Algebraická geometrie

algebraická část

Aleš Drápal

Kapitola 1

Diskrétní valuační obory

Úmluvy a připomenutí: Okruhy budou vždy komutativní, nebude-li řečeno jinak. Totéž platí o tělesech.
Připomeňme, že ideál I okruhu R se nazývá:
- *vlastní*, je-li $I \neq R$
- *maximální*, je-li $I = J$ pro každý vlastní ideál $J \supseteq I$.

R je těleso $\iff$ 0 je maximální ideál.
R je lokální okruh $\iff$ má jediný maximální ideál a ten je nenulový.
$R^* = \{a \in R; \exists b \in R : ba = 1\}$
$R^\# = R \setminus \{0\}$.
Připomeňmě, že $\forall a, b \in R,$ je $aR = bR \iff \exists r \in R^*,$ že $b = ar$.

Lemma 1.1. *R je lokální $\iff$ $R \setminus R^*$ je nenulový ideál.*

Důkaz. Připomeňme nejprve, že každý vlastní ideál je obsažen v nějakém maximálním. Proto pro M jediný maximální máme $aR = R$ pro každé $a \in R \setminus M$. Odtud $R^* = R \setminus M$, neboť M žádný invertibilní prvek obsahovat nemůže.
Je-li $M = R \setminus R^*$ ideál, tak je jediný maximální, protože $I \subseteq R \setminus R^*$ platí pro každý vlastní ideál I. $\square$

Budou nás zvláště zajímat lokální obory hlavních ideálů. Jejich vlastnosti se promítají i do vlastností jejich podílového tělesa.

Definice 1.1 (Lomený ideál) Ať F je podílové těleso oboru integrity R. *Lomeným ideálem* nazveme každý podmodul F, kde F chápeme jako R-modul. (Podmodulem F je každá podmnožina F uzavřená na + a násobení prvky z R)

Pozn.: Ideály R jsou právě všechny lomené ideály F, které jsou obsaženy v R.
Pozn.: F a 0 jsou *triviální* lomené ideály. Ostatní jsou *netriviální.*

Tvrzení 1.2. *Ať R je lokální obor hlavních ideálů. Ať F je jeho podílové těleso a ať $M = aR$ je maximální ideál R. Pak*

$$\cdots \supsetneq a^{-2}R \supsetneq a^{-1}R \supsetneq R = a^0R \supsetneq aR \supsetneq a^2R \supsetneq \cdots$$

jsou právě všechny netriviální lomené ideály F.
Přitom $\forall i \in \mathbb{Z}$ je $a^iR \setminus a^{i+1}R = a^iR^*$ a pro $\forall b \in F^*$ $\exists! i \in \mathbb{Z}$, že $b \in a^iR^*$.
Navíc pro $\forall b \in F^*$ platí právě jedna z možností $b \in R^*, b \in M, b^{-1} \in M$.

Důkaz. Ať $a^iR = a^{i+1}R$. Pak $a^i = a^{i+1}r$ pro nějaké $r \in R$. Z $M \neq 0$ plyne $a \neq 0$, takže $1 = ar$ a $a \in R^*$, což je spor. Vždy je $a^iR \supseteq a^{i+1}R$, takže máme $a^iR \supsetneq a^{i+1}R$. Pro $r \in R^*$ je $a^iR = a^irR \supsetneq a^{i+1}R$, takže $a^ir \notin a^{i+1}R$. Proto $a^iR^* \subseteq a^iR \setminus a^{i+1}R$. Je-li $b = a^ir$ a $r \in M = aR$, je $b \in a^{i+1}R$. Proto $a^iR \setminus a^{i+1}R \subseteq a^iR^*$. Položme $I = \bigcap_{i\geq 1} a^iR$. Máme $aI = \bigcap_{i\geq 1} a^{i+1}R = I$. Víme, že $I = bR$ pro nějaké $b \in R$. Proto $b \in aI = abR$, takže $b = abr$ pro nějaké $r \in R$. Je-li $b \neq 0$, je $1 = ar$, což je spor, neboť $a \notin R^*$. Proto $I = 0$. To znamená, že $\forall b \in R^\#$ $\exists i \geq 0$, že $b \notin a^iR$. Tedy $\forall b \in R^\#$ $\exists! i \geq 0$, že $b \in a^iR \setminus a^{i+1}R = a^iR^*$. Každé $b \in F^*$ lze proto vyjádřit jako $\frac{a^is}{a^jt}$, kde $i, j \geq 0$ a $s, t \in R^*$. Pišme $\frac{a^is}{a^jt} = a^kr$, kde $k = i - j \in \mathbb{Z}$ a $r = st^{-1} \in R^*$. Je-li $k \geq 1$, je $b \in M$. Je-li $k \leq -1$, je $b^{-1} \in M$. Je-li $b^{-1} \in M$, tak $\exists! i \geq 0$, že $b^{-1} \in a^iR^*$. Pak $b \in a^{-i}R^*$. Vidíme, že $\forall b \in F^*$ $\exists! i \in \mathbb{Z}$, že $b \in a^iR^*$. $\square$

Důsledek 1.3. *Každé $b \in F^*$ lze jediným způsobem vyjádřit jako a^ir, $r \in R^*$.*

Definujme nyní $\nu : F \to \mathbb{Z} \cup \{\infty\}$ tak, že

- $\nu(b) = i$, je-li $b \in a^iR \setminus a^{i+1}R$
- $\nu(0) = \infty$.

Lemma 1.4. *Hodnota $\nu(b), b \in F$, nezávisí na volbě a, kde aR je maximální ideál R. Přitom $a^iR = \{b \in F; \nu(b) \geq i\}$.*

Důkaz. Je-li $a'R = M$, je $a' = au$ pro nějaké $u \in R^*$. Pak ovšem $(a')^iR = a^iu^iR = a^iR$ pro $\forall i \in \mathbb{Z}$. Zbytek je jasný. $\square$

Definice 1.2 (Uniformizující prvkek) Z lemma 1.4 plyne, že $\nu(a) = 1 \iff M = aR$. Každý takový prvek se nazývá *uniformizující*

Pozorování: Vidíme též, že $\nu(a) = 0 \iff a \in R^*$.

Konečně vidíme, že:

(DV1) $\nu(xy) = \nu(x) + \nu(y)$ pro $\forall x, y \in F$;

(DV2) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ pro $\forall x, y \in F$;

(DV3) $\nu(x) = \infty \iff x = 0$.

Důvody jsou jasné: Je-li $x = a^i r, y = a^j s$, kde $r, s \in R^*$, tak $xy = a^{i+j} rs$. Odsud (1). Je-li $\nu(x) \geq i$ a $\nu(y) \geq i$, tak $x, y \in a^i R$, takže $x + y \in a^i R$ a $\nu(x + y) \geq i$. Odtud (2).

Definice 1.3 (Diskrétní valuace) Je-li F těleso a $\nu : F \to \mathbb{Z} \cup \{\infty\}$ splňuje (1)–(3), nazýváme ν *diskrétní valuací.*

Lemma 1.5. *Nechť F je těleso a ν diskrétní valuace na F. Pak $R = \{a \in F; \nu(a) \geq 0\}$ je okruh, pro který platí $R^* = \{a \in F; \nu(a) = 0\}$.*

Důkaz. Z $\nu(1) = \nu(1 \cdot 1) = \nu(1) + \nu(1)$ plyne $\nu(1) = 0$. Proto $1 \in R$, takže dle (DV1) a (DV2) je R vskutku podokruh F. Pro $x \in F$ je $\nu(x) + \nu(x^{-1}) = \nu(1) = 0$. Proto $x, x^{-1} \in R$ implikuje $\nu(x) = 0$ a naopak. □

Definice 1.4 (Diskrétní valuační okruhy) Okruh R se nazývá *diskrétní valuační* (DVR), pokud je oborem interity, pro jehož podílové těleso F existuje diskrétní valuace ν taková, že $R = \{a \in F; \nu(a) \geq 0\}$.

Definice 1.5 (Valuační okruhy) Ať F je těleso. Okruh $R \subseteq F$ je *valuačním okruhem (tělesa)* F, pokud pr $\forall a \in F^*$ je $a \in R$ nebo $a^{-1} \in R$. V takovém případě je F podílovým tělesem R.
Okruh R se nazývá *valuační*, je-li valuačním okruhem svého podílového tělesa.

Poznamenejme, že je-li R diskrétním valuačním okruhem, je valuačním ve smyslu uvedené definice, neboť $\nu(a) + \nu(a^{-1}) = 0$ pro $\forall a \in F$.

Lemma 1.6. *Ať R je valuačním okruhem F. Pak pro každé $a \in F^*$ platí právě jedna z možností: $a \in R^*$, $a \notin R$, $a^{-1} \notin R$. Přitom $R \setminus R^* = \{a \in F;\ a^{-1} \notin R\}$ je ideálem R. Pro každé dva lomené ideály I a J platí, že je $I \subseteq J$ nebo $J \subseteq I$.*

Důkaz. V libovolném okruhu R z $ab \in R^*$ plyne $a \in R^*$ i $b \in R^*$. Proto $a \in R \setminus R^* \implies ra \in R \setminus R^*$ pro $\forall r \in R$. Ať R je valuačním a ať $a, b \in R \setminus R^*$ jsou nenulová. Je $\frac{a}{b} \in R$ nebo $\frac{b}{a} \in R$. Ať bez újmy na obecnosti

$\frac{a}{b} \in R$. Pak $a + b = b(1 + \frac{a}{b})$ leží v R, nikoliv však v R^* (pak by bylo $b \in R^*$). Proto $a + b \in R \setminus R^*$, takže $R \setminus R^*$ je ideál. Předpokládejme, že I a J jsou lomené ideály takové, že $a \in I \setminus J$ a $b \in J \setminus I$. Ať například $\frac{a}{b} \in R$. Pak $a = (\frac{a}{b}) \cdot b \in RJ = J$, což je spor. Proto $I \subseteq J$ nebo $J \subseteq I$. Konečně je zřejmé, že nenulový prvek F, který neleží v R^*, splňuje právě jednu z podmínek $a \in R$, $a^{-1} \in R$. Proto buď $a \in R^*$, nebo $a \notin R$, nebo $a^{-1} \notin R$. $\square$

Tvrzení 1.7. *Každý DVR je lokální obor hlavních ideálů a naopak.*

Důkaz. Ukážeme nejprve, že v diskrétním valuačním okruhu R jsou všechny ideály hlavní. Ať $I \neq 0$ je ideál R. Položme $m = \min\{\nu(a); a \in I\}$. Pak $m \geq 0$ a lze zvolit $a \in I$, že $\nu(a) = m$. Máme $I \supseteq aR$. Ať $b \in I \setminus aR$. Pak neplatí $bR \subseteq aR$, takže $bR \supsetneq aR$ dle lemmatu 1.6. Tudíž $a = br$, kde $r \notin R^*$. Tedy $\nu(r) > 0$ dle lemmatu 1.5 a $\nu(a) = \nu(b) + \nu(r) > \nu(b)$, což je spor.
Je-li naopak R lokální obor hlavních ideálů, lze zavézt valuaci způsobem výše popsaným (za důsledkem 1.3). $\square$

Máme-li diskrétní valuační okruh R s valuací ν, tak vedle této valuace lze na R definovat valuaci popsanou za důsledkem 1.3. Pro $b \in F^*$ podle tvrzení 1.2 existuje jediné $i \in \mathbb{Z}$, že $b = a^i r$, kde $r \in R^*$ a $aR = R \setminus R^*$. Dle **(DV1)** a **(DV2)** platí $\nu(b) = \nu(r) + i\nu(a)$, takže $\nu(b) = i\nu(a)$, dle lemmatu 1.5. Existuje tedy $k = \nu(a) \geq 1$, že $\nu(b) = ki$. Vidíme, že všechny možné valuace ν se shodují až na tento faktor k. Je-li $k = 1$ jde o normalizovanou diskretní valuaci ve smyslu následující definice. Normalizovaná diskrétní valuace existuje pro DVR jediná.

Definice 1.6 (Normalizovaná diskrétní valuace) Ať R je DVR s valuací ν. Ta se nazývá *normalizovaná*, pokud splňuje

(DV4) $\nu(a) = 1$ právě když $a \in R$ je uniformizující.

Každý DVR má právě jednu normalizovanou valuaci a každý diskrétní valuace je kladným celočíselným násobkem normalizované.

Lemma 1.8. *Ať $I \subseteq M = R \setminus R^*$ je ideál valuačního oboru R. Ať $a = a_0 \in I$ a ať I není hlavní ideál. Pak pro $\forall n \geq 0\, \exists a_1, \ldots, a_n \in I$ a $r_1, \ldots, r_n \in M$, že $a_{i-1} = a_i r_i, 1 \leq i \leq n$.*

Důkaz. Pro $n = 0$ je tvrzení zřejmé. Ať $n \geq 1$ a ať jsou nalezena $a_0, \ldots, a_{n-1}$ a $r_1, \ldots, r_{n-1}$. Zvolme $a_n \in I \setminus a_{n-1}R$. Není $a_n R \subseteq a_{n-1}R$, takže dle lemmatu 1.6 je $a_n R \supsetneq a_{n-1}R$. Tedy $a_{n-1} = a_n r_n$ pro nějaké $r_n \in R$. Z $r_n \in R^*$ plyne $a_n R = a_{n-1}R$, takže $r_n \in M$. $\square$

K lemmatu 1.8 se ještě vrátíme. Nyní uvedeme několik dalších vlastností DVR.

Lemma 1.9. *Ať $R \subseteq S \subseteq F$, kde F je podílové těleso okruhu R a S je okruh. Je-li R DVR, je $R = S$ nebo $F = S$. (DVR je tedy vždy maximální podokruh svého podílového tělesa).*

Důkaz. Ať $R \setminus R^* = aR$ a ať $R \subsetneq S$. Pak $\exists i \geq 1$, že $a^{-i} \in S$. Z $a^{i-1} \in R \subseteq S$ plyne $a^{-1} = a^{-i}a^{i-1} \in S$ a odsud $S = F$. $\square$

Uveďme ještě jeden z důsledků tvrzení 1.2.

Důsledek 1.10. *Ať R je DVR a ať $M = R \setminus R^*$. Potom $R^* = \{a^{-1}b; a, b \in M \setminus M^2\}$.*

Důkaz. Je-li $a, b \in M \setminus M^2$, je $M = aR = bR$. $\square$

Tvrzení 1.11. *Ať R_i je DVR tělesa F a ať $M_i = R_i \setminus R_i^*, i \in \{1, 2\}$. Je-li $R_1 \subseteq R_2$ nebo $M_1 \subseteq M_2$, je $R_1 = R_2$.*

Důkaz. Z $M_1 \subseteq M_2$ plyne $R_1 \subseteq R_2$ dle důsledku 1.10. Z $R_1 \subseteq R_2$ plyne $R_1 = R_2$ dle lemmatu 1.9. $\square$

Připomeňme nyní pár drobností o okruzích a ideálech. Ať $R \subseteq S$ jsou okruhy a ať I je ideál R. Pak $IS = \{\sum a_i s_i; a_i \in I, s_i \in S\}$ je ideál S. Je to nejmenší ideál S, který obsahuje I (je generovaný I). Obecně může nastat, že $I \subsetneq R$, ale přitom $IS = S$.

Je-li $a \in S$, tak $R[a] = \{\sum_{i \geq 0} r_i a^i; r_i \in R\}$ je nejmenší podokruh S, který obsahuje $R \cup \{a\}$ (je generovaný $R \cup \{a\}$). Je homomorfním obrazem $R[x]$ při použití dosazovacího homomorfismu $j_a : R[x] \to R[a], j_a(r) = r$ a $j_a(x) = a$. Pokud I je ideál R, tak $I[a] = \{\sum_{i \geq 0} r_i a^i; r_i \in I\}$ je ideál $R[a]$ generovaný I. Obecně může nastat, že $I \subsetneq R$, ale $I[a] = R[a]$.

Tvrzení 1.12. *Ať F je těleso, které obsahuje obor R a ať I je vlastní ideál R. Pak existuje valuační obor $\mathcal{O}$ tělesa F takový, že $R \subseteq \mathcal{O} \subsetneq F$ a $I\mathcal{O} \subseteq \mathcal{O} \setminus \mathcal{O}^*$.*

Důkaz. Označme $\mathcal{S}$ množinu všech meziokruhů S (tj. $R \subseteq S \subsetneq F$) takových, že $IS \subsetneq S$. Pokud $(M, <)$ je lineárně uspořádaná množina a $S_m \in \mathcal{S}$ pro $\forall m \in M$, přičemž $S_m \subseteq S_{m'}$ pro $m < m'$, tak $S = \bigcup(S_m; m \in M)$ je okruh. Protože $1 \notin IS_m$ pro $\forall m \in M$, platí $1 \notin IS$. Tedy $S \in \mathcal{S}$. Podle Zornova lemmatu obsahuje $\mathcal{S}$ alespoň jeden (co do inkluse) maximální prvek. Označme ho $\mathcal{O}$. Ukážeme sporem, že $\mathcal{O}$ je valuační obor.

Ať tedy $a \in F^*$ splňuje, že $a \notin \mathcal{O}, a^{-1} \notin \mathcal{O}$. Položme $J = I\mathcal{O}$. Víme, že $1 \notin J$. Ať $\varepsilon \in \{-1, 1\}$. $J[a^\varepsilon] = I\mathcal{O}[a^\varepsilon]$ je ideál $\mathcal{O}[a^\varepsilon]$. Z maximality $\mathcal{O}$ vyplývá, že $J[a^\varepsilon] = I\mathcal{O}[a^\varepsilon]$, tedy že $1 \in J[a]$ i $1 \in J[a^{-1}]$. Ukážeme, že odsud plyne $1 \in J$, což je hledaný spor.
Existují $g_0, \ldots, g_m \in J$ a $h_0, \ldots, h_n \in J$, že

$$1 = g_0 + g_1 a + \cdots + g_m a^m = h_0 + h_1 a^{-1} + \cdots + h_n a^{-n}.$$

Z $1 \notin J$ plyne $n \geq 1$ a $m \geq 1$. Ať $n + m$ je minimální možné a ať například $m \geq n$. Vynásobme první rovnici $1 - h_0$. Dostáváme

$$1 = h_0 + (1 - h_0)g_0 + (1 - h_0)g_1 a + \cdots + (1 - h_0)g_{m-1}a^{m-1} + (1 - h_0)g_m a^m.$$

Ukážeme, že poslední člen $(1 - h_0)g_m a^m$ lze nahradit prvkem $J[a]$, který má stupeň ostře menší než m. Odsud vyplyne, že $1 = g'_0 + g'_1 a + \cdots + g'_{m-1}a^{m-1}$ pro $g'_0, \ldots, g'_{m-1} \in J$, což je spor s volbou $m + n$. Máme $g_m a^m(1 - h_0) = g_m a^m(h_1 a^{-1} + \cdots + h_n a^{-n}) = g_m(h_n a^{m-n} + h_{n-1}a^{m-n+1} + \cdots + h_1 a^{m-1})$. $\square$

Lemma 1.13. *Ať $\nu : F \to \mathbb{Z} \cup \{\infty\}$ je diskrétní valuace. Jsou-li $a, b \in F$ taková, že $\nu(a) < \nu(b)$, je $\nu(a + b) = \nu(a)$.*

Důkaz. Ať $\nu(a+b) > \nu(a)$. Máme $\nu(a) = \nu(a+b-b) \geq \min\{\nu(a+b), \nu(-b)\}$. To nelze splnit, neboť $\nu(a) < \nu(a + b)$ a $\nu(a) < \nu(b) = \nu(-b)$. $\square$

Kapitola 2

Algebraické funkční těleso

Úmluvy a připomenutí: Ať $K \subseteq F$ jsou tělesa. Prvek $\alpha \in F$ je *algebraický* nad K, je-li $p(\alpha) = 0$ pro nějaké $p \in K[x]^{\#}$. Prvky, které nejsou algebraické, jsou *transcendentní.*

Pro α transcedententní je $K[x] \cong K[\alpha]$. V F tedy leží obor integrity $K[\alpha] = \{\sum a_i \alpha^i; a_i \in K\}$, který lze ztotožnit s polynomiálním okruhem. F obsahuje i podílové těleso $K(\alpha) \cong K(x)$, což je těleso všech (formálních) racionálních funkcí $\frac{p(\alpha)}{q(\alpha)}$, resp. $\frac{p(x)}{q(x)}$. Isomorfismy $K[\alpha] \cong K[x]$ a $K(\alpha) \cong K(x)$ jsou důvodem, proč se transcendentní prvky F značí x, y, z atd.
Budeme se zabývat tělesy T, kde $K(x) \subseteq T \subseteq F$. Proto pro nás bude důležité následující kritérium lineární závislosti nad $K(x)$.

Lemma 2.1. *Ať $x \in F$ je transcendentní nad K. Prvky $f_1, \ldots, f_n \in F$ jsou lineárně závislé nad $K(x)$ právě když existují $p_1, \ldots, p_n \in K[x]$ takové, že $\sum p_i f_i = 0$ a $\exists j, 1 \leq j \leq n$, že $p_j \neq 0$. Navíc lze předpokládat, že p_j není násobkem x (tedy neexistuje $q_j \in K[x]$, že $p_j = xq_j$).*

Důkaz. Pokud $f_1, \ldots, f_n$ jsou LZ nad $K(x)$, tak existují racionální $r_i = \frac{t_i}{s_i} \in K(x), \sum r_i f_i = 0$, kde $t_i, s_i \in K[x]$. Převedením na společného jmenovatele dostáváme situaci, kdy $s_1 = \cdots = s_n = s$. Přitom $s \neq 0$ a $\exists j$, že $r_j \neq 0$. Nyní stačí položit $p_i = t_i s$. Je-li $p_i = xq_i$ pro všechna i, pak $x(\sum q_i f_i) = 0$, odkud $\sum q_i f_i = 0$. □

Lemma 2.1 lze obecněji zjevně vyslovit s požadavkem, aby $p_1, \ldots, p_n$ neměla společný dělistel stupně alespoň 1. Případ, kdy tento dělitel je roven x se vyskytuje v důkazech nejčastěji.

Jsou-li $x, y \in F$ transcendentní, tak $K[x, y]$ nemusí být isomorfní $K[x_1, x_2]$. Stejně tak y nemusí být transcendentní nad $K[x]$.

Lemma 2.2. *Ať $x, y \in F$ transcendentní nad K. Pak je ekvivalentní:*

(i) $[K(x, y) : K(x)] < \infty$ *(y je algebraické nad $K(x)$)*

(ii) $[K(x, y) : K(y)] < \infty$ *(x je algebraické nad $K(y)$)*

(iii) $\exists p \in K[x_1, x_2]^\#$*, že* $p(x, y) = 0$.

Důkaz. Podmínka (i) znamená existenci $k \geq 1$, že $1, y, \ldots, y^k$ jsou LZ nad $K(x)$. Podle lemmatu 2.1 $\exists p_0, \ldots, p_k \in K(x)$, že $\sum p_i(x)y^i = 0$ a že $p(x_1, x_2) = \sum p_i(x_1)x_2^i \neq 0$. Proto (i) $\implies$ (ii). Platí-li (iii), vyjádříme $p(x_1, x_2)$ jako $\sum_{i=0}^k p_i(x_1)x_2^i$. Musí být $k \geq 1$, neboť jinak $p_0(x) = 0$ a $p_0 \neq 0$. $\square$

Definice 2.1 (Algebraické funkční těleso) Jsou-li $K \subseteq F$ taková, že $\exists x \in F$ transcendentní, jež splňuje $[F : K(x)] < \infty$, nazýváme dvojici (K, F) *algebraickým funkčním tělesem.* Místo (K, F) se píše F/K a často se K vynechává.

Pozn.: Algebraický uzávěr K v F budeme značit $\tilde{K}$ a nazývat *těleso konstant.*

Tvrzení 2.3. *Ať F/K je algebraické funkční těleso. Pak pro $a \in F$ platí* $a \notin \tilde{K} \iff [F : K(a)] < \infty$.

Důkaz. Ať $[F : K(x)] < \infty$, x transcendentní nad K. Uvažujme $K(a, x)$. Víme, že $[F : K(a, x)] < \infty$ a $[K(a, x) : K(x)] < \infty$. Je-li a transcendentní, je $[K(a, x) : K(x)] < \infty$ dle lemmatu 2.2. Odtud $[F : K(a)] < \infty$. Je-li $a \in \tilde{K}$, tak z $[F : K(a)] < \infty$ plyne, že $[K(x) : K] \leq [F : K] = [F : K(a)] \cdot [K(a) : K] < \infty$, což je spor. $\square$

Pozn.: Valuačním oborem F/K budeme rozumět valuační obor O tělesa F, který splňuje $K \subseteq O^*$. Přitom F/K bude nějaké pevně zvolené algebraické funkční těleso.

Lemma 2.4. *Ať O je valuační obor F/K. Pak $\tilde{K}^* \subseteq O^*$.*

Důkaz. Pro $a \in O \cap \tilde{K}^*$ můžeme nalézt $\gamma_0, \ldots, \gamma_k \in K$, že $\sum \gamma_i a^i = 0$ a $\gamma_0 = 1$. Pak $a^{-1} = -\gamma_1 - \gamma_2 a - \cdots - \gamma_k a^{k-1} \in O$. $\square$

Tvrzení 2.5. *Každý valuační obor F/K je diskrétní.*

Důkaz. Ať O je valuační obor F/K. Podle tvrzení 1.7 potřebujeme ověřit, že O je obor hlavních ideálů. Ať I je ideál O, který není hlavní. Zvolme $x \in I^{\#}$ a položme $M = O \setminus O^*$. Podle lemmatu 2.4 je $x \notin \tilde{K}$. Podle tvrzení 2.3 je $[F : K(x)] < \infty$. Zvolme $n > [F : K(x)]$ a zkonstruujme $x = a_0, \ldots, a_n \in I$ a $k_1, \ldots, k_n \in M$ dle lemmatu 1.8. Máme $a_{i-1} = k_i a_i \ \forall 1 \leq i \leq n$. Tudíž $a_i/a_j \in M$, je-li $0 \leq i < j \leq n$ a $a_i/a_j \in O$, je-li $0 \leq i \leq j \leq n$. Podle lemmatu 2.1 existují $\varphi_i = \alpha_i + x\psi_i \in K[x]$, že $\sum \varphi_i a_i = 0,\ \alpha_i \in K$ a existuje $j \leq n$, že $\alpha_j \neq 0$. Vyberme největší takové j. Máme $x\psi_i \in I \subseteq M$, neboť $\psi_i \in K[x] \subseteq O$. Dokážeme-li $\varphi_j \in M$, dostaneme spor, neboť pak $\alpha_j = \varphi_j - x\psi_j \in M$, zatímco podle lemmatu 2.4 je $\alpha_j \in O^*$. Pro $i > j$ je $\alpha_i = 0$, pro $i < j$ je $\frac{a_i}{a_j} \in M$. Vždy $\frac{x}{a_j} = \frac{a_0}{a_j} \in O$. Z $-\varphi_j a_j = \sum_{i<j} \varphi_i a_i + \sum_{i>j} x\psi_i a_i$ plyne $-\varphi_j = \sum \varphi_i \underbrace{\frac{a_i}{a_j}}_{\in M} + \sum \underbrace{\frac{x}{a_j}}_{\in O} \psi_i \underbrace{a_i}_{\in I \subseteq M} \in M$. □

Definice 2.2 (Místo) *Místem* se rozumí každá množina P, pro kterou existuje valuační obor O v F/K, že $P = O \setminus O^*$. Z důsledku 1.10 plyne, že z P lze O jednoznačně odvodit. Píšeme $O = O_P$.
Množina všem míst algebraického funkčního tělesa F/K se značí $\mathbb{P} = \mathbb{P}_{F/K}$.

Pozn.: Ať $P_1, P_2 \in \mathbb{P}$. Z tvrzení 1.11 plyne, že $P_1 \subseteq P_2 \implies P_1 = P_2$ a $O_{P_1} \subseteq O_{P_2} \implies P_1 = P_2$. Každé $P \in \mathbb{P}$ určuje (jedinou) normalizovanou diskrétní valuaci $\nu : F \to \mathbb{Z} \cup \{\infty\}$ takovou, že $O_P = \{a \in F; \nu(a) \geq 0\}$ a $P = \{a \in F; \nu(a) > 0\}$. Píšeme $\nu = v_p$.

Lemma 2.6. *Pro $\forall x \in F$ transcendentní (tedy $x \in F \setminus \tilde{K}$) existuje $P \in \mathbb{P}_{F/K}$, že $v_P(x) > 0$. Speciálně je tedy $\mathbb{P}_{F/K} \neq \emptyset$.*

Důkaz. Nerovnost $v_P(x) > 0$ vyjadřuje $x \in P$. Položme $R = K[x]$ a $I = xK[x]$. Podle tvrzení 1.12 existuje valuační obor $O \supseteq R$ algebraického funkčního tělesa F/K takový, že $O = O_P$ a $P \supseteq I$. Je tedy $x \in P$. □

Pozn.: Ať $P \in \mathbb{P}$. Máme $K \subseteq O_P$ a $K \cap P = 0$. Uvažujme projekci $\pi_P : O_P \to O_P/P$. Pak $\pi_P \restriction K$ je vnořením $K \hookrightarrow O_P/P$. Faktorokruh O_P/P je těleso a $\pi_P(K)$ jeho podtěleso. Položme $\deg(P) = [O_P/P : \pi_P(K)]$. Většinou se $\pi_P(K)$ a K ztotožňují a klade se pak $\deg(P) = [O_P/P : K]$. Platí $\pi_P(K) = \{\alpha + P; \alpha \in K\} = (P + K)/P$.

Tvrzení 2.7. *Ať $x \in P \in \mathbb{P}, x \neq 0$. Pak x je transcendentní nad K a platí $\deg(P) \leq [F : K(x)] < \infty$.*

Důkaz. Podle tvrzení 2.3 a lemmatu 2.4 stačí ukázat $\deg(P) \leq [F : K(x)]$. K tomu bude stačit, že kdykoliv $a_1, \ldots, a_n \in O_P$ jsou takové, že $a_1+P, \ldots, a_n+P$ jsou LNZ nad K, tak $a_1, \ldots, a_n$ jsou LNZ nad $K(x)$. Postupujme sporem. Podle lemmatu2.1 existují $\psi_i \in K[x]$ a $\alpha_i \in K$, $1 \leq i \leq n$, že $\alpha_j \neq 0$ pro některé $j, 1 \leq j \leq n$, a že

$$\sum (x\psi_i + \alpha_i)a_i = \underbrace{x\sum \psi_i a_i}_{\in P,\ \text{neboť}\ x\in P\,\&K[x]\subseteq O_P} + \sum \alpha_i a_i = 0$$

. Vidíme, že $\sum \alpha_i(a_i + P) \subseteq P$. Protože $\alpha_j \neq 0$, jsou $a_1 + P, \ldots, a_n + P$ LZ nad K. $\square$

Podle lemmatu 2.4 je $\tilde{K} \subseteq O_P$, takže $\pi_P \restriction \tilde{K}$ je také vnořením $\tilde{K} \hookrightarrow O_P/P$. Můžeme proto i $\tilde{K}$ považovat za podtěleso O_P/P. Je tedy

Lemma 2.8. $\deg(P) = [O_P/P : \tilde{K}][\tilde{K} : K]$ *a speciálně* $[\tilde{K} : K] < \infty$.

Každý prvek $x \in F \setminus \tilde{K}$ je transcendentní nad $\tilde{K}$ (kdyby byl algebraický, byl by algebraický i nad K). Přitom $[F : \tilde{K}[x]] \leq [F : K(x)] < \infty$. To znamená, že $F/\tilde{K}$ je rovněž algebraické funkční těleso. Z lemmatu 2.4 vyplyne, že $\mathbb{P}_{F/K} = \mathbb{P}_{F/\tilde{K}}$. Lemma 2.8 lze zapsat jako $\deg_{F/K}(P) = \deg_{F/\tilde{K}}[\tilde{K} : K]$. V dalším budeme předpokládat, že $\tilde{K} = K$. Abychom získané výsledky mohli použít na F/K, potřebujeme vědět, že $[\tilde{K}(x) : K(x)] = [\tilde{K} : K]$ pro každé $x \in F \setminus \tilde{K}$. To vyplyne ze závěrečného lemmatu této kapitoly, které má obecný charakter.

Lemma 2.9. *Ať* $K \subseteq K' \subseteq F$ *jsou tělesa. Ať* $x \in F$ *je transcendentní nad* K*. Pak* $[K' : K] \leq [K'(x) : K(x)]$*. Je-li* $[K' : K] < \infty$*, je* $[K' : K] = [K'(x) : K(x)]$.

Důkaz. Ať $a_1, \ldots, a_n \in K'$ jsou LNZ nad K. LZ nad $K(x)$ podle lemmatu 2.1 znamená, že $\sigma = \sum a_i(x\psi_i + \alpha_i) = 0$, kde $\psi_i \in K[x], \alpha_i \in K$ a $\alpha_j \neq 0$ pro nějaké $j \in \{1, \ldots, n\}$. Máme $\sigma \in K'[x]$, takže $\sigma = 0 \implies \sum a_i\alpha_i = 0$, což je spor. Proto platí, že $[K' : K] \leq [K'(x) : K(x)]$. Ať $n = [K' : K]$. Uvažme $S = \{\sum c_i a_i; c_i \in K(x)\}$. $S \subseteq K'(x)$ je nad $K(x)$ vektorovým prostorem dimenze $\leq n$. Z $K \subseteq K(x)$ plyne, že $K' \subseteq S$, neboť $a_1, \ldots, a_n$ je báze K' nad K. Tím pádem každé $a_1^{i_1}, \ldots, a_n^{i_n} \in K'$ leží v S, takže S je okruh. Je to podokruh F generovaný $K(x) \cup \{a_1, \ldots, a_n\}$, čili $S = K(x)[a_1, \ldots, a_n]$. Každé a_i je algebraické nad $K \subseteq K(x)$, takže S je těleso. Obsahuje K' i x, a proto $S = K'(x)$. Tudíž $[K'(x) : K(x)] = \dim_{K(x)} S \leq n = [K' : K]$. $\square$

Kapitola 3

Valuace

Pozn. Ať F/K je algebraické funkční těleso. Valuace $v_P(x)$ jsou shodné pro F/K i $F/\tilde{K}$. Budeme předpokládat $\tilde{K} = K$.

Lemma 3.1. *Ať $a, b \in F, P \in \mathbb{P}_{F/K}$ a ať $v_P(a) \neq 0$ nebo $v_P(b) \neq 0$. Pak existuje nanejvýš jedno $k \in \mathbb{Z}$, že $v_P(a + b^k) \neq \min(v_P(a), kv_P(b))$.*

Důkaz. Abychom mohli použít lemma 1.13, potřebujeme vědět, že $v_P(a) = kv_P(b)$ pro nanejvýš jedno $k \in \mathbb{Z}$. Je.li $v_P(b) = 0$, žádné takové k neexistuje. Ať $v_P(b) \neq 0$. Pak takové k je skutečně nejvýše jedno. □

Tvrzení 3.2 (**Weak approximation theorem (WAT)**). *Ať $P_1, \dots, P_n \in \mathbb{P}_{F/K}$, kde $P_i \neq P_j$ $\forall 1 \leq i < j \leq n$. Ať $r_1, \dots, r_n \in \mathbb{Z}$. Položme $v_i = v_{P_i}$. Pro všechna $x_1, \dots, x_n \in F$ existuje $x \in F$, že $v_i(x - x_i) = r_i$.*

Důkaz rozdělíme do řady dílčích kroků. Přitom budeme často předpokládat, že lemma 3.1 platí ve tvaru $v_P(a+b^k) = \min(v_P(a), kv_P(b))$. Důvodem je, že k budeme vybírat vždy z nekonečné množiny možných hodnot a bude nám stačit existence jednoho k, pro které daná rovnost (nebo několik rovností) platí. Každé v_i nabývá všech hodnot v $\mathbb{Z} \cup \{\infty\}$, takže pro $n = 1$ je tvrzení triviální. Ať $n \geq 2$ a ať pro $n' < n$ všechna dokazovaná tvrzení (včetně dílčích) platí. Položme $O_i = O_{p_i}$.

(W1) $\exists c \in F$, že $v_1(c) > 0$ & $v_2(c) < 0$.

Důkaz. Ať $a \in O_1 \setminus O_2$ a $b \in O_2 \setminus O_1$. Máme $v_1(a) \geq 0, v_2(a) < 0, v_2(b) \geq 0, v_1(b) < 0$. Odtud $v_1(a/b) = v_1(a) - v_1(b) > 0$ a $v_2(a/b) = v_2(a) - v_2(b) < 0$. Lze tedy položit $c = a/b$.

□

(W2) $\exists c \in F$, že $v_1(c) > 0, v_2(c) < 0, \ldots, v_n(c) < 0$.

Důkaz. Z indukčního předpokladu plyne existence $c \in F$, že $v_1(c) > 0$, $v_2(c) < 0, \ldots, v_{n-1}(c) < 0$. Podle **(W1)** můžeme předpokládat $n \geq 3$. Je-li $v_n(c) < 0$, jsme hotovi. Ať $v_n(c) \geq 0$. Zvolme $d \in F$ dle **(W1)** tak, že $v_1(d) > 0$ a $v_n(d) < 0$. Položme $c' = c + d^k$, kde $k \geq 1$. Máme $v_1(c') = \min\{v_1(c), kv_1(d)\} > 0$. Pro $i \in \{2, \ldots, n-1\}$ je $v_i(c') = \min\{v_i(c), kv_i(d)\} < 0$. Konečně $v_n(c') = \min\{v_n(c), kv_n(d)\} = kv_n(d) < 0$.

□

(W3) $\exists d \in F$, že $v_1(d-1) > r_1$ & $v_i(d) > r_i, 2 \leq i \leq n$.

Důkaz. Budeme hledat d ve tvaru $\frac{1}{1+c^k}$, kde $k \geq 1$. Pro $2 \leq i \leq n$ máme $v_i(d) = -v_i(1+c^k) = -kv_i(c)$. Prvek c je převzat z **(W2)**, čili $v_i(d)$ může být libovolně velké kladné. Dále $v_1(d-1) = v_1(1-d) = v_1(\frac{c^k}{1+c^k}) = kv_1(c) - v_1(1+c^k) = kv_1(c)$, neboť $v_1(1+c^k) = \min\{v(1), kv_1(c)\} = v(1) = 0$. Proto i $v_1(d-1)$ může být libovolně velké.

□

(W4) $\exists x \in F$, že $v_i(x - x_i) > r_i$, pro $\forall i 1 \leq i \leq n$.

Důkaz. Ať $d_1, \ldots, d_n \in F$ jsou taková, že $v_i(1-d_i) \,\&\, v_j(d_i), j \neq i$ jsou dostatečně velká. Budeme hledat x ve tvaru $\sum d_j x_j$. Pak $v_i(x - x_i) \geq \min\{v_i(d_j x_j), v_i((d_i - 1)x_i); j \neq i\}$. Chceme, aby $v_i(x - x_i)$ bylo dostatečně velké. Máme $v_i(d_j x_j) = v_i(d_j) + v_i(x_j)$, takže je třeba, aby $v_i(d_j) > r_i - v_i(x_j)$ a podobně, aby platilo $v_i(d_i - 1) > r_i - v_i(x_i)$. To lze podle **(W3)** skutečně zajistit. □

Pozn.: Volba $x_1 = x_2 = \cdots = x_n = 0$ znamená, že $\exists x \in F$, které splňuje $v_i(x) > r_i$.

(W5) Důkaz *WAT*

Důkaz. Zvolme y_i takové, že $v_i(y_i) = r_i$. To vždy lze. Podle **(W4)** $\exists z \in F$, že $\forall i$ je $v_i(z - y_i) > r_i$. Také $\exists x \in F$, že $\forall i$ je $v_i(x - z - x_i) > r_i$. Máme $x - x_i = y_i + (z - y_i) + (x - z - x_i)$. Protože $v_i(z - y_i)$ i $v_i(x - z - x_i)$ jsou větší než $v_i(y_i) = r_i$, tak $v_i(x - x_i) = v_i(y_i) = r_i$. □

Důsledek 3.3. *Množina $\mathbb{P}_{F/K}$ je nekonečná.*

Důkaz. Ať $\mathbb{P} = \{P_1, \ldots, P_n\}$. Podle tvrzení 3.2 existuje $x \in F$, že $v_i(x) = 1, 1 \leq i \leq n$. Podle lemmatu 2.6 $\exists P \in \mathbb{P}$, že $v_P(x^{-1}) > 0$. Tedy $v_P(x) < 0$, takže $P \notin \{P_1, \ldots, P_n\}$. $\square$

Tvrzení 3.4. *Ať $x \in F \setminus K$ je takové, že $v_i(x) > 0, 1 \leq i \leq n$, kde $v_i = v_{P_i}$ a $P_1, \ldots, P_n \in \mathbb{P}_{F/K}$ jsou po dvou různá. Pak $[F : K(x)] \leq \sum v_i(x) \deg(P_i)$.*

Důkaz. Rozdělíme důkaz do několika částí:

A. O bázi. Ať $P = P_i$ a ať $c_1, \ldots, c_f$ je báze O_P modulo P.
Čili $c_1 + P, \ldots, c_f + P$ je báze O_P/P. Jsou-li $\phi_1, \ldots, \phi_f \in O_o$ prvky takové, že $\sum \phi_j c_j \in P$, tak musí být $\phi_j \in P$. Pokud $\exists j$, že $\phi_j \in K[x]$ je tvaru $\sum \alpha_j x^r$ a $\alpha_0 \neq 0$, tak dostáváme spor, neboť $x \in P$ (je $v_P(x) > 0$), ale $\alpha_0 \notin P$.
Důkaz se opírá o nalezení popsaného sporu. Je třeba určit i a j a nalézt $\phi_j \in K[x]$. Je také třeba zvolit vhodnou bázi. Vyjdeme-li od nějaké báze $c_1, \ldots, c_f$, může se stát, že ji potřebujeme modifikovat na $b_1, \ldots, b_f$. K tomu stačí volit $b_j \in c_j + P$, tedy volit b_j tak, že $v_P(b_j - c_j) > 0$.

B. Volba parametrů. Položme $f_i = \deg P_i$.
Ať $c_{i1}, \ldots c_{if_i}$ je báze $O_i = O_{p_i}$ modulo P_o. Pro každé (i, j), kde $1 \leq i \leq n \,\&1 \leq j \leq f_i$, budeme hledat b_{ij} takové, že $v_i(b_{ij} - c_{ij}) > 0$ a $v_k(b_{ij}) = v_k(x)$ pro $k \neq i$. Takové b_{ij} existuje podle WAT (3.2). Podle části **(A)** je $b_{i1}, \ldots, b_{if_i}$ je báze O_i modulo P_i. Dle WAT ještě pro každé $k \in \{1, \ldots, n\}$ zvolíme t_k, že $v_i(t_k) = \delta_{ik}$ (Kroneckerovo delta). Konečně položíme $u_{ijk} = b_{ij} t_i^k, 0 \leq k < v_i(x)$. Hodnot u_{ijk} je právě $\sum_{i=1}^n f_i v_i(x)$. Máme dokázat, že toto číslo je $\leq [F : K(x)]$. Předpokládejme opak. Potom musí být hodnoty u_{ijk} LZ nad $K(x)$. Podle lemmatu 2.1 existují $\phi_{ijk} \in K[x]$, že $\sum \phi_{ijk} u_{ijk} = 0$ a že pro alespoň jednu trojici (i', j', k') je absolutní člen $\phi_{i'j'k'}$ nenulový. Takovou trojici (i', j', k') zvolíme. Přitom můžeme předpokládat, že vzhledem k (i', j') má k' nejmenší možnou hodnotu. Položme $v' = v_{i'}$ a $P' = P_{i'}, O' = O_{i'}$.

C. Podmínka a spor. Podmínkou je tvrzení, že pro $(i, k) \neq (i', k')$ je $\phi_{ijk} u_{ijk} t_{i'}^{-k'} \in P'$. Ať tato podmínka platí. Máme $(\sum \phi_{ijk} u_{ijk}) t_{i'}^{-k'} = 0$. Proto $\sum \phi_{i'jk'} u_{i'jk'} t_{i'}^{-k'} \in P'$. Položme $\phi_j = \phi_{i'jk'}$ a $c_j = u_{i'jk'} t_{i'}^{-k'}$, kde $1 \leq j \leq f' = f_{i'}$. Podle definice je $c_j = b_{i'j} t_{i'}^{k'-k'} = b_{i'j}$ pro $j = 1, \ldots, f'$ bází O' modulo P'. Přitom $\sum \phi_j c_j \in P', \phi_j \in K[x] \,\& \phi_{j'}$ má absolutní člen nenulový. Dostáváme spor podle části A. Zbývá dokázat podmínku.

D. Důkaz podmínky. Chceme ukázat, že pro $(i,k) \neq (i',k')$ je $v'(\phi_{ijk}) + v'(u_{ijk}) - k' > 0$. Po dosazení $u_{ijk} = b_{ij}t_i^k$ dostáváme požadavek $v'(\phi_{ijk}) + v'(b_{ij}) + kv'(t_i) > k'$. Protože $\phi_{ijk} \in K[x] \subseteq O_{i'}$, je vždy $v'(\phi_{ijk}) \geq 0$. Je-li $i' \neq i$, je $v'(t_i) = 0$ a $v'(b_{ij}) = v'(x) > k'$. Ať $i' = i$. Pak chceme $v'(\phi_{i'jk} + k - k' > 0$, neboť $v'(b_{i'j}) = 0 \,\&\, v'(t_{i'}) = 1$. Pak $k > k'$ zřejmé. Pro $0 \leq k < k'$ je $\phi_{i'jk}$ násobek x, čili $v'(\phi_{i'jk}) \geq v'(x) > k'$. □

Důsledek 3.5. *Pro každé $x \in F$ existuje jen konečně mnoho $P \in \mathbb{P}_{F/K}$, že $v_P(x) > 0$, a jen konečně mnoho P, že $v_P(x) < 0$.*

Důkaz. Pro $x \in K$ je vždy $v_P(x) = 0$. Ať $x \in F \setminus K$. Pokud existují $P_1, \ldots, P_n \in \mathbb{P}$, že $v_{p_i}(x) > 0$ a $n > [F : K(x)]$, dostáváme spor s tvrzením 3.4. Tedy $v_P(x) > 0$ nejvýše v $[F : K(x)]$ případech. Zbytek plyne z $v_P(x^{-1}) = -v_P(x)$. □

Kapitola 4

Divisory a Riemannova věta

Úmluvy: Ať F/K je algebraické funkční těleso takové, že každé $x \in F \setminus K$ je trancendentní nad K (tedy $\tilde{K} = K$). Množinu všech míst označme $\mathbb{P}$, tedy $\mathbb{P} = \mathbb{P}_{F/K}$.

Definice 4.1 (Divisory) Volná abelovská grupa s bází $\mathbb{P}$ se značí $\mathrm{Div}(F/K)$ nebo pouze $\mathrm{Div}(F)$. Její prvky jsou formální sumy $\sum_{P \in \mathbb{P}} a_P P$, kde $a_P \in \mathbb{Z}$, přičemž $a_P \neq 0$ jen v konečně mnoha případech.
Prvky $\mathrm{Div}(F)$ se nazývají *divisory*.
Divisor $A = \sum a_P P$ nazveme *kladný* (nebo *efektivní*), jestliže $a_P \geq 0$ pro $\forall P \in \mathbb{P}$.
Divisor $A = \sum a_P P$ se nazývá *prvodivisor*, jestliže $\exists Q \in \mathbb{P}$, že $a_Q = 1$ & $a_P = 0$ pro $P \neq Q$.

Pozn.: Zápis prvodivisoru se obvykle shoduje se zápisem místa, které daný prvodivisor určuje. Typické zápisy divisorů tedy jsou např. $P_1 + 2P_2 - 4P_3$, kde $P_1, P_2, P_3 \in \mathbb{P}$.
Každý kladný divisor lze vyjádřit jako součet prvodivisorů.
Každé $A \in \mathrm{Div}(F)$ lze také jednoznačně vyjádřit jako $A_+ - A_-$, kde A_+ i A_- jsou kladné. Je-li $A = \sum a_P P$, je $A_+ = \sum_{a_P \geq 0} a_P P$ a $A_- = \sum_{a_P \leq 0} -a_P P$.
Je-li $A(+)$ volná abelovská grupa s bází X a $H(+)$ další (ne nutně volná) abelovská grupa, tak každé zobrazení $f : X \to H$ lze jednoznačně rozšířit na homomorfismus grup $A \to H$. Proto lze i $\deg : \mathbb{P} \to \mathbb{Z}$ rozšířit na homomorfismus $\mathrm{Div}(F) \to \mathbb{Z}$. Zjevně $\deg(\sum a_P P) = \sum a_P \deg(P)$.
Každý prvek $x \in F^*$ určuje podle důsledku 3.5 divisor $\sum_{P \in \mathbb{P}} v_P(x) P$. Tento divisor je zvykem značit (x).

Definice 4.2 (Hlavní divisory) Každý divisor, který lze vyjádřit v tomto tvaru se nazývá *hlavní*.

Lemma 4.1. *Pro všechna* $x, y \in F^*$ *platí* $(xy) = (x) + (y)$. *Dále* $(x^{-1}) = -(x)$. *Navíc máme* $(x) = 0$ *právě když* $x \in K^*$. *Konečně* $(\alpha x) = (x)$ *pro každé* $\alpha \in K^*$.

Důkaz. Je-li $(x) = 0$, musí být x algebraické nad K podle lemmatu 2.6. Pak je $x \in K$ (předpokládáme $\tilde{K} = K$). Pro $x, y \in F^*$ a $P \in \mathbb{P}$ je $v_P(xy) = v_P(x) + v_P(y)$, a proto $(xy) = (x) + (y)$. Zbytek je snadný. □

Důsledek 4.2. *Hlavní divisory tvoří podgrupu* $\mathrm{Div}(F)$.

Definice 4.3 (Třídová grupa) Grupa hlavních divisorů se značí $\mathrm{Princ}(F)$. Faktorgrupa $\mathrm{Div}(F)/\mathrm{Princ}(F)$ je známa jako *třídová grupa*. Budeme ji značit $\mathrm{Cl}(F)$.

Následující fakt je pouze reformulací již dokázaného tvrzení 3.4.

Lemma 4.3. *Ať* $x \in F^*$. *Pak* $\deg(x)_+ \leq [F : K(x)]$ *a* $\deg(x)_- \leq [F : K(x)]$.

Důkaz. Ať $P_1, \ldots, P_k \in \mathbb{P}$ jsou všechna (po dvou různá) místa P, že $v_P(x) > 0$. Položme $v_i = v_{p_i}$. Máme $(x)_+ = \sum v_i(x) P_i$ a $\deg((x)_+) = \sum v_i(x) \deg(P_i)$. Nyní je souvislost s tvrzením 3.4 již zřejmá. Zbytek plyne z toho, že $(x^{-1})_+ = (x)_-$ (dle lemmatu 4.1). □

Naším prvním významným cílem bude dokázat, že nerovnosti v lemmatu 4.3 platí i jako rovnosti. Důležitým nástrojem budou Riemann-Rochovy prostory. Pro jejich definici potřebujeme nejdříve zmínit, že $A \leq B$, kde $A = \sum a_P P$ a $B = \sum b_p P$ jsou divisory, vyjadřuje, že $a_P \leq b_p$ pro všechna $P \in \mathbb{P}$.

Definice 4.4 (Riemann-Rochův prostor) Pro $A \in \mathrm{Div}(F)$ se *Riemann-Rochův* prostor $\mathcal{L}(A)$ definuje jako $\{x \in F^*; (x) \geq -A\} \cup \{0\}$.

Pozn.: Z $v_P(x + y) \geq \min\{v_P(x), v_P(y)\}$ vyplývá, že $\mathcal{L}(A)$ je uzavřeno na sčítání. Pro $\alpha \in K^*$ máme $(\alpha x) = (x)$. Proto je $\mathcal{L}(A)$ vektorový prostor nad K.

Lemma 4.4. *Ať* $A \leq B$ *jsou divisory. Pak* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *a* $\dim \mathcal{L}(B)/\mathcal{L}(A) \leq \deg(B - A)$.

Důkaz. Ať $x \in F^*$. Je-li $(x) \geq -A$, je i $(x) \geq -B$. Proto $\mathcal{L}(A) \subseteq \mathcal{L}(B)$. Zbytek dokážeme indukcí dle $\sum(b_p - a_P)$, kde $B = \sum b_p P$ a $A = \sum a_P P$. Je-li tato hodnota rovna 0, je $A = B$ a tvrzení je zřejmé. Ať platí až do nějakého $s \geq 0$ a ať $\sum(b_p - a_P) = s + 1$. Vyberme $Q \in \mathbb{P}$, že $b_q > a_Q$ a položme $C = B - Q$. Pak $\dim \mathcal{L}(C)/\mathcal{L}(A) \leq \deg(C - A)$ podle indukčního předpokladu. Máme $\mathcal{L}(A) \subseteq \mathcal{L}(C) \subseteq \mathcal{L}(B)$, takže stačí ukázat, že $\dim \mathcal{L}(B)/\mathcal{L}(C) \leq \deg(B-C)$. Ovšem $B-C = Q$. Zkontruujme lineární zobrazení $\varphi : \mathcal{L}(B) \to O_Q$, které splňuje podmínku $x \in \mathcal{L}(C) \iff \varphi(x) \in Q$. Označme π přirozenou projekci $O_Q \to O_Q/Q$. Pak $\mathcal{L}(C) = \mathrm{Ker}(\pi\varphi)$, takže $\dim \mathcal{L}(B)/\mathcal{L}(C) = \dim \mathrm{Im}(\pi\varphi) \leq \dim(O_Q/Q) = [O_Q/Q : (K + Q)/Q] = \deg(Q)$. Zbývá tedy zkonstruovat φ tak, aby požadovaná podmínka byla splněna. Položme $\varphi(x) = xt^{b_Q}$, kde $t \in Q$ je uniformizující prvek. Zobrazení φ je F-lineární, takže stačí ověřit, že pro $x \in \mathcal{L}(B)$ je $\varphi(x) \in O_Q$ (tedy $v_Q(\varphi(x)) \geq 0$), přičemž $x \in \mathcal{L}(C)$ právě když $\varphi(x) \in Q$ (tedy $v_Q(\varphi(x)) \geq 1$). Pro $x \in \mathcal{L}(B)$ platí $v_Q(x) + b_Q \geq 0$, takže $v_Q(\varphi(x)) = v_Q(x) + b_Q \geq 0$. Dále $x \in \mathcal{L}(C) \iff v_Q(x) + b_Q + 1 \geq 0 \iff v_Q(\varphi(x)) > 0$. □

Dimenzi Riemann-Rochova prostoru $\mathcal{L}(A)$ označme $\ell(a)$. Z lemmat 2.6 a 4.1 plyne, že $x \in \mathcal{L}(0)$ právě když $x \in K$. Proto $\ell(0) = 1$.

Důsledek 4.5. *Ať* $A \leq B$ *jsou divisory. Potom* $\deg(A) - \ell(A) \leq \deg(B) - \ell(B)$. *Je-li* $A \geq 0$, *je* $0 < \ell(A) \leq \deg(A) + 1$. *Speciálně,* $\ell(0) = 1$.

Důkaz. Podle lemmatu 4.4 je $\dim \mathcal{L}(B)/\mathcal{L}(A) = \ell(B) - \ell(A) \leq \deg(B-A) = \deg(B) - \deg(A)$. Pro $A \geq 0$ máme $\dim \mathcal{L}(A)/\mathcal{L}(0) \leq \deg(A) - \deg(0) = \deg(A)$. Proto $\ell(A) = \dim \mathcal{L}(A) \leq \deg(A) + \ell(0) = \deg(A) + 1$ je vždy konečné.

□

Budeme potřebovat následující pozorování obecné povahy:

Lemma 4.6. *Ať* $K \subseteq F$ *je (libovolné) rozšíření těles a ať* $x \in F$ *je transcendentní nad* K. *Pak* $f_1, \ldots, f_k \in F$ *jsou lineárně nezávislá nad* $K(x)$ *právě když je množina* $\{f_i x^j; 1 \leq i \leq k \;\&\; j \geq 0\}$ *lineárně nezávislá nad* K.

Důkaz. Podle lemmatu 2.1 jsou $f_1, \ldots, f_k$ lineárně závislá nad $K(x)$, pokud $\sum p_i f_i = 0$ pro nějaká $p_i = \sum p_{ij} x^j \in K[x]$, přičemž $p_{ij} \neq 0$ v alespoň jednom případě. Máme $\sum_{i,j} p_{ij}(f_i x^j) \neq 0$, a tudíž je potom množina $\{f_i x^j; 1 \leq i \leq k \;\&\; j \geq 0\}$ nad K vskutku lineárně závislá. Na druhou stranu, pokud je lineárně závislá, obsahuje lineárně závislou konečnou podmnožinu. Proto existuje $m \geq 0$ a $p_{ij} \in K, 1 \leq i \leq k$ a $0 \leq j \leq m$ takové, že $\sum p_{ij}(f_i x^j) \neq 0$, přičemž alespoň jedno p_{ij} je nenulové. Položíme-li $p_i = \sum p_{ij} x^j$, dostaneme $\sum p_i f_i = 0$. $\square$

Lemma 4.7. *Pro každé $x \in F \setminus K$ existuje kladný divisor, že pro $\forall k \geq 1$ je $(k+1)[F : K(x)] \leq \ell(k(x)_- + C)$.*

Důkaz. Ať $m = [F : K(x)]$ a ať $e_1, \ldots, e_m \in F$ tvoří bázi F nad $K(x)$. Podle lemmatu 4.6 je množina všech $x^r e_j, r \geq 0, 1 \leq j \leq m$ lineárně nezávislá nad K. Proto stačí zvolit C tak, aby pro každé $k \geq 1$ platilo $x^r e_j \in \mathcal{L}(k(x) + C)$ pokud $0 \leq r \leq k$, neboť pak $\mathcal{L}(k(x) + C)$ obsahuje $(k+1)m$ prvků, které jsou lineárne nezávislé nad K. Chceme tedy, aby pro každé $Q \in \mathbb{P}$ platilo $rv_q(x) + v_q(e_j) \geq -ka_Q - c_q$, kde $(x)_- = \sum a_P P$ a $C = \sum c_p P$. Je-li $v_q(x) \geq 0$, je $a_Q = 0$, takže pro platnost nerovnosti stačí, bude-li $c_q \geq -v_q(e_j)$. Je-li $v_q(x) < 0$, je $a_Q = -v_q(x)$ a $0 \geq (k-r)v_q(x)$. Vidíme tedy, že $x^r e_j \in \mathcal{L}(k(x)_- + C)$ pro $0 \leq r \leq k$, pokud $c_q \geq -v_q(e_j)$ pro $\forall Q \in \mathbb{P}$. Podle důsledku 3.5 existuje jen konečně mnoho dvojic (Q, j), pro které $v_q(e_j) \neq 0$, a proto lze požadovaný kladný divisor C jistě sestrojit. $\square$

Důsledek 4.8. *Pro každé $x \in F \setminus K$ platí* $\deg((x)_+) = \deg((x)_-) = [F : K(x)]$ *a* $\deg((x)) = 0$.

Důkaz. Položme $m = [F : K(x)]$ a $B = (x)_-$. Podle lemmatu 4.7 a důsledku 4.5 pro $\forall k \geq 1$ platí $(k+1)m \leq \ell(kB + C) \leq \deg(kB + C) + 1 = k\deg(B) + \deg(C) + 1$. Tedy $k(m - \deg(B)) \leq \deg(C) + 1 - m$, což není možné splnit pro všechna kladná k, je-li $m > \deg(B)$. Proto $m \leq \deg(B)$, a tedy $m = [F : K(x)] = \deg((x)_-) = \deg(B)$, dle lemmatu 4.3. Zbytek plyne z $(x)_+ = (x^{-1})_-$ a z $(x) = (x)_+ - (x)_-$. $\square$

Důsledek 4.9. *Ať $x \in F \setminus K$ a ať $B = (x)_-$. Pak existuje kladný divisor C, že pro $\forall k \geq 1$ platí* $\deg(kB) - \ell(kB) \leq \deg(C - B)$.

Důkaz. Vyjdeme opět z nerovnosti $(k+1)m \leq \ell(kB + C)$, kde $m = [F : K(x)]$ je podle důsledku 4.8 rovno $\deg(B)$. Podle lemmatu 4.4 je $\ell(kB + C) \leq \ell(kB) + \deg(C)$, takže $km = \deg(kB) \leq \ell(kB) + \deg(C) - \deg(B)$. $\square$

Pro $A, B \in \mathrm{Div}(F)$ pišme $A \sim B$, je-li $A - B \in \mathrm{Princ}(F)$, tedy je-li $A - B = (x)$ pro nějaké $x \in F^*$.

Tvrzení 4.10. *Ať $A \sim B$, kde $A, B \in$* $\mathrm{Div}(F)$. *Potom $\ell(A) = \ell(B)$ a* $\deg(A) = \deg(B)$.

Důkaz. Pro každé $x \in F^*$ je $\deg(B+(x)) = \deg(B)+\deg((x)) = 0$. Rovnost $\ell(B) = \ell(B+(x))$ dokážeme tak, že zkonstruujeme isomorfismus $\varphi : \mathcal{L}(B+(x)) \cong \mathcal{L}(B)$. Stačí položit $\varphi(y) = yx$. Pak je totiž $yx \in \mathcal{L}(B) \iff (yx) + B \geq 0 \iff (y) + ((x) + B) \geq 0 \iff y \in \mathcal{L}((x) + B)$. $\square$

Lemma 4.11. *Ať $A, B \in \mathrm{Div}(F)$. Pak $\ell(B - A) \geq 1$ právě když existuje $A' \sim A$ takové, že $A' \leq B$.*

Důkaz. Je-li x nenulový prvek $\mathcal{L}(B - A)$, je $(x) + (B - A) \geq 0$, takže $B \geq A - (x) = A + (x^{-1})$. Je-li $A' = A - (x) \leq B$, je $x \in \mathcal{L}(B - A)$. $\square$

Tvrzení 4.12 (Riemannova věta)**.** *Ať F/K je algebraické funkční těleso. Pak existuje $\gamma > 0$, že pro $\forall A \in \mathrm{Div}(F/K)$ je $\deg(A) - \ell(A) < \gamma$.*

Důkaz. Zvolme $x \in F \setminus K$ a položme $B = (x)_-$. Podle důsledku 4.9 existuje $\gamma > 0$, že $\deg(kB) - \ell(kB) < \gamma$ pro všechna $k \geq 1$. Je-li $A \geq 0$, tak podle důsledku 4.5 máme $\deg(kB - A) - \ell(kB - A) \leq \deg(kB) - \ell(kB) < \gamma$. Máme $\deg(B) = [F : K(x)] \geq 1$, takže pro $k \to \infty$ roste $\deg(kB - A) - \gamma \leq \ell(kB - A)$ nade všechny meze. Tudíž $\ell(kB - A) > 0$ pro k dostatečně velké. Pro obecné $A \in \mathrm{Div}(F)$ máme $A = A_+ - A_-$ a $kB - A \geq kB - A_+$, takže platí pro všechna $A \in \mathrm{Div}(F)\ell(kB - A) > 0$ pro k dostatečně velké. Podle lemmatu 4.11 to znamená existenci $A' \sim A$ takového, že $A' \leq kB$. Podle důsledku 4.5 je $\deg(A') - \ell(A') \leq \deg(kB) - \ell(kB) < \gamma$. Podle tvrzení 4.10 je $\deg(A') - \ell(A') = \deg(A) - \ell(A)$. $\square$

Definice 4.5 (Rod) Nejmenší celé $\gamma \geq 0$ takové, že $\deg(A) - \ell(A) < \gamma$ pro všechna $A \in \mathrm{Div}(F/K)$ se nazývá *rod* (genus) a obvykle se značí g. Je tedy $g = \max\{\deg(A) - \ell(A) + 1; A \in \mathrm{Div}(F/K)\}$.

Tvrzení 4.13. *Ať F/K je algebraické funkční těleso rodu g. Ať $D \in \mathrm{Div}(F/K)$ je takové, že $\deg(D) - \ell(D) = g - 1$. Pak pro každé $A \in \mathrm{Div}(F/K)$, které splňuje $A \geq D$ nebo $\ell(A - D) \geq 1$, platí $\deg(A) - \ell(A) = g - 1$. Podmínka $\ell(A - D) \geq 1$ platí vždy, je-li $\deg(A) \geq \deg(D) + g$.*

Důkaz. Ať $\deg(A) \geq \deg(D) + g$. Pak $\ell(A - D) \geq \deg(A - D) + 1 - g = \deg(A) - \deg(D) + 1 - g \geq 1$. Ať $\ell(A - D) \geq 1$. Podle lemmatu 4.11 existuje $D' \sim D$ takové, že $D' \leq A$. Protože $\deg(D') - \ell(D')$ je podle tvrzení 4.10 rovno $\deg(D) - \ell(D)$, můžeme předpokládat přímo $D \leq A$. Pak $\deg(A) - \ell(A) \geq \deg(D) - \ell(D) = g - 1$ podle lemmatu 4.5. Máme ale také $g - 1 \geq \deg(A) - \ell(A)$, a to z definice rodu g. Tudíž $\deg(A) - \ell(A) = g - 1$. $\square$

Vlastnosti uvedené v důsledku 4.5, tvrzení 4.10 a lemmatu 4.11 budeme používat i v dalších kapitolách. Tuto kapitolu ukončíme seznamem některých elementárních vlastností divisorů.

Tvrzení 4.14. *Ať F/K je algebraické funkční těleso. Ať $A, B \in \mathrm{Div}(F/K)$. Potom platí:*

(P1) $A \sim B \implies \ell(A) = \ell(B)$ & $\deg(A) = \deg(B)$.

(P2) $\ell(A) \geq 1 \iff \exists x \in F$, *že* $A + (x) \geq 0 \iff \exists A' \sim A$, *že* $A' \geq 0$.

(P3) $A \leq B \implies \deg(A) - \ell(A) \leq \deg(B) - \ell(B)$.

(P4) $A < 0 \implies \deg(A) < 0 \implies \ell(A) = 0$.

(P5) *Pro každé* $x \in F$ *je* $\mathcal{L}((x)) = Kx^{-1}, \ell((x)) = 1$ & $\deg((x)) = 0$.

(P6) *Ať* $\deg(A) = 0$. *Je-li* $\ell(A) \geq 1$, *je* $\ell(A) = 1$. *Přitom* $\ell(A) = 1 \iff A = (x)$ *pro nějaké* $x \in F$.

Důkaz. **(P1)** se shoduje s tvrzení 4.10 a **(P3)** se shoduje s důsledku 4.5. Z definice $\mathcal{L}(A)$ plyne **(P2)** zcela bezprostředně. Je-li $\ell(A) \geq 1$ a $A' \sim A$ je takové, že $A' \geq 0$, tak $\deg(A) = \deg(A') \geq 0$. Tím jsme dokázali druhou implikaci z **(P4)**. První implikace z **(P4)** je triviální. Uvažme nyní, kdy platí $y \in \mathcal{L}((x)), y \in F^*$. Je to právě tehdy, když $(y) + (x) \geq 0$, tedy $(yx) \geq 0$. To znamená, že $(yx)_- = 0$, odkud $yx \in K^*$, dle důsledku 4.8. Tím je dokázána vlastnost **(P5)**. Konečně ať $\deg(A) = 0$. Je-li $A = (x)$, je $\ell(A) = 1$ dle **(P5)**. Ať $\ell(A) \geq 1$. Podle **(P2)** existuje $x \in F$, že $A' = A + (x) \geq 0$. Podle **(P1)** je $\deg(A') = 0$. Ovšem $A' \geq 0$ & $\deg(A') = 0$ implikuje $A' = 0$, a tedy $A = (x^{-1})$. Důkaz **(P6)** je u konce. $\square$

Kapitola 5

Adèle

Tuto kapitolu zahájíme několika snadnými tvrzeními obecné povahy

Lemma 5.1. *Ať V je vektorový prostor nad K a ať $U_2 \subseteq U_1$ a W jsou jeho podprostory. Potom $U_2 + (U_1 \cap W) = (U_2 + W) \cap U_1$.*

Důkaz. Z $U_2 \subseteq U_1, U_2 \subseteq U_2 + W, U_1 \cap W \subseteq U_2 + W$ a $U_1 \cap W \subseteq U_1$ plyne $U_2 + (U_1 \cap W) \subseteq (U_2 + W) \cap U_1$. Jsou-li $u \in U_2$ a $w \in W$ taková, že $u + w \in U_1$, je $w = (u + w) - u \in U_1$, takže $u + w \in U_2 + (U_1 \cap W)$ a tedy $(U_2 + W) \cap U_1 \subseteq U_2 + (U_1 \cap W)$. □

Lemma 5.2. *Ať V je vektorový prostor nad K a ať $U_2 \subseteq U_1$ a W jsou jeho podprostory takové, že $\dim(U_1/U_2) < \infty$. Potom $\dim((U_1+W)/(U_2+W)) = \dim(U_1/U_2) - \dim((U_1 \cap W)/(U_2 \cap W))$.*

Důkaz. Označme $\pi : V \to V/W$ a $\sigma : V/W \to (V/W)/((U_2 + W)/W)$ přirozené projekce. Ať $\tau : (V/W)/((U_2+W)/W) \cong V/(U_2+W)$ je kanonický izomorfismus (2. věta o izomorfismu). Pak pro každé $u \in U_1$ máme $\tau\sigma\pi(u) = \tau\sigma(u + W) = \tau((u + W) + ((U_2 + W)/W)) = u + (U_2 + W)$. Existuje tedy $\varphi : U_1 \to (U_1 + W)/(U_2 + W)$ surjektivní homomorfismus takový, že $\varphi(u) = u + (U_2 + W)$ pro každé $u \in U_1$. Protože $\operatorname{Ker}\varphi \supseteq U_2$, můžeme definovat $\psi : U_1/U_2 \to (U_1+W)/(U_2+W)$ tak, že $\psi(u+U_2) = u+(U_2+W)$. Zkoumejme $\operatorname{Ker}\psi$. Máme $u+(U_2+W) = 0 \iff u \in U_2+W$. Tedy $\operatorname{Ker}\psi = ((U_2 + W) \cap U_1)/U_2 = (U_2 + (U_1 \cap W))/U_2 \cong (U_1 \cap W)/(U_2 \cap U_1 \cap W) = (U_1 \cap W)/(U_2 \cap W)$. Homomorfismus existuje dle 3. věty o izomorfismu a jemu předcházející rovnost je dokázaná v lemmatu 5.1. Požadovaná rovnost dimenzí plyne ze vztahu $\dim(U_1/U_2) = \dim \operatorname{Ker}(\psi) = \dim \operatorname{Im}(\psi)$. □

Jsou-li M a N množiny, značíme někdy M^N množinu všech zobrazení $N \to M$. Je-li $M = R$ okruh, je R^N také okruh (operace jsou definovány po

složkách; pro $N = \{1, \ldots, n\}$ se místo R^N píše $R^n = \underbrace{R \times \cdots \times R}_{n\text{–krát}}$). Podobně je V^N vektorový prostor nad F, je-li V vektorový prostor nad F.
Předpokládejme nyní, že F/K je algebraické funkční těleso takové, že každé $x \in F \setminus K$ je transcendentní nad K. Nechť dále g označuje rod F/K a $\mathbb{P} = \mathbb{P}(F/K)$.
Všimněme si, že $\mathrm{Div}(F/K)$ je podmnožina $\mathbb{Z}^{\mathbb{P}}$ tvořená všemi zobrazeními $A : \mathbb{P} \to \mathbb{Z}$ takovými, že $A(P) \neq 0$ jen pro konečně mnoho $P \in \mathbb{P}$. Je přitom zřejmé, že $\mathbb{Z}^{\mathbb{P}}$ můžeme chápat jako abelovskou grupu a že $\mathrm{Div}(F/K)$ je její podgrupa.
Uvažujme nyní vektorový prostor $F^{\mathbb{P}}$. Tento vektorový prostor je současně okruhem, neboť F je (mimo jiné) okruh. Vidíme také, že $F^{\mathbb{P}}$ je takzvaná F–algebra (okruh, který je současně vektorovým prostorem a splňuje $\lambda(xy) = \lambda x \cdot y = x \cdot \lambda y$, kde λx je skalární násobení.

Definice 5.1 (Adéle) Prvek $f \in F^{\mathbb{P}}$ se nazývá *adéle*, je-li $f(P) \notin O_P$ jen pro konečně mnoho $P \in \mathbb{P}$. Množinu všech takových f označíme $\mathrm{Adèle}(F/K)$

Položme $\mathbb{Z}_\infty = \mathbb{Z} \cup \{\infty\}$. Množinu $\mathbb{Z}_\infty^P$ lze částečně uspořádat tak, že $a \leq b$ pokud $a(P) \leq b(P)$ pro všechna $P \in \mathbb{P}$. Již dříve bylo definováno částečné uspořádání $\mathrm{Div}(F/K)$, a to je zúžením právě zavedeného částečného uspořádání. Pišme $c = \min(a, b)$, je-li $c(P) = \min\{a(P), b(P)\}$ pro všechna $P \in \mathbb{P}$. Pro každé $f \in F^{\mathbb{P}}$ definujme $\vartheta(f) \in \mathbb{Z}_\infty^P$ tak, že $\vartheta(f)(P) = v_P(f(P))$ pro každé $P \in \mathbb{P}$.

Lemma 5.3. *Ať $f, g \in F^{\mathbb{P}}$ a ať $x \in F$. Definujme $c_x \in F^{\mathbb{P}}$ tak, že $c_x(P) = x$ pro každé $P \in \mathbb{P}$. Potom platí*

(i) $\vartheta(f + g) \geq \min(\vartheta(f), \vartheta(g))$ *a* $\vartheta(fg) = \vartheta(f) + \vartheta(g)$;

(ii) $xf = c_x f, \vartheta(c_x) = (x)$ *a* $\vartheta(xf) = (x) + \vartheta(f)$.

Důkaz. Pro $P \in \mathbb{P}$ je $\vartheta(f + g)(P) = v_P((f + g)(P)) = v_P(f(P) + g(P)) \geq \min\{v_P(f(P)), v_P(g(P))\} = \min\{\vartheta(f)(P), \vartheta(g)(P)\}$, neboť $v_P : F \to \mathbb{Z}_\infty$ je diskrétní valuace. Podobně snadno lze ověřit, že $\vartheta(fg) = \vartheta(f) + \vartheta(g)$. Máme $(xf)(P) = x \cdot f(P)$ (zde x určuje skalární násobek prvku $f \in F^{\mathbb{P}}$) a $(c_x \cdot f)(P) = c_x(P) \cdot f(P) = x \cdot f(P)$. Proto $xf = c_x f$. Současně $\vartheta(c_x)(P) = v_P(c_x(P)) = v_P(x)$, takže $\vartheta(c_x) = (x)$. Rovnost $\vartheta(xf) = (x) + \vartheta(f)$ plyne z rovnosti předchozí a z bodu (i). □

Důsledek 5.4. $\mathrm{Adèle}(F/K)$ *je podalgebrou F–algebry $F^{\mathbb{P}}$. Pro každé $x \in F$ je $c_x \in \mathrm{Adèle}(F/K)$.*

Důkaz. Z definice adèle plyne, že $f \in F^{\mathbb{P}}$ padne do Adèle(F/K) právě když $\vartheta(f)(P) < 0$ jen pro konečně mnoho $P \in \mathbb{P}$. Pokud takovou podmínku splňují $f, g \in F^{\mathbb{P}}$, splňují ji jistě i $\vartheta(f) + \vartheta(g)$ a $\min\{\vartheta(f), \vartheta(g)\}$. Z důsledku 3.5 víme, že $v_P(x) < 0$ jen pro konečně mnoho $P \in \mathbb{P}$. Vidíme, že jde skutečně o přímý důsledek lemmatu 5.3. $\square$

Při práci s Adèle(F/K) je zvykem ztotožnit c_x a x pro každé $x \in F$. Z tohoto ztotožnění vyplývá inkluze $F \subseteq$ Adèle(F/K). Pro $A \in \mathrm{Div}(F/K)$ položme $\mathcal{A}(A) = \{f \in \text{Adèle}(F/K); \vartheta(f) + A \geq 0\}$.

Lemma 5.5. *$\mathcal{A}(A)$ je vektorový prostor nad K, který splňuje $\mathcal{A}(A) \cap F = \mathcal{L}(A)$.*

Důkaz. Jsou-li $f, g \in \mathcal{A}(A)$ a $\lambda \in K^*$, tak podle lemmatu 5.3 máme $\vartheta(\lambda f) = (\lambda) + \vartheta(f) = \vartheta(f) \geq -A$ a $\vartheta(f+g) \geq \min(\vartheta(f), \vartheta(g)) \geq -A$. Proto je $\mathcal{A}(A)$ uzavřeno jak na součty, tak na skalární násobky prvky z K. Pro $x \in F^*$ platí $c_x \in \mathcal{A}(A)$ právě když $\vartheta(c_x) = (x) \geq -A$, tedy právě když $x \in \mathcal{L}(A)$. $\square$

Lemma 5.6. *Ať $A, B \in \mathrm{Div}(F/K)$ splňují $A \leq B$. Potom $\mathcal{A}(A) \subseteq \mathcal{A}(B)$ a $\dim(\mathcal{A}(B)/\mathcal{A}(A)) = \deg(B - A)$.*

Důkaz. Podobnou úvahou jako v důkazu lemmatu 4.4 nahlédneme, že stačí vyřešit případ kdy $C = A$ a $B = C + Q$ pro nějaké $Q \in \mathbb{P}$. K důkazu, že $\mathcal{A}(C+Q)/\mathcal{A}(C)$ má dimenzi $\deg Q$ stačí sestrojit K–lineární surjektivní zobrazení $\varphi : \mathcal{A}(B) \to O_q$ takové, že $\mathcal{A}(C) = \mathrm{Ker}(\pi\varphi)$, kde $\pi : O_q \to O_q/Q$ je přirozená projekce. Vidíme, že $\mathrm{Ker}(\pi\varphi) = \{f \in \mathcal{A}(C); \varphi(f) \in Q\}$. Ať $B = \sum b_p P$. Položme $\varphi(f) = f(Q)t^{b_q}$, kde t je uniformizující prvek O_q (tedy $v_q(t) = 1$). Uvedený předpis poskytuje K–lineární homomorfismus $F^{\mathbb{P}} \to F$. Je třeba ověřit, že zobrazuje $\mathcal{A}(B)$ do O_q. To ovšem plyne z $v_q(f(Q)t^{b_q}) = v_q(f(Q)) + b_q \geq b_q - b_q = 0$. Současně $v_q(f(Q)t^{b_q}) \geq 1$ právě když $v_q(f(Q)) \geq -(b_q - 1)$. Přitom pro $f \in \mathcal{A}(B)$ je $f \in \mathcal{A}(C)$ právě když $v_q(f(Q)) \geq -(b_q - 1)$. Zbývá ukázat surjektivitu φ. Je-li $y \in O_q$, definujme $f \in$ Adèle(F/K) tak, že $f(P) = 0$ pro $P \neq Q$ a $f(Q) = yt^{-b_q}$. Pak $v_P(f(P)) = \infty > -b_p$ a $v_q(f(Q)) = v_q(y) - b_q \geq -b_q$. Proto je $f \in \mathcal{A}(B)$. Zobrazení φ je surjektivní. Je tedy surjektivní i $\pi\varphi$. Víme, že $\mathrm{Ker}(\pi\varphi) = \mathcal{A}(C)$, takže $\mathcal{A}(B)/\mathcal{A}(C) \cong O_q/Q$. $\square$

Definice 5.2 (Index specializace) Rod g je definován tak, že pro každé $A \in \mathrm{Div}(F/K)$ je $i(A) = \ell(A) - \deg(A) + g - 1 \geq 0$, přičemž $i(A) = 0$ pokud je $\deg(A)$ dostatečně velké (viz tvrzení 4.13). Hodnota $i(A)$ se nazývá *index specializace*.

Lemma 5.7. *Ať $A, B \in \mathrm{Div}(F/K)$ splňují $A \leq B$. Potom $\mathcal{A}(A) + F \subseteq \mathcal{A}(B) + F$ a $\dim((\mathcal{A}(B) + F))/(\mathcal{A}(A) + F)) = (\deg(B) - \ell(B)) - (\deg(A) - \ell(A)) = i(A) - i(B)$.*

Důkaz. Podle lemmatu 5.2 je uvažovaná dimenze rovna $\dim(\mathcal{A}(B)/\mathcal{A}(A)) - \dim(\mathcal{L}(B)/\mathcal{L}(A))$, neboť podle lemmatu 5.5 je $\mathcal{A}(B) \cap F = \mathcal{L}(B)$ a $\mathcal{A}(A) \cap F = \mathcal{L}(A)$. Rovnost tudíž plyne z lemmatu 5.6. □

Lemma 5.8. *Ať $i(D) = 0$, kde $D \in \mathrm{Div}(F/K)$. Potom $\mathcal{A}(D) + F = \mathrm{Adèle}(F/K)$.*

Důkaz. Ať $f \in \mathrm{Adèle}(F/K)$. Existuje jen konečně mnoho $P \in \mathbb{P}$ takových, že $\vartheta(f)(P) < 0$ nebo že $d_P < 0$, kde $D = \sum d_P P$. Proto lze zvolit kladný divisor P takový, že $\vartheta(f) + B + D \geq 0$. Tím pádem $f \in \mathcal{A}(D + B)$. Pro $A = D + B$ máme $A \geq D$, takže z tvrzení 4.13 dostáváme $i(A) = 0 = i(D)$. Podle lemmatu 5.7 je proto $F + \mathcal{A}(A) = F + \mathcal{A}(D)$, takže z $f \in \mathcal{A}(A)$ plyne $f \in F + \mathcal{A}(D)$. □

Z lemmat 5.7 a 5.8 okamžitě dostáváme:

Důsledek 5.9. *Pro každé $A \in \mathrm{Div}(F/K)$ platí:*

$$i(A) = \dim(\mathrm{Adèle}(F/K)/\mathcal{A}(A) + F).$$

Důsledek 5.9 je hlavním výsledkem této kapitoly. Využijeme v následujícím ještě tato dvě snadná tvrzení.

Lemma 5.10. *Ať je $A \in \mathrm{Div}(F/K)$ a $x \in F^*$. Potom $x\mathcal{A}(A) = \mathcal{A}(A - (x))$.*

Důkaz. Buď $g \in \mathrm{Adèle}(F/K)$. Podle lemmatu 5.3 je $\vartheta(x^{-1}g) = \vartheta(g) - (x)$. Máme tedy $g \in x\mathcal{A}(A) \iff x^{-1}g \in \mathcal{A}(A) \iff \vartheta(x^{-1}g) + A \geq 0 \iff \vartheta(g) + A - (x) \geq 0 \iff f \in \mathcal{A}(A - (x))$. □

Lemma 5.11. *Ať $A, B \in \mathrm{Div}(F/K)$. Pak $\mathcal{A}(A) + \mathcal{A}(B) = \mathcal{A}(\max(A, B))$.*

Důkaz. Ať $A = \sum a_P P, B = \sum b_p P$ a $C = \max(A, B)$. Je tedy $C = \sum c_p P$, kde $c_p = \max(a_P, b_p)$. Z $A \leq C$ a $B \leq C$ plyne $\mathcal{A}(A) \subseteq \mathcal{A}(C)$ a $\mathcal{A}(B) \subseteq \mathcal{A}(C)$, takže $\mathcal{A}(A) + \mathcal{A}(B) \subseteq \mathcal{A}(C)$. Opačnou inkluzi dokážeme tak, že každé $f \in \mathcal{A}(C)$ vyjádříme jako $f_1 + f_2$, kde $f_1 \in \mathcal{A}(A)$ a $f_2 \in \mathcal{A}(B)$. Je-li $v_P(f(P)) + a_P < 0$, položíme $f_1(P) = 0$ a $f_2(P) = f(P)$. Je-li $v_P(f(P)) + a_P \geq 0$, položme $f_1(P) = f(P)$ a $f_2(P) = 0$. Protože f_1 i f_2 vzniknou z f tak, že některé hodnoty se nahradí nulou, vidíme, že f_1 i f_2 jsou adèle. Okamžitě je patrné, že $f = f_1 + f_2$ a že $f_1 \in \mathcal{A}(A)$. Zbývá ověřit, že $v_P(f_2(P)) = v_P(f(P)) \geq -b_p$ v případě, kdy $v_P(f(P)) + a_P < 0$. Tehdy ovšem z $v_P(f(P)) + c_p \geq 0$ plyne $c_p = b_p$. □

Kapitola 6

Weilovy diferenciály

Ať K je těleso a ať V je vektorový prostor nad K. Jsou-li U_1 a U_2 podprostory V, platí, jak je dobře známo, že $\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$. Z toho vyplývá následující kritérium nenulovosti $U_1 \cap U_2$.

Lemma 6.1. *Ať je V konečné dimenze n. Jsou-li $U_1 \subseteq V$ a $U_2 \subseteq V$ podprostory takové, že $\dim(U_1) + \dim(U_2) > n$, potom $\dim(U_1 \cap U_2) \geq 1$.*

Důkaz. Stačí použít nerovnost $\dim(U_1 \cap U_2) + n \geq \dim(U_1) + \dim(U_2)$. $\square$

Množinu všech lineárních forem $\mathrm{Hom}(V, K)$ budeme v této kapitole značit V^*. Je-li $\sigma : V \to U$ homomorfismus vektorových prostorů, je $\sigma^* : U^* \to V^*, \psi \mapsto \psi\sigma$ rovněž homomorfismus. Budeme uvažovat o obrazu π^*, kde $\pi : V \to V/W$ je přirozená projekce modulo podprostor W. Je zřejmé, že $\mathrm{Im}\,\pi^* \subseteq \mathrm{Ann}_V(W) = \{\varphi \in V^*; W \subseteq \mathrm{Ker}\,\varphi\}$. (Zde Ann označuje *anihilátor*). Vidíme, že $\mathrm{Ann}_V(W)$ je podprostor V^*. Pro každé $\varphi \in \mathrm{Ann}_V(W)$ definujme $\overline{\varphi} : V/W \to K$ tak, že $\overline{\varphi}(v + W) = \varphi(v)$. Je-li $v_1 = v_2 + w$, kde $w \in W$, je $\varphi(v_1) = \varphi(v_2) + \varphi(w) = \varphi(v_2)$, takže definice je korektní. Okamžitě nahlédneme, že $\overline{\varphi} \in (V/W)^*$ a že zobrazení $\varphi \mapsto \overline{\varphi}$ je homomorfismus $\mathrm{Ann}_V(W) \to (V/W)^*$. Pro $v \in V$ a $\varphi \in \mathrm{Ann}_V(W)$ máme $(\pi^*\overline{\varphi})(v) = \overline{\varphi}(\pi(v)) = \overline{\varphi}(v + W) = \varphi(v)$, takže $\pi^*(\overline{\varphi}) = \varphi$. Pro $\Phi \in (V/W)^*$ je $\overline{\pi^*(\Phi)}(v + W) = \pi^*(\Phi)(v) = \Phi(\pi(v)) = \Phi(v + W)$, takže $\overline{\pi^*(\Phi)} = \Phi$. Dokázali jsme, že zobrazení $\varphi \mapsto \overline{\varphi}$ a $\phi \mapsto \pi^*(\phi)$ jsou vzájemně inverzní.

Lemma 6.2. *Ať V je vektorový prostor nad K s podprostory W a W'.*

(i) $\mathrm{Ann}_V(W) \cong (V/W)^*$. *Je-li V/W konečné dimenze, je* $\dim(\mathrm{Ann}_V(W)) = \dim(V/W)$;

(ii) $\mathrm{Ann}_V(W + W') = \mathrm{Ann}_V(W) \cap \mathrm{Ann}_V(W')$;

(iii) *Je-li* $W' \leq W$, *je* $\mathrm{Ann}_V(W) \subseteq \mathrm{Ann}_V(W')$.

Důkaz. Izomorfismus uvedený v bodu (i) je dokázaný výše. Je-li U prostor konečné dimenze, je $\dim U = \dim U^*$, z čehož plyne druhá část bodu (i). Forma $\varphi \in V^*$ se nuluje na $W + W'$ právě když se anuluje současně na W i W'. Odtud bod (ii). Bod (iii) je jeho důsledkem. □

Uvažme nyní situaci, kdy V je navíc vektorový prostor nad $F \supseteq K$. Přitom V^* stále označuje prostor forem $V \to K$.

Lemma 6.3. *Pro* $x \in F$ *a* $\varphi \in V^*$ *definujme* $x\varphi : V \to K$ *tak, že pro každé* $v \in V$ *je* $(x\varphi)(v) = \varphi(xv)$. *Pak* $x\varphi \in V^*$. *Takto definované skalární násobení vytváří z* V^* *vektorový prostor nad* F. *Je-li* $W \subseteq V$ *podprostor a* $x \in F^*$, *je* $\mathrm{Ann}_V(x^{-1}W) = x\,\mathrm{Ann}_V(W)$.

Důkaz. Násobení prvkem $x \in F$ je K–lineární transformací V, takže jistě $x\varphi \in V^*$. Ověřená vztahů $x(\varphi_1 + \varphi_2) = x\varphi_1 + x\varphi_2, 1\varphi = \varphi, (x+y)\varphi = x\varphi + y\varphi, x(y\varphi) = (xy)\varphi$ nečiní potíže, takže V^* lze vskutku považovat za vektorový prostor nad F. Máme $\varphi \in \mathrm{Ann}_V(xW) \iff \varphi(xw) = 0$ pro $\forall w \in W \iff (x\varphi)(w) = 0$ pro $\forall w \in W \iff x\varphi \in \mathrm{Ann}_V(W) \iff \varphi \in x^{-1}\,\mathrm{Ann}_V(W)$. □

Ve zbytku kapitoly bude F/K algebraické funkční těleso rodu g, kde každé $x \in F \setminus K$ je trancendentní nad K.

Pro $A \in \mathrm{Div}(F/K)$ ať $\Omega(A) = \Omega_{F/K}(A) = \mathrm{Ann}_{\mathrm{Adèle}(F/K)}(\mathcal{A}(A) + F)$. Položme dále $\Omega(F/K) = \bigcup_{A \in \mathrm{Div}(F/K)} \Omega(A)$.

Definice 6.1 (Weilův diferenciál) Lineární forma $\omega \in (\mathrm{Adèle}(F/K))^*$ se nazývá *Weilův diferenciál* právě když padne do $\Omega(F/K)$.

Lemma 6.4. *Ať* $A, B, C \in \mathrm{Div}(F/K)$ *a ať* $x \in F^*$. *Pak:*

(i) $\dim(\Omega(A)) = i(A) = \ell(A) - \deg(A) + g - 1$;

(ii) *Je-li* $A \leq B$, *je* $\Omega(A) \supseteq \Omega(B)$;

(iii) *Je-li* $C \leq A$ *a* $C \leq B$, *je* $\Omega(C) \supseteq \Omega(A) + \Omega(B)$;

(iv) *Je-li* $C = \max(A, B)$, *je* $\Omega(C) = \Omega(A) \cap \Omega(B)$;

(v) $x\Omega(A) = \Omega(A + (x))$.

Důkaz. (i) Máme $\dim \Omega(A) = \dim \mathrm{Adèle}(F/K)/(\mathcal{A}(A)+F) = i(A)$ dle lemmatu 5.9.
Bod (ii) vyplývá z lemmatu 6.2 a z lemmatu 5.6: Neboť $A \leq B \implies \mathcal{A}(A) \subseteq \mathcal{A}(B) \implies \Omega(A) \supseteq \Omega(B)$. Bod (iii) je přímým důsledkem bodu (ii). K důkazu bodu (iv) využijeme, že podle lemmatu 5.11 je $\mathcal{A}(C) = \mathcal{A}(A)+\mathcal{A}(B)$. Tedy $\mathcal{A}(C)+F = (\mathcal{A}(A)+F)+(\mathcal{A}(B)+F)$, takže $\Omega(C) = \Omega(A)\cap\Omega(B)$ podle bodu (ii) z lemmatu 6.2. Podle lemmatu 6.3 je $x\Omega(A)$ rovno anihilátoru prostoru $x^{-1}(\mathcal{A}(A)+F) = x^{-1}\mathcal{A}(A)+F = \mathcal{A}(A+(x))+F$, kde poslední rovnost je dána lemmatem 5.10. Tím je dokázán bod (v). □

Důsledek 6.5. *$\Omega(F/K)$ je podprostorem $(\mathrm{Adèle}(F/K))^*$ chápaným jako vektorový prostor nad F.*

Důkaz. Podle důsledku 5.4 je $\mathrm{Adèle}(F/K)$ vskutku vektorový prostor nad F, a proto je podle lemmatu 6.3 takovým prostorem i $(\mathrm{Adèle}(F/K))^*$. Podle bodu (iii) z lemmatu 6.4 máme, že $\Omega(F/K)$ je uzavřené na sčítání, zatímco z bodu (v) vidíme, že je uzavřené i na skalární násobení. □

V dalších úvahách budou významnou úlohu mít zobrazení $F \to F\omega, x \mapsto x\omega$, kde ω je nenulový Weilův diferenciál. Takové zobrazení je možné chápat podle důsledku 6.5 jako izomorfismus vektorových prostorů nad K.

Lemma 6.6. *Ať $\omega \in \Omega(F/K), \omega \neq 0$, a ať $A, B \in \mathrm{Div}(F/K)$. Je-li $\omega \in \Omega(A)$ a $x \in \mathcal{L}(A+B)$, je $x\omega \in \Omega(-B)$.*

Důkaz. Podmínka $x\omega \in \Omega(-B)$ je podle lemmatu 6.5(v) ekvivalentní podmínce $\omega \in x^{-1}\Omega(-B) = \Omega(-(x)-B)$. Protože $x \in \mathcal{L}(A+B)$ znamená $(x)+A+B \gneq 0$, máme $A \gneq -B-(x)$, takže z $\omega \in \Omega(A)$ podle lemmatu 6.4(ii) plyne $\omega \in \Omega(-(x)-B)$. □

Lemma 6.7. *$\Omega(F/K)$ má jako vektorový prostor nad F dimenzi rovnou jedné.*

Důkaz. Stačí ověřit, že pro nenulová $\omega_1, \omega_2 \in \Omega(F/K)$ existuje $x \in F^*$ takové, že $\omega_2 = \omega_1 x$. K tomu stačí existence $x_1, x_2 \in F^*$, že $x_1\omega_1 = x_2\omega_2$. Ať $\omega_i \in \Omega(A_i)$, kde $i \in 1, 2$. Pro každý divisor B podle lemmatu 6.6 existuje vnoření $\mathcal{L}(A_i+B) \to \Omega(-B), x \mapsto \omega_i x$. Pokud obrazy $\mathcal{L}(A_1+B)$ a $\mathcal{L}(A_2+B)$ budodu mít nenulový průnik, tak hledaná $x_1, x_2 \in F^*$ existují. K tomu podle lemmatu 6.1 a lemmatu 6.4(i) stačí, aby platila nerovnost $\ell(A_1+B)+\ell(A_2+B) > i(-B)$. Volme $B \geq 0$ dostatečně velkého stupně. Pro takový podle tvrzení 4.13 máme $\ell(A_i+B) = \deg(A_i)+\deg(B)-g+1$. Dále $i(-B) = \ell(-B)-\deg(-B)+g-1 = \deg(B)+g-1$ podle vlastnosti (P4) z tvrzení 4.14.

Požadovaná nerovnost má pak tvar $\deg(A_1)+\deg(A_2)+2\deg(B)-2g+2 > \deg(B)+g-1$, což je totéž jako $\deg(B) > 3(g-1)-\deg(A_1)-\deg(A_2)$. To samozřejmě splnit volbou B lze. $\square$

Představme si nyní, že každý divisor A je spojen hranou s nenulovým Weilovým diferenciálem ω právě když $\omega \in \Omega(A)$. Dostáváme tak bipartitní graf mezi $\mathrm{Div}(F/K)$ a množinou $\Omega^{\#} = \Omega(F/K) \setminus \{0\}$. Definujme $M(\omega)$ jako množinu divisorů spojeným s $\omega \in \Omega^{\#}$ hranou popsaného grafu. Je tedy $M(\omega) = \{A \in \mathrm{Div}(F/K); \omega \in \Omega(A)\}$.

Tvrzení 6.8. *Pro každý nenulový Weilův diferenciál ω existuje právě jeden divisor $W = (\omega) \in M(\omega)$ takový, že $A \leq W$ pro každé $A \in M(\omega)$.*

Důkaz. Ať $W \in M(\omega)$. Je-li $A \in \mathrm{Div}(F/K)$ takový, že $i(A) = 0$, je $\Omega(A) = 0$ podle lemmatu 6.4(i). Protože $\omega \neq 0$ leží v $\Omega(W)$, musí být $i(W) > 0$. Podle tvrzení 4.13 platí $i(A) = 0$, kdykoliv $\deg(A)$ je dostatečně velké. Proto je $\{\deg(W); W \in M(\omega)\}$ množina shora omezená. Zvolíme nějaké $W \in M(\omega)$ tak, aby $\deg(W)$ bylo maximální možné. Je-li $A \leq W$, je $\omega \in \Omega(W) \subseteq \Omega(A)$, takže $A \in M(\omega)$. Je-li $A \in M(\omega)$, máme $\omega \in \Omega(A) \cap \Omega(W) = \Omega(C)$, kde $C = \max(A, W)$, dle bodu (iv) z lemmatu 6.4. Tedy $C \in M(\omega)$ a $\deg(C) \leq \deg(W)$. Z $C \geq W$ plyne, že musí být $C = W$, a tedy i $A \leq W$. $\square$

Důsledek 6.9. *Ať $A \in \mathrm{Div}(F/K)$ a $\omega \in \Omega(F/K), \omega \neq 0$. Pak $A \leq (\omega) \iff \omega \in \Omega(A)$.*

Důkaz. Podle tvrzení 6.8 jsou oba vztahy ekvivalentní vztahu $A \in M(\omega)$. $\square$

Důsledek 6.10. *Ať $x \in F^*$ a ať $\omega \in \Omega(F/K), \omega \neq 0$. Potom $(x\omega) = (x) + (\omega)$.*

Důkaz. Ať A je divisor. Použitím důsledku 6.9 a bodu (v) z lemmatu 6.4 dostáváme $A \leq (x\omega) \iff x\omega \in \Omega(A) \iff \omega \in x^{-1}\Omega(A) \iff \omega \in \Omega(A-(x)) \iff A-(x) \leq (\omega) \iff A \leq (x)+(\omega)$. Nyní stačí uvážit případ, kdy $A = (x\omega)$ a $A = (x)+(\omega)$. $\square$

Definice 6.2 (Kanonické divisory) Divisor W se nazývá *kanonický*, lze-li vyjádřit jako (ω), kde $\omega \in \Omega(F/K), \omega \neq 0$.

Důsledek 6.11. *Všechny kanonické divisory tvoří v $\mathrm{Div}(F/K)$ právě jednu rozkladovou třídu modulo $\mathrm{Princ}(F/K)$.*

Tvrzení 6.12. *Ať* $B \in \mathrm{Div}(F/K), \omega \in \Omega(F/K), \omega \neq 0$. *Zobrazení* $x \mapsto x\omega$ *poskytuje izomorfismus* $\mathcal{L}((\omega)-B) \cong \Omega(B)$ *vektorových prostorů nad tělesem* K.

Důkaz. Položíme-li $A = (\omega)$, tak z lemmatu 6.6 okamžitě vidíme, že jde o vnoření $\mathcal{L}(A-B)$ do $\Omega(B)$. Stačí dokázat surjektivitu. Každý nenulový prvek $\Omega(F/K)$ lze podle lemmatu 6.7 zapsat jako $x\omega, x \in F^*$. Chceme ukázat, že z $x\omega \in \Omega(B)$ plyne $x \in \mathcal{L}((\omega) - B)$. Z důsledku 6.9 a důsledku 6.10 máme $x\omega \in \Omega(B) \iff B \leq (x\omega) \iff B \leq (x) + (\omega) \iff (x) + ((\omega) - B) \geq 0 \iff x \in \mathcal{L}((\omega) - B)$. □

Tvrzení 6.13 (Riemann-Rochova)**.** *Ať* W *je kanonický divisor. Potom pro každé* $B \in \mathrm{Div}(F/K)$ *platí, že* $\ell(B) = \deg(B) + \ell(W - B) + 1 - g$.

Důkaz. Ať $W = (\omega)$. Podle tvrzení 6.12 a lemmatu 6.4 je $\ell(W-B) = i(B) = \ell(B) - \deg(B) + g - 1$. □

Podle důsledku 4.5 je $\ell(0) = 1$. Dosazením $B = W$ a $B = 0$ proto okamžitě dostáváme:

Důsledek 6.14. *Ať* W *je kanonický divisor. Pak* $\ell(W) = g, \deg(W) = 2g-2$ *a* $i(W) = 1$.

Jako Riemann-Rochova věta se často uvádí následující fakt:

Tvrzení 6.15. *Ať* F/K *je algebraické funkční těleso rodu* g. *Ať každé* $x \in F \backslash K$ *je transcendentní nad* K. *Je-li* $A \in \mathrm{Div}(F/K)$ *takové, že* $\ell(A) \geq 2g-1$, *tak* $i(A) = 0$ *(to jest* $\ell(A) = \deg(A) + g - 1$*).*

Důkaz. Použijeme-li tvrzení 6.13 pro $A = B$, tak dostaneme uvedený vztah, neboť podle důsledku 6.14 je $\deg(W - A) < 0$, takže $\ell(W - A) = 0$ podle tvrzení 4.14. □

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 $i \in \{0, \dots, n\}$ 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 důsledku 4.8). $\square$

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 6.15. $\square$

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

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

Důkaz. Máme $\mathcal{L}(0) = K$, například podle lemmatu 6.15. Je tedy $\ell(0) = 1$. Pro $k \geq 1$ máme $\deg(kP) \geq 1 = 2g - 1$, a proto podle tvrzení 6.15 je $\ell(kP) = \deg(kP) = k$. $\square$

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. Platí-li $[F : K(x)] = n$ a $[F : K(y)] = m$, je $F = K(x, y)$.*

Důkaz. Máme $[F : K(x)] = [F : K(x, y)][K(x, y) : K(x)] = n$, takže $[F : K(x, y)]$ dělí n. Podobně $[F : K(x, y)]$ dělí m. Protože n a m jsou nesoudělná, musí být $[F : K(x, y)] = 1$. $\square$

Tvrzení 7.6. *Ať $g = 1$ a ať $P \in \mathbb{P}$ je stupně 1. Pak existují $x, y \in F$ taková, 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 $Q \neq P$ je $v_Q(z) \geq 0$ kdykolik $z \in Z$, neboť $(x)_- = 2P$ a $(y)_- = 3P$ (viz lemma 7.1). To znamená, že $Z \subseteq \mathcal{L}(6P)$. 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 $\mathcal{L}(6P)$, protože každá z těchto množin obsahuje právě jeden prvek $\mathcal{L}(L)(jP) \setminus \mathcal{L}(L)((j-1)P)$, $1 \leq j \leq 6$. 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. $\square$

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.

Budeme tedy předpokládat jednak situaci, kdy $F = K(x)$, x transcendentní, jednak $F = K(x, y)$, kde $x, y \in F$ jsou transcendentní nad K a spňují Weierstraßovu rovnici. Tu budeme popisovat též ve tvaru $w(x, y) = g(x, y) - f(x)$, kde $g(x, y) = y^2 + a_1xy + a_3y$ a $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Nevíme předem, zda $K = \tilde{K}$. To bude třeba dokázat. V případě $F = K(x)$ je však rovnost $K = \tilde{K}$ zřejmá.

Tvrzení 7.7. *Ať $F = K(x)$, kde $x \in F$ je transcendentní nad K. Definujme $v = v_\infty : F \to \mathbb{Z}$ tak, že $v(a/b) = \deg(b) - \deg(a)$, jsou-li $a, b \in K[x]$ nenulové a $v(0) = \infty$. Pak je v normalizovaná valuace algebraického funkčního tělesa F/K, které odpovídá místu $P = P_\infty = \{0\} \cup \{a/b \in K(x); 0 \leq \deg(a) < \deg(b)\}$. Pro každé $r \geq 1$ je $(x^r)_- = rP$. Rod F/K je roven 0.*

Důkaz. Ať $a, b, c, d \in K[x]$ jsou nenulová. Jistě $v((a/b) \cdot (c/d)) = \deg(a) + \deg(c) - \deg(b) - \deg(d) = v(ac/bd)$. Ať je například $\deg(ad) \geq \deg(bc)$. Pak $v(a/b - c/d) = \deg(bd) - \deg(ad + bc) \geq \deg(bd) \deg(ad) = \deg(b) - \deg(a) = v(a/b)$. Nyní je již zřejmé, že v je valuace. Přitom $v(x^{-1}) = 1$, takže $v(x^r) = -r$ pro každé $r \in \mathbb{Z}$. Podle důsledku 4.8 je $\deg(P(x)_-) = [F : K(x)] = 1$. Jelikož $v(x) = -1$, musí být $(x)_- = P$ a $\deg(P) = 1$. Je tedy i $(x^r)_- = rP$ pro každé $r \geq 1$. Tudíž $x^r\ in \mathcal{L}(rP) \setminus \mathcal{L}((r - l)P)$ pro každé $r \geq 1$, takže $1 = x^0, x, x^2, \ldots, x^k$ jsou v $\mathcal{L}(rP)$ prvky lineárně nezávislé. Máme tedy $\ell(rP) \geq r$. Podle tvrzení 6.15 je pro r dostatečně velké $\deg(rP) - \ell(rP) = g - 1$, takže $g - 1 \leq r - (r + 1) = -1$. Odtud $g = 0$, neboť rod je vždy nezáporný. $\square$

Tvrzení 7.8. *Ať F/K je rozšíření těles takové, že $F = K(x, y)$, x i y jsou transcendentní nad K a že platí Weierstraßova rovnice $w(x, y) = 0$. Potom $[F : K(x)] = 2, [F : K(y)] = 3$ a každý polynom $u \in K[x, y]$, který v F spňuje $u(x, y) = 0$, je násobkem polynomu w.*

Důkaz. Rovnost $w(x, y) = 0$ mimo jiné znamená, že $x \in F$ je algebraický nad $K(y)$, takže $F = K(y, x) = K(y)[x]$. Minimální polynom x nad $K(y)$ dělí $w(x, y)$ (kde $w(x, y)$ chápeme jako polynom v x), a proto $[F : K(y)]$ (což je stupeň uvažovaného minimálního polynomu) musí dělit $\deg_x w(x, y) = 3$. Tudíž 3 dělí $[F : K(y)]$. Podobně ukážeme, že 2 dělí $[F : K(x)]$. Je tedy třeba vyloučit situace $F = K(x)$ a $F = K(y)$. Ať $F = K(x)$. Zvolme valuaci $v = v_\infty$ podle tvrzení 7.7. Máme $g(x, y) = f(x)$ a $v(f(x)) = -3$. Je-li $v(y) \geq -1$, tak $v(g(x, y)) \geq -2$. Je-li $v(y) \leq -2$, je $v(g(x, y)) =$

$-2v(g) \leq -4$. Oba předpokladu pak vedou ke sporu. Ať $F = K(y)$. Uvažme opět valuaci $v = v_\infty$, tentokrát však vztaženou na y (je tedy $v(y) = -1$). Případ $v(x) \geq 0$ nastat nemůže, neboť pak $v(g(x, y)) - -2$ a $v(f(x)) \geq 0$. Pro $v(x) \leq -1$ máme $v(f(x) = 3v(x)$ a $v(g(x, y)) \geq -1 + v(x)$. Ovšem $-3r < -1 - r$ pro každé $r \geq 1$. Je tedy $[F : K(x)] = 2$ a $[F : K(y)] = 3$. Pokud polynom u dává v F hodnotu 0, tak můžeme každý výskyt $y^r, r \geq 2$, redukovat na y^{r-1}, pokud za y^2 dosadíme podle Weierstraßovy rovnice. Tím pádem $u = aw + t$, kde a, t, w chápeme jako polynomy v x a y, přičemž $t(x, y) = 0$ v F a současně t neobsahuje výskyt y^2. Chceme ukázat, že musí být $t = 0$. Přepokládejme opak. Pokud v t nefuguruje proměnná y, je $t(x) = 0$, což je ve sporu s předpokladem, že $x \in F$ je transcendentní nad K. Je tedy $t(x) = yt_1(x) + t_2(x)$, kde $t_1(x) \neq 0$. To ale znamená, že v F máme $y = -t_2(x)/t_1(x)$, takže $y \in K(x)$ a $F = K(x)$. To je opět spor. □

Zápis $K[x, y]$ může být v souvislosti s F/K chápán nejednoznačně. Je $K[x, y]$ okruh polynomů v proměnných x a y nebo podokruh F? Vyberme si možnost $K[x, y] \subseteq F$ a okruh polynomů dvou proměnných budeme značit $K[x_1, x_2]$. Označme φ homomorfismus $K[x_1, x_2] \to K[x, y], \varphi(x_1) = x, \varphi(x_2) = y, \varphi(s) = s$ pro každé $s \in K$. Pro $u \in K[x_1, x_2]$ je $\varphi(u) = 0$ právě když $u(x, y) = 0$ v F. To podle tvrzení 7.8 nastane právě když $u \in (W)$. Připomeňme, že okruh $K[x_1, x_2]/(f)$, kde $f \in K[x_1, x_2]$ se nazývá *souřadnicový* a značí se $K[f]$. Je-li f reducibilní, značíme podílové těleso $K[f]$ jako $K(f)$ a nazýváme ho *funkční*. Vidíme, že φ indukuje izomorfismus $K[w] \cong K[x, y]$. Protože $F = K(x, y)$, musí být F podílovým tělesem $K[x, y]$ (to plyne z faktu, že toto podílové těleso je nejmenší podtěleso F, které obsahuje $K \cup \{x, y\}$, což je právě $K(x, y)$).

Tvrzení 7.9. *Ať F/K je rozšíření těles takové, že $F = K(x, y)$, že x i y jsou transcendentní nad K a že platí Weierstraßova rovnice $w(x, y) = 0$. Potom je $w(x_1, x_2) \in K[x_1, x_2]$ reducibilní a $K(w) \cong F$, přičemž za izomorfismus lze zvolit zobrazení, které $\frac{u(x_1,x_2)+(w)}{v(x_1,x_2)+(x)} \in K(w)$ posílá na $\frac{u(x,y)}{v(x,y} \in F$.*

Důkaz. Tvrzení je dokázané v textu výše. Skutečnost, že w je ireducibilní vyplývá z faktu, že $K[x_1, x_2]/(w) \cong K[x, y] \subseteq F$ je obor integrity. □

Nyní budeme zkoumat, za jakých okolností určuje Weierstraßova rovnice $w(x, y) = 0$ eliptické funkční těleso F/K. Připomeňme, že součástí definice tohoto tělesa je i předpoklad $K = \tilde{K}$.

Lemma 7.10. *Ať F/K je algebraické funkční těleso. Předpokládejme, že existuje $x \in F$ takové, že $[F : K(x)]$ je prvočíslo. Potom $\tilde{K} = K$ nebo $F = \tilde{K}(x)$.*

Důkaz. Podle lemmat 2.8 a 2.9 máme

$$[F : K(x)] = [F : \tilde{K}(x)][\tilde{K}(x) : K(x)] = [F : \tilde{K}(x)][\tilde{K} : K]$$

$\square$

Tvrzení 7.11. *Ať F/K je takové rozšíření těles, že $F = K(x, y)$, že x i y jsou transcendentní nad K a že platí Weierstraßova rovnice $w(x, y) = 0$. Potom platí:*

(i) F/K je algebraické funkční těleso, ve kterém $\tilde{K} = K$, $2 = [F : K(x)]$ a $3 = [F : K(y)]$.

(ii) Pro každé $Q \in \mathbb{P}_{F/K}$ je buď $v_Q(x) \geq 0$ a $v_Q(y) \geq 0$, nebo $v_Q(x) < 0$ a $v_Q(y) < 0$.

(iii) Existuje jediné místo $P = P_\infty \in \mathbb{P}_{F/K}$ takové, že je současně $v_P(x) < 0$ a $v_P(y) < 0$. Přitom $\deg(P) = 1, (x)_- = 2P$ a $(y)_- = 3P$.

(iv) Rod g algebraického funkčního tělesa F/K je roven 0 nebo 1. Je-li $g = 1$ je F/K eliptické funkční těleso.

(v) $g = 0$ právě když existuje $t \in F$ takové, že $F = K(t)$. Prvek $t \in F$ lze v takovém případě zvolit tak, že existují $a, b \in K[t]$, které splňují $x = a(t), y = b(t), \deg(a) = 2$ a $\deg(b) = 3$.

Důkaz. Ať $\tilde{K} = \{x \in F; x \text{ je albebraické nad } K\}$. Pak $x, y \in F$ jsou transcendentní nad $\tilde{K}$, takže $F = \tilde{K}(x, y)$ a $w(x, y) = 0$. Podle tvrzení 7.8 je $[F : \tilde{K}(x)] = 2$ a $[F : \tilde{K}(y)] = 3$. Polde lemmatu 7.10 je tedy $\tilde{K} = K$. Vyjádříme $w(x, y)$ jako $g(x, y) - f(x)$ a položme $g = g(x, y) \in F$ a $f = f(x) \in F$. Ať $Q \in P$. Je-li $v_Q(x) < 0$ a $v_Q(y) \geq 0$, je $v_Q(g) \geq v_Q(x) > 3v_Q(x) = v_Q(f)$. Je-li $v_Q(x) \geq 0$ a $v_Q(y) < 0$, je $v_Q(f) \geq 0 > -2v_P(y) = v_P(g)$. V obou případech dostáváme spor s $f = g$. Dokázali jsme bod **(ii)**. Existuje tedy $P \in \mathbb{P}$, že $v_P(x) < 0$ a $v_P(y) < 0$ (viz například lemma 2.6). Pokud $v_P(x) \leq v_P(y)$, tak $v_P(f) = 3v_P(x) < v_P(x) + v_P(y) \leq v_O(g)$. Musí tedy být $v_P(f) = 3v_P(x) = 2v_P(y) = v_P(g)$. Z důsledku 4.8 máme $2 = [F : K(x)] = \deg((x)_-)$. Ať $(x)_- = \sum a_Q Q$. Je-li $a_P \neq 0$, je $a_P = -v_P(x) < 0$, takže $3v_P(x) = 2v_P(y)$ a vidíme, že a_P je sudé. To ale znamená, že existuje jediné P, pro které je $a_P \neq 0$ (je totiž $2 = \sum a_Q \deg(Q)$). Tudíž $(x)_- = 2P, \deg(P) = 1$ a obdobně se dokáže $(y)_- = 3P$. Tím je završen důkaz bodu **(iii)**. Každé $k \geq 2$ lze, jak snadno nahlédneme, vyjádřit jako $2i + 3j$, kde $i \geq 0$ a $j \geq 0$. V takovém případě $(x^i y^j)_- = kP$, jak plyne z bodů **(ii)** a **(iii)**. Tudíž $\mathcal{L}(kP) \setminus \mathcal{L}((k-1)P) \neq \emptyset$ pro každé $k \geq 2$, odkud

$\ell(kP) \geq k$. Podle tvrzení 6.15 je $g - 1 = \deg(kP) - \ell(kP) \leq 0$ pro každé k dostatečně velké. Tedy $g \leq 1$. Je-li $g = 0$, je $-1 = \deg(P) - \ell(P) = 1 - \ell(P)$ (opět podle tvrzení 6.15), takže $\ell(P) = 2$. Pro libovolné $t \in \mathcal{L}(P) \setminus K$ je $\{1, t, t^2\}$ bází $\mathcal{L}(2P)$ a $\{1, t, t^2, t^3\}$ bází $\mathcal{L}(3P)$. (máme totiž $\ell(kP) = k+1$, dle tvrzení 6.15). Zbytek plyne z $x \in \mathcal{L}(2P) \setminus \mathcal{L}(P)$ a $y \in \mathcal{L}(3P) \setminus \mathcal{L}(L)(2P)$. $\square$

O rozšíření F/K, které spňuje přepoklady tvrzení 7.11, řekneme, že je *určeno* Weierstraßovou rovnicí $w(x, y) = 0$. Podle lemmatu 7.10 je $F \cong K(w)$. Místo P_∞ označme jako $P_\infty(w)$. Ukážeme ještě, že za w lze zvolit libovolný polynom, který určuje Weierstraßovu rovnici.

Tvrzení 7.12. *Ať $w \in K[x_1, x_2]$ poskytuje Weierstraßovu rovnici $w(x, y) = 0$. Pak je w ireducibilní a pro $F = K(w)$ platí, že $x = x_1 + (w), y = x_2 + (w)$ jsou transcendentní nad K a splňují $w(x, y) = 0$.*

Důkaz. Žádný nenulový polynom $a(x_1)$ nebo $a(x_2)$ není násobkem $w(x_1, x_2)$, takže $x_1 + (w)$ i $x_2 + (w)$ jsou v $K(w)$ transcendentní nad K, je-li w ireducibilní. Předpokládejme opak. Potom $w = uv$, kde $3 = \deg_x(u) + \deg_x(v)$ a $2 = \deg_y(u) + \deg_y(v)$. Ať je nejprve $\deg_y(u) = 2$. To znamená, že u obsahuje y^2 a (x), kde $a \neq 0$ je vedoucí koeficient. Vedoucí koeficient y^2 ve w je tudíž $a(x)v(x)$, odkud $\deg_x(a) = \deg_x(v) = 0$ a $v \in K$. Můžeme proto předpokládat, že $\deg_y(u) = \deg_y(v) = 1$ a $\deg_x(u) > \deg_x(v)$. Úvahou o vedoucích koeficientech dostáváme, že $u = \alpha y + a(x)$ a $v = \alpha^{-1} y + b(x)$, kde $\alpha \in K^*$. Z $\deg(a) + \deg(b)$ plyne $\deg(a) \geq 2$. Máme $uv = y^2 + yc(x) + a(x)b(x)$, kde $c(x) = \alpha^{-1}a(x) + \alpha b(x)$ je stupně alespoň 2. A to je spor $\square$

Každá Weierstraßova rovnice určuje funkční těleso, ale ne vždy je takové těleso eliptické. Rovnice, které dávají rod 0, nazýváme *singulární*. Později popíšeme přesně, které to jsou. Jako závdavek už nyní vyřešíme jeden důležitý speciální případ.

Tvrzení 7.13. *Ať* $\mathrm{Char}(K) \neq 2$ *a ať je F/K určeno Weierstraßovou rovnicí $y^2 = f(x)$, kde $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Pak je F/K rodu 0 právě když má f vícenásobné kořeny.*

Důkaz. Mějme $y = b(t)$ a $x = a(t)$, kde a, b, t jsou dány tvrzením 7.11. Je tedy $y^2 = b^2(t) = f(a(t))$. Polynom $b^2(t) \in K[t]$ je stupně 6 a má nejvýše 3 kořeny v $\overline{K}$. Polynom $f(a(t))$ lze zapsat jako $(a(t)-\alpha_1)(a(t)-\alpha_2)(a(t)-\alpha_3)$, kde $\alpha_1, \alpha_2, \alpha_3 \in \overline{K}$ jsou kořeny polynomu $f(x) \in K[x]$. Každý z polynomů $a(t) - \alpha_i$ je kvadratický polynom. Existuje jediná hodnota β, pro kterou má $a(t) - \beta$ dvounásobný kořen. Je-li $\alpha_i \neq \alpha_j$, tak $a(t) - \alpha_i$ nemá s $a(t) - \alpha_j$ společný kořen. Jsou-li $\alpha_1, \alpha_2, \alpha_3$ vesměs kladné, má $f(a(t))$ proto alespoň 5 různých kořenů, což je spor. Ať tedy $y^2 = (x-\alpha)^2(x-\beta)$. Máme $\alpha, \beta \in K$, neboť α je vícenásobný. Položme $s = x-\alpha$. Pak $y^2 = s^2(s-\gamma)$, kde $\gamma = \beta-\alpha$. Ať $t = y/s$. Pka $s - \gamma = t^2$, takže $s = t^2 + \gamma$ a $x = t^2 + \beta$. Tedy $x \in K[t]$ a $y = ts = t(t^2+\gamma) \in K[t]$. Odsud $F = K(x,y) = K(t)$, takže F/K je rodu 0. $\square$

Jsou-li $A \subseteq B \subseteq C$ abelovské grupy, tak B/A je podgrupou C/A. Představme si, pro libovolné algebraické funkční těleso F/K, že tyto grupy jsou rody $\mathrm{Princ}(F/K)$, $\deg^{-1}(0)$ a $\mathrm{Div}(F/K)$. Každý kladný divisor (x) splňuje $\deg((x)) = 0$, takže vskutku $\mathrm{Princ}(F/K) \leq \deg^{-1}(0)$. Přitom deg zde chápeme jako homomorfismus $\mathrm{Div}(F/K) \to \mathbb{Z}$, takže $\deg^{-1}(0)$ je jeho jádro. Grupě $\deg^{-1}(0)/\mathrm{Princ}(F/K)$ budeme říkad *Picardova* a značit $\mathrm{Pic}(F/K)$. Je tedy $\mathrm{Pic}(F/K) \subseteq Cl(F/K)$. Body Picardovy grupy eliptického funkčního tělesa F/K odpovídají místům stupně 1. To dokážeme níže přímým způsobem, bez využití Weierstraßovy rovnice $w(x,y)$. Časem nahlédneme, že body stupně 1 odpovídají bodům (projektivní) variety určené rovnicí $w(x,y)$. Vyvstane tak před námi úkol operaci Picardovy grupy interpretovat jako operaci na bodech dané projektivní variety. Úvaha o Picardově grupě vyžaduje formulaci několika jednoduchých důsledků. Přípomeňme, že $A\ B$ značí $A - B \in \mathrm{Princ}(F/K)$.

Lemma 7.14. *Ať F/K je eliptické funkční těleso a ať $A \in \mathrm{Div}(F/K)$.*

(i) *Je-li* $\deg(A) \geq 1$*, je* $\ell(A) = \deg(A)$

(ii) *Je-li* $\deg(A) = 1$*, existuje* $P \in \mathbb{P}_{F/K}$*, že* $A\ P$*. Přitom* P *je určeno jednoznačně a splňuje* $\deg(P) = 1$*.*

(iii) *Je-li* $\deg(A) > 0$ *je-li* $P \in \mathbb{P}_{F/K}, \deg(P) = 1$*, pak existuje* $Q \in \mathbb{P}_{F/K}$*, že* $A\ Q - P$*. Přitom* $\deg(Q) = 1$ *a* Q *je určeno jednoznačně.*

Důkaz. Bod **(i)** je přímým důsledkem tvrzení 6.15, $\deg(A) - \ell(A) = 1$. Dle bodu **(P2)** tvrzení 4.14 existuje $A'\ A$, že $A' \geq 0$. Dle **(P1)** je $\deg(A') = \deg(A) = 1$, takže musí být $A' = P$ pro nějaké $P \in \mathbb{P}_{F/K}, \deg(P) = 1$. Pokud by P_1 a P_2 byly dvě možné volby, byl by divisor $P_1 - P_2$ hlavní, tedy $P_1 = (t)_+$ pro nějaké $t \in F$. Pak by ale bylo $[F : K(t)] = 1$, čili $F = K(t)$ a $g = 0$, dle důsledku 4.8. Místo P je určeno jednoznačně. Je-li $\deg(A) = 0$ a $\deg(P) = 1$, je $\deg(P + A) = 1$, takže podle předpokládané části existuje jediné $Q \in \mathbb{P}_{F/K}$, že $P + A\ Q$, tedy $A\ Q - P$. $\square$

Bez nutnosti výslovného důkazu můžeme nyní bod **(iii)** předchozího lemmatu parafrázovat jako

Důsledek 7.15. *Ať F/K je eliptické funkční těleso a ať $\mathbb{P}^{(1)} = \{Q \in \mathbb{P}_{F/K}; \deg(Q) = 1\}$. Pak pro každé $P \in \mathbb{P}^{(1)}$ je zobrazení $Q \mapsto Q - P$ bijekcí množin $\mathbb{P}^{(1)}$ a* $\mathrm{Pic}(F/K)$.

Jsou-li dány dvě množiny a jejich bijekce přičemž na jedné je dána struktura grupy, lze pomocí bijekce přenést tuto strukturu na druhou množinu. V našem případě to znamená, že pro každé $P\ in \mathbb{P}^{(1)}$ poskytuje operace

$$Q_1 \boxplus Q_2 = Q_3 \iff [Q_1 - P] \ + [Q_2 - P] \ = [Q_3 - P]$$

Strukturu grupy na $\mathbb{P}^{(1)}$. Jinak řečeno $Q_1 \boxplus Q_2$ je to jediné $Q \in \mathbb{P}^{(1)}$, že $Q\ Q_1 + Q_2 - P$.

Obsah