mu)}$, ale rovnost platit nemusí.
Předpokládejme nyní, že $V \subseteq \mathbb{A}^n, \mathbb{N} \subseteq \mathbb{A}^m$ a $\mathbb{Z} \subseteq \mathbb{A}^l$ jsou variety takové, že $\varphi(V \cap D_{(\varphi)}) \subseteq W$ a $\psi(W \cap D_{(\psi)}) \subseteq Z$. Předpokládejme, že $V \cap D_{(\varphi)} \neq \emptyset$ a $W \cap D_{(\psi)} = \emptyset$. Pak může nastat, že každé $\varphi(\alpha)$, kde $\alpha \in V \cap D_{(\varphi)}$ leží

mimo $D_{(\psi)}$. To se stane právě tehdy, když je množina $U = V \cap \varphi^{-1}(W \cap \psi^{-1}(Z))$ prázdná. Množina U je podle lemmatu 2.11 vždy ve V otevřená. Je-li neprázdná, je hustá. Pro každé $\alpha \in U$ je $\mu(\alpha) = (\psi \circ \varphi)(\alpha) \in Z$, takže podle lemmatu 2.12 existuje racionální zobrazení $t : V \to Z$, které μ representuje. Tuto úvahu použijeme v důkazu tvrzení 2.13.

Definice 2.7 (Dominantní zobrazení)**.** Racionální zobrazení r z variety V do variety W nazveme *dominantní*, je-li $\{r(\alpha); \alpha \in D_{(r)}\}$ hustou podmnožinou W.

Tvrzení 2.13. *Ať r je racionální zobrazení z variety V do variety W a s racionální zobrazení z variety W do variety Z. Předpokládejme, že $U = r^{-1}(s^{-1}(Z)) \neq \emptyset$. Pak je U hustá otevřená podmnožina V a existuje právě jedno racionální zobrazení $t : V \to Z$ takové, že $U \subseteq D_{(t)}$ a $s(r(\alpha)) = t(\alpha)$ pro každé $\alpha \in U$. Je-li r dominantní, je vždy $r^{-1}(s^{-1}(Z)) \neq \emptyset$.*

Důkaz. Pro $\alpha \in U$ existují $\varphi = \varphi_\alpha$ a $\psi = \psi_\alpha$ takové, že φ representuje r, ψ representuje s a $\alpha \in \varphi^{-1}(D_{(\psi)})$. Je tedy $\psi(\varphi(\alpha)) = s(r(\alpha))$ a $\alpha \in U_\alpha = V \cap \varphi^{-1}(W \cap \psi^{-1}(Z))$, přičemž U_α je hustá otevřená podmnožina V. Sestrojme $\mu = \mu_\alpha$ jako v úvaze výše a uvažme racionální zobrazení $t_\alpha : V \to Z$ určené zobrazením μ_α. Postupujeme-li stejně pro nějaké $\beta \in U$, zjistíme, že μ_α a μ_β se shodují na otevřené husté podmnožině $U_\alpha \cap U_\beta$. Z tvrzení 2.9 plyne, že $t_\alpha = t_\beta$ a že $t = t_\alpha$ je jediné možné. Zbývá ukázat, že $U \neq \emptyset$, je-li r dominantní. To je však snadné, protože neprázdná otevřená množina $D_{(\psi)} \cap W$ má podle lemmatu 2.5 neprázdný průnik s hustou množinou $\{r(\alpha); \alpha \in D_{(\varphi)}\}$. □

Definice 2.8 (Biracionálně ekvivalentní variety)**.** Pokud racionální zobrazení t popsané v tvrzení 2.13 existuje, označme ho $\mathrm{comp}(s, r)$. Víme, že existuje vždy, když je r dominantní.
Variety $V \subseteq \mathbb{A}^n$ a $W \subseteq \mathbb{A}^m$ se nazývají *biracionálně ekvivalentní*, pokud existují dominantní racionální zobrazení r z V do W a s z W do V taková, že $\mathrm{comp}(s, r) = \mathrm{id}_V$ a $\mathrm{comp}(r, s) = \mathrm{id}_W$.

V následující kapitole ukážeme, že $K(V) \cong K(W)$ právě když V a W jsou biracionálně ekvivalentní.

Kapitola 3

Afinní zobrazení a algebra

Ať $\varphi : X \to Y$ je zobrazení množin. Pak pro každé $g : Y \to K$ se místo $g \circ \varphi$ někdy píše $\varphi^*(g)$. Je-li $\psi : W \to X$ jiné zobrazení, pak

$$\psi^*(\varphi^*(g)) = g \circ \varphi \circ \psi = (\varphi \circ \psi)^*(g).$$

Ať například $X = \mathbb{A}^n, Y = \mathbb{A}^m$ a $f = (f_1, \ldots, f_m)$, kde $f_i \in K[x] = K[x_1, \ldots, x_n], 1 \leq i \leq m$. Pak pro $g \in K[x_1, \ldots, x_m]$ je $f^*(g)$ možno ztotožnit s polynomem $h \in K[x], h(x_1, \ldots, x_n) = f(f_1(x), \ldots, f_m(x))$.
Je-li $g_1, g_2 \in K[x_1, \ldots, x_m]$ a $\lambda \in K$, pak zjevně platí $f^*(g_1 + g_2) = f^*(g_1) + f^*(g_2), f^*(g_1 g_2) = f^*(g_1) f^*(g_2)$ a $f^*(\lambda g) = \lambda f^*(g)$. Vidíme, že f^* lze považovat za homomorfismus K–algeber $K[x_1, \ldots, x_m] \to K[x_1, \ldots, x_n]$.
Je-li $g_1, g_2 \in K[x_1, \ldots, x_m]$ takové, že $g_1 - g_2 \in \mathbb{I}(W)$, kde $W \subseteq \mathbb{A}^m$ je varieta, je $g_1(\beta) = g_2(\beta)$ pro každé $\beta \in W$. Proto prvky $\gamma \in K[W]$ můžeme považovat za zobrazení $W \to K$ a psát $\gamma(\beta) = \lambda$ právě když $g \in K[x_1, \ldots, x_m]$ representuje γ a splňuje $g(\beta) = \lambda$ (je tedy $\gamma = \mathbb{I}(W) + g$.
Z lemmatu 2.4 vyplývá, že morfismy $\varphi : V \to W$, kde $V \subseteq \mathbb{A}^n$ a $W \subseteq \mathbb{A}^m$ jsou variety odpovídají m–ticím $(\varphi_1, \ldots, \varphi_m)$, kde $\varphi_i \in K[V], 1 \leq i \leq m$, jsou takové, že $(\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) \in W$ pro každé $\alpha \in V$. Jestliže $\varphi_i = f_i + K[V]$, tak říkáme, že $f = (f_1, \ldots, f_m)$ *representuje* morfismus $\varphi = (\varphi_1, \ldots, \varphi_m)$.
Předpokládejme, že φ je representováno také m–ticí $f' = (f'_1, \ldots, f'_m)$ a že $\gamma \in K[W$ je representováno jak $g \in K[x_1, \ldots, x_m]$, tak $g' \in K[x_1, \ldots, x_m]$. Potom pro každé $\alpha \in V$ máme $((f')^*(g'))(\alpha) = g'(f'_1(\alpha), \ldots, f'_m(\alpha)) = g'(f_1(\alpha), \ldots, f_m(\alpha)) = g(f_1(\alpha), \ldots, f_m(\alpha)) = (f^*(g))(\alpha)$. Tuto společnou hodnotu označme $(\varphi^*(\gamma))(\alpha)$. Definovali jsme tak zobrazení $\varphi^* : K[W] \to K[V]$. Z vlastností $f^* : K[x_1, \ldots, x_m] \to K[x_1, \ldots, x_n$ vyplývá, že φ^* je homomorfismus K–algeber. Zjevně $\varphi^*(\gamma) = \varphi^*(g + \mathbb{I}(W)) = f^*(g) + \mathbb{I}(V)$.

Předpokládejme nyní, že variety V a W jsou izomorfní. Existují tedy morfismy $\varphi : V \to W$ a $\psi : W \to V$ takové, že $\varphi \circ \psi = \mathrm{id}_W$ a $\psi \circ \varphi = \mathrm{id}_V$. Odtud plyne $(\varphi \circ \psi)^* = \psi^* \circ \varphi^* = (\mathrm{id}_W)^* = \mathrm{id}_{K[W]}$ a podobně $\varphi^* \circ \psi^* = \mathrm{id}_{K[V]}$. Vidíme, že $\varphi^* : K[W] \cong K[V]$ a $\psi^* : K[V] \cong K[W]$ jsou vzájemně inverzní izomorfismy K–algeber $K[V]$ a $K[W]$.
Buďte nyní $a : K[V] \cong K[W]$ a $b : K[W] \cong K[V]$ izomorfismy K–algeber. Je možné najít φ a ψ tak, že $b = \varphi^*$ a $a = \psi^*$? Řekněme, že $b : K[W] \to K[V]$ je nějaký homomorfismus K–algeber. Algebra $K[x_1, \ldots, x_m]$ je generována polynomy $x_1, \ldots, x_m$, K–algebra $K[W]$ je generována prvky $x_j + \mathbb{I}(W) = \pi_W(x_j), 1 \leq j \leq m$. Zde $\pi_W : K[x_1, \ldots, x_m] \to K[W]$ je přirozená projekce modulo $\mathbb{I}(W)$. Ze znalosti $b(\pi_W(x_j))$ lze tudíž odvodit homomorfismus b jednoznačně. Je-li $b = \varphi^*$, kde $\varphi : V \to W$ je representováno $f = (f_1, \ldots, f_m)$, bude $b(\pi_W(x_j)) = \varphi^*(x_j + \mathbb{I}(W)) = f^*(x_j) + \mathbb{I}(V) = \pi_V(f^*(x_j))$, kde $\pi_V : K[x_1, \ldots, x_n] \to K[V]$ je projekce modulo $\mathbb{I}(V)$. Ovšem $f^*(x_j) = f_j$, neboť f_j dostaneme, pokud do polynomu $x_j \in K[x_1, \ldots, x_m]$ dosadíme za $x_1, \ldots, x_m$ polynomy $f_1, \ldots, f_m$.

Lemma 3.1. *Ať $b : K[W] \to K[V]$ je homomorfismus K–algeber. Pak existuje jednoznačně určený morfismus $\varphi : V \to W$ takový, že $b = \varphi^*$.*

Důkaz. Hledáme $\varphi = (\varphi_1, \ldots, \varphi_n)$ takové, že $b = \varphi^*$. Ať φ_i je representováno $f_i, 1 \leq i \leq n$. Pro každé $j, 1 \leq j \leq m$, má být

$$b(\pi_W(x_j)) = \pi_V(f^*(x_j)) = \pi_V(f_j) = \varphi_j.$$

Vidíme, že pokud φ existuje, je určeno jednoznačně. Potřebujeme ukázat, že pro každé $\alpha \in V$ je $(f_1(\alpha), \ldots, f_m(\alpha)) = (\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) \in W$. K tomu nám poslouží následující zobrazení:

- $f^* : K[x_1, \ldots, x_m] \to K[x_1, \ldots, x_n]$
- $\pi_W : K[x_1, \ldots, x_m] \to K[W]$
- $\pi_V : K[x_1, \ldots, x_n] \to K[V]$
- $b : K[W] \to K[V]$.

Jde o homomorfismy K–algeber, přičemž z $b\pi_W(x_j) = \pi_V(f^*(x_j)), 1 \leq j \leq n$ plyne, že $b \circ \pi_W = \pi_V \circ f^*$, neboť $x_1, \ldots, x_m$ generují $K[x_1, \ldots, x_m]$. Implikaci $\alpha \in V \implies f(\alpha) \in W$ ověříme tak, že dokážeme, že $hf(\alpha) = 0$ pro každé $h \in \mathbb{I}(W)$. Ovšem pro $h \in \mathbb{I}(W)$ máme $\pi_W(h) = 0$, odkud $0 = b\pi_W(h) = \pi_V(f^*(h)) = \pi_V(hf)$, což značí $hf \in \mathbb{I}(V)$, a tedy $hf(\alpha) = 0$. □

Důsledek 3.2. *Ať V a W jsou afinní variety. K–algebry $K[V]$ a $K[W]$ jsou izomorfní právě tehdy, když jsou izomorfní variety V a W.*

Důkaz. Implikace $V \cong W \implies K[V] \cong K[W]$ je snadná a již jsme ji zmínili. Pro důkaz opačné implikace ať $a : K[V] \cong K[W]$ a $b : K[W] \cong K[V]$ jsou vzájemně inverzní. Podle lemmatu 3.1 sestrojme morfismy $\psi : V \to W$ a $\varphi : W \to V$, že $a = \psi^*$ a $b = \varphi^*$. Pak $\mathrm{id}_{K[W} = ab = (\varphi \circ \psi)^*$. Odtud $\varphi \circ \psi = \mathrm{id}_W$, neboť podle L3.1 existuje jediný morfismus $\mu : W \to W$, že $\mu^* = \mathrm{id}_{K[W]}$, a tím je nutně id_W. Podobně platí $\psi \circ \varphi = \mathrm{id}_V$. □

Těleso K lze ztotožnit s afinním prostorem $\mathbb{A}^1$. Ten lze považovat za varietu (máme $\mathbb{I}(\mathbb{A}^1) = 0$ a 0 je prvoideál K). Aplikujeme-li tvrzení 2.13 na situaci $Z = \mathbb{A}^1$, dostaneme, že pro dané racionální zobrazení $r : V \to W$ a danou racionální funkci $\gamma : W \to K$ existuje racionální funkce $s = \mathrm{comp}(\gamma, r)$, kdykoliv $r^{-1}(D_{(\gamma)}) \neq \emptyset$. V takovém případě budeme psát $s = r^*(\gamma)$. Víme, že pokud r je representováno $(t_1, \ldots, t_m)$ a γ je representováno g, je $r^*(\gamma)$ representováno $g(t_1, \ldots, t_m)$. Je zřejmé, že $\mathrm{comp}(\gamma, r)$ existuje, kdykoliv je $\gamma = \varphi \in K[W]$. Podle T2.13 existuje také pro každé $\gamma \in K[W]$, je-li r dominantní.

Lemma 3.3. *Ať je r racionální zobrazení z variety V do variety W. Potom je $\varphi mapstor^*(\varphi)$ homomorfismus K–algeber $K[W] \to K(V)$. Je-li navíc dominantní, je $r^* : K(W) \to K(V)$ takvé homomorfismus K–algeber.*

Důkaz. Pro $\varphi_i \in K[W], i \in \{1, 2\}$, je definováno $r^*(\varphi_i) = \mathrm{comp}(\varphi_i, r) \in K(V)$ i $r^*(\varphi_1 + \varphi_2) = \mathrm{comp}(\varphi_1 + \varphi_2, r)$. Potřebujeme ověřit, že $r^*(\varphi_1 + \varphi_2) \in K(V)$ se shoduje s $r^*(\varphi_1) + r^*(\varphi_2) \in K(V)$. Podle tvrzení 2.9 tomu tak bude, pokud se representace prvků $K(V)$ shodují na nějaké husté podmnožině V. Existenci takové množiny lze snadno ověřit: Je-li φ_i representováno g_i a r je representováno $t = (t_1, \ldots, t_m)$ (zde $g_i \in K[x_1, \ldots, x_m]$ a $t_k \in K(x_1, \ldots, x_n), 1 \leq k \leq m$), je jistě možné nelézt otevřenou hustou množinu ve V takovou, že pro každý její prvek α jsou definovány hodnoty $g_1(t(\alpha)) = g_1(t_1(\alpha), \ldots, t_m(\alpha)), g_2(t(\alpha))$ i $(g_1 + g_2)(t(\alpha))$. Přitom zjevně $(g_1 g_2)(t(\alpha)) = g_1(t(\alpha)) + g_2(t(\alpha))$. Podobně se dokáže $r^*(\varphi_1 \cdot \varphi 2) = r^*(\varphi_1) \cdot r^*(\varphi_2)$ a $r^*(\lambda\varphi) = \lambda(r^*(\varphi))$, kde $\lambda \in K$ a $\varphi \in K[W]$. V případě r dominantního je $r^*(\gamma)$ definováno podle tvrzení 2.13 pro každé $\gamma \in K(W)$. Ověřit, že $r^* : K(W) \to K(V)$ je homomorfismus lze stejnou metodou, jaká byla použita v první části důkazu. □

Ať V a W jsou biracionálně ekvivalentní variety. Ověřit, že pak je $K(V) \cong K(W)$ se zdá být snadné, pokud dokážeme nějaký vztah typu $(r \circ s)^* = s^* \circ r^*$, kde r a s jsou dominantní racionální zobrazení. Takto zaptasný

vztah, byť se v literatuře vyskytuje, neodpovídá ovšem přesně naší definici racionálního zobrazení. Definiční obor $r \circ s$ totiž může být menší, než definiční obor $\mathrm{comp}(r,s)$. Budeme tedy definovat $(\mathrm{comp}(r,s))^* = s^* \circ r^*$. Jako první krok uvedeme následující fakta:

Lemma 3.4. *Ať je r dominantní racionální zobrazení z variety V do variety W. Je-li r representováno $u = (u_1, \ldots, u_m)$, kde $u_j \in K(x_1, \ldots, x_n), 1 \leq j \leq n$, je $U \cap \{u(\alpha); \alpha \in D(u) \cap V\} \neq \emptyset$ pro každé $U \subseteq W$ otevřenou neprázdnou. Je-li s dominantní racionální zobrazení z variety W do variety Z, je* $\mathrm{comp}(s,r)$ *dominantní racionální zobrazení z V do Z.*

Důkaz. Potřebujeme ověřit, že $u^{-1}(U) \cap D(u) \cap V \neq \emptyset$. Víme, žře $u^{-1}(U) \cap V$ je otevřená a $D(u) \cap V$ je otevřená hustá. Stačí tedy ukázat, že $u^{-1}(U) \cap V \neq \emptyset$ Ovšem $u^{-1}(U) \cap V = r^{-1}(U) \cap D(u)$. Protože předpokládáme $r^{-1}(U) \neq \emptyset$, je i $r^{-1}(U) \cap D(u) \neq \emptyset$. Buď nyní $v = (v_1, \ldots, v_l)$, kde $v_k \in K(x_1, \ldots, x_m)$, representací s. Ať $S \subseteq Z$ je neprázdná otevřená. Pak $v^{-1}(S) \cap W$ je podle první části důkazu neprázdná otevřená a tedy i $(u^{-1}(v^{-1}(S) \cap W)) \cap V \neq \emptyset$. Tudíž $(v \circ u)^{-1}(S) \cap V \neq \emptyset$, takže i $t^{-1}(S) \cap V \neq \emptyset$, kde $t = \mathrm{comp}(s,r)$ je representováno $v \circ u$ (dle tvrzení 2.13). □

Lemma 3.5. *Ať r a s jsou dominantní racionální zobrazení, r z variety V do variety W a s z W do Z. Potom $r^* \circ s^* = (\mathrm{comp}(s,r))^*$.*

Důkaz. Ať u a v jsou stejné jako v důkazu lemmatu 3.4. Tedy u representuje r a v representuje s. Ať $\varphi \in K(x_1, \ldots, x_l)$ representuje $\gamma \in K(Z)$. Víme, že $v \circ u$ representuje $\mathrm{comp}(s,r)$ a $(r^* \circ s^*)(\gamma)$ má representaci $\varphi(v_1, \ldots, v_l) \circ (u_1, \ldots, u_m) = \varphi(v_1(u_1, \ldots, u_m), \ldots, v_l(u_1, \ldots, u_m)) = \varphi \circ (v \circ u)$, což je representací $(\mathrm{comp}(s,r))^*(\gamma)$. Protože $(r^* \circ s^*)(\gamma)$ a $(\mathrm{comp}(s,r))^*(\gamma)$ mají stejné representace, jsou si rovny. □

Tvrzení 3.6. *Ať V a W jsou variety a ať $b : K(W) \to K(V)$ je homomorfismus K–algeber. Pak existuje právě jedno dominantní racionální zobrazení r z V do W takové, že $b = r^*$.*

Důkaz. Ptejme se nejprve, zda existuje racionální zobrazení r takové, že $r^*(\psi) = b(\psi)$ pro každé $\psi \in K[W]$. Podle lemmatu 3.4 můžeme r^* považovat za homomorfismus $K[W]$ do $K(V)$. Ten se shoduje s restrikcí b na $K[W]$ právě když se shodují na množině generátorů $\pi_W(x_j), 1 \leq j \leq m$, kde π_W je projekce $K[x_1, \ldots, x_m] \to K[W]$. Ať $r = (r_1, \ldots, r_m)$ a ať $r_i \in K(V)$ je representováno $\varphi_i \in K(x_1, \ldots, x_n)$. Pak $b(\pi_W(x_j)) = r^*(\pi_W(x_j))$ je representováno $x_j(\varphi_1, \ldots, \varphi_m) = \varphi_j$, takže $b(\pi_W(x_j)) = r_j$. Odtud vyplývá jednoznačnost r Aby r takto definované bylo opravdu zobrazením z V do W,

musí být $(r_1(\alpha), \ldots, r_m(\alpha))qinW$ pro každé $\alpha \in D(r)$. Zvolíme-li nějakou pevnou representaci $\varphi = (\varphi_1, \ldots, \varphi_m)$, kde φ_i representují $r_i = b(\pi_W(x_i))$, stačí podle lemmatu 2.12 ukázat, že $(\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) \in W$ pro každé $\alpha \in D_{(\varphi)} \cap V$. Uvažme homomorfismus $\Phi : K[x_1, \ldots, x_m] \to K(V)$ takový, že $\Phi(x_j) = r_j$. Takový homomorfismus K–algeber je právě jeden, přičemž pro $f = \sum \lambda_{e_1,\ldots,e_n} x_1^{e_1} \cdots x_m^{e_m}$ je $\Phi(f) = \sum \lambda_{e_1,\ldots,e_m} r_1^{e_1} \cdots r_m^{e_m}$. Je zřejmé, že $\Phi(f)$ je representováno $\sum \lambda_{e_1,\ldots,e_m} \varphi_1^{e_1} \cdots \varphi_m^{e_m}$. Protože $\Phi(x_j) = b\pi_W(x_j), 1 \leq j \leq m$, máme $\Phi = b\pi_W$. Chceme ukázat, že $h(\varphi_1(\alpha), \ldots, \varphi_m(\alpha)) = 0$ kdykolik $\alpha \in D_{(\varphi)} \cap V$ a $h \in \mathbb{I}(W)$. To je podle lemmatu 2.12 totéž, jako že $h(\varphi_1(x), \ldots, \varphi_m(x))$ representuje nulový prvek $K(V)$.
Ovšem $h(\varphi_1(x), \ldots, \varphi_m(x))$ representuje $\Phi(h) = b\pi_W(h) = b(0) = 0$. Dostali jsme tudíž r taková, že $r^*(\psi) = b(\psi)$ pro každé $\psi \in K[W]$. Homomorfismus $\kappa : R \to U$, kde R je obor integrity s podílovým tělesem T a U je těleso, lze rozšířit na homomorfismus $T \to U$ právě když $\kappa(t) \neq 0$ pro každé $t \in R^*$. Přitom toto rozšíření je jednoznačné. Protože zúžení b na $K[W]$ lze rozšířit na $b : K(W) \to K(V)$, musí být $b(\psi) = r^*(\psi) \neq 0$ pro každé $\psi \in K[W], \psi \neq 0$. Podmínka $r^*(\psi) \neq 0$ stačí k důkazu, že r je dominantní. Vskutku, v opačném případě můžeme za ψ zvolit $\pi_W(h)$, kde $D_h \cap W \neq \emptyset$ a kde $r(\alpha) \notin D_h$ pro žádné $\alpha \in D(r)$. To znamená, že $hr(\alpha) = 0$ pro každé $\alpha \in D(r)$, takže $r^*(\psi) = 0$, kde $\psi \neq 0$. Protože r je dominantní, je $r^* : K(W) \to K(V)$ homomorfismus. Ten se na $K[W]$ shoduje s b, a proto se oba homomorfismy musí rovnat. □

Tvrzení 3.7. *Ať V a W jsou afinní variety. Pak $K(V) \cong K(W)$ právě když V a W jsou biracionálně ekvivalentní.*

Důkaz. Jsou-li biracionálně ekvivalentní, existují racionální zobrazení r a s taková, že $\mathrm{comp}(s, r) = \mathrm{id}_V$ a $\mathrm{comp}(r, s) = \mathrm{id}_W$. Máme $(\mathrm{comp}(s, r))^* = r^* \circ s^* = (\mathrm{id}_V)^* = \mathrm{id}_{K[V]}$, a podobně $s^* \circ r^* = \mathrm{id}_{K[W]}$. Proto $K(V) \cong K(W)$. Je-li naopak $K(V) \cong K(W)$, pak lze podle tvrzení 3.6 odvodit dominantní racionální zobrazení r a s, kde r je z V do W a s je z W do V taková, žež r^* a s^* jsou vzájemně inverzní izomorfismy. Zbytek opět plyne z lemmatu 3.5, tedy ze vztahu $(\mathrm{comp}(s, r))^* = r^* \circ s^* = (\mathrm{id}_V)^*$, který podle T3.6 dává $\mathrm{comp}(s, r) = \mathrm{id}_V$ a symetricky $\mathrm{comp}(r, s) = \mathrm{id}_W$. □

Výklad racionálních zobrazení mohl vézt k otázce absence algebraické struktury, který by vyjadřovala, že $a = \frac{b}{c} \in K(x)$ representuje $\gamma \in K(V)$. Pro $\varphi \in K[V]$ totiž máme homomorfismus $\pi_V : K[x] \to K[V]$ (jeho projekce modulo $\mathbb{I}(V)$), který splňuje, že $b \in K[x]$ representuje φ právě když $\pi_V(b) = \varphi$. Je zřejmé, že π_V nelze rozšířit na homomorfismus $K(x) \to K(V)$, neboť by to byl homomorfismus těles (který má triviální jádro). Nicméně

π_V lze rozšířit na $K[x]_V = \{\frac{b}{c} \in K(x); c \notin \mathbb{I}(V)\}$. To je podokruh $K[x]$, který je roven lokalizaci $K[x]$ pomocí prvoideálu $\mathbb{I}(V)$. Vskutku, zobrazení $\frac{b}{c} \to \frac{b+\mathbb{I}(V)}{c+\mathbb{I}(V)}$ je korektně definovaným homomorfismem $K[x]_V \to K(V)$, jehož jádro je tvořeno všemi $\frac{b}{c} \in K[x]_V$ takovými, že $b \in \mathbb{I}(V)$. Okruh $K[x]$ lze pomocí $b \mapsto \frac{b}{1}$ vnořit do $K[x]_V$ a zúžení popisovaného homomorfismu na $K[x]$ dá π_V. Proto budeme označovat popisovaný homomorfismus také jako π_V. Skutečnost, že $\pi_V : K[x]_V \to K(V)$ je vskutku homomorfismus, vyplývá z obecných vlastností lokalizace. Přímý důkaz lze samozřejmě také snadno provézt.

Kapitola 4

Homogenní polynomy

Poznámky a připomenutí:

- Z každého vektorového prostoru W nad tělesem K lze odvodit projektivní prostor $P(W)$ tak, že jeho prvky, tedy *projektivní body* se shodují s 1–dimenzionálnímy podprostory W. Množina projektivních bodů obsažených ve 2–dimenzionálním podprostoru W pak určuje *projektivní přímku*. Obecně $(k+1)$–rozměrný podprostor W indukuje k–rozměrný projektivní podprotor $P(W)$. V dalším je vždy $n \geq 1$.

- Píšeme $\mathbb{P}^n(K) = P(\mathbb{A}^{n+1}(K))$ a $\mathbb{P}^n = \mathbb{P}^n(\bar{K})$. Prvky $\mathbb{P}^n(K)$ (tedy *projektivní K–racionální body*) jsou množiny

  $$\{(\lambda_{\alpha_0}, \ldots, \lambda_{\alpha_n}); \lambda, \alpha_0, \ldots, \alpha_n \in K \text{ a } \exists j \in \{0, \ldots, n\}, \text{ že } \alpha_j \neq 0\}$$

  Takový projektivní bod zapisujeme $(\alpha_0 : \cdots : \alpha_n)$. Mluví se pak o *homogenních souřadnicích*. Je zřejmé, že $(\alpha_0 : \cdots : \alpha_n) = (\beta_0 : \cdots : \beta_n)$ právě když se zlomky α_i/α_j a β_i/β_j shodují. Protože ale některý jmenovatel může být nulový, je třeba použít vyjádření, že $\alpha_i\beta_j = \alpha_j\beta_i$ kdykoliv $0 \leq i < j \leq n$. Samozřejmě také platí, že $(\alpha_0 : \cdots : \alpha_n) = (\beta_0 : \cdots : \beta_n)$ právě když existuje $j \in \{0, \ldots, n\}$, že $\alpha_j \neq 0, \beta_j \neq 0$ a $\alpha_i/\alpha_j = \beta_i/\beta_j$ pro každé $i \in \{0, \ldots, n\}$. Vidíme, že $(\alpha_0 : \cdots : \alpha_n)$ může popisovat K–racionální projektivní bod i v případě, kdy některé souřadnice α neleží v K. V tělese K ovšem vždy musí ležet podíly α_i/α_j, kde $\alpha_j \neq 0$, což je i podmínkou postačující.

- Je zvykem psát U_i ve významu $\{(\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n; \alpha_i = 1\}$. Všimněte si, že definice U_i se nezmění, pokud píšeme $\alpha_i \neq 0$. Množinu U_i můžeme ztotožnit s $\mathbb{A}^n$ tak, že $(\alpha_0 : \alpha_1 : \cdots : \alpha_{i-1} : 1 : \alpha_{i+1} : \cdots : \alpha_n)$

ztotožníme s $(\alpha_0, \alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$. Projektivní body ležící v U_i pokládáme za *vlastní* vzhledem k souřadnici i. Ostatní projektivní body splňují $\alpha_i = 0$ a říkáme jim *nevlastní*. Obvykle se při úvahách o vlastních bodech předpokládá, že $i = 0$, nebo $i = n$.

Vývoj geometrie přinesl pojem nevlastních bodů a později i pojem projektivního prostoru z důvodů, které byly v počátcích ryze praktické. Později se ukázalo, žže bez těchto pojmů zůstává teorie variet matematicky i esteticky neuspokojivá.
Projektivní varietu $\bar{V}$ chceme definovat tak, aby $V_i = U_i \cap \bar{V}$ bylo pro každé i také varietou (připouštíme ale i možnost $V_i = \emptyset$). Jak ale říci, že polynom $f \in K[x_0, x_1, \ldots, x_n]$ má za projektivní bod $(\alpha_0 : \alpha_1 : \cdots : \alpha_n)$?. Odpověď lze najít v lemmatu 4.1.

Definice 4.1 (Homogenní polynomy)**.** Polynom $f \in K[x_0, \ldots, x_n], f = \sum \lambda_{r_0,\ldots,r_n} x_0^{r_0} \cdots x_n^{r_n}$ se nazývá *homogenní*, jestliže existuje číslo $d \geq 0$, že $r_0 + \cdots + r_n = d$, kdykoliv je $\lambda_{r_0,\ldots,r_n} \neq 0$. Je-li $f \neq 0$ je d určeno jednoznačně a je rovno stupni polynomu f.

Abychom naznačili, že se úvahy týkají homogenních polynomů, bueme používat velká písmena, například $F = 3X_0^2 + 2X_1X_2 \in K[X_0, X_1, X_2]$. Místo $K[X_0, \ldots, X_N]$ budeme též psát $K[X]$. Pro všechny homogenní polynomy obsažené v $K[X]$ zvolíme označení $K\lfloor X \rfloor$.

Definice 4.2 (Homogenní část množiny)**.** Je-li $A \subseteq K[X]$, tak $\lfloor A \rfloor = K\lfloor X \rfloor \cap A$ se nazývá *homogenní část* množiny A.

Definice 4.3 (Homogenní dekompozice)**.** Každý polynom $f \in K[X]$ stupně $d \geq 0$ lze jednoznačně vyjádřit ve tvaru $f = F_d + F_{d-1} + \cdots + F_1 + F_0$, kde F_i je homogenní polynom stupně $i \geq 0$. Takovému vyjádření říkáme *homogenní dekompozice.*

Je zřejmé, že f je homogenní právě když $f = F_d$, tedy právě když $F_{d-1} = F_{d-2} = \cdots = F_1 = F_0 = 0$.

Lemma 4.1. *Ať $f \in K[X]$ má homogenní dekompozici $f = F_d + \cdots + F_0$. Pak následující podmínky jsou ekvivalentní:*

(1) *Pro každé $(\alpha_0 : \cdots : \alpha_n) = (\beta_0 : \cdots : \beta_n) \in \mathbb{P}^n$ je $f(\alpha_0, \ldots, \alpha_n) = 0$ právě když $f(\beta_0, \ldots, \beta_n) = 0$.*

(2) *Pro každé $(\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n$ platí $f(\alpha_0, \ldots, \alpha_n) = 0$ právě když $F_r(\alpha_0, \ldots, \alpha_n) = 0$ pro každé $r \in \{0, \ldots, n\}$.*

Důkaz. Ať $f(\alpha_0, \ldots, \alpha_n) = 0$, kde $\alpha_0, \ldots, \alpha_n \in \bar{K}$ a kde $\alpha_i \neq 1$ pro nějaké $i \in \{0, \ldots, n\}$. Chceme zjistit za jakých podmínek pak platí $f(\lambda_{\alpha_0}, \ldots, \lambda_{\alpha_n}) = 0$ pro každé $\lambda \in \bar{K}$. To nastává právě když λ je kořenem polynomu $\sum_{r=0}^{d} f_r y^r$, kde $f_r = F_r(\alpha_0, \ldots, \alpha_n)$. Těleso $\bar{K}$ je nekonečné, a proto platí, že $f(\lambda_{\alpha_0}, \ldots, \lambda_{\alpha_n}) = 0$ pro každé $\lambda \in \bar{K}$ právě když $0 = F_0(\alpha_0, \ldots, \alpha_n) = \cdots = F_d(\alpha_0, \ldots, \alpha_n)$. □

Vidíme, že pro homogenní polynomy je podmínka $F(\alpha_0 : \cdots : \alpha_n) = 0$ nezávislá na volbě homogenních souřadnic projektivního bodu $P = (\alpha_0 : \cdots : \alpha_n)$.

Lemma 4.2. *Ať je I ideál $K[X]$. Označme J množinu všech $f \in K[X]$, pro která platí $F_r \in I$ pro každé $r \in \{0, \ldots, d\}$, kde $f = F_d + \cdots + F_0$ je homogenní dekompozice. Množina J je ideálem $K[X]$ a $J = (\lfloor I \rfloor)$.*

Důkaz. Podle definice je J tvořeno všemi konečnými součty $\sum F_r$, kde F_r je homogenní stupně r a $F_r \in I$. Máme $\sum F_r + \sum F_r = \sum(F_r + G_r)$. Přitom z $F_r, G_r \in I$ plyne $F_r + G_r \in I$, přičemž buď $F_r + G_r = 0$, nebo $\deg(F_r + G_r) = r$. Proto je J uzavřeno na součty. Pro $\lambda \in K^*$ ptalí, že $\lambda F_d + \cdots + \lambda F_0$ je homogenní dekompozice λf, je-li $F_d + \cdots + F_0$ homogenní dekompozice f. Podobně je $X_i F_d + \cdots + X_i F_0$ homogennídekompozicí $X_i f, 0 \leq i \leq n$. Vidíme, že J je uzavřené i na skalární násobky a násobky pomocí proměnných X_i, takže je to ideál okruhu $K[X]$. Je-li $f = \sum F_r \in J$, je každé f_r prvkem $\lfloor I \rfloor$, takže $\lfloor I \rfloor \subseteq J$, odkud $(\lfloor I \rfloor) \subseteq J$. Součty prvků z $\lfloor I \rfloor$ leží v ideálu touto množinou generovaném, takže platí i opačná inkluze. Ideál J lze tedy popsat jako množinu všech součtů prvků $\lfloor I \rfloor$. □

Důsledek 4.3. *Ať I je ideál $K[X]$. Pak $I = (\lfloor I \rfloor)$ právě když $I = (A)$ pro nějaké $A \subseteq K\lfloor X \rfloor$.*

Důkaz. Je-li $I = (\lfloor I \rfloor)$, stačí položit $A = \lfloor I \rfloor$. Je-li $I = (A)$, máme $A \subseteq \lfloor I \rfloor$, a tedy $I = (A) \subseteq (\lfloor I \rfloor)$, takže platí rovnost. □

Definice 4.4 (Homogenní ideály)**.** Ideál splňující podmínky D4.3 se nazývá *homogenní.*

Důsledek 4.4. *Pro každý ideál I okruhu $\lfloor X \rfloor$ platí, že $(\lfloor I \rfloor)$ je největším homogenním ideálem v I obsaženým.*

Důkaz. Ideál $(\lfloor I \rfloor)$ je generovaný podmnožinou $K\lfloor X \rfloor$. Proto je homogenní. Je-li $J = (A) \subseteq I$, kde $A \subseteq K\lfloor X \rfloor$, je $A \subseteq \lfloor I \rfloor$, a tedy $J = (A) \subseteq (\lfloor I \rfloor)$. □

Z lemmatu 4.2 také plyne, že $\lfloor(\lfloor I\rfloor)\rfloor = \lfloor I\rfloor$.

Chceme-li charakterizovat množiny $\lfloor I\rfloor$, stačí tedy charakterizovat množiny $\lfloor H\rfloor$, kde H je homogenní ideál.

Lemma 4.5. *Množinu $A \subseteq K\lfloor X\rfloor$ lze vyjádřit jako $\lfloor H\rfloor$, kde H je homogenní ideál v $K[X]$, právě když A splňuje*

(1) *Pro $F, G \in A$ z $\deg(F) = \deg(G)$ vyplývá, že $F + G \in A$,*

(2) *$\lambda F \in A$ a $X_i F \in A$ pro každé $\lambda \in K, 0 \leq i \leq n$ a $F \in A$.*

Platí, že $A = \lfloor H\rfloor$, a žře A určuje H jednoznačně.

Důkaz. Je-li $A = \lfloor H\rfloor$, tak jsou podmínky (1) a (2) jistě splněny. Naopak, pokud A splňuje (1) a (2), tak je množina všech $f \in K[X]$ s homogenní dekompozicí $F_d + \cdots + F_0$ takovou, že $F_i \in A, 0 \leq i \leq d$, ideálem (uzavřenost na součty vyplývá z (1) a uzavřenost na násobky vyplývá z (2)). Jsou-li H_1 a H_2 dva homogenní ideály, tak z $H_i = (\lfloor H_i\rfloor), i \in \{1, 2\}$, plyne jednoznačnost v lemmatu postulovaná. □

Definice 4.5 (i–části)**.** Podmnožinu $K\lfloor X\rfloor$, která splňuje (1) a (2), nazveme *homogenní ideálovou částí*, zkráceně *i–částí*.

Lemma 4.6. *Ať $f, g \in K[X]$ jsou takové, že $fg \in K\lfloor X\rfloor$. Jsou-li f i g nenulové, je $f \in K\lfloor X\rfloor$ a $g \in K\lfloor X\rfloor$.*

Důkaz. Ať $0 \notin \{f, g\}$. Ať $r = \deg(f)$ a $s = \deg(g)$ a ať $f = \sum F_i$ a $g = \sum G_j$ jsou homogenní dekompozice. Označmě r' nejmenší $i \leq r$, že $F_i \neq 0$. Podobně odvoďme s' jako nejmenší j, že $G_j \neq 0$. Součty $F_r G_s$ a $F_{r'} G_{s'}$ figurují v homogenní dekompozici polynomu fg. Je-li fg homogenní, musí tedy být $r = r'$ a $s = s'$. □

Lemma 4.7. *Ať $A \subseteq K\lfloor X\rfloor$ je i–část, a ať $H = (A)$. Ideál H je prvoideálem, právě když pro všechna $F, G \in K\lfloor X\rfloor$ platí implikace $FG \in A \implies F \in A \vee G \in A$.*

Důkaz. Je-li H prvoideál, musí podle lemmatu 4.6 uvedená implikace platit. Pro důkaz opačným směrem předpokládejme, že $fg \in H$, kde f a g jsou nenulové polynomy s homogenními dekompozicemi $f = \sum_{i=0}^{r} F_i$ a $g = \sum_{j=0}^{s} G_j$. Postupujme indukcí, dle $r+s$. Součin $F_r G_s$ je vedoucím členem homogenní dekompozice polynomu $fg \in H$, a proto máme $F_r G_s \in A$. Můžeme tedy přepokládat, že $F_r \in A$. Položme $\bar{f} = f - F_r$. Pak $\bar{f} g = fg - F_r g \in H$, takže podle indukčního předpokladu je $f = \bar{f} + F_r \in H$, nebo $g \in H$. □

Definice 4.6 (Prvočásti)**.** Homogenní ideálová část (i–část), která splňuje implikaci lemmatu 4.7 se nazývá *prvočást.*

Lemma 4.8. *Zobrazení $H \to \lfloor H \rfloor$ je bijekcí homogenních ideálů $K[X]$ a všech i–částí obsažených v $K\lfloor X \rfloor$. Tato bijekce převádí prvoideály na prvočásti a naopak.*

Důkaz. To je pouze shrnutí lemmat 4.5 a 4.7 □

Nyní se budeme zabývat vztahem i–částí (což jsou podmnožiny $K\lfloor X \rfloor$) a ideálů $K[X]$). Pro $j \in \{0, \ldots, n\}$ označíme π_j homomorfismus $K[X] \to K[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$ takový, že $\pi_j(X_j) = x_j$ a $\pi_j(X_j) = 1$. Například $\pi_1(3X_0X_1X_2 - 3X_0X_2 + 2X_1^2) = 3x_0x_2 - 3x_0x_2 + 2 = 2$. Kvůli úspornosti zápisu budeme psát $\pi_j : K[X] \to K[x]$, byť toto platí přísně vzato pouze pro $j = 0$. Protože pravdivost následujících tvrzení není závislá na volbě $j \in \{0, \ldots, n\}$, budeme v důkazech vždy předpokládat, že $j = 0$. Dále označíme restrikci π_j na množinu $K\lfloor X \rfloor \nu_j$.

Lemma 4.9. *Ať I je ideál $K[x]$. Pak $\nu_j^{-1}(I)$ je i–část. Je-li $A \subseteq K\lfloor X \rfloor$ nějaká i–část, tak je $nu_j(A)$ ideál $K[x]$. Tento ideál je vlastní právě když $X_j^r \notin A$ pro žádné $r \geq 0$.*

Důkaz. Máme $\nu_0^{-1}(I) = \lfloor \pi_0^{-1}(I) \rfloor$, přičemž $\pi_0^{-1}(I)$ ideál jistě je. Ať $A \subseteq K\lfloor X \rfloor$ je i–část. Pak $\nu_0(\lambda F) = \lambda\nu_0(F)$ a $\nu_0(X_iF) = x_i\nu_0(F)$ pro každé $F \in A, \lambda \in K$ a $i \in \{1, \ldots, n\}$. Stačí tedy ověřit, že $\nu_0(A)$ je uzavřená na součty. Jsou-li $F, G \in A$, zvolíme $s, t \geq 0$ taková, že X_0^sF i X_0^tG mají stejný stupeň. Pak $X_0^sF + X_0^tG \in A$ a současně $\nu_0(X_0^sF + X_0^tG) = \nu_0(F) + \nu_0(G)$. Je-li $X_0^r \in A$, je $1 = \nu_0(X_0^r) \in \nu_0(A)$, takže $\nu_0(A) = K[x]$. Pokud $\nu_0(A)$ není vlastní, tak $1 = \nu_0(F)$ pro nějaké $F \in A$. Je zřejmé, že v F nemůže figurovat X_i, kde $i \geq 1$. Proto je $F = \lambda X_0^r$ pro nějaké $r \geq 0$ a $\lambda \in K^*$ (pak ovšem nutně $\lambda = 1$). □

Lemma 4.10. *Ať $f \in K[x]$ má homogenní dekompozici $F_d + \cdots + F_0$ a ať $f \neq 0$. Pak $\nu_0^*(f) = \sum_{0 \leq r \leq d} X_0^{d-r}F_r \in K\lfloor X \rfloor$. Přitom $G \in K\lfloor X \rfloor$ splňuje $\nu_0(G) = f$ právě když $G = X_0^s\nu_0^*(f)$ pro nějaké $s \geq 0$.*

Důkaz. Je zřejmé, že $\nu_0^*(f) \in K\lfloor X \rfloor$ a že $\nu_0(X_0^s\nu_0^*(f)) = f$. K dokončení důkazu stačí ověřit, že $G = \nu_0^*(f)$ pokud G není násobkem X_0 a splňuje $\nu_0(G) = f$. V takovém případě G lze zapsat jako $G_{d'} + X_0G_{d'-1} + \cdots + X_0^{d'}G_0$, kde $G_0, \ldots, G_{d^prime} \in K[x]$ jsou homogenní, $r = \deg(G_r)$, je-li $0 \leq r \leq d'$ a $G_r \neq 0$ a $G_{d'} \neq 0, d' = \deg(G)$. Podmínka $\nu_0(G) = f$ znamená, že $G_{d'} + G_{d'-1} + \cdots + G_0$ je homogenní dekompozice f, takže nutně $d' = d$ a $G = \nu_0(f)$. □

Lemma 4.11. *Ať $f, g \in K[x]$ jsou nenulová. Pak $\nu_0^*(fg) = \nu_0^*(f)\nu_0^*(g)$.*

Důkaz. Máme $\nu_0(\nu_0^*(f)\nu_0^*(g)) = \nu_0(\nu_0^*(f))\nu_0(\nu_0^*(g)) = fg$. Podle L4.10 stačí nyní ověřit, že $\nu_0^*(f)\nu_0^*(g)$ není násobek X_0. To je skutečně pravda, neboť násobkem X_0 není ani $\nu_0^*(f)$, ano $\nu_0^*(g)$. Z lemmatu 4.10 mimo jiné plyne, že ν_j je surjektivní zobrazení. Tudíž π_j je surjektivní homomorfismus okruhu, což je ostatně zřejmé. Pro surjektivní homomorfismy ale platí, že vzorem prvoideálu je vždy prvoideál. □

Lemma 4.12. *Ať P je prvoideál $K[x]$. Pak $\nu_j^{-1}(P)$ je prvočást a $\nu_j(\nu_j^{-1}(P)) = P$. Je-li $A \subseteq K\lfloor X\rfloor$ taková prvočást, že $X_j \notin A$, tak je $\nu_j(A)$ prvoideál a $\nu_j^{-1}(\nu_j(A)) = A$.*

Důkaz. Máme $\nu_0^{-1}(P) = \lfloor \pi_O^{-1}(P)\rfloor$, přičemž $\pi_0^{-1}(P)$ je prvoideál. Pro každé $M \subseteq K[x]$ platí $\nu_0(\nu_0^{-1}(M)) = M$, neboť zobrazení ν_0 je surjektivní. Z předpokladu $X_j \notin A$ podle L4.9 dostáváme, že $\nu_0(A)$ je vlastní ideál $K[x]$. Ať $f, g \in K[x]$ jsou nenulová a ať $fg \in \nu_0(A)$, kde A je prvočást, $X_0 \notin A$. Podle L4.10 existuje $s \geq 0$ takové, že $X_0^s\nu_0^*(fg) \in A$. Protože A je prvočást a $X_0 \notin A$, musí být $\nu_0^*(fg) \in A$. Podle L4.11 je $\nu_0^*(f)\nu_0^*(g) \in A$, a tedy $\nu_0^*(f) \in A$ (pak $f = \nu_0(\nu_0^*(f)) \in \nu_0(A)$), nebo $\nu_0^*(g) \in A$ (pak $g \in \nu_0(A)$). Vidíme, žře $\nu_0(A)$ vskutku je prvoideál. Jistě $\nu_0^{-1}(\nu_0(A)) \supseteq A$. Zbývá dokázat opačnou inkluzi. Ať $G \in K\lfloor X\rfloor$ je takové, že $\nu_0(G) = \nu_0(F) = f$ pro nějaké $F \in A$. Podle L4.10 existují $s \geq 0$ a $t \geq 0$, že $G = X_0^s\nu_0^*(f)$ a $F = X_0^t\nu_0^*(f)$. Z $F \in A$ a $X_0 \notin A$ plyne, že $\nu_0^*(f) \in A$, takže i $G \in A$. □

Lemma 4.12 říká, že ν_j vytváří jednoznačný vzájemný vztah mezi prvoideály $K[x]$ a prvočástmi $K\lfloor X\rfloor$, které neobsahují X_j. Vzniká tak i vzájemně jenoznačná vazba mezi prvoideály $K[x]$ a homogenními prvoideály $K[X]$, které neobsahují X_j (viz lemma 4.8).
Pro $S \subseteq \mathbb{P}^n$ položme $\bar{\mathbb{I}}(S) = \{F \in K\lfloor X\rfloor; F(\alpha_0, \ldots, \alpha_n) = 0$ pro všechna $(\alpha_0 : \cdots : \alpha_n) \in S\}$. pro $M \subseteq K\lfloor X\rfloor$ buď $\bar{\mathbb{V}}(M) = \{(\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n; F(\alpha_0, \ldots, \alpha_n) = 0$ pro každé $F \in M\}$. Dvojice $(\bar{\mathbb{I}}, \bar{\mathbb{V}})$ tvoří Galoisovu korespondenci mezi $\mathbb{P}^n$ a $K\lfloor X\rfloor$. Důkaz je snadný (téměř doslova lze zopakovat důkaz lemmatu 1.4).
Další naše úvahy se budou opírat o dvojici $(\bar{\mathbb{I}}, \bar{\mathbb{V}})$. V literatuře je však daleko častější dvojice $(\mathbb{I}_j, \mathbb{V}_h)$, která je s $\bar{\mathbb{I}}, \bar{\mathbb{V}})$ v následujícím vzájemném vztahu:

- Pro $M \subseteq K[X]$ položme nejprve $M_h = \{G \in K\lfloor X\rfloor; \exists f \in M$ s homogenní dekompozicí $f = F_d + \cdots + F_0$ takové, že $G = F_j, 0 \leq j \leq d\}$. Klademe $\mathbb{V}_h(M) = \bar{\mathbb{V}}(M_h)$.

- Dále $\mathbb{I}_h(S) = \{f \in K(X]; F_j \in \bar{\mathbb{I}}(S)$ pro každé $j, 0 \leq j \leq d$, kde $f = F_d + \cdots + F_0$ je homogenní dekompozice$\}$.

Lemma 4.13. *(i) Je-li $M \subseteq K\lfloor X \rfloor$, tak $\mathbb{V}_h(M) = \bar{\mathbb{V}}(M)$.*

(ii) Je-li $S \subseteq \mathbb{P}^n$, je $\bar{\mathbb{I}}(S)$ vždy i–část, $\bar{\mathbb{I}}(S) = \lfloor \mathbb{I}_h(S) \rfloor$ a $\mathbb{I}_h(S) = (\bar{\mathbb{I}}(S))$ je homogenní ideál v $K[X]$.

(iii) $\mathbb{V}_h\mathbb{I}_h(S) = \bar{\mathbb{V}}\bar{\mathbb{I}}(S)$ pro každé $S \subseteq \mathbb{P}^n$.

(iv) $\mathbb{I}_h\mathbb{V}_h(M) = \lfloor \bar{\mathbb{I}}\bar{\mathbb{V}}(M_h) \rfloor$ pro každé $M \subseteq K[X]$.

Důkaz. Pro $M \subseteq K\lfloor X \rfloor$ je $M = M_h$. Odtud (i). Je zřejmé, že $A = \bar{\mathbb{I}}(S)$ splňuje podmínky (1) a (2) z lemmatu 4.5. Proto je A homogenní částí homogenního ideálu H, který podle lemmatu 4.2 je tvořen součty prvků z A. Odtud plyne (ii). Z definice operátoru $\mathbb{I}_h$ plyne, že $(\mathbb{I}_h(S))_h = \lfloor \mathbb{I}_h(S) \rfloor = \bar{\mathbb{I}}(S)$. Odtud $\mathbb{V}_h\mathbb{I}_h(S) = \bar{\mathbb{V}}\bar{\mathbb{I}}(S)$. Z definice $\mathbb{V}_h$ máme $\mathbb{V}_h(M) = \bar{\mathbb{V}}(M_h)$ a zbytek části (iv) plyne z části (ii). □

Definice 4.7 (Projektivní algebraické množiny a uzávěr)**.** Vidíme, že operátory $\mathbb{V}_h\mathbb{I}_h$ a $\bar{\mathbb{V}}\bar{\mathbb{I}}$ se shodují. Tento operátor se nazývá *projektivní uzávěr.*
Pokud $\bar{\mathbb{V}}\bar{\mathbb{I}}(S) = S$, nazýváme $S \subseteq \mathbb{P}^n$ *projektivní algebraickou množinou.*

Z vlastností Galoisovy korespondence plyne, že to jsou právě všechny množiny, které lze vyjádřit ve tvaru $\bar{\mathbb{V}}(M)$, kde $M \subseteq K\lfloor X \rfloor$, případně $\mathbb{V}_h(M)$, kde $M \subseteq K[X]$. V dalším budeme pracovat s dvojicí $(\bar{\mathbb{V}}, \bar{\mathbb{I}})$. Vlastnosti Galoisovy korespondence $(\mathbb{V}_h, \mathbb{I}_h)$ jsou podle lemmatu 4.13 nutně rovnocenné.

Kapitola 5

Projektivní algebraické množiny

Naším cílem bude ukázat, že vlastnosti projektivních algebraických množin jsou podobné těm, které jsme popsali v afinním případě. K tomu však budeme potřebovat více vědět o homogenních ideálech, tedy i–částech.

Lemma 5.1. *Ať $M \subseteq K\lfloor X\rfloor$. Pak (M) je homogenní ideál a $\lfloor(M)\rfloor$ je nejmenší i–část, která obsahuje M.*

Důkaz. To, že (M) je homogenní, plyne z L4.3. Je-li $A \supseteq M$ nějaká i–část, tak $(A) \supseteq (M)$ a $A = \lfloor(A)\rfloor \supseteq \lfloor(M)\rfloor$, opět podle L4.3. □

Lemma 5.2. *Ať $A_j = \lfloor H_j\rfloor$, kde $H_j \subseteq K[X]$ jsou homogenní ideály, $j \in J$, kde $J \neq \emptyset$. Pak $A = \bigcap(A_j; j \in J)$ je i–část, která je rovna $\lfloor H\rfloor$, kde $H = \bigcap(H_j; j \in J)$. Platí, že H je homogenní ideál.*

Důkaz. Množina A zjevně splňuje podmínky (1) a (2) lemmatu 4.5. Proto je i–částí. Pro každé $j \in J$ je $(A) \subseteq H_j$, takže $(A) \subseteq H$. Z $H \subseteq H_j$ plyne, $\lfloor H\rfloor \subseteq \lfloor H_j\rfloor = A_j$, takže $\lfloor H\rfloor \subseteq A$. Zbývá ukázat, že $H = (\lfloor H\rfloor)$, tedy že H je homogenní (viz D4.4). Je-li $f \in H$ s homogenní dekompozicí $f = F_d + \cdots + F_0$, je $F_i \in H_j$ pro každé $j \in J$ a $i \in \{0, \ldots, d\}$. □

Pro i–části $A, B \subseteq K\lfloor X\rfloor$ definujme AB jako $\{0\} \cup (\bigcup_{d\geq 0} M_d)$, kde $M_d = \{\sum_{i=0}^{d} F_i G_{d-i}; F_i \in A, G_{d-i} \in B$, přičemž $F_i = 0$, nebo $\deg(F_i) = i$ a současně $G_j = 0$, nebo $\deg(G_j) = j\}$.

Lemma 5.3. *Ať $A_j = \lfloor H_j\rfloor, j \in \{1, 2\}$. Pak $A_1A_2 = \lfloor H_1H_2\rfloor$ a H_1H_2 je homogenní. Přitom platí, že A_1A_2 je nejmenší i–část, která obsahuje $\{F_1F_2; F_1 \in A_1$ & $F_2 \in A_2\}$.*

Důkaz. Je zřejmé, že $A_1A_2 \subseteq \lfloor H_1H_2 \rfloor$ a že A_1A_2 je i–část (viz lemma 4.5). Protože H_j je tvořeno součty prvků z A_j, je H_1H_2 generováno množinou všech F_1F_2, kde $(F_1, F_2) \in A_1 \times A_2$. Proto je H_1H_2 homogenní ideál a z $H_1H_2 \subseteq (A_1A_2)$ máme $\lfloor H_1H_2 \rfloor \subseteq \lfloor (A_1A_2) \rfloor = A_1A_2$. □

Lemma 5.4. *Ať $P \subseteq K[X]$ je prvoideál. Pak je $(\lfloor P \rfloor)$ největší homogenní prvoideál obsažený v P.*

Důkaz. Je zřejmé, že $\lfloor P \rfloor$ splňuje podmínku lemmatu 4.7. Zbytek plyne z důsledku 4.4. □

Pro i–část A položme $\sqrt{A} = \{F \in K\lfloor X \rfloor; F^d \in A \text{ pro nějaké } d \geq 0\}$.

Lemma 5.5. *Ať $A = \lfloor H \rfloor$, kde $H \subseteq K(X)$ je vlastní homogenní ideál. Pak $\sqrt{H}$ je rovněž homogenní ideál a platí, že $\sqrt{A} = \lfloor \sqrt{H} \rfloor$. Přitom $\sqrt{A} = \bigcap(B \supseteq A; B \text{ je prvočást})$.*

Důkaz. Označme $\mathcal{P}$ množinu všech prvoideálů $K[X]$ a $\mathcal{H}$ množinu všech homogenních prvoideálů. Z obecné teorie víme, že $\sqrt{H} = \bigcap(P \supseteq H; P \in \mathcal{P})$. Z $P \supseteq H$ podle důsledku 4.4 plyne $P \supseteq (\lfloor P \rfloor) \supseteq H$, takže z lemmatu 5.4 máme $\sqrt{H} = \bigcap(P \supseteq H; P \in \mathcal{H})$. Homogennost $\sqrt{H}$ je důsledkem lemmatu 5.2, ze kterého též plyne, že $\lfloor \sqrt{H} \rfloor = \bigcap(\lfloor P \rfloor; P \supseteq H \text{ a } P \in \mathcal{H})$. Protože $P \supseteq H$ právě když $\lfloor P \rfloor \supseteq \lfloor H \rfloor = A$, zbývá dokázat, že $\sqrt{A} = \lfloor \sqrt{H} \rfloor$. Máme $F \in \lfloor \sqrt{H} \rfloor$ právě když $F \in K\lfloor X \rfloor$ a $F^d \in H$ pro nějaké $d \geq 1$. Ovšem po $F \in K\lfloor X \rfloor$ z $F^d \in H$ plyne, že $F^d \in \lfloor H \rfloor = A$. □

Připomeňme, že pro $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n(K)$ je $M(\alpha) = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$ maximální vlastní ideál $K[x]$ (a tedy i prvoideál). Je-li $K = \bar{K}$, mají všechny maximální ideály $K[x]$ tento tvar.

Lemma 5.6. *$(X_0, \ldots, X_n)$ je v $K[X]$ největším vlastním homogenním ideálem a je to prvoideál. Největší vlastní i–část je rovna $K\lfloor X \rfloor \setminus K^*$ a je to prvočást.*

Důkaz. Ideál $(X_0, \ldots, X_n) = (X_0 - 0, \ldots, X_n - 0)$ je maximálním ideálem $K[X]$, a proto je prvoideálem. Je homogenní, protože je generován homogenními polynomy. Je-li $H \subseteq K[X]$ homogenní ideál, tak jsou dvě možnosti. Buď $H \subseteq (X_0, \ldots, X_n)$, nebo existuje $f \in H$ s nenulovým absolutním členem. V takovém případě máme $F_0 \neq 0$, kde $f = F_d + \cdots + F_0$ je homogenní dekompozice. Pak ovšem $F_0 \in H$ a $H = K[X]$. Zjevně $\lfloor (X_0, \ldots, X_n) \rfloor = K\lfloor X \rfloor \setminus K^*$, zbytek tedy plyne z lemmatu 4.8. □

Důsledek 5.7. *Ať $A \subsetneq K\lfloor X \rfloor \setminus K^*$ je prvočást. Pak existuje $j \in \{0, \ldots, n\}$, žež $X_j^r \notin A$ pro všechna $r \geq 0$.*

Důkaz. Postupujme sporem. Je-li $1 = X_j^0 \in A$, je $A = K\lfloor X \rfloor$. Pro všechna X_j tedy $X_j^r \in A$ pro nějaké $r \geq 1$. Odtud vyplývá, že $X_0, \ldots, X_n \in A$ a $A = K\lfloor X \rfloor \setminus K^*$, neboť o A předpokládáme, že je to prvočást. □

Definice 5.1 (Maximální prvočást)**.** Prvočást A nazveme *maximální*, je-li $A \subsetneq K\lfloor X \rfloor \setminus K^*$ a současně neexistuje prvočást B, že $A \subsetneq B \subsetneq K\lfloor X \rfloor \setminus K^*$.

Lemma 5.8. *Ať $A \subseteq K\lfloor X \rfloor$ je prvočást taková, že $X_j \notin A$, kde $j \in \{0, \ldots, n\}$. Ideál $\nu_j(A)$ je v $K[x]$ maximální, právě když A je maximální prvočást.*

Důkaz. Toto je přímý důsledek lemmatu 4.12 □

Zvolme nyní $\bar{\alpha} = (\alpha_0 : \cdots : \alpha_n) \in \mathbb{P}^n(K)$. Víme, že můžeme předpokládat, že $\alpha_0, \ldots, \alpha_n \in K$ a $\alpha_j \neq 0$ pro nějaké $j \in \{0, \ldots, n\}$. Položme $M\lfloor \bar{\alpha} \rfloor = \{F \in K\lfloor X \rfloor; F(\bar{\alpha}) = 0\}$. Z lemmat 4.5 a 4.7 plyne, že $M\lfloor \bar{\alpha} \rfloor$ je prvoideál. Typickými prvky $M\lfloor \bar{\alpha} \rfloor$ jsou $\alpha_r X_s - \alpha_s X_r$. Ideál, který tyto prvky generují, je homogenní a je roven ideálu, který je pro ta j, že $\alpha_j \neq 0$ generován všemi polynomy $\alpha_j X_s - \alpha_s X_j$, neboť $\alpha_j(\alpha_r X_s - \alpha_s X_r) = \alpha_r(\alpha_j X_s - \alpha_s X_j) - \alpha_s(\alpha_j X_r - \alpha_r X_j)$. Ukážeme, že polynomy $\alpha_j X_s - \alpha_s X_j$ ideál $(M\lfloor \bar{\alpha} \rfloor)$ generují. Můžeme předpokládat, že $j =$ a $\alpha_j = 1$. Každý prvek $F \in K\lfloor X \rfloor$ lze vyjádřit jako $X_0^k \nu_0^*(f)$, kde $k \geq 0$ a $f \in K[x]$ (lemma 4.10). $f = g((x_1 - \alpha_1), \ldots, (x_n - \alpha_n))$. Ať je $d = \deg(f) = \deg(g)$ a ať λ je absolutní člen polynomu $g \in K[x]$. Pak $X_0^k \nu_0^*(f)(1, \alpha_1, \ldots, \alpha_n) = 1^k 1^d \lambda = \lambda$. Vidíme, že F padne do $M\lfloor \bar{\alpha} \rfloor$ právě když $\lambda = 0$. To lze vyjádřit též jako $F \in M\lfloor \bar{\alpha} \rfloor \iff \nu_0(F) \in M(\alpha)$, neboť $\nu_0(X_0^k \nu_0^*(f)) = f$. Současně vidíme, že pro $\lambda = 0$ leží $X_0^k \nu_0^*(f)$ v ideálu generovaném polynomy $\nu_0^*(x_s - \alpha_s) = X_s - \alpha_s X_0$. Protože $M(\alpha)$ je v $K[x]$ ideál maximální, tak jsme vzhledem k lemmatu 5.8 dokázali následující tvrzení:

Lemma 5.9. *Pro každé $\bar{\alpha} \in \mathbb{P}^n(K)$ je $M\lfloor \bar{\alpha} \rfloor$ maximální prvočást. Jsou-li $\alpha_0, \ldots, \alpha_n \in K$ takové, že $\bar{\alpha} = (\alpha_0 : \cdots : \alpha_n)$, je $(M\lfloor \bar{\alpha} \rfloor)$ generován polynomy $\alpha_r X_s - \alpha_s X_r$, kde $r, s \in \{0, \ldots, n\}$.*

Důkaz. □

Podle definice je $M\lfloor \bar{\alpha} \rfloor = \bar{\mathbb{I}}(\bar{\alpha})$. Proto pro každou projektivní algebraickou množinu S platí $\bar{\mathbb{I}}(S) \subseteq \bigcap(M\lfloor \bar{\alpha} \rfloor; \bar{\alpha} \in S)$. Je-li $S = \bar{\mathbb{V}}(A)$, kde A je i–část, tak $\sqrt{A} \subseteq \bar{\mathbb{I}}\bar{\mathbb{V}}(A) \subseteq \bigcap(M\lfloor \bar{\alpha} \rfloor; \bar{\alpha} \in \bar{\mathbb{V}}(A))$. Podobné vztahy platí i v afinním případě, kde víme, že pro $K = \bar{K}$ dostáváme rovnosti, což je vlastně obsahem Hilbertovy věty o nulách. Následující tvrzení lze pokládat za její projektivní verzi.

Tvrzení 5.10. *Ať A je vlastní i–část obsažená v $K\lfloor X\rfloor$. Ať $\bar{K} = K$. Pak buď*

(i) $\sqrt{A} = K\lfloor X\rfloor \setminus K^*$ *a* $\bar{\mathbb{V}}(A) = \emptyset$, *nebo*

(ii) $\bar{\mathbb{I}}\bar{\mathbb{V}}(A) = \sqrt{A} = \bigcap(M\lfloor\bar{\alpha}\rfloor; \bar{\alpha} \in \bar{\mathbb{V}}(A))$ *a* $\bar{\mathbb{V}}(A) \neq \emptyset$.

Důkaz. Prvý případ jistě nastane, pokud pro každé $j \in \{0, \ldots, n\}$ existuje $r \geq 1$,že $X_j^r \in A$. Ať tedy existuje $j \in \{0, \ldots, n\}$, že $X_j^r \notin A$ pro každé $r \geq 0$. Podle lemmatu 5.5 je $\sqrt{A}$ rovna průniku všech prvočástí $B \supseteq A$. Stačí tedy dokázat, že B je možné vyjádřit jako průnik prvočástí $M\lfloor\bar{\alpha}\rfloor$. (Z $A \subseteq B \subseteq M\lfloor\bar{\alpha}\rfloor$ plyne, že $\bar{\alpha} \in \bar{\mathbb{V}}(A)$). Případ $B = K\lfloor X\rfloor \setminus K^*$ lze pominout, takže lze předpokládat, že $X_j \notin B$. Pak je $\nu_j(B) = \bigcap(M(\beta); \beta \in S)$, kde $S = \mathbb{V}(\nu_j(B))$, podle Hilbertovy věty o nulách. Tudíž $B = \nu_j^{-1}(\nu_j(B)) = \bigcap(\nu_j^{-1}(M(\beta); \beta \in S) = \bigcap(M\lfloor\bar{\beta}\rfloor; \varphi_j(\beta) \in S\}$. Zde $\varphi_j(\beta_1, \ldots, \beta_{j-1}, \beta_{j+1}, \ldots, \beta_n) = (\beta_1 : \cdots : \beta_{j-1} : 1 : \beta_{j+1} : \cdots : \beta_n)$. □

Tvrzení 5.11. *Ať A je vlastní i–část obsažená v $K\lfloor X\rfloor$. Pak buď*

(i) $\sqrt{A} = K\lfloor X\rfloor \setminus K^*$ *a* $\bar{\mathbb{V}}(A) = \emptyset$, *nebo*

(ii) $\bar{\mathbb{I}}\bar{\mathbb{V}}(A) = \sqrt{A}$ *a* $\bar{\mathbb{V}}(A) \neq \emptyset$.

Důkaz. Případ, kdy $\{X_0, \ldots, X_n\} \subseteq \sqrt{A}$ můžeme řešit stejně jako v důkazu tvrzení 5.10. Proto lze předpokládat, že $X_j \notin \sqrt{A}$ pro nějaké $j \in \{0, \ldots, n\}$. Postupujme podobně jako v důkazu 1.18 a uvažujme vedle dvojice $(\bar{\mathbb{I}}, \bar{\mathbb{V}})$ i dvojici $(\underline{\bar{\mathbb{I}}}, \underline{\bar{\mathbb{V}}})$. Nejmenší i–část $K\lfloor X\rfloor$, která obsahuje A ,se skládá z polynomů $\sum_{i=0}^{k} F_i G_i$, kde $F_i \in A, G_i \in K\lfloor X\rfloor$ a $\deg(F_1) + \deg(G_1) = \cdots = \deg(F_k) + \deg(G_k)$. Tato množina, označme ji B, totiž zjevně vyhovuje podmínkám lemmatu 4.5. Současně snadno nahlédneme, že $B = \lfloor(A)\bar{K}[X] \cap K[X]\rfloor = \lfloor(A)\rfloor = A$. Je $\bar{\mathbb{A}}(A) = \underline{\bar{\mathbb{V}}}(A) = \underline{\bar{\mathbb{V}}}(B) \neq \emptyset$ dle T5.10, neboť $X_j^r \notin B$ pro všechna $r \geq 0$. Podle T5.10 je $\bar{\mathbb{I}}\bar{\mathbb{V}}(A) = \underline{\bar{\mathbb{I}}}\underline{\bar{\mathbb{V}}}(B) \cap K\lfloor X\rfloor = \sqrt{B} \cap K\lfloor X\rfloor$, a to je rovno $\sqrt{A}$. □

Definice 5.2 (Projektivní variety)**.** Projektivní algebraickou množinu S nazveme *ireducibilní*, nebo též *projektivní varietou*, jestliže neexistují projektivní algebraické množiny S_1 a S_2 takové, že $\emptyset \subsetneq S_1 \subsetneq S, \emptyset \subsetneq S_2 \subsetneq S$ a $S = S_1 \cup S_2$.

Předchozí úvahy nám dovolují uhádnout, že projektivní variety a projektivní algebraické množiny vykazují chování velmi podobné afinnímu případu.

Tvrzení 5.12. *(i) Ať $S_i \subseteq \mathbb{P}^n, i \in I$. Pak $\bigcap_{i\in I} \bar{\mathbb{I}}(S_i) = \bar{\mathbb{I}}(\cup_{i\in I} S_i)$;*

(ii) *Ať* $M_i \subseteq K\lfloor X \rfloor, i \in I$. *Pak* $\bigcap_{i\in I} \bar{\mathbb{V}}(M_i) = \bar{\mathbb{V}}(\cup_{i\in I} M_i)$;

(iii) $\bar{\mathbb{I}}(S)$ *je i–část pro každé* $S \subseteq \mathbb{P}^n$ *a* $\bar{\mathbb{V}}(M) = \bar{\mathbb{V}}(\lfloor (M) \rfloor)$ *pro každé* $M \subseteq K\lfloor X \rfloor$;

(iv) *Ať* $S_1, \ldots, S_k$ *jsou podmnožiny* $\mathbb{P}^n$. *Pak* $\bar{\mathbb{I}}(S_1 \cup \cdots \cup S_k) \supseteq \bar{\mathbb{I}}(S_1) \cdots \bar{\mathbb{I}}(S_k)$;

(v) *Ať* $A_1, \ldots, A_k$ *jsou i–části v* $K\lfloor X \rfloor$. *Pak* $\bar{\mathbb{V}}(A_1 \cdots A_k) = \bar{\mathbb{V}}(A_1) \cup \cdots \cup \bar{\mathbb{V}}(A_k)$;

(vi) *Všechny projektivní algebraické množiny tvoří topologii uzavřených množin (Zariského topologii) a* $\bar{\mathbb{V}}\bar{\mathbb{I}}$ *je v této topologii uzávěrovým operátorem; (Říká se mu projektivní uzávěr)*

(vii) *Neexistuje nekonečná posloupnost* $S_1, S_2, \ldots$ *projektivních algebraickýh množin, že* $S_1 \supsetneq S_2 \supsetneq \cdots$;

(viii) *Každou neprázdnou projektivní algebraickou množinu lze vyjádřit jako konečné sjednocení ireducibilních;*

(ix) *Projektivní algebraická množina* S *je ireducibílní, právě když* $\bar{\mathbb{I}}(S)$ *je prvočást v* $K\lfloor X \rfloor$;

(x) *Každá projektivní algebraická množina* S *má jediné vyjádření ve tvaru* $S_1 \cup \cdots \cup S_k$, *kde* S_i *jsou ireducibilní a žádné* $S_j, 1 \leq j \leq k$ *nelze vynechat.*

Důkaz. Body (i) a (ii) vyplynou přímo z definice operátorů $\bar{\mathbb{I}}$ a $\bar{\mathbb{V}}$. První část (iii) je obsažena v lemmatu 4.13. Druhá část plyne z lemmatu 5.1. Bod (iv) je jednoduchý důsledek bodu (i), neboť i–část $\bar{\mathbb{I}}(S_1) \cdots \bar{\mathbb{I}}(S_k)$ je obsažena v i–části $\bar{\mathbb{I}}(S_1) \cap \cdots \cap \bar{\mathbb{I}}(S_k)$. Bod (v) je založen na tom, že $A_1, \ldots, A_k$ je tvořeno vhodnými součty polynomů $F_1, \ldots, F_k$, kde $F_i \in A_i, 1 \leq i \leq k$. Bod (vi) je přímým důsledkem bodu (v). Bod (vii) je důsledek noetherovskosti $K[X]$. Bod (viii) vyplývá z bodu (vii). Bod (ix) odpovídá tvrzení 1.15 a bod (x) tvrzení 1.16. Musíme si ovšem pomocí lemmatu 4.7 nejprve vyjasnit, že i prvočásti A lze charakterizovat podmínkou $BC \subseteq A \implies B \subseteq A \vee C \subseteq A$, kde B, C jsou i–části. Přitom platnost implikace stačí ověřit pro případy, kdy $B \supseteq A$ a $C \supseteq A$. □

Kapitola 6

Souvislosti afinních a projektivních variet

Poznámky a připomenutí: Ať $n \geq 2$. Připomeňme definici $\psi_i : \mathbb{A}^n \to P^n, \psi_i((\alpha_0, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)) = (\alpha_0 : \cdots : \alpha_{i-1} : 1 : \alpha_{i+1} : \cdots : \alpha_n)$. Obraz ψ_i označme U_i. Vidíme, že $(\alpha_0 : \cdots : \alpha_n) \in U_i$, právě když $\alpha_i \neq 0$. Podobně jako v afinním případě platí, jak snadno nahlédneme, i v případě projektivním, že množiny $D_F = \{\bar{\alpha} \in \mathbb{P}^n; F(\alpha) \neq 0\}$ tvoří bázi otevřených množin v Zariského topologii. Každá jiná otevřená množina je jejich konečným sjednocením.
Naším cílem nyní bude ukázat, že afinní a projektivní Zariského topologie se prostřednictvím množin U_i vzájemně jednoznačně určují. Platí $U_i = D_{x_i}$, takže U_i je množina otevřená. Heuristickou pomůckou nám bude diagram:

$$\begin{array}{ccc} K\lfloor X \rfloor & \xrightarrow{\nu_i} & K[x] \\ {\scriptstyle \bar{\mathbb{V}}}\downarrow & & \downarrow{\scriptstyle \mathbb{V}} \\ \mathbb{P}^n & \xleftarrow{\psi_i} & \mathbb{A}^n \end{array}$$

Z něj obrácením šipek lze získat diagramy, kde má smysl uvažovat komutaci:

$$\begin{array}{ccc} K\lfloor X \rfloor & \xleftarrow[\nu_i^{-1}]{} & K[x] \\ {\scriptstyle \bar{\mathbb{V}}}\downarrow & & \downarrow{\scriptstyle \mathbb{V}} \\ \mathbb{P}^n \supseteq U_i & \xleftarrow{\psi_i} & \mathbb{A}^n \end{array} \qquad \begin{array}{ccc} K\lfloor X \rfloor & \xrightarrow{\nu_i} & K[x] \\ {\scriptstyle \bar{\mathbb{V}}}\downarrow & & \downarrow{\scriptstyle \mathbb{V}} \\ \mathbb{P}^n & \xrightarrow[\psi_i^{-1}]{} & \mathbb{A}^n \end{array}$$

Lemma 6.1. *Pro každý ideál $I \subseteq K[x]$ platí $U_i \cap \bar{\mathbb{V}}(\nu_i^{-1}(I)) = \psi_i(\mathbb{V}(I))$.*

Důkaz. Ať $i = 0$ a ať $\bar{\alpha} = \psi_0(\beta) \in U_0$, kde $\beta \in \mathbb{A}^n$. Z L4.10 víme, že $\nu_0^{-1}(I) = \{X_0^s \nu_0^*(f); s \geq 0, f \in I\}$. Pak $\bar{\alpha} \in U_0 \cap \bar{\mathbb{V}}(\nu_0^{-1}(I)) \iff \forall f \in I \forall s \geq 0$ je $X_0^s \nu_0^*(f)(\bar{\alpha}) = 0 \iff \forall f \in I$ je $f(\beta) = 0 \iff \beta \in \mathbb{V}(I) \iff \psi_0(\beta) \in \psi_0(\mathbb{V}(I))$. Tím je důkaz u konce, neboť $\bar{\alpha} = \psi(\beta)$. □

Lemma 6.2. *Pro každou i–část $C \subseteq K\lfloor X \rfloor$ je $\psi_i^{-1}(\bar{\mathbb{V}}(C)) = \mathbb{V}(\nu_i(C))$.*

Důkaz. Ať $\psi_O(\beta) = \bar{\alpha}$, kde $\beta \in \mathbb{A}^n$. Pak $\beta = \psi_0^{-1}(\bar{\alpha})$.
Máme $\beta \in \psi_0^{-1}(\bar{\mathbb{V}}(C)) \iff \bar{\alpha} \in \bar{\mathbb{V}}(C) \iff \forall F \in C$ je $F(\bar{\alpha}) = 0 \iff \forall F \in C$ je $\nu_0(F)(\beta) = 0 \iff \forall f \in \nu_0(C) jef(\beta) = 0 \iff \beta \in \mathbb{V}(\nu_0(C))$.
□

Připomeňme, že podmnožina $\mathbb{A}^n$ je algebraická, právě když je uzavřená (v Zariského topologii). Podobně jsou pohmy algebraický a uzavřený synonymy v $\mathbb{P}^n$. Pro $i \in \{0, \ldots, n\}$ je $\mathbb{P}^n = U_i \cup \bar{\mathbb{V}}(X_i)$.

Lemma 6.3. *Ať $i \in \{0, \ldots, n\}$. Pro $S \subseteq \mathbb{A}^n$ platí S je uzavřená $\iff$ $\psi_i(S) \cup \bar{\mathbb{V}}(X_i)$ je uzavřená.*

Důkaz. Ať S je uzavřená, tedy ať $S = \mathbb{V}(I)$, kde $I \subseteq K[x]$ je ideál. Podle lemmatu 6.1 je $\psi_i(S) = U_i \cap \bar{\mathbb{V}}(\nu_i^{-1}(I))$. Tudíž $\psi_i(S) \cup \bar{\mathbb{V}}(X_i) = (U_i \cup \bar{\mathbb{V}}(X_i)) \cap (\bar{\mathbb{V}}(X_i) \cup \bar{\mathbb{V}}(\nu_i^{-1}(I))) = \mathbb{P}^n \cap (\bar{\mathbb{V}}(X_i) \cup \bar{\mathbb{V}}(\nu_i^{-1}(I)) = \bar{\mathbb{V}}(X_i) \cup \bar{\mathbb{V}}(\nu_i^{-1}(I))$ je sjednocení dvou uzavřených množin, a tedy je to množina uzavřená. Ať naopak je $\psi_i(S) \cup \bar{\mathbb{V}}(X_i)$ uzavřená množina. Jistě $\psi_i^{-1}(\psi_i(S) \cup \bar{\mathbb{V}}(X_i)) = \psi_i^{-1}(\psi_i(S)) \cup \psi_i^{-1}(\bar{\mathbb{V}}(X_i)) = S \cup \emptyset = S$. Víme, že $\psi_i(S) \cup \bar{\mathbb{V}}(X_i) = \bar{\mathbb{V}}(C)$ pro nějakou i–část C. Podle L6.2 je $S = \psi_i^{-1}(\bar{\mathbb{V}}(C)) = \mathbb{V}(\nu_i(C))$, takže S je uzavřená. □

Důsledek 6.4. *Ať $i \in \{0, \ldots, n\}$. Množina $D \subseteq \mathbb{A}^n$ je otevřená v afinní Zariského topologii, právě když $\psi_i(D)$ je otevřená v projektivní Zariského topologii.*

Důkaz. Položme $S = \mathbb{A}^n \setminus D$. Pak $\mathbb{P}^n = U_i \cup \bar{\mathbb{V}}(X_i)$ a $\mathbb{P}^n \setminus \psi_i(D) = \psi_i(S) \cup \bar{\mathbb{V}}(X_i)$. Jde tedy o přímý důsledek lemmatu 6.3 □

Ztotožníme-li U_i s $\mathbb{A}^n$, vidíme, že afinní Zariského topologie je indukována projektivní Zariského topologií.

Opačným směrem poukazuje následující fakt:

Tvrzení 6.5. *Ať $S \subseteq \mathbb{P}^n$. Pak S je otevřená v $\mathbb{P}^n$, právě když $\psi_i^{-1}(S)$ je otevřená v $\mathbb{A}^n$ pro každé $i \in \{0, \ldots, n\}$. Podobně S je uzavřená, právě když $\psi_i^{-1}(S)$ je uzavřená pro každé $i \in \{0, \ldots, n\}$.*

Důkaz. Pro $S \subseteq \mathbb{P}^n$ je $\psi_i(\psi_i^{-1}(S)) = S \cap U_i$. Množina U_i je otevřená. Je-li S otevřená, že otevřená i $S \cap U_i$, a tedy i $\psi_i^{-1}(S)$, podle důsledku 6.4. Platí-li otevřenost $\psi_i^{-1}(S)$ pro každé $i \in \{0, \ldots, n\}$, je podle D6.4 otevřená každá $S \cap U_i$. Z toho plyne i otevřenost $S = S \cap \mathbb{P}^n = S \cap (U_0 \cup \cdots \cup U_n) = (S \cap U_0) \cup \cdots \cup (S \cap U_n)$. Dále platí, že $S \subseteq \mathbb{P}^n$ je uzavřená $\iff$ $\mathbb{P}^n \setminus S$ je otevřená $\iff$ $\psi_i^{-1}(\mathbb{P}^n \setminus S) = \mathbb{A}^n \setminus \psi_i^{-1}(S)$ je otevřená pro $\forall i \in \{0, \ldots, n\}$ $\iff$ $\psi_i^{-1}(S)$ je uzavřená pro $\forall i \in \{0, \ldots, n\}$. □

Tvrzení 6.6. *Ať $i \in \{0, \ldots, n\}$. Zobrazení $V \mapsto \bar{\mathbb{V}}\bar{\mathbb{I}}(\psi_i(V))$ a $\bar{V} \mapsto \psi_i^{-1}(\bar{V})$ vytvářejí bijekci mezi afinními varietami $V \subseteq \mathbb{A}^n$ a těmi projektivními varietami $\bar{V} \subseteq \mathbb{P}^n$, které neleží ve $\bar{\mathbb{V}}(X_i)$. V této bijekci je obrazem $V = \mathbb{V}(I)$, I prvoideál, varieta $\bar{\mathbb{V}}(\nu_i^{-1}(I))$ a obrazem $\bar{V} = \bar{\mathbb{V}}(C)$, kde C je prvočást, varieta $\mathbb{V}(\nu_i(C))$.*

Důkaz. Ať $\bar{V} = \bar{\mathbb{V}}(C)$. Podle lemmatu 6.2 je $\psi_i^{-1}(\bar{V}) = \mathbb{V}(\nu_i(C))$ varieta, neboť $\nu_i(C)$ je podle L4.12 prvoideál, pokud předpokládáme $X_i \notin C$. Ovšem $X_i \in C$ vede na $\bar{V} = \bar{\mathbb{V}}(C) \subseteq \bar{\mathbb{V}}(X_i)$, a tyto variety jsme ze svých úvah vyloučili. Je-li $V = \mathbb{V}(I)$, kde I je prvoideál, tak $\nu_i^{-1}(I)$ je prvočást a $\bar{\mathbb{V}}(\nu_i^{-1}(I))$ je projektivní varieta. Podle lemmatu 6.1 je $\psi_i(V) = U_i \cap \bar{\mathbb{V}}(\nu_i^{-1}(I))$. Chceme ukázat, že $\bar{\mathbb{V}}(\nu_i^{-1}(I))$ je nejmenší projektivní algebraická množina, která obsahuje $\psi_i(V)$. Máme $\psi_i(V) \cup \bar{\mathbb{V}}(X_i) = \bar{\mathbb{V}}(\nu_i^{-1}(I)) \cup \bar{\mathbb{V}}(X_i)$, neboť $\bar{\mathbb{V}}(\nu_i^{-1}(I)) = (\bar{\mathbb{V}}(\nu_i^{-1}(I)) \cap U_i) \cup (\bar{\mathbb{V}}(\nu_i^{-1}(I)) \cap \bar{\mathbb{V}}(X_i))$. Podle lemmatu 6.3 je $\psi_i(V) \cup \bar{\mathbb{V}}(X_i)$ algebraická projektivní varieta. Je-li $\bar{\mathbb{V}}\bar{\mathbb{I}}(\psi_i(V)) = \bar{V}_1 \cup \cdots \cup \bar{V}_k$ ireducibilní rozklad, tak $\bar{V}_j \subseteq \bar{\mathbb{V}}(X_i)$ neplatí pro žádné $j \in \{1, \ldots, n\}$ (Jinak by $\bar{V}_j$ bylo možno ze seznamu vynechat). Tím pádem $\bar{\mathbb{V}}\bar{\mathbb{I}}(\psi_i(V)) \cup \bar{\mathbb{V}}(X_i) = \psi_i(V) \cup \bar{\mathbb{V}}(X_i)$ má ireducibilní rozklad $\bar{V}_1 \cup \cdots \cup \bar{V}_k \cup \bar{\mathbb{V}}(X_i)$. Současně je tato množina rovna sjednocení variet $\bar{\mathbb{V}}(\nu_i^{-1}(I)) \cup \bar{\mathbb{V}}(X_i)$. Z jednoznačnosti ireducibilního rozkladu pak plyne, že $\bar{\mathbb{V}}(\nu_i^{-1}(I)) = \bar{V}_1 = \bar{\mathbb{V}}\bar{\mathbb{I}}(\psi_i(V))$. Zbývá ověřit, že jde o vzájemně inverzní zobrazení. To je však snadné, neboť $\nu_i(\nu_i^{-1}(I)) = I$ a $\nu_i^{-1}(\nu_i(C)) = C$, dle L4.12. □

Kapitola 7

Eliptické funkční těleso

Ať F/K je algebraické funkční těleso, přičemž K se shoduje s tělesem konstant (tedy $\tilde{K} = K$). Ať $\mathbb{P} = \mathbb{P}_{F/K}$ a ať g je rod F/K.

Lemma 7.1. *Pro $n \geq 1, x \in F$ a $P \in \mathbb{P}$ platí, $x \in \mathcal{L}(nP)$, právě když existuje $i \in \{0, \ldots, n\}$ takové, že $(x)_- = iP$. Přitom $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$, právě když $(x)_- = nP$. V takovém případě je $[F : K(x)] = n \deg(P)$.*

Důkaz. Ať $(x)_+ = \sum a_Q Q$ a $(x)_- = \sum b_Q Q$. Je tedy $(x) = \sum (a_Q - b_Q)Q$, kde $0 \in \{a_Q, b_Q\}$ pro každé $Q \in \mathbb{P}$. Podmínka $x \in \mathcal{L}(nP)$ znamená, že $b_Q = 0$ pro $Q \neq P$ a $a_P - b_P \geq -n$, odkud $n \geq b_P \geq 0$. Zbytek je jasný (pro závěrečnou rovnost je třeba ověřit podmínky D4.8). □

Lemma 7.2. *Ať $(n-1)\deg(P) \geq 2g-1$, kde $P \in \mathbb{P}$ a n je celé. Pak existuje $x \in F$ takové, že $(x)_- = nP$.*

Důkaz. Podle lemmatu 7.1 potřebujeme ukázat, že $\dim \mathcal{L}(nP) > \dim \mathcal{L}((n-1)P)$. K tomu stačí ověřit, že $\ell(jP) = j \deg(P) + 1 - g$ kdykolik $j \deg(P) \geq 2g - 1$. To je však důsledek tvrzení 6.5. □

Důsledek 7.3. *Ať $g = 0$ a ať existuje $P \in \mathbb{P}$ stupně 1. Pak existuje $x \in F$, že $F = K(x)$.*

Důkaz. Máme $(0-1)\cdot 1 = -1 = 2g-1$, takže podle lemmatu 7.2 je $(x)_- = P$ pro nějaké $x \in F$. Podle lemmatu 7.1 je $[F : K(x)] = 1$, a tedy $F = K(x)$. □

Lemma 7.4. *Ať $g = 1$ a ať $P \in \mathbb{P}$ je stupně 1. Potom $\mathcal{L}(P) = \mathcal{L}(0)$ a $\ell(kP) = k$ pro každé $k \geq 1$.*

Důkaz. Víme, že $\mathcal{L}(0) = k$, takže $\ell(0) = 1$. Pro $k \geq 1$ máme $\deg(kP) \geq 1 = 2g - 1$, a proto podle tvrzení 6.5 je $\ell(kP) = \deg(kP) = k$. □

Všimněte si, že v situaci lemmatu 7.4 je $\mathcal{L}((k+1)P) \setminus \mathcal{L}(k(P)) \neq \emptyset$ pro každé $k \geq 1$, avšak pro $k = 0$ uvedený vztah neplatí.

Lemma 7.5. *Ať n a m jsou dvě nesoudělná čísla, přičemž jedno z nich je prvočíslo. Platí-li $[F : K(x)] = n$ a $[F : (K(y)] = m$, je $F = K(x, y)$.*

Důkaz. Je-li $n = 1$ nebo $m = 1$, je vztah triviální. Ať je $n > 1$, $m > 1$ a ať je n prvočíslo. Ze vztahu $n = [F : K(x, y)] \cdot [K(x, y) : K(x)]$ plyne, že je buď $[F : K(x, y)] = 1$, nebo $[K(x, y) : K(x)] = 1$. Prvá rovnost znamená, že $F = K(x, y)$. Ať platí ta druhá. Pak je $y \in K(x)$, tedy $K(y) \subseteq K(x)$, takže $n = [F : K(x)]$ dělí $[F : K(y)] = [F : K(x)] \cdot [K(x) : K(y)] = m$. To je však našimi předpoklady vyloučeno. □

Tvrzení 7.6. *Ať $g = 1$ a ať $P \in \mathbb{P}$ je stupně 1. Pak existují $x, y \in F$ takové, že $F = K(x, y), x \in \mathcal{L}(2P) \setminus \mathcal{L}(P), y \in \mathcal{L}(3P) \setminus \mathcal{L}(2P), [F : K(x)] = 2, [F : K(y)] = 3$ a pro vhodná $a_i \in K$, kde $i \in \{1, 2, 3, 4, 6\}$ platí*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Důkaz. Podle lemmatu 7.4 můžeme zvolit $x \in \mathcal{L}(2P) \setminus \mathcal{L}(P)$ a $y \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$. Máme $v_p(x) = -2, v_p(y) = -3, v_p(x^2) = -4, v_p(xy) = -5$ a $v_p(x^3) = v_p(y^2) = -6$. Položme $Z = \{1, x, y, x^2, xy, x^3, y^2\}$. Pro každý divisor $Q = P$ je $v_Q(z) \geq 0$ kdykolik $z \in Z$, neboť $(x)_- = 2P$ a $(y)_- = 3P$ (viz lemma 7.1). To znamená, žře $Z \subseteq \mathcal{L}(6P)$. Ovšem $\ell(6P) = 6$ podle lemmatu 7.4. Existují tedy $u_1, u_2, u_3 \in K$ a $v_1, v_2, v_3, v_4 \in K$, že

$$u_1y^2 + u_2xy + u_3y = v_1x^3 + v_2x^2 + u_3x + v_4$$

přičemž ne všechny prvky množiny $\{u_i; 1 \leq i \leq 3\} \cup \{v_i; 1 \leq i \leq 4\}$ jsou nulové. Množiny $Z \setminus \{x^3\}$ a $Z \setminus y^2\}$ poskytují bázi vektorového prostoru $\mathcal{L}(6P)$, a proto musí být $u_1 \neq 0$ a $v_1 \neq 0$. Máme

$$(u_1^4v_1^2)y^2 + u_1^3v_1^2u_2xy + u_1^3v_1^2u_3y = u_1^3v_1^3x^3 + u_1^3v_1^2v_2x^2 + u_1^3v_1^2v_3x + u_1^3v_1^2v_4$$

Substituce $y = u_1^{-2}v_1^{-1}y_1$ a $x = u_1^{-1}v_1^{-1}x_1$ pak vedou na požadovaný tvar. Zbytek plyne z lemmat 7.1 a 7.5. □

Poznámka: Rovnici v tvrzení 7.6 se říká *Weierstraßova*

Naším cílem nyní bude vyslovení tvrzení, které jsou v jistém smyslu opačná vůči důsledku 7.3 a tvrzení 7.6.

Tvrzení 7.7. *Ať $F = K(x)$. Pak $g = 0, K[x]$ je valuační obor, x je jeho uniformizující prvek a* $\deg(xK[x]) = 1$.

Důkaz. Z $1 = [F : K(x)]$ plyne, že $\deg(x)_{=}1$. Označme P to jediné místo, pro které je $(x)_- = P$. Pak $(x^k)_- = kP$ pro každé $k \geq 1$, takže $\{1, x, \ldots, x^k\} \subseteq \mathcal{L}(kP)$ dle lemmatu 7.1, přičemž $x^k \in \mathcal{L}(kP) \setminus \mathcal{L}((k-1)P)$. Odtud $\ell(kP) \geq k+1$. Je-li $k+1 \geq 2g-1$, tak podle tvrzení 6.5 máme $k+1 \leq \ell(kP) = \deg(kP) - g + 1 = k - g + 1$, takže $g \leq 0$, a tedy $g = 0$. Z $(x)_- = P$ plyne $v_p(x^{-1}) = 1$, a odtud $O_p = K[x^{-1}]$. Máme $K(x) = K(x^{-1})$, takže i $K[x]$ je valuační obor příslušný místu stupně 1, a to je rovno $xK[x]$. □

Tvrzení 7.8. *Ať $F = K(x, y)$, přičemž x a y splňují Weierstraßovu rovnici pro vodná $a_i \in K, i \in \{1, 2, 3, 4, 6\}$. Pak $g \in \{0, 1\}, 2 = [F : K(x)], 3 = [F : K(y)]$ a existuje jediné místo P stupně 1 takové, že $(x)_- = 2P, (y)_- = 3P$. Je-li $g = 0$, tak existuje $t \in F$, že $F = K(t), (t)_- = P$ a pro vhodná $f_x, f_y \in K[t]$ je $x = f_x(t)$ a $y = f_y(t)$, přičemž* $\deg(f_x) = 2$ *a* $\deg(f_y) = 3$.

Důkaz. Položme

$$l = y^2 + a_1xy + a_3y \text{ a } r = x^3 + a_2x^2 + a_4x + a_6$$

Předpokládejme, že $l = r$. Nejprve vyloučíme, že by mohlo nastat $F = K(x)$ nebo $F = K(y)$. Je-li $F = K(x)$, zvolíme $P \in \mathbb{P}$, že $(x)_- = P$. Pak $v_p(r) = -3$. Z $v_p(y) \geq 0$ máme $v_p(l) \geq -1$. Z $v_p(y) \leq -1$ plyne $2v_p(y) = -3$. Je-li $F = K(y)$, zvolíme $P \in \mathbb{P}$, že $(y)_- = P$. Pak $v_p(l) = -2$ nebo $v_p(l) = -1 + v_p(x) \leq -3$. Aby $v_p(r)$ bylo záporné, musí být $v_p(x) \leq 0$. Pak $v_p(r) = 3v_p(x)$, takže $v_p(l) = v_p(r)$ opět platit nemůže. Z $F = K(x)[y] = K(y)[x]$ nyní uvídíme, že musí být $2 = [F : K(x)]$ a $3 = [F : K(y)]$. Srovnáním $v_Q(l)$ a $v_Q(r)$ lze snadno ukázat, že nemůže platit $v_Q(x) < 0$ a $v_Q(y) \geq 0$, ani $v_Q(x) \geq 0$ a $v_Q(y) < 0$, pro žádné $Q \in \mathbb{P}$. Je-li $v_Q(x) \leq v_Q(y) < 0$, je $v_Q(r) = 3v_Q(x) < 2v_Q(x) \leq v_Q(x) + v_Q(y) \leq 2v_Q(y)$, přičemž $v_Q(l) \in \{v_Q(x) + v_Q(y), 2v_Q(y)\}$. Čili ani tento případ nemůže nastat. Vidíme, že pro $v_Q(x) < 0$ je $v_Q(r) = 3v_Q(x)$ a $v_Q(l) = 2v_Q(y)$. Z $r = l$ tedy plyne $3(x)_- = 2(y)_-$. Přitom $\deg(x)_- = 2$. Je-li $(x)_- = \sum a_Q Q$, tak z podmínky $3(x)_- = 2(y)_-$ plyne, že každé a_Q musí být sudé. Tudíž $(x)_- = 2P$ pro právě jedno $P \in \mathbb{P}, \deg(P) = 1$. Pak nutné $(y)_- = 3P$. Každé $k \geq 2$ lze vyjádřit jako $2i + 3j$, kde $i \geq 0$ a $j \geq 0$. Pak je $(x^i y^j) = kP$, takže $\dim \mathcal{L}(kP) \geq k$ pro každé $k \geq 2$. Je-li $k \geq 2g - 1$, je $k \leq \dim \mathcal{L}(kP) = k + 1 - g$, odkud $g \leq 1$. Je-li $g = 0$, musí být $\ell(P) = 2$, takže $(t)_- = P$. Zbytek vyplývá z toho, že $1, t, t^2$ tvoří bázi $\mathcal{L}(2P)$ a $1, t, t^2, t^3$ tvoří bázi $\mathcal{L}(3P)$. □

Obsah