KŘIVKY A FUNKČNÍ TĚLESA

Obsah

Motivace

Cíl: vybudovat (algebraický) aparát pro popis křivek nad konečnými tělesy.
Prostředek: zobecnění geometrické teorie (s geometricky popsatelnými analogiemi)
Klíčový nástroj: popis struktury funkčních těles (místa/places $\leftrightarrow$ body křivky)
Klíčová potíž: situace $\mathbb{R} \subseteq \mathbb{C}$ snazší než $\mathbb{F}_q \subseteq \overline{\mathbb{F}_q}$ ($[\mathbb{C} : \mathbb{R}] = 2$ vs. $[\overline{\mathbb{F}_q} : \mathbb{F}_q] = \infty$)

Struktura přednášky:

(1) *Okruhy* - algebry nad tělesem, valuační obory,
(2) *Polynomy* - WEP, souřadnicové okruhy,
(3) *Ideály* - místa ve funkčních tělesech,
(4) *Prostory* - divisory, Weilovy diferenciály,
(5) *Grupy* - asociativní zákon,
(6) *Projektivita* - projektivní křivky.

Date: 3. června 2021.

1. Algebry nad tělesem

Termínem **okruh** budeme vždy mínit komutativní okruh s operacemi $+$, $-$, $\cdot$, 0 a 1 a obvykle je budeme psát R místo $(R, +, -, \cdot, 0, 1)$.

Podobně **tělesem** míníme vždy komutativní těleso.

T&N. Nechť K je těleso a A okruh obsahující K jako podokruh. Pak A se nazývá *K-algebra* (nebo algebra nad K). Jsou-li A a B dvě K-algebry, pak $f : A \to B$ je *homorfismus K-algeber*, jde-li o okruhový homomorfismus a $f(k) = k$ pro každé $k \in K$.

K je vždy těleso a $R \leq K$ znamená, že R je podokruh K.

Pozorování. Jsou-li A a B dvě K-algebry a I je ideál A, pak

(1) A/I je K-algebra,
(2) A je vektorový prostor nad K a I jeho podprostor,
(3) je-li $f : A \to B$ homomorfismus K-algeber, pak je f lineární nad K.

T&N. Nechť R je okruh, $M \subset R$ a $a \in R$. Pak (M) značí ideál okruhu R generovaný množinou M a $(a) := (\{a\})$.

$R[x_1, \ldots, x_n]$ je okruh polynomů a $K(x_1, \ldots, x_n)$ podílové těleso okruhu $K[x_1, \ldots, x_n]$.

Příklad 1.1. (1) $K[x]$, $K[x, y]$, $K(x)[y]$ či $K(x, y)$ jsou K-algebry.
(2) $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}[\sqrt{2}]$ jsou $\mathbb{Q}$-algebry.
(3) $\mathbb{Q}[x] \cong \mathbb{Q}[\pi] \ncong \mathbb{Q}(\pi) \cong \mathbb{Q}(x)$ jsou $\mathbb{Q}$-algebry.

T&N. Jsou-li A a B dva vektorové prostory nad K, pak $\mathrm{Hom}_K(A, B)$ je abelovská grupa všech lineárních zobrazení $A \to B$ a je-li V vektorový prostor, pak $U \leq V$ znamená, že U je podprostor V.

Poznámka 1.2. Jsou-li A a B dva vektorové prostory nad K, $I \leq A$, $J \leq B$ a $\varphi \in \mathrm{Hom}_K(A, B)$ splňuje $\varphi(I) \subseteq J$, pak $\tilde{\varphi}(a + I) = \varphi(a) + J$ je dobře definované lineární zobrazení $\tilde{\varphi} \in \mathrm{Hom}(A/I, B/J)$ a

(1) $\tilde{\varphi}$ je prosté, právě když $\varphi^{-1}(J) = I$,
(2) $\tilde{\varphi}$ je na a $J \subseteq \varphi(A)$, právě když φ je na.

Poznámka 1.3. Nechť V je vektorový prostor nad K, dále $A, B, C \leq V$ a $A \leq C$, pak

(1) $A + (B \cap C) = (A + B) \cap C$,
(2) jestliže $\dim(C/A) < \infty$, pak $\dim((C + B)/(A + B)) = \dim(C/A) - \dim((C \cap B)/(A \cap B))$.

T&N. Nechť V je vektorový prostor nad K a $A \leq V$, pak značme

$$V^* = \mathrm{Hom}_K(V, K) \quad \text{a} \quad A^o = \{f \in V^* \mid f(A) = 0\}.$$

Poznámka 1.4. Nechť V je vektorový prostor nad K a $A, B \leq V$, pak platí, že V^* je vektorový prostor nad K a $A^o, B^o \leq V^*$ a dále

(1) $A^o \cong (V/A)^*$,
(2) jestliže $\dim(V/A) < \infty$, pak $A^o \cong V/A$,
(3) jestliže $A \leq B$, pak $B^o \leq A^o$,
(4) $(A \cap B)^o = A^o + B^o$, $(A + B)^o = A^o \cap B^o$,

Tvrzení 1.5. Nechť $K \subseteq L$ je rozšíření těles a V je vektorový prostor nad tělesem L. Pokud pro $\varphi \in V^* = \mathrm{Hom}_K(V, K)$ a $l \in L$ definujeme $l\varphi(v) = \varphi(lv)$, pak

(1) V je vektorový prostor nad K,
(2) V^* je vektorový prostor nad L,
(3) $A_K \leq V_K$ a $\alpha^{-1}A^o = (\alpha A)^o$ pro každé $\alpha \in L^*$.

T&N. Je-li R obor a K jeho podílové těleso, V vektorový prostor nad K. $A \subset V$ je *lineárně nezávislá* (LN) nad R, jestliže $\forall\{a_1 \dots, a_k\} \subseteq A$ a $\forall r_1, \dots, r_k \in R$ platí $\sum_i r_i a_i = 0 \Rightarrow r_i = 0\forall$. Množina je je *lineárně závislá* (LZ) nad R, pokud není LN.

Poznámka 1.6. Nechť R je obor s podílovým tělesem K, V je vektorový prostor nad K a $M \subset V$. Pak je M LN nad $R \Leftrightarrow$ je M LN nad K.

2. Algebraická funkční tělesa

$K \subseteq L$ bude celou přednášku značit rozšíření tělesa K tělesem L.

Poznámka 2.1. Nechť V je vektorový prostor nad $K(x)$ a $v_1, \dots, v_n \in V$. Pak je $v_1, \dots, v_n$ je LZ nad $K(x) \Leftrightarrow \exists a_1, \dots a_n \in K[x]$ takové, že $a_j(0) \neq 0$ aspoň pro jedno j a $\sum_i a_i v_i = 0$.

T&N. Nechť je R okruh a $A, B \subset R$, značíme

$AB := \langle ab \mid a \in A, b \in B\rangle$ je podgrupa aditivní grupy $(R, +, -, 0)$ generovaná množinou $\{ab \mid a \in A, b \in B\}$.

$A[B] := \{f(b_1, \dots, b_k) \mid k \in \mathbb{N}, f \in A[x_1 \dots, x_k], b_1, \dots, b_k \in B\}$

$A[b_1, \dots, b_k] := A[\{b_1, \dots, b_k\}]$ pro $b_1, \dots, b_k \in R$.

Pozorování. Nechť je R okruh a $A, B, C \subset R$, pak

(1) $A(BC) = (AB)C$,
(2) jsou-li A, B podokruhy (ideály) R, pak $A[B] = AB$ je podokruh (ideál) R,
(3) $A[b_1, \dots, b_k] = \{f(b_1, \dots, b_k) \mid f \in A[x_1 \dots, x_k]\}\ \forall b_1, \dots, b_k \in R$.

Připomeňme, že pro rozšíření $K \subseteq L \subseteq U$ značíme stupeň rozšíření $[L : K] = \dim_L K$ a platí $[U : K] = [U : L][L : K]$.

Poznámka 2.2. Buď $K \subseteq L$ algebraické rozšíření těles.

(1) je-li B báze L jako vektorového prostoru nad K, pak B je i báze $L(x)$ jako vektorového prostoru nad $K(x)$
(2) $[L(x) : K(x)] = [L : K]$.

Poznámka 2.3. Nechť V je vektorový prostor nad tělesem $K(x)$. Pak $\{v_1, \dots, v_n\} \subset V$ je lineárně nezávislá množina nad $K(x) \Leftrightarrow \{v_i x^j \mid i = 1, \dots, n, j \geq 0\}$ je lineárně nezávislá množina nad K

Definice. Nechť $K \subseteq L$. Řekneme, že L je algebraické funkční těleso nad K (AFF), jestliže existuje prvek $\alpha \in L$ transcendentní nad K, pro který platí $[L : K(\alpha)] < \infty$.

Příklad 2.4. (1) $\mathbb{R}(x)$ je AFF nad $\mathbb{R}$.

(2) $\mathbb{Q}(\sqrt[3]{5})(x) = \mathbb{Q}(\sqrt[3]{5}, x) \cong \mathbb{Q}(\sqrt[3]{5}, \pi) \subseteq \mathbb{R}$, pak $\mathbb{Q}(\sqrt[3]{5}, x)$ je AFF nad $\mathbb{Q}$.

(3) Nechť $g \in K[x,y]$ je ireducibilní polynom a $R := K[x,y]/(g)$, L je podílové těleso R a položme $\xi := x+(g)$ a $\upsilon := y+(g)$. Pak $R = K[\xi,\upsilon]$ a $L = K(\xi,\upsilon)$. Kdyby ξ, υ byly oba algebraické nad K, pak by $[K(\xi,\upsilon) : K] < \infty$, a proto $R = K[\xi,\upsilon] = K(\xi,\upsilon) = L$, tudíž $(g) \cap K[x] \neq 0$ a $(g) \cap K[y] \neq 0$. Z toho by plynulo, že $g \in K^*$, tedy spor. Tedy ξ nebo υ je transcendentní nad K, buď BÚNO $\alpha := \xi$ transcendentní, pak $g(\alpha,\upsilon) = 0$, tedy $[L : K(\alpha)] < \infty$, proto je L AFF nad K.

Poznámka 2.5. Nechť $K \subseteq U \subseteq L$ jsou rozšíření těles, L je AFF nad K a U je algebraické nad K, pak $[U : K] < \infty$.

T&N. Nechť $K \subseteq L$ a L je AFF nad K, pak

$$\tilde{K} := \{\alpha \in L \mid [K(\alpha) : K] < \infty\}$$

se nazývá *těleso konstant*.

Důsledek 2.6. $\tilde{K}$ je je pro AFF L nad K podtěleso L a $[\tilde{K} : K] < \infty$.

Tvrzení 2.7. Nechť $K \subseteq L$, α je transcendentní nad K a $[L : K(\alpha)] < \infty$. Potom jsou pro $u \in L$ následující podmínky ekvivalentní:

(1) $[L : K(u)] < \infty$,
(2) $\exists g \in K[x,y]$, pro které $g(x,u) \neq 0$ a $g(\alpha,u) = 0$,
(3) u je transcendentní nad K.

Poznámka 2.8. Pokud $[L : K] < \infty$ a I je ideál $K[x_1,\ldots,x_n]$, pak $(IL[x_1,\ldots,x_n]) \cap K[x_1,\ldots,x_n] = I$.

3. Valuační okruhy

Celou přednášku je K těleso a $R \leq K$ znamená, že R je podokruh K.

T&N. (R,M) označuje *l*okální okruh R s (jediným) maximálním ideálem M.

Pozorování. Následující podmínky jsou pro ideál M okruhu R ekvivalentní :

(1) (R,M) je lokální okruh,
(2) každý vlastní ideál R je obsažen v M,
(3) $M = R \setminus R^*$,
(4) $R^* = R \setminus M$.

Poznámka 3.1. Je-li (R,M) lokální okruh a A konečně generovaný ideál splňující $AM = A$, pak $A = 0$.

Tvrzení 3.2. Nechť (R,M) je lokální obor, $M = (t)$ pro $t \neq 0$ a položme $A := \bigcap_i M^i = \bigcap_i (t^i)$. Pak platí:

(1) pro každé $s \in R \setminus A$ existuje jediné $i \geq 0$ a jediné $u \in R^*$ splňující $s = t^i u$,
(2) jestliže je A konečně generovaný, potom $A = 0$.

Připomeňme, že okruh je noetherovský, právě když všechny ideály konečně generované.

Důsledek 3.3. Jestliže je (R,M) noetherovský lokální obor s podílovým tělesem K a $M = (t)$ pro nějaké $t \in M$, pak

(1) pro každé $s \in R \setminus \{0\}$ existuje jediné $i \geq 0$ a jediné $u \in R^*$, pro něž $s = t^i u$,

(2) pro každé $s \in K \setminus \{0\}$ existuje jediné $i \in \mathbb{Z}$ a jediné $u \in R^*$, pro něž $s = t^i u$,
(3) R je obor hlavních ideálů.

Poznámka 3.4. Nechť $R \leq K$, $\alpha \in K \setminus R$ tak, že $\alpha^{-1} \notin R$. Jestliže je J vlastní ideál R, pak buď $J[\alpha] \subsetneq R[\alpha]$ nebo $J[\alpha^{-1}] \subsetneq R[\alpha^{-1}]$.

T&N. Nechť $R \leq K$. R se nazývá valuační okruh (VR) tělesa K, jestliže pro každé $\alpha \in K \setminus \{0\}$ buď $\alpha \in R$ nebo $\alpha^{-1} \in R$. R je *valuační okruh*, jestliže je valuační ve svém podílovém tělese.

R je *uniseriální*, jestliže pro každou dvojici ideálů I, J buď $I \subseteq J$ nebo $J \subseteq I$.

Pozorování. Nechť K je podílové těleso oboru R a označme $i : K \to K$ dané vztahem $i(\alpha) = \alpha^{-1}$.

(1) R je VR $\Rightarrow$ R je uniserální $\Rightarrow$ R je lokální,
(2) $i(R^*) = R^*$
(3) jestliže R je VR, pak $i(M) = i(R \setminus R^*) = K \setminus R$.

Příklad 3.5. (1) $\mathbb{Z}_{(p)} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}, p \text{ nedělí } b\}$ je pro každé prvočíslo p valuační okruh (podílového tělesa $\mathbb{Q}$).

(2) $R_{x,y} = \{\frac{r}{s} \in \mathbb{R}(x,y) \mid r, s \in \mathbb{R}[x,y], s(0,0) \neq 0\} \subseteq \mathbb{R}(x,y)$ je noetherovský lokální obor s maximálním ideálem (x,y), který není valuační: například $\frac{x+y}{xy}$ ani $\frac{xy}{x+y}$ neleží v $R_{x,y}$.

Věta 3.6. Nechť $R \leq K$ a I je ideál splňující $0 \neq I \neq R$.

(1) Existuje valuační okruh S tělesa K s maximálním ideálem M, pro který platí, že $R \subseteq S \subsetneq K$ a $I \subseteq M$.
(2) Je-li R maximální podokruh K, pak jde o valuační okruh.

4. Diskrétní valuační okruhy

V následujícím $R \leq K$ znamená, že K je podílové těleso oboru R.

Pozorování. Nechť pro $j = 1, 2$ jsou R_j valuační okruhy tělesa K a $0 \neq M_j = R_j \setminus R_j^*$ a nechť $i(a) = a^{-1}$ $\forall a \in K^*$ a $i(0) = 0$. Pak

(1) $M_1 \subseteq M_2 \Leftrightarrow K \setminus R_1 = i(M_1) \subseteq i(M_2) = K \setminus R_2 \Leftrightarrow R_2 \subseteq R_1$,
(2) $M_1 = M_2 \Leftrightarrow R_1 = R_2$.

Pozorování. Je-li R podokruh okruhu S a P prvoideál S, pak $P \cap R$ je prvoideál okruhu R.

Poznámka 4.1. Nechť R_i je noetherovský valuační okruh tělesa K s maximálním ideálem $0 \neq M_i = R_i \setminus R_i^*$ pro $= 1, 2$. Pak pro $i = 1, 2$

(1) R_i je obor hlavních ideálů, tedy M_i je hlavní,
(2) R_i je maximální vlastní podokruh K,
(3) $M_1 \subseteq M_2 \Leftrightarrow M_1 = M_2 \Leftrightarrow R_1 = R_2 \Leftrightarrow R_1 \subseteq R_2$.

Připomeňme důsledek Gaussova lemmatu: je-li K podílové těleso Gaussova oboru R, Pak $p \in R[x]$ je ireducibilní, právě když buď $p = ct(p) \in R$ je ireducibilní v R nebo je p primitivní v $R[x]$ a ireducibilní v $K[x]$.

Pozorování. $g \in K[x,y] = (K[x])[y]$ je ireducibilní, právě když

- buď $g \in K[x]$ je ireducibilní,
- nebo neexistuje žádný dělitel $b \in K[x] \setminus K$ polynomu g a g je ireducibilní v $K(x)[y]$.

Poznámka 4.2. Nechť $a, b \in K[x,y] \setminus K$ jsou nesoudělné, pak

(1) $(a,b) \cap K[x] \neq 0$,
(2) jestliže P je prvoideál obsahující (a,b), pak P je maximální ideál $K[x,y]$.

Důsledek 4.3. Prvoideály $K[x,y]$ jsou právě:
(a) $\{0\}$, (b) (p) pro $p \in K[x,y]$ ireducibilní, (c) maximální ideály.

Definice. zobrazení $\nu : K \to \mathbb{Z} \cup \{\infty\}$ se nazývá *diskrétní valuace* K, jestliže pro všechna $a, b \in K$ platí:

(D1) $\nu(ab) = \nu(a) + \nu(b)$,
(D2) $\nu(a+b) \geq \min(\nu(a), \nu(b))$,
(D3) $\nu(a) = \infty$, právě když $a = 0$.

ν je *triviální diskrétní valuace* (DV), pokud $\nu(K^*) = 0$. Nadále budeme předpokládat, že jsou všechny valuace netriviální.

T&N. Nechť R je noetherovský obor a $p \in R$ prvočinitel. Pro každé $a, b \in R \setminus \{0\}$ definujme

$$\nu_p(a) = \max\{i \mid p^i / a\}, \quad \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b), \quad \nu_p(0) = \infty.$$

Příklad 4.4. Nechť $R \leq K$, R je noetherovský, K podílové těleso R a p prvočinitel R. Pak ν_p je korektně definovaná diskrétní valuace tělesa K.

Pozorování. Nechť ν je diskrétní valuace tělesa K a definujme $S = \{x \in K \mid \nu(x) \geq 0\}$, $M = \{x \in K \mid \nu(x) > 0\}$ a zvolme $x \in K^*$. Pak

(1) $\nu|_{K^*}$ je podle (D1) grupový homomorfismus grupy $(K^*, \cdot, ^{-1}, 1)$ do $(\mathbb{Z}, +, -, 0)$, proto $\nu(1) = 0$ a $\nu(x^{-1}) = -\nu(x)$,
(2) S je podokruh K,M jeho ideál a S je VR tělesa K,
(3) $\nu(x) = 0 \Leftrightarrow \nu(x^{-1}) = -\nu(x) = 0 \Leftrightarrow x \in S^*$, $M = S \setminus S^*$ je maximální ideál S,
(4) je-li $I \neq 0$ ideál S a $a \in I \setminus 0$ má minimální hodnotu $\nu(a)$, pak $(a) = I$, neboť pro $b \in I$ splňující $\nu(b) \geq \nu(a)$ je $\nu(ba^{-1}) \geq 0$, tedy $ba^{-1} \in S$ a $b = aba^{-1} \in (a)$,
(5) S je obor hlavních ideálů.

Definice. Jestliže $R \leq K$, řekneme, že R je *d*iskrétní valuační okruh (DVR), jestliže existuje diskrétní valuace ν tak, že $R = \{a \in K \mid \nu(a) \geq 0\}$.

Tvrzení 4.5. Pro obor $R \leq K$ je následující ekvivalentní:

(1) R je diskrétní valuační okruh,
(2) R je noetherovský valuační okruh,
(3) R je lokální obor hlavních ideálů,
(4) R je a noetherovský lokální okruh, jehož maximální ideál je hlavní.

T&N. jestliže R je DVR s maximálním ideálem (t) pak t se nazývá *u*niformizační prvek a ν_t se nazývá *normalizovaná diskrétní valuace* (NDV).

Příklad 4.6. Pro R noetherovský a p prvočinitel, je lokalizace $R_{(p)}$ DVR s diskrétní valuací ν_p z 4.4.

Konkrétně okruh $\mathbb{Z}_{(p)} \leq \mathbb{Q}$ z 3.5(1) je pro každé prvočíslo p DVR.

Poznámka 4.7. Nechť $R \leq K$ a R je DVR s uniformizačním prvkem t, pak pro každou diskrétní valuaci μ s $R = \{a \in K \mid \mu(a) \geq 0\}$ existuje jediné $k \in \mathbb{N}$, pro něž $\mu = k\nu_t$.

Poznámka 4.8. Je-li ν diskrétní valuace tělesa K a $a, b \in K$ $\nu(a) \neq \nu(b)$, pak $\nu(a+b) = \min(\nu(a), \nu(b))$.

Pozorování. Nechť ν je diskrétní valuace. Pak ν je NDV $\Leftrightarrow \exists t : \nu(t) = 1$.

T&N. Nechť L je AFF nad K. Řekneme, že R je valuační okruh algebraického funkčního tělesa L nad K, jestliže R je valuační okruh a $K \subseteq R$. ν je (normalizovaná) diskrétní valuace algebraického funkčního tělesa L nad K, jestliže ν je (normalizovaná) diskrétní valuace a $\nu(K^*) = 0$.

Definujme $\nu_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$ pro $a, b \in K[x] \setminus \{0\}$ na AFF $K(x)$ a $\nu_\infty(0) = \infty$.

Pozorování. x^{-1} je prvočinitel $K[x^{-1}]$ ($\cong K[x]$), dále $K(x) = K(x^{-1})$ a $\nu_\infty = \nu_{x^{-1}}$ je NDV na AFF $K(x)$ nad K.

Tvrzení 4.9. Normalizovaná diskrétní valuace AFF $K(x)$ nad tělesem K je buď ν_∞ nebo ν_p pro nějaký ireducibilní polynom $p \in K[x]$.

Definice. Nechť L je AFF nad K. Definujme

$$\mathbb{P}_{L/K} = \{M \subset L \mid \exists \text{ valuační obor } R : K \subseteq R \subsetneq L, M = R \setminus R^*\}.$$

Prvek $P \in \mathbb{P}_{L/K}$ se nazývá *místo* algebraického funkčního tělesa L nad K. Značme $\mathcal{O}_P$ valuační obor AFF L s maximálním ideálem P a číslo

$$\deg P = \dim_K(\mathcal{O}_P/P) = [\mathcal{O}_P/P : \ (K+P)/P]$$

se nazývá *stupeň* P.

Věta 4.10. Nechť L je AFF nad K, $P \in \mathbb{P}_{L/K}$ a $\tilde{K}$ těleso konstant AFF L. pak

(1) $\tilde{K} \subseteq \mathcal{O}_P$,
(2) $\mathcal{O}_P$ je jednoznačně určený diskrétní valuační okruh,
(3) $\deg P < \omega$.

Nechť je nadále L AFF nad K a $\tilde{K}$ jeho těleso konstant.

T&N. Pro $P \in \mathbb{P}_{L/K}$ označme $\nu_P = \nu_t$ NDV určenou oborem $\mathcal{O}_P$, kde $P = (t)$.

Nechť $a = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in K[x_1, \ldots, x_n]$. pak mult $a = \min(\sum_{j=1}^n i_j \mid a_{i_1 \ldots i_n} \neq 0)$ se nazývá *multiplicita* polynomu a.

Pozorování. Je-li $a \in K[x]$, pak mult $a = \max\{i \geq 0 \mid x^i \text{ dělí } a\}$, tedy jde o násobnost kořene 0.

Poznámka 4.11. Jestliže $z \in L \setminus \tilde{K}$, pak existují $P, Q \in \mathbb{P}_{L/K}$, pro která $\nu_P(z) > 0$ a $\nu_Q(z) < 0$.

Poznámka 4.12. Nechť $z \in L \setminus \tilde{K}$, $a \in K[x]$, $P \in \mathbb{P}_{L/K}$, pak

(1) $\nu_P(z) \geq 0 \Rightarrow \nu_P(a(z)) \geq 0$,
(2) $\nu_P(z) > 0 \Rightarrow \nu_P(a(z)) = \mathrm{mult}(a) \cdot \nu_P(z)$,
(3) $\nu_P(z) < 0 \Rightarrow \nu_P(a(z)) = \deg(a) \cdot \nu_P(z)$.

5. Weierstrassovy rovnice

K je nadále těleso a $K \leq L$ značí rozšíření těles a $n \in \mathbb{N}$.

T&N. Nechť $K \leq L$ a A je K-algebra. Označme
$\mathrm{End}_K(A) = \{\varphi : A \to A \mid \varphi \text{ je } K\text{-homomorfismus}\}$
$\mathrm{Aut}_K(A) = \{\varphi \in \mathrm{End}_K(A) \mid \varphi \text{ je bijekce}\}$
Nechť $n \in \mathbb{N}$, $A \in K^{n\times n}$, $b \in K^n$, definujme zobrazení $\vartheta_A, \tau_b : K^n \to K^n$ předpisy $\vartheta_A(v) = Av$, $\tau_b(v) = v + b$. Označme $\mathrm{Aff_n(K)} = \{\tau_\mathrm{b}\vartheta_\mathrm{A} \mid \mathrm{A} \in \mathrm{GL_n(K)}, \mathrm{b} \in \mathrm{K^n}\}$ a prvky $\mathrm{Aff_n(K)}$ se nazývají *afinní zobrazení.*

Pozorování. Nechť $K \leq L$, $A, B \in K^{n\times n}$, $b, c \in K^n$. Pak
(1) $\tau_b\tau_c = \tau_{b+c}$, $\vartheta_A\vartheta_B = \vartheta_{AB}$, $\vartheta_A\tau_b = \tau_{\vartheta_A(b)}\vartheta_A$,
(2) $\tau_b\vartheta_A$ je bijekce $\Leftrightarrow A \in GL_n(K)$,
(3) $\mathrm{Aff_n(K)}$ je podgrupa grupy permutací $S(K^n)$,
(4) $\mathrm{Aff_n(K)} \leq \mathrm{Aff_n(L)}$, kde ztotožníme $\tau_b\vartheta_A$ na K^n a L^n.

T&N. Nechť $\sigma \in \mathrm{Aff_n(K)}$ a $\mathbb{X} = (x_1, \ldots, x_n)$. Definujem $\sigma^* \in \mathrm{End}_K(K[\mathbb{X}])$ předpisem $\sigma^*(f(x_1, \ldots, x_n)) = f(\sigma((x_1, \ldots, x_n)))$, kde σ uvažujeme jako prvek $\mathrm{Aff}_n(K(\mathbb{X})^n)$. Prvky množiny $\mathrm{Aff}_n^*(K) = \{\sigma^* \mid \sigma \in \mathrm{Aff_n(K)}\}$ nazveme *afinní automorfismy.*

Pozorování. Nechť $\sigma, \rho \in \mathrm{Aff_n(K)}$, $\mathbb{X} = (x_1, \ldots, x_n)$ a $f \in K[\mathbb{X}]$
(1) $\rho^*\sigma^*(f(\mathbb{X})) = \rho^*(f(\sigma(\mathbb{X}))) = f(\sigma\rho(\mathbb{X})) = (\sigma\rho)^*(f(\mathbb{X}))$,
(2) $\mathrm{id}^*_{K^n} = \mathrm{id}_{K[\mathbb{X}]}$, $(\sigma^{-1})^* = (\sigma^*)^{-1}$,
(3) $\mathrm{Aff}_n^*(K)$ je podgrupa grupy $\mathrm{Aut}(K[\mathbb{X}])$.

T&N. Označme třídy čtvercových matic
- $T_n(K) = \{(d_{ij}) \in K^{n\times n} \mid d_{ii} \neq 0 \forall i,\ d_{ij} = 0 \forall i < j\}$,
- $U_n(K) = \{(d_{ij}) \in T_n(K) \mid d_{ii} = 1 \forall i\}$,
- $D_n(K) = \{(d_{ij}) \in T_n(K) \mid d_{ij} = 0 \forall i \neq j\}$.

Pozorování. $T_n(K)$, $U_n(K)$ a $D_n(K)$ jsou podgrupy $GL_n(K)$ a platí rovnosti $T_n(K) = U_n(K)D_n(K) = D_n(K)U_n(K)$.

Definice. Nechť $f, g \in K[x]$ splňují $\deg g \leq 1$, $\deg f = 3$, $lc(f) = 1$. Pak se rovnice tvaru $y^2 + yg(x) = f(x)$ se nazývá *Weierstrassova rovnice* (WE) a polynomu $y^2 + yg(x) - f(x) \in K[x, y]$ budeme říkat *Weierstrassův polynom* (WEP).

Pozorování. Nechť $w = y^2 + yg(x) - f(x)) \in K[x, y]$ je WEP, $A = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix} \in U_2(K)$, $b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in K^2$.
(1) $\tau_b^*(w) = (y + b_2)^2 + (y + b_2)g(x + b_1) - f(x + b_1) = y^2 + y(2b_2 + g(x + b_1)) - (f(x + b_1) - b_2^2 - b_2g(x + b_1))$ je WEP,

(2) $\vartheta_A^*(w) = (y+ux)^2+(y+ux)g(x)-f(x) = y^2+y(2ux+g(x))-(f(x)-u^2x^2-uxg(x))$ je WEP,
(3) $U^* = \{(\tau_c\vartheta_B)^* \mid c \in K^2, B \in U_2(K)\}$ je podgrupa $\mathrm{Aff}_2(\mathrm{K})$ a pro každé $\sigma^* \in U^*$ je $\sigma^*(w)$ je WEP.

Poznámka 5.1. Jestliže je $\mathrm{char}\, K \neq 2$ a w je WEP, pak $\exists A \in U_2(K)$ a $b \in K^2$ pro které $(\tau_b\vartheta_A)^*(w) = y^2 - h(x)$ pro vhodné $h \in K[x]$, $\deg h = 3$ a $lc(h) = 1$, tedy $y^2 - h(x)$ je opět WEP.

T&N. Weierstrassův polynom nazveme *krátký*, jestliže je pro nějaká $a_2, a_3, a_4, a_6 \in K$ tvaru

(SH1) $y^2 - (x^3 + a_4x + a_6)$ pokud $\mathrm{char}\, K \neq 2, 3$,
(SH2) $y^2 - (x^3 + a_4x + a_6)$ nebo $y^2 + xy - (x^3 + a_4x + a_6)$ pokud $\mathrm{char}\, K = 2$,
(SH3) $y^2 - (x^3 + a_4x + a_6)$ nebo $y^2 - (x^3 + a_2x^2 + a_6)$ pokud $\mathrm{char}\, K = 3$.

Poznámka 5.2. Nechť $\lambda \in K^*$, w je WEP a $\sigma \in \mathrm{Aff}_2(\mathrm{K})$. Pak existuje WEP $\tilde{w}$, pro který $\sigma^*(w) = \lambda\tilde{w} \Leftrightarrow \exists\alpha, \delta, \gamma \in K$ a $\exists b \in K^2$, pro něž $\alpha^3 = \delta^2 = \lambda$, $A = \begin{pmatrix} \alpha & 0 \\ \gamma & \delta \end{pmatrix}$ a $\sigma = \tau_b\vartheta_A$.

Uvážíme-li rovnost $c = \delta\alpha^{-1}$ dostaneme

Pozorování. Nechť $\alpha, \delta \in K^*$. Pak $\alpha^3 = \delta^2 \Leftrightarrow \exists c \in K^*$ splňující $\delta = c^3$ a $\alpha = c^2$.

Tvrzení 5.3. Nechť $w \in K[x, y]$ je WEP a $\sigma \in \mathrm{Aff}_2(\mathrm{K})$. Pak jsou následující tvrzení ekvivalentní:

(1) existuje $\lambda \in K^*$ tak, že $\lambda\sigma^*(w)$ je WEP,
(2) existuje WEP $\tilde{w}$ tak, že $(\sigma^*(w)) = (\tilde{w})$,
(3) existuje $c \in K^*$, $d \in K$ a $b \in K^2$ tak, že $A = \begin{pmatrix} c^2 & 0 \\ d & c^3 \end{pmatrix} \in T_2(K)$ a $\sigma = \tau_b\vartheta_A$.

T&N. Řeknem, že dva Weierstrassovy polynomy $w, \tilde{w} \in K[x, y]$ jsou K-*ekvivalentní*, pokud existuje $\sigma \in \mathrm{Aff}_2(\mathrm{K})$ splňující $(\sigma^*(w)) = (\tilde{w})$.

Důsledek 5.4. Pro dva WEP $w, \tilde{w} \in K[x, y]$ jsou následující podmínky ekvivalentní:

(1) w a $\tilde{w}$ jsou K-ekvivalentní,
(2) $\exists\, c \in K^*$, $d \in K$ a $b \in K^2$ tak, že $A = \begin{pmatrix} c^2 & 0 \\ d & c^3 \end{pmatrix} \in T_2(K)$ a $(\tau_b^*\vartheta_A^*(w)) = (\tilde{w})$,
(3) $\exists\, c \in K^*$ a $d, b_1, b_2 \in K$ tak, že $\tilde{w} = c^{-6}w(c^2x + b_1, c^3y + dx + b_2)$.

Důsledek 5.5. Nechť $\mathrm{char}\, K \neq 2$ a $f, \tilde{f} \in K[x]$ splňuje $\deg f = \deg \tilde{f} = 3$ a $lc(f) = lc(\tilde{f}) = 1$. Potom

(1) polynomy $w = y^2 - f(x)$ a $\tilde{w} = y^2 - \tilde{f}(x)$ jsou K-ekvivalentní WEP $\Leftrightarrow \exists c \in K^*$ a $b \in K$, pro něž $\tilde{f}(x) = c^{-6}f(c^2x + b) = c^{-6}(\tau_b\vartheta_{(c^2)})^*(f)$,
(2) každý WEP $w \in K[x, y]$ je K-ekvivalentní nějakému krátkému WEP.

Příklad 5.6. (1) Uvažujme $w = y^2 + y(2x + 2) - (x^3 - 4x^2 + 1) \in \mathbb{R}[x, y]$. Pak w je WEP. Najdeme krátký WEP $\mathbb{R}$-ekvivalentní s w. Nejprve se pomocí lineární transformace dané

maticí $A = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \in U_2(\mathbb{R})$ zbavíme monomu xy:

$$\vartheta_A^*(w) = (y-x)^2 + (y-x)(2x+2) - (x^3 - 4x^2 + 1) = y^2 + 2y - (x^3 - 3x^2 + 2x + 1)$$

a poté posuneme o vektor $b = (1, -1)$, abychom se zbavili monomů y a x^2:

$$\tau_b^* \vartheta_A^*(w) = (y-1)^2 + 2(y-1) - ((x+1)^3 - 3(x+1)^2 + 2(x+1) + 1) = y^2 - (x^3 - x + 2).$$

(2) Polynom $\tilde{w} = y^2 - (x^3 - x + 2)$ je

(a) $\mathbb{R}$-ekvivalentní polynomu $y^2 - (x^3 - \frac{1}{16}x + \frac{1}{32})$, protože $\vartheta_{A_1}^*(\tilde{w}) = 64y^2 - 64(x^3 - \frac{1}{16}x + \frac{1}{32})$ pro $A_1 = \begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$,

(b) $\mathbb{C}$-ekvivalentní polynomu $y^2 - (x^3 - x - 2)$, protože $\vartheta_{A_2}^*(\tilde{w}) = -y^2 - (-x^3 + x + 2)$ pro $A_2 = \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}$.

6. Singularity

K je komutativní těleso, $\overline{K}$ jeho algebraický uzávěr a $\mathbb{X} := (x_1, \ldots, x_n)$.

T&N. Nechť $K \leq L \leq \overline{K}$. Značme afinní prostory

- $\mathbb{A}^n := \overline{K}^n$ nad tělesem $\overline{K}$ a
- $\mathbb{A}^n(L) := L^n$ nad tělesem L (L-racionální body).

Pro $a \in K[\mathbb{X}]$, $M \subset K[\mathbb{X}]$ dále značme:

- $V_M = \{\alpha \in \mathbb{A}^n \mid a(\alpha) = 0 \forall a \in M\}$ (varieta),
- $V_M(L) = V_M \cap \mathbb{A}^n(L)$, $V_a = V_{\{a\}}$, $V_a(L) = V_{\{a\}}(L)$.

Pokud $a \in K[x, y]$ a $\deg a \geq 1$, pak V_a říkáme *afinní rovinná křivka*.

Pozorování. Nechť $a \in K[\mathbb{X}]$, $M \subset K[\mathbb{X}]$, $\beta = (\beta_1, \ldots, \beta_n) \in \mathbb{A}^n$.

(1) $V_M = V_{(M)}$,

(2) mult $\tau_\beta^*(a) \geq 1 \Leftrightarrow$ mult $a(x_1 + \beta_1, \ldots, x_n + \beta_n) \geq 1 \Leftrightarrow a(\beta_1, \ldots, \beta_n) = 0 \Leftrightarrow \beta \in V_a$.

T&N. Nechť $a = \sum_j b_j x_i^j = \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in K[\mathbb{X}]$, kde $b_j \in K[\mathbb{X} \setminus \{x_i\}]$. Pak

$$L(a) = \sum_{i_1 \ldots i_n : \sum_j i_j = 1} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} = \sum_{j=1}^{n} a_{\delta_{1j} \ldots \delta_{1j}} x_j$$

se nazývá *lineární část* polynomu a a

$\frac{\partial a}{\partial x_i} = \sum_j (j+1) b_{j+1} x_i^j$ je (parciální) *derivace* polynomu a v proměnné x_i.

Definice. $a = \sum a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in K[\mathbb{X}]$, $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_a$ a položme $c_i := \frac{\partial a}{\partial x_i}(\alpha)$.

Pak $t_\alpha(a) := \sum_i c_i x_i - \sum_i c_i \alpha_i = \sum_i c_i (x_i - \alpha_i)$ je *tečna* a (nebo V_a) v bodě α.

Řekneme, že a (nebo V_a) je v bodě α *hladký* (hladká), pokud $t_\alpha(a) \neq 0$, a *singulární*, pokud $t_\alpha(a) = 0$.

Polynom a / varieta V_a je

- *hladký/á* , pokud je hladký/á ve všech bodech $\alpha \in V_a$ a
- *singulární*, pokud $\exists$ singulární bod $\alpha \in V_a$ (takové α je singularitou V_a).

Pozorování. Pokud $a \in K[\mathbb{X}]$ a $\alpha \in V_a$, potom

(1) a je hladký v bodě $\alpha \Leftrightarrow \exists i \frac{\partial a}{\partial x_i}(\alpha) \neq 0$,

(2) $\alpha \in V_{t_\alpha(a)}$.

Příklad 6.1. Nechť $w = y^2 - (x^3 + x - 2) \in \mathbb{R}[x, y]$ je krátký WEP, pak $L(w) = -x$, $\frac{\partial w}{\partial x} = -3x^2 - 1$, $\frac{\partial w}{\partial y} = 2y$.

Pro $\alpha = (1, 0) \in V_w$ máme $t_\alpha(w) = -4(x - 1)$.

Poznámka 6.2. Jestliže $a \in \overline{K}[\mathbb{X}]$ a $\alpha \in V_a$, pak $t_\alpha(a) = \tau^*_{-\alpha}(L(\tau^*_\alpha(a)))$.

Poznámka 6.3. Nechť $a \in \overline{K}[\mathbb{X}]$ a $\alpha \in \mathbb{A}^n$ a $\sigma \in \mathrm{Aff_n}(\overline{\mathrm{K}})$, pak $\alpha \in V_{\sigma*(a)} \Leftrightarrow \sigma(\alpha) \in V_a$ a v takovém případě $t_\alpha(\sigma^*(a)) = \sigma^*(t_{\sigma(\alpha)}(a))$.

Důsledek 6.4. $a \in \overline{K}[\mathbb{X}]$ a $\alpha \in \mathbb{A}^n$ a $\sigma \in \mathrm{Aff_n}(\overline{\mathrm{K}})$, pak

(1) $\sigma(V_{\sigma*(a)}) = V_a$,

(2) $\sigma^*(a)$ je singulární v bodě $\alpha \in V_{\sigma*(a)} \Leftrightarrow$ a je singulární v bodě $\sigma(\alpha) \in V_a$.

Důsledek 6.5. Nechť $w, \tilde{w} \in K[x, y]$ jsou K-ekvivalentní WEP. Pak w je hladký $\Leftrightarrow$ $\tilde{w}$ je hladký.

Připomeňme, že polynom je separabilní, jsou-li všechny jeho kořeny v kořenovém nadtělese jednoduché a těleso je perfektní jsou-li nad ním všechny ireducibilní polynomy separabilní.

Tvrzení 6.6. Jestliže $w = y^2 - f(x)$ je WEP pro $f(x) \in K[x]$, potom w má nejvýše 1 singularitu. Nechť navíc $charK \neq 2$,

(1) jestliže je K perfektní těleso, pak je singularita K-racionální,

(2) w je hladký $\Leftrightarrow$ f je separabilní.

Příklad 6.7. (1) $y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ je hladký krátký WEP,

(2) $(y + 1)^2 - (x^3 + 1) \in \mathbb{F}_3[x, y]$ je singulární WEP se singularitou $(2, 2)$,

(3) $y^2 - (x^3 - x^2 - x + 1) \in \mathbb{R}[x, y]$ je singulární WEP se singularitou $(1, 0)$.

7. Souřadnicové okruhy

K je v následujícím komutativní těleso a $\overline{K}$ jeho algebraický uzávěr. $\mathbb{X} := (x_1, \ldots, x_n)$.

T&N. Nechť $U \subseteq \mathbb{A}^n$. pak

$$I_U = \{a \in K[\mathbb{X}] \mid a(\alpha) = 0 \forall \alpha \in U\}, \quad \overline{I}_U = \{a \in \overline{K}[\mathbb{X}] \mid a(\alpha) = 0 \forall \alpha \in U\}$$

a $I_\alpha = I_{\{\alpha\}}$, $\overline{I}_\alpha = \overline{I}_{\{\alpha\}}$.

Pozorování. (1) Je-li I takový ideál $K[\mathbb{X}]$, že $I \cap K[x_i] = (a_i) \neq 0 \ \forall i$, pak $K[\mathbb{X}]/I$ je generován množinou $\{\prod_i x_i^{j_i} \mid j_i < \deg(a_i)\}$ jako vektorový prostor nad K, proto a $\dim_K K[\mathbb{X}]/I \leq \prod_i \deg(a_i) < \infty$.

(2) Je-li R obor a K-algebra splňující $\dim_K R < \infty$, pak $K[\alpha] \subseteq K(\alpha) \subseteq R$, proto je R těleso.

Poznámka 7.1. Nechť $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n$

(1) I_α je maximální,

(2) $\alpha \in \mathbb{A}^n(K) \Leftrightarrow K + I_\alpha = K[\mathbb{X}]$,
(3) $\alpha \in \mathbb{A}^n(K) \Rightarrow I_\alpha = (x_1 - \alpha_1, \ldots, x_n - \alpha_n)$.

Tvrzení 7.2. Je-li P prvoideál $K[\mathbb{X}]$ tak, že $P \cap K[x_i] \neq 0$ pro všechna $i = 1, \ldots n$, pak existuje $\alpha \in \mathbb{A}^n$ pro které $P = I_\alpha$

Tvrzení 7.3. Je-li P prvoideál $K[x, y]$, pak buď (a) $P = \{0\}$ nebo (b) $P = (p)$ pro $p \in K[x, y]$ ireducibilní, nebo (c) P je maximální a existuje $\alpha \in \mathbb{A}^2$ pro které $P = I_\alpha$.

Důsledek 7.4. Nechť P je nenulový prvoideál $K[x, y]$.
(1) P je maximální $\Leftrightarrow$ existuje $\alpha \in \mathbb{A}^n$ pro něž $P = I_\alpha \Leftrightarrow V_P$ je konečná.
(2) existuje $p \in K[x, y]$ ireducibilní tak, že $P = (p) \Leftrightarrow V_P \subsetneq \mathbb{A}^2$ je nekonečná.
(3) jestliže $p, q \in K[x, y]$ jsou ireducibilní tak, že $q \notin (p)$, pak $V_{\{p,q\}} = V_p \cap V_q$ je konečná.

Příklad 7.5. Pro WEP $w = y^2 - (x^3 + 1) \in \mathbb{R}[x, y]$ jsou například ideály

$$(w) \subseteq (y, x + 1) = I_{(-1,0)}, \quad (y, x^2 - x + 1) = I_u, \quad (y^2 + 1, x) = I_{(0,i)},$$

$u = (e^{\frac{\pi}{3}i}, 0)$, prvoideály.

T&N. Nechť $C = V_a$ je afinní rovinná křivka, kde $a \in K[x, y]$ a $I_C = (a)$. Potom $K[C] = K[x, y]/I_C = K[x, y]/(a)$ je *souřadnicový okruh* křivky C. Řekneme, že C je *ireducibilní*, pokud je $K[C]$ obor a prvek $p(x, y) + I_C$ nazveme polynom na křivce C pro libovolný polynom $p \in K[x, y]$.

Je-li w WEP, pak V_w se nazývá *Weierstrassova křivka*.

Pozorování. Nechť $C = V_a \subset \mathbb{A}^2$ je afinní rovinná křivka.
(1) C je ireducibilní $\Leftrightarrow I_C = (a)$ je prvoideál $\Leftrightarrow$ a je ireducibilní,
(2) zobrazení $\nu : K[C] \to \overline{K}^C$ dané vztahem $\nu(p + (a))(\alpha) = p(\alpha)$ je dobře definované prosté zobrazení.

T&N. Je-li $C = V_a \subset \mathbb{A}^2$ ireducibilní křivka, potom podílové těleso

$$K(C) = \{\frac{n + (a)}{d + (a)} \mid n \in K[x, y], d \in K[x, y] \setminus (a)\}$$

oboru $K[C]$ se nazývá *funkční těleso* křivky C.

Pozorování. Nechť $a, f \in K[x, y]$, kde a je ireducibilní a $C = V_a$, pak
(1) $f(x + (a), y + (a)) = 0$ v $K(C) \Leftrightarrow f \in (a)$,
(2) $K(C) = K(x + (a), y + (a))$,
(3) $x + (a)$ je algebraický nad $K \Leftrightarrow \exists p \in K[x] \setminus \{0\}$ splňující $p(x) \in (a) \Leftrightarrow \deg_y a = 0$.

Poznámka 7.6. Nechť $K \leq L$, $w \in K[x, y]$ je ireducibilní a nechť $\alpha, \beta \in L$ splňují, že α je transcendentí nad K, $L = K(\alpha, \beta)$ a $w(\alpha, \beta) = 0$. Potom $[L : K(\alpha)] = \deg_y w$.

Tvrzení 7.7. Nechť $w \in K[x, y]$ je ireducibilní, $C = V_w$, $\alpha = x + (w)$, $\beta = y + (w) \in K[C] \subset K(C) = K(\alpha, \beta)$. Pak
(1) α je transcendentní nad $K \Leftrightarrow \deg_y w > 0$,
(2) je-li α transcendentní nad K, pak $[K(C) : K(\alpha)] = \deg_y w$,

(3) $K(C)$ je AFF nad K.

Důsledek 7.8. Nechť $K \leq L$. Pak $\exists \alpha, \beta \in L$ tak, že $L = K(\alpha, \beta)$ je AFF nad $K \Leftrightarrow$ existuje ireducibilní afinní křivka $C \subset \mathbb{A}^2$ splňující $L \cong_K K(C)$.

T&N. $f \in K[x, y]$ se nazývá *absolutně ireducibilní*, pokud je f ireducibilní v oboru $\overline{K}[x, y]$

Příklad 7.9. Polynom $x^2 + y^2$ je ireducibilní, ale není absolutně ireducibilní v $\mathbb{R}[x, y]$ ($\mathbb{F}_3[x, y]$), protože $x^2 + y^2 = (x + iy)(x - iy)$ v $\mathbb{C}[x, y]$ ($\mathbb{F}_9$ obsahuje prvek řádu 4).

Polynom $x^2 + y$ ovšem v $\mathbb{R}[x, y]$ ($\mathbb{F}_3[x, y]$) absolutně ireducibilní je.

Poznámka 7.10. Jesliže pro $f, g \in K[x]$ platí, že $\deg g \leq 1$ a $\deg f \geq 3$ je lichý, potom $w = y^2 + yg(x) - f(x)$ je v $K[x, y]$ absolutně ireducibilní. Speciálně, každý WEP je absolutně ireducibilní.

Poznámka 7.11. Nechť $w \in K[x, y]$ je ireducibilní a $\tilde{K}$ je těleso konstant AFF $K(V_w)$ nad K. Potom $K = \tilde{K} \Leftrightarrow w$ je ireducibilní v $\tilde{K}[x, y]$. Předchozích podmínky jsou splněny, je-li w absolutně ireducibilní.

Důsledek 7.12. Je-li C Weierstrassova křivka, pak je každý prvek $\gamma \in K(C) \setminus K$ transcendentní nad K.

Příklad 7.13. Mějme WEP $w = y^2 + yx + x^3 + 1 \in \mathbb{F}_2[x, y]$ a označme L podílové těleso oboru $\mathbb{F}_2[x, y]/(w)$, tedy L je funkční těleso křivky V_w, což je AFF nad $\mathbb{F}_2$ podle 7.7. Protože je podle 7.10 w absolutně ireducibilní, platí, že pro těleso konstant $\tilde{\mathbb{F}}_2 = \mathbb{F}_2$ podle 7.11. tedy například polynomy $x^2 + x + 1$ či $x^3 + x + 1$ jsou ireducibilní nad L.

T&N. Nechť $w \in K[x, y]$ a L je AFF nad K a $\alpha, \beta \in L$. Řekneme, že *AFF L je dané* (nad K) rovnicí $w(\alpha, \beta) = 0$, pokud

(1) $L = K(\alpha, \beta)$,
(2) w je ireducibilní,
(3) $w(\alpha, \beta) = 0$.

Pozorování. Je-li $w \in K[x, y]$ ireducibilní a $\alpha = x + (w)$, $\beta = y + (w)$, pak $K(V_w)$ je dané nad K rovnicí $w(\alpha, \beta) = 0$.

8. Místa určená dvojicí

V následujícím předpokládejme, že K je komutativní těleso a $f = yg(x, y) + h(x) + y \in K[x, y]$, kde $h \in K[x] \setminus \{0\}$, $g \in K[x, y]$ splňuje $m := \text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$.

T&N. Nechť $a = \sum_{i,j \geq 0} a_{ij} x^i y^j$, pak definujme:
$\mu(a) := \text{mult}(a(x, y^m))$,
$s(a) := \{(i, j) |\ i, j \geq 0, i + jm = \mu(a)\}$,
$S(a) := \sum_{(i,j) \in s(a)} a_{ij} x^i y^j$ (*m-sokl polynomu* a).

Pozorování. Nechť $a, b \in K[x, y] \setminus \{0\}$ a $i, j, k, l \geq 0$.

(1) $\text{mult}(a \cdot b) = \text{mult}(a) + \text{mult}(b)$ a pokud $\text{mult}(a) < \text{mult}(b)$, pak $\text{mult}(a + b) = \text{mult}(a)$,

(2) $\mu(a\cdot b) = \mathrm{mult}(a(x,y^m)\cdot b(x,y^m)) = \mathrm{mult}(a(x,y^m))+\mathrm{mult}(b(x,y^m)) = \mu(a)+\mu(b)$, a pokud $\mu(a) < \mu(b)$, pak $\mu(a+b) = \mu(a) \geq \mathrm{mult}(a)$,

(3) Uvážíme-li, že $(i+jm)+(k+lm) = \mu(a)+\mu(b) = \mu(ab)$ a $(i+jm) > \mu(a) \Rightarrow (k+lm) < \mu(b) \Rightarrow b_{kl} = 0$, a proto

$$S(a)S(b) = \sum_{(i,j)\in s(a)} \sum_{(k,l)\in s(b)} a_{ij}b_{kl}x^{i+k}y^{j+l} = \sum_{(q,r)\in s(ab)} x^q y^r \sum_{(i,j)+(k,l)=(q,r)} a_{ij}b_{kl} = S(ab)$$

(4) $\mu(a) = \mu(S(a))$ a pokud $\mu(a) < \mu(b)$, pak $S(a+b) = S(a)$.

T&N. Definujme K-endomorphimy Λ algebry $K[x,y]$ podmínkou

$$\Lambda(u(x,y)) := u(x, -h(x) - yg(x,y))$$

pro každé $u \in K[x,y]$.

Poznámka 8.1. Pro každé $i,j \geq 0$ platí, že $\mu(\Lambda(x^iy^j)) = i+jm$, a existuje takové $\lambda \in K \setminus \{0\}$, že $S(\Lambda(x^iy^j)) = \lambda x^{i+jm}$.

Příklad 8.2. Nechť $w = (y+x+1)^2 - (x^3+2x+1) \in \mathbb{R}[x,y]$.

Protože $\gcd(x^3+2x+1, 3x^2+2) = 1$, je w WEP a platí

$$f = \frac{1}{2}w = \frac{1}{2}(y^2+x^2+2yx+2y-x^3) = y(x+\frac{1}{2}y) + \frac{1}{2}(x^2-x^3) + y.$$

a proto $f = yg(x,y) + h(x) + y$ pro $g = x + \frac{1}{2}y$ a $h = \frac{1}{2}(x^2-x^3)$. Všimněme si, že $\mathrm{mult}(g) = 1$ a $m = \mathrm{mult}(h) = 2$ a spočítejme

$\mu(g) = \mathrm{mult}(x+\frac{1}{2}y^2) = 1$, $S(g) = x$,

$\mu(h) = \mathrm{mult}(h) = 2$, $S(h) = \frac{1}{2}x^2$,

$\mu(x^3y^2) = 3+2\cdot 2 = 7$, $\mu(x^2y^3) = 2+3\cdot 2 = 8 \Rightarrow \mu(x^3y^2+x^2y^3) = 7$,

$S(\Lambda(x^3y^2+x^2y^3)) = S(\Lambda(x^3y^2)) = \frac{1}{4}x^7$ podle 8.1

Nadále budeme předpokládat, že f je ireducibilní polynom a L je AFF nad K dané rovnicí $f(\alpha,\beta) = 0$.

Poznámka 8.3. Existuje takové místo $P \in \mathbb{P}_{L/K}$, že $\nu_P(\alpha) > 0$ $\nu_P(\beta) > 0$. Navíc platí, že $\nu_P(\beta) = m\nu_P(\alpha)$.

Pozorování. Nechť $a = \sum_{ij} a_{ij}x^iy^j \in K[x,y] \setminus \{0\}$.

(1) $\Lambda(a)(\alpha,\beta) = a(\alpha, -h(\alpha) - \beta g(\alpha,\beta)) = a(\alpha,\beta)$,

(2) Nechť $P \in \mathbb{P}_{L/K}$ $\nu_P(\alpha) > 0$, $\nu_P(\beta) > 0$ a nechť $u = a(\alpha,\beta)$. Potom

$$\nu_P(u) \geq \min\{\nu_P(\alpha^i\beta^j) \mid a_{ij} \neq 0\} = \min\{(i+mj)\nu_P(\alpha) \mid a_{ij} \neq 0\} = \mu(a)\nu_P(\alpha)$$

$$\Rightarrow \mu(a) \leq \tfrac{\nu_P(u)}{\nu_P(\alpha)}.$$

T&N. Položme $\mu(u) = \max\{\mu(a) \mid a \in K[x,y] : a(\alpha,\beta) = u\}$ pro každé $u \in K[\alpha,\beta]$.

Poznámka 8.4. Nechť $u \in K[\alpha,\beta]\setminus\{0\}$ a $k := \mu(u)$. Potom existuje $\lambda \in K^*$ a $b \in K[x,y]$ splňující $\mu(b) > k$ a $u = \lambda x^k + b(\alpha,\beta)$.

Věta 8.5. Existuje právě jedno $P \in \mathbb{P}_{L/K}$, pro něž $\nu_P(\alpha) > 0$ a $\nu_P(\beta) > 0$. Navíc platí, že $\nu_P(\alpha) = 1$, $\nu_P(\beta) = m$ a $\nu_P(u\cdot v^{-1}) = \mu(u) - \mu(v)$ pro každé $u,v \in K[\alpha,\beta] \setminus \{0\}$.

Příklad 8.6. Uvažujme polynom $f = y(x + \frac{1}{2}y) + \frac{1}{2}(x^2 - x^3) + y$ z 8.2. Pak $L = \mathbb{R}(\alpha, \beta)$ a označme jednoznačně určené místo P z předchozí věty.

Pak $\nu_P(\alpha) = 1$ a $\nu_P(\beta) = \text{mult}(h) = 2$. Spočítáme hodnotu $\nu_P(\alpha^2 + \beta)$ a $\nu_P(\alpha^2 + 2\beta)$.
$f(\alpha, \beta) = 0 \Rightarrow \beta = -\beta(\alpha + \frac{1}{2}\beta) + \frac{1}{2}(\alpha^3 - \alpha^2)$, proto
$\nu_P(\alpha^2 + \beta) = \nu_P(\frac{1}{2}\alpha^2 - \beta\alpha - \frac{1}{2}\beta^2 + \frac{1}{2}\alpha^3) = \min(2, 3, 4, 3) = 2$ a
$\nu_P(\alpha^2 + 2\beta) = \nu_P(\alpha^3 - 2\beta\alpha - \beta^2) = \min(3, 5, 4) = 3$.

Pozorování. Pro každé $\sigma \in \text{Aff}_2(\text{K})$ existuje právě jedno $\overline{\sigma} \in \text{Aff}_2(\text{L})$ takové, že $\sigma(\gamma) = \overline{\sigma}(\gamma)$ pro všechna $\gamma \in \mathbb{A}^2(K)$.

T&N. Označme $\overline{\sigma}$ rozšíření $\sigma \in \text{Aff}_2(\text{K})$ z předchozího pozorování.

Pozorování. Nechť $a \in K[x, y] \subseteq L[x, y]$ a $\sigma \in \text{Aff}_2(\text{K})$.

(1) $(\sigma^{-1})^*(a(\sigma^*(x), \sigma^*(y))) = a(x, y)$,
(2) jestliže $f(x, y) = a(\sigma^*(x), \sigma^*(y))$, pak $a = (\sigma^{-1})^*(f)$,
(3) $\overline{\sigma}^*(a) = \sigma^*(a) \in K[x, y]$.

Pozorování. Nechť $\sigma \in \text{Aff}_2(\text{K})$, $\tilde{\alpha}$, $\tilde{\beta} \in L$ a $u = \sigma^*(x)(\tilde{\alpha}, \tilde{\beta})$, $t = \sigma^*(y)(\tilde{\alpha}, \tilde{\beta})$. Potom

(4) $(u, t) = (\sigma^*(x)(\tilde{\alpha}, \tilde{\beta}), \sigma^*(y)(\tilde{\alpha}, \tilde{\beta})) = \overline{\sigma}(\tilde{\alpha}, \tilde{\beta})$,
(5) $(\tilde{\alpha}, \tilde{\beta}) = \overline{\sigma}^{-1}(u, t)$, proto $K(\tilde{\alpha}, \tilde{\beta}) = K(u, t)$
(6) $(\sigma^{-1})^*(f)(u, t) = f(\overline{\sigma}^{-1}(u, t)) = f(\tilde{\alpha}, \tilde{\beta})$.

V následujícím buď L AFF nad K dané dané (obecnou) rovností $w(\alpha, \beta) = 0$.

Poznámka 8.7. Nechť w je hladký v bodě $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, $A \in \text{GL}_2(K)$, $\sigma := \vartheta_A \tau_{-\gamma}$ a položme $(u, t) = \overline{\sigma}(\alpha, \beta)$ a $f_\sigma = (\sigma^{-1})^*(w)$.

(1) Potom L je AFF nad K dané $f_\sigma(u, t) = 0$.
(2) Existuje taková matice A, že buď $f_\sigma = y$ nebo $f_\sigma = yg(x, y) + h(x) + y$ kde $h \in K[x] \setminus \{0\}$, $g \in K[x, y]$, $\text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$.
(3) Jestliže $t_\gamma(f) = a_1(x - \gamma_1) + a_2(y - \gamma_2)$, pak A je matice z (2) (tj. $\sigma := \vartheta_A \tau_{-\gamma}$ splňující $f_\sigma = yg(x, y) + h(x) + y$ pro $h \in K[x]$, $g \in K[x, y]$, $\text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$) právě když $\exists\, (b_1, b_2) \in K^2 \setminus \text{LO}_\text{K}((a_1, a_2))$ takové, že $A = \begin{pmatrix} b_1, b_2 \\ a_1, a_2 \end{pmatrix}$.

Věta 8.8. Nechť w je hladký v bodě $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$.

(1) Existuje jednoznačně určené $P \in \mathbb{P}_{L/K}$ splňující $\nu_P(\alpha - \gamma_1) > 0$ a $\nu_P(\beta - \gamma_2) > 0$.
(2) Jestliže $l = l_0 + l_1 x + l_2 y \in K[x, y]$ kde $l_0, l_1, l_2 \in K$ pak pro P z (1) platí:

$$\nu_P(l(\alpha, \beta)) \begin{cases} = 0 & \text{jestliže } l(\gamma) \neq 0 \\ = 1 & \text{jestliže } l(\gamma) = 0 \text{ a } l \notin (t_\gamma(w)) \\ \geq 2 & \text{jestliže } l(\gamma) = 0 \text{ a } l \in (t_\gamma(w)) \end{cases}$$

Předpokládejme, že L je AFF nad K dané rovností $w(\alpha, \beta) = 0$ s $\deg w \geq 2$ a zároveň rovností $f_\sigma(u, v) = 0$ kde $f_\sigma = yg(x, y) + h(x) + y$ pro $h \in K[x] \setminus 0$, $g \in K[x, y]$, $\text{mult}(h) \geq 2$, $\text{mult}(g) \geq 1$ (a kde oba polynomu w i f_σ jsou ireducibilní).

T&N. Nechť $p \in K[x]$ a $\gamma \in K$. Násobnost kořenu γ polynomu p je nezáporné celé číslo k splňující $(x - \gamma)^k$ dělí p a $(x - \gamma)^{k+1}$ nedělí p.

Pozorování. Nechť $p, s \in K[x]$, $g \in K[x, y]$ a $\gamma \in K$.

(1) Násobnost kořenu γ v p je $k \Leftrightarrow \mathrm{mult}(\tau^*_{-\gamma}(p)) = k$,
(2) jestliže $s(\gamma) = 0$ a $\hat{g} = g(x - \gamma, s(x)) \in K[x]$, pak násobnost kořenu γ v $\hat{g}$ je větší nebo rovna $\mathrm{mult}(g)$.

Tvrzení 8.9. Nechť $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$, $\deg w \geq 2$, $\frac{\partial w}{\partial y}(\gamma) \neq 0$ a $\lambda, \mu \in K$ jsou takové, že $\gamma_2 = \lambda\gamma_1 + \mu$. Pak existuje právě jedno $P \in \mathbb{P}_{L/K}$ pro které $(\alpha - \gamma_1, \beta - \gamma_2) \subset P$, a $\nu_P(\beta - \lambda\alpha + \mu)$ je rovno násobnosti kořenu γ polynomu $\hat{w}(x) = w(x, \lambda x + \mu)$.

Příklad 8.10. Nechť $f = y^2 + xy + x^5 + 32 \in \mathbb{R}[x]$, pak jde o absolutně ireducibilní polynom podle 7.10. Označme L AFF nad $\mathbb{R}$ dané rovností $f(\alpha, \beta) = 0$ pro $\alpha = x + (f)$ a $\beta = y + (f) \in K[x, y]/(f)$.

Vidíme, že $(-2, 2) \in V_f$ a $\frac{\partial f}{\partial x} = y + 5x^4$, $\frac{\partial f}{\partial y} = 2y + x$, proto $\frac{\partial f}{\partial x}(-2, 2) = 82$, $\frac{\partial f}{\partial y}(-2, 2) = 2$ a $t = t_{(-2,2)}(f) = 82x + 2y + 160$.

Podle 8.9 existuje právě jedno místo $P \in \mathbb{P}_{L/K}$ obsahující $\alpha + 2, \beta - 2$.

Pro $u = \beta + 41\alpha + 80 = \frac{1}{2}t(\alpha, \beta)$určíme hodnotu $\nu_P(u)$:

$\hat{f} = f(x, -41x - 80) = x^5 + 40 \cdot 41x^2 - 80 \cdot 81 + 80^2 + 32$.

Protože $0 = \hat{f}(-2) = \hat{f}'(-2) \neq \hat{f}''(-2)$ dostáváme, že $\nu_P(u) = 2$.

9. Lokalizace v souřadnicovém okruhu

Uvažujme nadále AFF L nad K dané dané rovností $w(\alpha, \beta) = 0$ a zároveň rovností $f_\sigma(u, v) = 0$ z 8.7, kde $f_\sigma = yg(x, y) + h(x) + y$ a $\mathrm{mult}(h) \geq 2$, $\mathrm{mult}(g) \geq 1$.

T&N. Nechť $\gamma = (\gamma_1, \gamma_2) \in V_w(K) \subset \mathbb{A}^2(K)$. Pak $(w) \subseteq I_\gamma = (x - \gamma_1, y - \gamma_2)$. Označme

$$R_\gamma := K[x, y]_{(I_\gamma)} = \{\frac{a}{b} \mid a, b \in K[x, y] : b(\gamma) \neq 0\}$$

lokalizaci $K[x, y]$ v maximálním ideálu I_γ, $(I_\gamma) = I_\gamma R_\gamma = \{\frac{a}{b} \in R_\gamma \mid a \in I_\gamma\}$ označuje (jediný) maximální ideál R_γ a zobrazení $\omega_\gamma : R_\gamma \to L$ je určeno pravidlem $\omega_\gamma(\frac{a}{b}) = \frac{a(\alpha,\beta)}{b(\alpha,\beta)}$.

Označme

$${}_w\mathcal{O}_\gamma := \{\rho \in L \mid \exists r \in R_\gamma : \omega_\gamma(r) = \rho\}, \quad {}_wP_\gamma := \{\rho \in L \mid \exists r \in (I_\gamma) : \omega_\gamma(r) = \rho\}.$$

Pro pevné w budeme psát $\mathcal{O}_\gamma$ místo ${}_w\mathcal{O}_\gamma$ a P_γ místo ${}_wP_\gamma$.

$Dom_w(r) = \{\epsilon \in V_w \mid r \in \mathcal{O}_\epsilon\}$ $\forall r \in L$.

Pozorování. Pro výše zavedené značení, kde $\gamma \in V_w(K)$ a $\sigma(\gamma) = (0, 0)$ platí:

(1) ω_γ je dobře definovaný okruhový homomorfismus,
(2) $\mathcal{O}_\gamma = \omega_\gamma(R_\gamma)$, $P_\gamma = \omega_\gamma(I_\gamma R_\gamma)$,
(3) $\mathcal{O}_\gamma$ je lokální okruh s maximálním ideálem P_γ, $\mathcal{O}_\gamma = K + P_\gamma$, proto platí, že $\dim_K(\mathcal{O}_\gamma/P_\gamma) = 1$,
(4) nechť $r = \frac{a(\alpha,\beta)}{b(\alpha,\beta)}$ pro $a, b \in K[x, y]$, $b \notin (w)$ a $b = \prod_i b_i$ je ireducibilní rozklad b, pak $V_w \setminus Dom_w(r) = \{\epsilon \in V_w(K) \mid r \notin \mathcal{O}_\epsilon\} \subseteq \bigcup_i V_{(w,b_i)}$ je konečný,
(5) ${}_w\mathcal{O}_\gamma = {}_{f_\sigma}\mathcal{O}_{(0,0)}$ a ${}_wP_\gamma = {}_{f_\sigma}P_{(0,0)}$, speciálně ${}_w\mathcal{O}_\gamma = {}_{\tau^*_\gamma(w)}\mathcal{O}_{(0,0)}$ a ${}_wP_\gamma = {}_{\tau^*_\gamma(w)}P_{(0,0)}$.

Poznámka 9.1. Je-li w singulární v $\gamma \in V_w(K)$, pak $\mathcal{O}_\gamma$ není valuační okruh.

Příklad 9.2. Buď $w = (y + 1)^2 - (x + 2)^3$ a nechť L je AFF nad $\mathbb{F}_5$ dané rovností $w(\alpha, \beta) = 0$ pro $\alpha = x + (w)$ a $\beta = y + (w) \in K[x, y]/(w)$. Pak $(3, 4) \in V_w(\mathbb{F}_5)$ je singularita w a v předchozím důkazu jsme si rozmysleli, že $\frac{\alpha+2}{\beta+1} \notin {}_wO_{(3,4)}$ ani $\frac{\beta+1}{\alpha+2} \notin {}_wO_{(3,4)}$.

Poznámka 9.3. Nechť L je AFF nad K dané rovností $f_\sigma(u,v)=0$ a předpokládejme, že $P \in \mathbb{P}_{L/K}$ splňuje $\nu_P(u)=1$ a $\nu_P(v)>0$. Pokud $z \in K[u,v] \setminus \{0\}$, pak existuje $a,b \in K[x,y]$ s $a(0,0)\neq 0$, $b(0,0)\neq 0$ (tj. $\mathrm{mult}(a)=\mathrm{mult}(b)=0$) a $\frac{z}{u^{\nu_P(z)}} = \frac{a(u,v)}{b(u,v)} \in {}_{f_\sigma}\mathcal{O}^*_{(0,0)} = {}_{f_\sigma}\mathcal{O}_{(0,0)} \setminus {}_{f_\sigma}\mathcal{P}_{(0,0)}$.

Tvrzení 9.4. Nechť w je hladký v bodě $\gamma=(\gamma_1,\gamma_2) \in V_w(K)$ a $P \in \mathbb{P}_{L/K}$ a platí, že, $\frac{\partial w}{\partial y}(\gamma)\neq 0$, $\nu_P(\alpha-\gamma_1)>0$ a $\nu_P(\beta-\gamma_2)>0$. Potom

(1) existuje takové $u \in P_\gamma$, že $\nu_P(u)=1$ a $\frac{z}{u^{\nu_P(z)}} \in \mathcal{O}^*_\gamma$ pro každý $z \in K[\alpha,\beta]\setminus\{0\}$,
(2) $P=P_\gamma$,
(3) $\mathcal{O}_p=\mathcal{O}_\gamma$.

Příklad 9.5. Uvažujme opět $f=y^2+xy+x^5+32 \in \mathbb{R}[x]$ z 8.10, kde L je AFF nad $\mathbb{R}$ dané rovností $f(\alpha,\beta)=0$. Označme $t=t_{(-2,2)}(f)=82x+2y+160$. Určíme $P=P_{(-2,2)} \in \mathbb{P}_{\mathbb{R}(\alpha,\beta)/\mathbb{R}}$. Protože je prvek $(-2,2)$ nulou přímky $x+2$ a $\notin (t)$, dostáváme z 8.8, že $\nu_P(\alpha+2)=1$.

Proto $P_{(-2,2)}=(\alpha+2)=\{(\alpha+2)\frac{p(\alpha,\beta)}{q(\alpha,\beta)} \mid q(-2,2)\neq 0\}$.

Pozorování. Nechť $\omega: K[x,y]\to K[\alpha,\beta]$ je dosazovací homomorfismus $\omega(m)=m(\alpha,\beta)$ a $0\neq P \subsetneq K[\alpha,\beta]$ je prvoideál. Pak díky 7.4 dostáváme:

(1) ω je okruhový surjektivní homomorfismus a $\mathrm{Ker}\omega=(w)$,
(2) $(w)\subsetneq \omega^{-1}(P)$ a $\omega^{-1}(P)$ je prvoideál K[x,y], proto $\exists \gamma \in V_w$ splňující $P=\omega(I_\gamma)$,
(3) P je maximální ideál .

Poznámka 9.6. Nechť $0\neq P\subsetneq K[\alpha,\beta]$ je prvoideál a $\hat{K}=K[\alpha,\beta]/P$. Pak je $\hat{K}=K[\alpha+P,\beta+P]$ těleso, pro něž $[\hat{K}:K]<\infty$. Navíc $[\hat{K}:K]=1 \Leftrightarrow \gamma \in V_w(K)$.

Poznámka 9.7. Nechť $P \in \mathbb{P}_{L/K}$ a $\tilde{P}=P\cap K[\alpha,\beta]$.

(1) Pokud $K[\alpha,\beta]\subseteq \mathcal{O}_P$, pak $\tilde{P}$ je maximální ideál $K[\alpha,\beta]$, $\dim_K(K[\alpha,\beta]/\tilde{P})<\infty$, $\nu_P(\alpha)\geq 0$, a $\nu_P(\beta)\geq 0$.
(2) Jestliže $K[\alpha,\beta]\not\subseteq \mathcal{O}_P$, pak $\tilde{P}=0$ a buď $\nu_P(\alpha)<0$ nebo $\nu_P(\beta)<0$.
(3) Platí-li $K[\alpha,\beta]\not\subseteq \mathcal{O}_P$ a w je WEP, potom $\nu_P(\alpha)<0$, $\nu_P(\beta)<0$ a $3\nu_P(\alpha)=2\nu_P(\beta)$.

T&N. Označme $\mathbb{P}^{(1)}_{L/K} := \{P \in \mathbb{P}_{L/K} \mid \deg P=1\}$.

Věta 9.8. Nechť $P \in \mathbb{P}^{(1)}_{L/K}$ a polynom w je hladký ve všech bodech $\gamma \in V_w(K)$. Potom jsou následující podmínky ekvivalentní:

(1) $K[\alpha,\beta]\subseteq \mathcal{O}_P$,
(2) $\exists$ právě jedno $(\gamma_1,\gamma_2)\in V_w(K)$, pro které $\nu_P(\alpha-\gamma_1)>0$ a $\nu_P(\beta-\gamma_2)>0$,
(3) existuje jediný bod $\gamma \in V_w(K)$, pro který $P=P_\gamma$.

Důsledek 9.9. Je-li f hladký WEP ve všech bodech $\gamma \in V_w(K)$ a $P \in \mathbb{P}^{(1)}_{L/K}$, pak buď existuje $\gamma \in V_w(K)$, pro které $P=P_\gamma$ nebo $\alpha^{-1},\beta^{-1}\in P$.

10. Slabá aproximační věta a její důsledky

L nadále značí AFF nad K s tělesem konstant $\tilde{K}$.

Pozorování. Nechť $a, b \in L$.

(1) Pokud $a \notin \tilde{K}$, pak $\exists P \in \mathbb{P}_{L/K}$ takové, že $\nu_P(a) > 0$ díky 3.6,
(2) $\tilde{K} = \{s \in L \mid \nu_P(s) = 0 \ \forall P \in \mathbb{P}_{L/K}\}$,
(3) jestliže $P \in \mathbb{P}_{L/K}$ splňuje $\nu_P(a) \neq 0 \neq \nu_P(b)$, pak díky 4.8 $\nu_P(a+b^k) = \min(\nu_P(a), k\nu_P(b))$ pro všechna kromě nejvýše jednoho, tedy $\exists k_0$ tak, že rovnost platí $\forall k \geq k_0$.

Poznámka 10.1. Nechť $n \geq 1$ a $P_1, \ldots, P_n \in \mathbb{P}_{L/K}$ jsou po dvou různá místa. Pokud $\nu_i := \nu_{P_i}$ pro všechna i, $a_1, \ldots a_n \in L$ a $z \in \mathbb{Z}$, pak

(1) $\exists\ s \in L^*$ tak, že $\nu_1(s) > 0$ a $\nu_i(s) < 0$ pro všechna $i = 2, \ldots, n$,
(2) $\exists\ t \in L$ tak, že $\nu_i(t - a_i) > z$ pro všechna $i = 1, \ldots, n$.

Věta 10.2 (Slabá aproximační věta)**.** Nechť $n \geq 1$ a $P_1, \ldots, P_n \in \mathbb{P}_{L/K}$ jsou po dvou různá místa. Jestliže $a_1, \ldots a_n \in L$ a $z_1, \ldots, z_n \in \mathbb{Z}$, pak existuje $s \in L$ tak, že $\nu_{P_i}(s - a_i) = z_i$ pro všechna $i = 1, \ldots, n$.

T&N. Je-li W podprostor vektorového prostoru V nad K, řekneme, že B je lineárně nezávislá množina (báze) V *modulo* W jestliže $\{b + W \mid b \in B\}$ tvoří lineárně nezávislou množina (bázi) faktoru V/W.

Důsledek 10.3. Nechť $n \geq 1$, $e \geq 0$ a $P, P_1, \ldots, P_n$ jsou po dvou různá místa

(1) $\mathbb{P}_{L/K}$ je nekonečná.
(2) Existuje báze B K-algebry $\mathcal{O}_P$ modulo P tak, že $B \subset P_j^e \setminus P_j^{e+1}$ (tj. $\nu_{P_j}(b) = e$ $\forall b \in B$) $\forall i = 1, \ldots, n$.

Pozorování. Nechť $P \in \mathbb{P}_{L/K}$ a nechť $b_1, \ldots, b_n \in \mathcal{O}_P$ jsou lineárně nezávislé modulo P nad tělesem K, $t \in P$, $\nu_P(t) = 1$, λ_i, $\lambda_{ij} \in K$ pro $i = 1, \ldots, n$, $j = 0, \ldots, e-1$ a $\exists i : \lambda_i \neq 0$ a $\exists (i,j) : \lambda_{ij} \neq 0$.

(1) $\nu_P(\sum_i \lambda_i b_i) = 0$,
(2) $\nu_P(\sum_i \lambda_i b_i t^j) = \nu_P(\sum_i \lambda_i b_i) + \nu_P(t^j) = j$,
(3) $\nu_P(\sum_{ij} \lambda_{ij} b_i t^j) = \min\{j \mid \exists i : \lambda_{ij} \neq 0\}$ podle 4.8,
(4) $\{b_i t^j \mid i = 1, \ldots, n,\ j = 0, \ldots, e-1\}$ je lineárně nezávislá modulo P^e.

Tvrzení 10.4. Nechť $P_1, \ldots, P_n \in \mathbb{P}_{L/K}$ jsou po dvou různá místa pro $n \geq 1$. Pokud $s \in \bigcap_{i=1}^n P_i$ (tedy $\nu_{P_i}(s) \geq 1\ \forall i$), potom $[L : K(s)] \geq \sum_{i=1}^n \nu_{P_i}(s) \deg P_i$.

Důsledek 10.5. Jestliže $s \in L^*$, pak je množina $\{P \in \mathbb{P}_{L/K} \mid \nu_P(s) \neq 0\}$ konečná.

Důsledek 10.6. Je-li w WEP a L je dané rovností $w(\alpha, \beta) = 0$, pak existuje právě jedno místo $P_\infty \in \mathbb{P}_{L/K}$ tak, že $\nu_{P_\infty}(\alpha) < 0$ nebo $\nu_{P_\infty}(\beta) < 0$. Navíc $P_\infty \in \mathbb{P}_{L/K}^{(1)}$, $\nu_{P_\infty}(\alpha) = -2$ a $\nu_{P_\infty}(\beta) = -3$.

T&N. Jednoznačně určené místo nad WEP z předchozího důsledku budeme značit P_∞.

Tvrzení 10.7. Je-li w hladký WEP v $V_w(K)$, pak $\mathbb{P}_{L/K}^{(1)} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}$.

Příklad 10.8. Nechť $w = y^2 + y - (x^3 + 1) = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ a $\alpha := x + (w)$, $\beta := y + (w) \in K[x, y]/(w)$. Potom je w je WEP a $L := \mathbb{F}_2(\alpha, \beta)$ je AFF nad $\mathbb{F}_2$ dané $w(\alpha, \beta) = 0$.

Z 10.7 plyne, že $P \in \mathbb{P}^{(1)}_{L/K}$, právě když $P \in \{P_{(1,0)}, P_{(1,1)}, P_\infty\}$, neboť $V_w(\mathbb{F}_2) = \{(1, 0), (1, 1)\}$.

Podle 10.3(1) je $\mathbb{P}_{L/K}$ nekonečná, proto jsou další místa stupně většího než 1, například pro každý ireducibilní $m \in \mathbb{F}_2[x]$ stupně většího než 1, existuje $P_m \in \mathbb{P}_{L/K}$ splňující $m(\alpha) \in P_m$, a proto $\deg P_m \geq \deg(m) > 1$.

11. Divizory

L je nadále AFF nad K a $\tilde{K}$ je jeho těleso konstant.

Definice. Nechť $\mathrm{Div(L/K)} = \{\sum_{P \in \mathbb{P}_{L/K}} a_p P \mid a_p \in \mathbb{Z}\}$ označuje volnou abelovskou grupu s (formální) volnou bází $\mathbb{P}_{L/K}$ (tedy jen konečně mnoho hodnot a_p je nenulových) s operacemi

$$\sum_{P \in \mathbb{P}_{L/K}} a_p P \pm \sum_{P \in \mathbb{P}_{L/K}} b_p P = \sum_{P \in \mathbb{P}_{L/K}} (a_p \pm b_p) P, \quad \underline{0} = \sum_{P \in \mathbb{P}_{L/K}} 0P.$$

Formální suma $\sum_{P \in \mathbb{P}_{L/K}} a_p P$ se nazývá *divizor* (AFF L nad K). *S*tupeň divizoru je definován jako $\deg_K(\sum_{P \in \mathbb{P}_{L/K}} a_p P) := \sum_{P \in \mathbb{P}_{L/K}} a_p \deg_K(P)$.

Příklad 11.1. $\sum_{P \in \mathbb{P}_{L/K}} \nu_p(r) P$ je divizor podle 10.5 pro každé $r \in L^*$.

Pozorování. Položme $k = [\tilde{K} : K] < \infty$, $P \in \mathbb{P}_{L/K}$, $a \in L^*$.

(A1) L je AFF nad $\tilde{K}$ a $\tilde{K} \subset \mathcal{O}_P$ podle 4.10, proto $\mathbb{P}_{L/\tilde{K}} = \mathbb{P}_{L/K}$ a $\mathrm{Div(L/\tilde{K})} = \mathrm{Div(L/K)}$,
(A2) $\deg_K P = \dim_K \mathcal{O}_P/P = k \cdot \deg_{\tilde{K}} P$ a $\deg_K(A) = k \cdot \deg_{\tilde{K}}(A)$,
(A3) $\deg_K : \mathrm{Div(L/K)} \to \mathbb{Z}$ je grupový homomorfismus,
(A4) $\sum_{P \in \mathbb{P}_{L/K}} \nu_P(a) P = 0 \Leftrightarrow \nu_P(a) = 0 \ \forall P \in \mathbb{P}_{L/K} \Leftrightarrow a \in \tilde{K}$.

Definice. Divizor $\sum_{P \in \mathbb{P}_{L/K}} \nu_p(r) P$ se pro $r \in L^*$ se nazývá *hlavní* budeme ho značit (r) a označme množinu hlavních divizorů $\mathrm{Princ(L/K)} := \{(r) \mid r \in L^*\}$.

T&N. Nechť $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P$, $B = \sum_{P \in \mathbb{P}_{L/K}} b_p P \in \mathrm{Div(L/K)}$. Pak budeme psát:

$$\max(A, B) := \sum_{P \in \mathbb{P}_{L/K}} \max(a_p, b_p) P, \quad \min(A, B) := \sum_{P \in \mathbb{P}_{L/K}} \min(a_p, b_p) P,$$

$A_+ := \max(A, \underline{0})$, $A_- := -\min(A, \underline{0}) = (-A)_+$, a řekneme, že A je *pozitivní*, jestliže $A = A_+$.

Definujme relace $\leq$ a $\sim$ na $\mathrm{Div(L/K)}$: $A \leq B$, pokud $a_p \leq b_p \ \forall \ P \in \mathbb{P}_{L/K}$, $A \sim B$, pokud $A - B \in \mathrm{Princ(L/K)}$. $\geq$ značí jí opačnou relaci k relaci $\leq$.

Označme $\mathcal{L}(A) := \{r \in L^* \mid (r) + A \geq \underline{0}\} \cup \{0\}$.

Pozorování. Nechť $A, B, C, D \in \mathbb{P}_{L/K}$, $r, s \in L^*$.

(B1) Protože $(rs) = \sum_{P\in\mathbb{P}_{L/K}} \nu_p(rs)P = \sum_{P\in\mathbb{P}_{L/K}} (\nu_p(r)+\nu_p(s))P = (r)+(s)$, je zobrazení $r \to (r)$ homomorfismus grup L^* a Div(L/K),
(B2) $-(r) = (r^{-1})$, $\underline{0} = (1)$ je neutrální prvek a Princ(L/K) podgrupa grupy Div(L/K), navíc $(r) = (s) \Leftrightarrow \exists\ \lambda \in \tilde{K}^*$ splňující $r = \lambda s$
(B3) $\sim$ je kongruence na Div(L/K),
(B4) $\leq$ je uspořádání na Div(L/K), pro něž platí $A \leq B$, $C \leq D \Rightarrow A + C \leq B + D$,
(B5) pokud $r \in L \setminus \tilde{K}$, pak $\exists P, Q \in \mathbb{P}_{L/K}$ splňující $\nu_P(r) > 0$, $\nu_Q(r) < 0$, proto $(r) \not\geq 0$
(B6) $\mathcal{L}(A)$ je vektorový prostor nad tělesem $\tilde{K}$ a tedy i nad K a platí, že

$$\mathcal{L}(\underline{0}) := \{r \in L^* \mid (r) + (1) \geq \underline{0}\} \cup \{0\} = \tilde{K}.$$

T&N. Cl(L/K) := Div(L/K)/Princ(L/K) je *třídová grupa* AFF L nad K.

Jestliže $A \in$ Div(L/K), pak $\mathcal{L}(A)$ se nazývá *Riemannův-Rochův prostor* divizoru A a $l(A) = \dim_{L/K} A := \dim_K \mathcal{L}(A)$.

Pokud $K = \tilde{K}$, pak o L řekneme, že je *plně konstantní* AFF.

Pozorování. Nechť $i \leq j \in \mathbb{N}$, $(p) = P \in \mathbb{P}_{L/K}$, tj. $\nu_P(p) = 1$.

(C1) Zobrazení $\psi_j : \mathcal{O}_P/P \to P^{j-1}/P^j$ určené vztahem $\psi_j(a+P) = ap^{j-1} + P^j$ je izomorfismus vektorových prostorů nad K,
(C2) $\deg P = \dim_K \mathcal{O}_P/P = \dim_K P^{j-1} = P^j$,
(C3) $\dim_K(P^i/P^j) = \sum_{k=i+1}^{j} \dim(P^{k-1}/P^k) = (j-i)\deg P$.

Poznámka 11.2. Jsou-li $A, B \in$ Div(L/K) takové, že $A \leq B$, pak $\mathcal{L}(A)$ je podprostor $\mathcal{L}(B)$ a $\dim_K(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg_K(B - A)$.

Tvrzení 11.3. Pokud $K = \tilde{K}$ (tj. L je plně konstantní AFF) a $A, B \in$ Div(L/K), potom

(D1) $1 \leq l(A) \leq \deg A + 1$, jestliže $A \geq \underline{0}$,
(D2) $l(A) = 0$, jestliže $A < \underline{0}$,
(D3) $l(A) < l(A_+) < \infty$,
(D4) $\deg A - l(A) \leq \deg B - l(B)$, jestliže $A \leq B$.

Poznámka 11.4. Jestliže $s \in L \setminus \tilde{K}$ (tj. s je transcendentní nad K), pak existuje takové $B \in$ Div(L/K), že $B \geq \underline{0}$ a pro každý $k \geq 0$:

(1) $(k+1)[L : K(s)] \leq l(k \cdot (s)_- + B)$,
(2) $(k+1)[L : K(s)] \leq k \cdot \deg((s)_-) + \deg B + 1$,
(3) $k[L : K(s)] - l(k \cdot (s)_-) \leq \deg B - [L : K(s)]$.

Věta 11.5. Jestliže $K = \tilde{K}$ a $s \in L \setminus \tilde{K}$ (tj. L je plně konstantní AFF a s je transcendentní nad K), pak $\deg((s)_-) = \deg((s)_+) = [L : K(s)]$ a $\deg((s)) = 0$.

Důsledek 11.6. Pokud $A \sim B$, pak $\deg A = \deg B$ a $\dim_{L/K} A = \dim_{L/K} B$.

Příklad 11.7. Nechť L je AFF nad $\mathbb{F}_2$ dané $w(\alpha, \beta) = 0$ pro $w = y^2 + y - (x^3 + 1) \in \mathbb{F}_2[x, y]$ jako v 10.8. Spočítáme hlavní divizory $(\alpha + 1)$ a (α).

(a) Podle 11.5

$$\deg((\alpha+1)_+) = \sum_{P:\ \alpha+1\in P} \nu_P(\alpha+1)\deg P = [L : \mathbb{F}_2(\alpha+1)] = [L : \mathbb{F}_2(\alpha)] = 2.$$

Protože $\alpha+1 \in P_{(1,0)} \cap P_{(1,1)}$ a $\nu_{P_\infty}(\alpha+1) = \nu_{P_\infty}(\alpha) = -2$, dostáváme

$$(\alpha+1) = 1 \cdot P_{(1,0)} + 1 \cdot P_{(1,1)} - 2 \cdot P_\infty.$$

(b) Opět díky 11.5 je $\deg((\alpha)_+) = \sum_{P:\ \alpha \in P} \nu_P(\alpha) \deg P = [L : \mathbb{F}_2(\alpha)] = 2$ a α není prvek P pro žádné $P \in \mathbb{P}_{L/K}{}^{(1)}$, tudíž existuje jediné P splňující $\alpha \in P$ a $\deg P = 2$, což znamená, že

$$(\alpha) = 1 \cdot P_\alpha - 2 \cdot P_\infty.$$

Tvrzení 11.8. Pro $K = \tilde{K}$ a $A, B \in \mathrm{Div(L/K)}$ platí:

(D5) $l(A) \geq 1 \Leftrightarrow$ existuje $s \in L^*$ tak, že $A + (s) \geq \underline{0}$,
(D6) $l(B-A) \geq 1 \Leftrightarrow$ existuje $A' \in \mathrm{Div(L/K)}$ tak, že $A \sim A' \leq B$,
(D7) jestliže $l(B-A) \geq 1$, pak $\deg A - l(A) \leq \deg B - l(B)$,
(D8) jestliže $\deg A < 0$, pak $l(A) = 0$,
(D9) $\mathcal{L}((s)) = Ks^{-1} = \{ks^{-1} \mid k \in K\}\ \forall s \in L^*$.

Poznámka 11.9. Nechť $K = \tilde{K}$ a pro $A \in \mathrm{Div(L/K)}$ platí, že $\deg A = 0$. Potom

(1) $l(A) \in \{0, 1\}$,
(2) $l(A) = 1 \Leftrightarrow A \in \mathrm{Princ(L/K)}$.

Věta 11.10 (Riemann)**.** Jestliže $K = \tilde{K}$, potom existuje celé γ splňující $\deg(A) - l(A) < \gamma$ pro každý divizor $A \in \mathrm{Div(L/K)}$.

Definice. Nejmenší celé γ, pro něž $\deg(A) - l(A) < \gamma$ pro každý divizor $A \in \mathrm{Div(L/K)}$, jehož existenci zaručuje Věta 11.10, se nazývá *rod* (genus) AFF L nad $\tilde{K}$.

Do konce kapitoly budeme předpokládat, že $K = \tilde{K}$ a rod AFF budeme v následujícím vždy značit písmenem g.

Pozorování. Nechť $K = \tilde{K}$ a $A, D \in \mathrm{Div(L/K))}$ a platí, že $\deg(D) - l(D) = g - 1$.

(E1) $g > \deg(\underline{0}) - l(\underline{0}) = -1$, proto $g \geq 0$,
(E2) $\deg(A-D) - l(A-D) \leq g-1$, proto $l(A-D) \geq \deg(A) - \deg(D) - g + 1$,
(E3) jestliže $\deg(A) \geq \deg(D) + g$, pak $l(A-D) \geq 1$,
(E4) pokud $l(A-D) \geq 1$ nebo $D \leq A$ pak díky (D4) a (D6) $g - 1 = \deg(D) - l(D) \leq \deg(A) - l(A) \leq g - 1$, proto $\deg(A) - l(A) = g - 1$.

Poznámka 11.11. Existuje takové celé γ, že pro každý $A \in \mathrm{Div(L/K)}$ splňující $\deg(A) \geq \gamma$ platí, že $l(A) = \deg(A) - g + 1$.

T&N. Nechť $\mathbb{P} := \mathbb{P}_{L/K}$ a uvažujme kartézskou mocninu $L^{\mathbb{P}}$ jako L-algebru s operacemi definovanými po složkách s neutrálním prvkem $\mathbf{1}$, kde $r \to r \cdot \mathbf{1} \in L^{\mathbb{P}}$ ztotožňuje prvky L s konstantami $L^{\mathbb{P}}$. Pak se $f \in L^{\mathbb{P}}$ nazývá *adèle*, je-li množina

$$\{P \in \mathbb{P} \mid f(P) \notin \mathcal{O}_P\} = \{P \in \mathbb{P} \mid \nu_P(f(P)) < 0\}$$

konečná a $\mathcal{A}_{L/K}$ označuje množinu všech adèle.

Nechť $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P \in \mathrm{Div(L/K)}$, pak

$$\mathcal{A}_{L/K}(A) := \{f \in L^{\mathbb{P}} \mid \nu_P(f(P)) + a_P \geq 0 \forall P \in \mathbb{P}\}.$$

Dále $i(A) := g - 1 - \deg(A) + l(A) \geq 0$ se nazývá *index specializace* A. A se nazývá *speciální* jestliže $i(A) > 0$ a A se nazývá *nespeciální*, jestliže $i(A) = 0$.

Připomeňme, že $P^k = \{r \in L \mid \nu_P(r) \geq k\}$ pro každé $k \in \mathbb{Z}$, $P \in \mathbb{P}_{L/K}$.

Pozorování. Nechť $r \in L$, $f \in L^{\mathbb{P}_{L/K}}$, $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P \in \mathrm{Div(L/K)}$ a $s \in L^*$.

(F1) $f \in \mathcal{A}_{L/K} \Leftrightarrow \nu_P(f(P)) < 0$ pro konečně mnoho $P \in \mathbb{P}_{L/K}$, tudíž $r \in \mathcal{A}_{L/K}$ díky 10.5
(F2) $f \in \mathcal{A}_{L/K}(A) \Leftrightarrow \nu_P(f(P)) \geq -a_p$ pro všechna $P \in \mathbb{P}_{L/K}$,
(F3) $\mathcal{A}_{L/K}$ je podalgebra L-algebry $L^{\mathbb{P}_{L/K}}$,
(F4) $\mathcal{A}_{L/K}(A) = \prod_{P \in \mathbb{P}_{L/K}} P^{-a_P}$ je podprostor vektorového prostoru $\mathcal{A}_{L/K}$ nad tělesem K a $\mathcal{A}_{L/K}(A) \cap L = \mathcal{L}(A)$,
(F5) $\mathcal{A}_{L/K} = \bigcup_{B \in \mathrm{Div(L/K)}} \mathcal{A}_{L/K}(B)$.

Poznámka 11.12. Nechť $A = \sum_{P \in \mathbb{P}_{L/K}} a_p P$, $B = \sum_{P \in \mathbb{P}_{L/K}} b_p P \in \mathrm{Div(L/K)}$ a $s \in L^*$.

(1) Jestliže $A \leq B$, pak $\mathcal{A}_{L/K}(A) \subseteq \mathcal{A}_{L/K}(B)$ a $\dim_K(\mathcal{A}_{L/K}(B)/\mathcal{A}_{L/K}(A)) = \deg(B - A)$,
(2) jestliže $A \leq B$, pak $\dim_K((\mathcal{A}_{L/K}(B) + L)/(\mathcal{A}_{L/K}(A) + L)) = i(A) - i(B)$,
(3) $\mathcal{A}_{L/K}(A) \cap \mathcal{A}_{L/K}(B) = \mathcal{A}_{L/K}(\min(A, B))$, $\mathcal{A}_{L/K}(A) + \mathcal{A}_{L/K}(B) = \mathcal{A}_{L/K}(\max(A, B))$,
(4) $\dim_K(\mathcal{A}_{L/K}/(\mathcal{A}_{L/K}(A) + L)) = i(A)$,
(5) $\mathcal{A}_{L/K} = \mathcal{A}_{L/K}(A) + L \Leftrightarrow i(A) = 0$,
(6) $s\mathcal{A}_{L/K}(A) = \mathcal{A}_{L/K}(A - (s))$.

Poznámka 11.13. Nechť $\mathcal{S} \subsetneqq \mathbb{P}_{L/K}$, , $P_1, \ldots, P_n \in \mathcal{S}$ jsou po dvou různá místa, $a_1, \ldots a_n \in L$ a $z \in \mathbb{Z}$. Pak existuje $t \in L$ tak, že $\nu_{P_i}(t - a_i) > z$ pro všechna $i = 1, \ldots, n$ a $\nu_P(t) \geq 0$ pro všechna $P \in \mathcal{S} \setminus \{P_1 \ldots, P_n\}$.

Věta 11.14 (Silná aproximační věta)**.** Nechť $\mathcal{S} \subsetneqq \mathbb{P}_{L/K}$, , $P_1, \ldots, P_n \in \mathcal{S}$ jsou po dvou různá místa. Pokud $a_1, \ldots a_n \in L$ a $z_1, \ldots, z_n \in \mathbb{Z}$, potom existuje takové $s \in L$, že $\nu_{P_i}(s - a_i) = z_i$ pro všechna $i = 1, \ldots, n$ a $\nu_P(s) \geq 0$ pro všechna $P \in \mathcal{S} \setminus \{P_1 \ldots, P_n\}$.

12. Weilovy diferenciály

Opět předpokládáme, že L je AFF nad K rodu g a $\tilde{K}$ je jeho těleso konstant.

T&N. Nechť $A \in \mathrm{Div(L/K)}$. Pak

$$\Omega_{L/K}(A) := (\mathcal{A}_{L/K}(A) + L)^o_K = \{\omega \in {\mathcal{A}_{L/K}}^* \mid \omega(\mathcal{A}_{L/K}(A) + L) = 0, \}$$

$$\Omega_{L/K} := \bigcup_{B \in \mathrm{Div(L/K)}} \Omega_{L/K}(B) = \{\omega \in {\mathcal{A}_{L/K}}^* \mid \omega(L) = 0, \exists B \in \mathrm{Div(L/K)} : \omega(\mathcal{A}_{L/K}(B)) = 0\}$$

Prvky $\Omega_{L/K}$ se nazývají *Weilovy diferenciály* (AFF L nad K).

Pozorování. Nechť $A, B \in \mathrm{Div(L/K)}$ a $s \in L^*$.

(1) $\dim_K(\Omega(A)) = \dim(\mathcal{A}_{L/K}/(\mathcal{A}_{L/K}(A) + L) = i(A)$ (1.4(2), 11.12(4)),
(2) $A \leq B \Rightarrow \mathcal{A}_{L/K}(A) \subseteq \mathcal{A}_{L/K}(B) \Rightarrow \Omega_{L/K}(B) \subseteq \Omega_{L/K}(A)$ (1.4(3), 11.12(1)),
(3) $\Omega_{L/K}(A) \cap \Omega_{L/K}(B) = (\mathcal{A}_{L/K}(A) + \mathcal{A}_{L/K}(B) + L)^o = \Omega_{L/K}(\max(A, B))$,
$\Omega_{L/K}(A) + \Omega_{L/K}(B) = ((\mathcal{A}_{L/K}(A) + L) \cap (\mathcal{A}_{L/K}(B) + L))^o \subseteq \Omega_{L/K}(\min(A, B))$
(1.4(1),(4), 11.12(3)),
(4) $s\Omega_{L/K}(A) = (s^{-1}(\mathcal{A}_{L/K}(A))^o = \Omega_{L/K}(A + (s)$ (1.5(3), 11.12(6)),
(5) Pro každé $\omega \in \Omega_{L/K}$ definujme předpisem $0 \cdot \omega = 0$ a $(s \cdot \omega)(t) = \omega(st)$ $\forall s \in L^*$. Potom je $\Omega_{L/K}$ vektorový prostor nad tělesem L díky 1.5, (3) a (4).

Poznámka 12.1. Jestliže $\mathbb{P}^{(1)}_{L/K} \neq \emptyset$, pak $K = \tilde{K}$

Celý zbytek kapitoly budeme předpokládat, že je L nad K plně konstantní AFF, tedy $K = \tilde{K}$.

Poznámka 12.2. Nechť $\omega \in \Omega_{L/K} \setminus \{0\}$. Potom existuje právě jeden $W \in \mathrm{Div(L/K)}$ splňující podmínky $\omega(\mathcal{A}_{L/K}(W)) = 0$ pro každé $A \in \mathrm{Div(L/K)}$ platí implikace $\omega(\mathcal{A}_{L/K}(A)) = 0$, pak $A \leq W$.

T&N. Divizor W z 12.2 jednoznačně určený Weilovým diferenciálem ω se nazývá the *kanonický divizor* diferenciálu ω a značíme ho (ω).

Poznámka 12.3. Nechť $\omega, \tilde{\omega} \in \Omega_{L/K} \setminus \{0\}$, $A \in \mathrm{Div(L/K)}$ a definujme zobrazení $\Psi_\omega : L \to \Omega_{L/K}$ podmínkou $\Psi_\omega(s) = s \cdot \omega$ pro každé $s \in L$. Potom platí:

(1) jestliže $s \in L^*$, pak $(s\omega) = (s) + (\omega)$,
(2) Ψ_ω je lineární vnoření nad tělesem L a tedy i nad K a $\Psi_\omega(\mathcal{L}((\omega) - A)) \subseteq \Omega_{L/K}(A)$,
(3) existuje takový $B \in \mathrm{Div(L/K)}$, že $\Psi_\omega(\mathcal{L}((\omega) - B)) \cap \Psi_{\tilde{\omega}}(\mathcal{L}((\tilde{\omega}) - B)) \neq 0$.

Věta 12.4. Pro $\Omega_{L/K}$ platí:

(1) $\dim_L(\Omega_{L/K}) = 1$,
(2) je-li $\omega \in \Omega_{L/K} \setminus \{0\}$ a $A \in \mathrm{Div(L/K)}$, pak $\Psi_{\omega,A} : \mathcal{L}((\omega) - A) \to \Omega_{L/K}(A)$ dané podmínkou $\Psi_{\omega,A}(s) = s\omega$ je izomorfismus vektorových prostorů nad K.

Důsledek 12.5. Všechny kanonoické divizory tvoří právě jednu rozkladovou třídu modulo Princ(L/K) (tedy pro kanonický divizor W platí, že $A \sim W \Leftrightarrow A$ je kanonický).

Věta 12.6 (Riemannova-Rochova)**.** Jestliže W je kanonický divizor, pak

$$l(A) = \deg A + l(W - A) + 1 - g$$

pro každé $A \in \mathrm{Div(L/K)}$.

Důsledek 12.7. Je-li $W \in \mathrm{Div(L/K)}$ kanonický divizor, pak $l(W) = g$, $\deg W = 2g - 2$, $i(W) = 1$.

Důsledek 12.8 (Hlavní důsledek Riemannovy-Rochovy věty)**.** Jestliže $\deg A \geq 2g - 1$ pro $A \in \mathrm{Div(L/K)}$, pak $l(A) = \deg A + 1 - g$.

Poznámka 12.9. Pro $A \in \mathrm{Div(L/K)}$ platí:

(1) jestliže $\deg A = 2g - 2$ a $l(A) \geq g$, pak je A kanonický,
(2) jestliže $g = 1$, pak A je kanonický $\Leftrightarrow A$ je hlavní .

Tvrzení 12.10. Jestliže $A, B \in \mathrm{Div(L/K)}$ a $g = 0$, pak:

(1) A je hlavní $\Leftrightarrow \deg A = 0$,
(2) $A \sim B \Leftrightarrow \deg A = \deg B$,
(3) A je kanonický $\Leftrightarrow \deg A = -2$.

13. Eliptické funkční těleso

Nechť L je AFF nad K rodu g.

Poznámka 13.1. Nechť $P \in \mathbb{P}^{(1)}_{L/K}$, $h \in \mathbb{Z}$, $h \geq 0$, $s \in L$. Potom

(1) $s \in \mathcal{L}(iP) \setminus \mathcal{L}((i-1)P) \Leftrightarrow (s)_- = iP$, kde $i \geq 1$,
(2) jestliže existuje $k \geq 0$ tak, že $l(iP) \geq i - h + 1$ pro každé $i \geq k$, pak $g \leq h$,
(3) jestliže pro každé $i \geq h+1$ existuje $s_i \in L$ tak, že $(s_i)_- = iP$, pak $g \leq h$.

Příklad 13.2. Připomeňme, že těleso $K(x)$ je AFF nad K a díky 4.9 máme

$$\mathbb{P}_{K(x)/K} = \{P_p \mid p \in K[x] \text{ je ireducibilní monický}\} \cup \{P_\infty\}$$

kde P_p je maximální ideál lokalizace $K[x]_{((p))}$ s $\nu_{P_p} = \nu_p$ a P_∞ je dané diskrétní valuací $\nu_\infty(\frac{a}{b}) = \deg(b) - \deg(a)$. Potom $\nu_p(x^i) \geq 0$ pro každé $i \geq 0$ a p ireducibilní monický a dále $\nu_\infty(x^i) = -i$ pro každé $i \geq 0$, proto $(x^i)_- = iP_\infty$. Tudíž $K(x)$ je díky 13.1(3) rodu 0.

Pro každé $s \in K(x)^*$ existuje $k \in K^*$, ireducibilní po dvou neasociované polynomy $p_i \in K[x]$ a exponenty $e_i \in \mathbb{Z}$, pro něž $s = k\prod_i p_i^{e_i}$. Označíme-li $d = \sum_i e_i \deg p_i$, pak máme hlavní divizor $(s) = \sum_i e_i P_{p_i} - dP_\infty$ a platí $e_i = \nu_{p_i}(s) = \nu_{P_{p_i}}(s)$, což nám dává postup, jak najít prvek tělesa L určující divizor stupně nula, jehož existenci nám pro AFF rodu 0 zaručuje Tvrzení 12.10(1).

Tvrzení 13.3. Nechť $\mathbb{P}^{(1)}_{L/K} \neq \emptyset$. Pak $g = 0 \Leftrightarrow$ existuje $s \in L$ tak, že $L = K(s)$

Definice. AFF L nad K se nazývá *eliptické funkční těleso* (EFF), jestliže je rodu 1 a $\mathbb{P}^{(1)}_{L/K} \neq \emptyset$.

Pozorování. Nechť L je EFF a $P \in \mathbb{P}^{(1)}_{L/K}$, pak je L plně konstantní podle 12.1, a $l(iP) = \deg(iP) = i$ pro každé $i \geq 1$ díky 12.8, proto $K = \mathcal{L}(1P) \subsetneqq \mathcal{L}(2P) \subsetneqq \mathcal{L}(3P)$ podle 13.1(1).

Poznámka 13.4. Je-li L EFF nad K a $P \in \mathbb{P}^{(1)}_{L/K}$, potom pro každé $u \in \mathcal{L}(2P) \setminus \mathcal{L}(1P)$ a pro každé $v \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$ existuje WEP $w \in K[x,y]$ a $\lambda \in K^*$ tak, že L je dané rovností $w(\lambda u, \lambda v) = 0$.

Pozorování. Nechť $w \in K[x,y]$ je WEP a L je dané rovností $w(\alpha,\beta) = 0$. Potom

(1) existuje právě jedno $P = P_\infty \in \mathbb{P}^{(1)}_{L/K}$ tak, že $\nu_P(\alpha) = -2$, $\nu_P(\beta) = -3$, $\nu_Q(\alpha) \geq 0$, $\nu_Q(\beta) \geq 0$ pro všechna $Q \in \mathbb{P}_{L/K} \setminus \{P_\infty\}$ díky 10.6,
(2) $(\alpha)_- = 2P_\infty$, $(\beta)_- = 3P_\infty$, $\mathcal{O}_{P_\infty} \cap K[\alpha,\beta] = K$ a $K[\alpha,\beta] \subseteq \mathcal{O}_Q$ pro všechna $Q \in \mathbb{P}_{L/K} \setminus \{P_\infty\}$ podle (1) a 9.7,
(3) jestliže w je hladký v $V_w(K)$, pak $\mathbb{P}^{(1)}_{L/K} = \{P_\infty\} \cup \{P_\gamma \mid \gamma \in V_w(K)\}$ podle 10.7.

Tvrzení 13.5. Pro $w \in K[x,y]$ WEP a AFF L nad K dané rovností $w(\alpha,\beta) = 0$

(a) buď $g = 1$ a L je EFF,
(b) nebo $g = 0$ a $l((0)) = 1$ a existuje $s \in L$ a polynomy $a, b \in K[x]$, pro něž $L = K(s)$, $\alpha = a(s)$, $\beta = b(s)$ a $\deg a = 2$, $\deg b = 3$.

Věta 13.6. Nechť L je AFF nad K dané rovností $w(\alpha,\beta) = 0$ pro WEP w. Pak L je EFF $\Leftrightarrow$ w je hladký na $V_w(K)$.

Příklad 13.7. (1) Nechť $w = y^2 + y + x^3 + 1 \in \mathbb{F}_2[x, y]$ je WEP z 10.8. Protože je w hladký v racionálních bodech $V_w(\mathbb{F}_2) = \{(1, 0), (1, 1))\}$, je podle 13.6 $\mathbb{F}_2(V_w)$ rodu 1, tedy EFF a $\mathbb{F}_2(s) \subsetneqq \mathbb{F}_2(V_w)$ pro každé $s \in \mathbb{F}_2(V_w)$

(2) Nechť $f = y^2 + x^3 + x + 1 \in \mathbb{F}_2[x, y]$ je WEP. Protože je f singulární v bodě $(1, 1) \in \mathbb{F}_2(V_f)$, je díky 13.6 rodu 0 a existuje takové $s \in \mathbb{F}_2(V_f)$, že $\mathbb{F}_2(s) = \mathbb{F}_2(V_f)$.

14. Asociativní zákon

V následujícím označme WEP $w = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)$.

Předpokládejme, že L je EFF nad K dané rovností $w(\alpha, \beta) = 0$. Potom je podle 13.6 w hladký na $V_w(K)$.

T&N. $\mathrm{Pic}^0(L/K) := \mathrm{Ker(deg)/Princ(L/K)}$ se nazývá *Picardova grupa*, $[A] := A + \mathrm{Princ(L/K)}$ označuje rozkladovou třídu grupy $\mathrm{Pic}^0(L/K)$ a zobrazení $\Psi_Q : \mathbb{P}^{(1)}_{L/K} \to \mathrm{Pic}^0(L/K)$ dané vztahem $\Psi_Q(P) := [P - Q]$ pro $Q \in \mathbb{P}^{(1)}_{L/K}$.

Poznámka 14.1. Nechť $P_1, P_2, Q \in \mathbb{P}^{(1)}_{L/K}$ a $A \in \mathrm{Div(L/K)}$.

(1) Jestliže $P_1 - P_2 \in \mathrm{Princ(L/K)}$, pak $P_1 = P_2$,
(2) jestliže $\deg A = 1$, pak existuje právě jedno místo $P \in \mathbb{P}^{(1)}_{L/K}$, pro něž $P - A \in \mathrm{Princ(L/K)}$,
(3) zobrazení Ψ_Q je bijekce.

T&N. Definujme pro libovolné $Q \in \mathbb{P}^{(1)}_{L/K}$ binární operaci $\oplus$ na $\mathbb{P}^{(1)}_{L/K}$ pravidlem $P_1 \oplus P_2 := \Psi_Q^{-1}(\Psi_Q(P_1) + \Psi_Q(P_2))$.

Pozorování. Jestliže $Q, P_0, P_1, \ldots, P_n \in \mathbb{P}^{(1)}_{L/K}$, pak

(1) $\mathbb{P}^{(1)}_{L/K}$ tvoří s operací $\oplus$ abelovskou grupu s neutrálním prvkem Q,
(2) Ψ_Q je grupový izomorfismus,
(3) $P_1 \oplus P_2 = P_0 \Leftrightarrow [P_1 + P_2] = [P_0 + Q]$,
(4) $P_1 \oplus \cdots \oplus P_n = P_0 \Leftrightarrow -P_0 + (1 - n)Q + \sum_{i=1}^{n} P_i \in \mathrm{Princ(L/K)}$,

T&N. Nechť $\hat{l} = cx + dy + e \in K[x, y]$ pro $c, d, e \in K$, kde $(c, d) \neq (0, 0)$. Potom $l = \hat{l} + (w) \in K[V_w] = K[\alpha, \beta]$ se pro $\alpha = x + (w), \beta = y + (w)$ nazývá *přímka* reprezentovaná $\hat{l}$. Řekneme, že l *prochází* bodem γ jestliže $\gamma \in V_{\hat{l}}$.

Tvrzení 14.2. Nechť $\gamma = (\gamma_1, \gamma_2) \in V_w(K)$ a $\hat{l} \in K[x, y]$ reprezentuje přímku $l = \hat{l} + (w) \in K[V_w]$.

(1) Pokud $\hat{l} \in (x - \gamma_1)$, pak existuje právě jedno $\delta = (\delta_1, \delta_2) \in V_w(K)$ splňující $(l) = P_\gamma + P_\delta - 2P_\infty$, a navíc platí, že $\gamma_1 = \delta_1$ a $\delta_2 = -a_1\gamma_1 - a_3 - \gamma_2$,
(2) pokud $\hat{l} \in (y - \lambda x - \mu)$ a l prochází γ, pak $(l)_- = 3P_\infty$ a
   (a) buď existuje jediné $P \in \mathbb{P}_{L/K}$ stupně 2 tak, že $(l)_+ = P_\gamma + P$, $\hat{l} \notin (t_\gamma(w))$ a $V_w(K) \cap V_{\hat{l}} = \{\gamma\}$,
   (b) nebo existují jednoznačně (až na pořadí) určené body $\delta = (\delta_1, \delta_2), \eta = (\eta_1, \eta_2) \in V_w(K)$ tak, že $(l)_+ = P_\gamma + P_\delta + P_\eta$, $V_w(K) \cap V_{\hat{l}} = \{\gamma, \delta, \eta\}$, $\eta_1 + \gamma_1 + \delta_1 = -a_2 + \lambda^2 + a_1\lambda$, navíc $\hat{l} \in (t_\gamma(w)) \Leftrightarrow \gamma \in \{\delta, \eta\}$.

Definice. Uvažujme na ${\mathbb{P}_{L/K}}^{(1)}$ grupovou strukturu danou Ψ_{P_∞}. Položme $E(K) = V_w(K) \cup \{\infty\}$ a definujme operace $\oplus$, $\ominus$ na $E(K)$:

$$\gamma \oplus \delta = \eta \Leftrightarrow P_\gamma \oplus P_\delta = P_\eta \Leftrightarrow [P_\gamma + P_\delta] = [P_\eta + P_\infty],$$
$$\ominus\gamma = \delta \Leftrightarrow P_\gamma \oplus P_\delta = P_\infty \Leftrightarrow [P_\gamma + P_\delta] = [2P_\infty].$$

Věta 14.3. $(E(K), \oplus, \ominus, \infty)$ je komutativní grupa a pro $\gamma = (\gamma_1, \gamma_2)$, $\delta = (\delta_1, \delta_2)$, $\eta = (\eta_1, \eta_2) \in V_w(K)$ platí:

(1) $\ominus\gamma = (\gamma_1, -\gamma_2 - a_1\gamma_1 - a_3)$,

(2) jestliže $\gamma \neq \ominus\delta$ a $\gamma \oplus \delta = \eta$, pak
$\eta = (-\gamma_1 - \delta_1 + \lambda^2 + a_1\lambda - a_2, \lambda(\gamma_1 - \eta_1) - \gamma_2 - a_1\eta_1 - a_3)$, kde

(a) $\lambda = \frac{\delta_2 - \gamma_2}{\delta_1 - \gamma_1}$ jestliže $\gamma_1 \neq \delta_1$,

(b) $\lambda = \frac{3\gamma_1^2 + 2a_2\gamma_1 - a_1\gamma_2 + a_4}{2\gamma_2 + a_1\gamma_1 + a_3}$ jestliže $\gamma_1 = \delta_1$.

Důsledek 14.4. Je-li $K \subseteq F \subseteq \overline{K}$ rozšíření těles, pak $E(K)$ je podgrupa $E(F)$.

Příklad 14.5. Nechť $w = y^2 - x^3 - 1 \in \mathbb{F}_5[x]$ je WEP. Protože $(x^3+1)' = 3x^2$ a 0 není kořenem $x^3 + 1$, je w hladký.

Snadno určíme $E(\mathbb{F}_5) = \{(0,1), (0,4), (4,0), (2,2), (2,3), \infty\}$. Protože je $E(\mathbb{F}_5)$ komutativní šestiprvková grupa, víme, že $E(\mathbb{F}_5) \cong \mathbb{Z}_6$. Pomocí 14.3 spočítáme:
$(0,1) = \ominus(0,4)$ $(4,0) \oplus (4,0) = (2,2) \oplus (2,3) = \infty$ a $(0,4) \oplus (4,0) = (2,3)$.
Najdeme-li pro stejný hladký WEP grupu $E(\mathbb{F}_{25})$, pak z 14.4 víme, že $E(\mathbb{F}_5) \leq E(\mathbb{F}_{25})$.

15. Projektivní křivky

Předpokládejme, že $n \geq 1$, K je komutativní těleso a $\overline{K}$ je jeho algebraický uzávěr.

T&N. Označme $a = (a_0 : a_1 : \cdots : a_n) = \mathrm{LO}_K((a_0, a_1, \ldots, a_n)) \subset K^{n+1}$ projektivní bod projektivního prostoru

$$\mathbb{P}^n(K) = \{(a_0 : a_1 : \cdots : a_n) \mid (a_0, a_1, \ldots, a_n) \in K^{n+1} \setminus \{0\}\}$$

s homogenními souřadnicemi $(a_0 : a_1 : \cdots : a_n)$ a položme $\mathbb{P}^n := \mathbb{P}^n(\overline{K})$.

Označme $\mathcal{H}_d = \mathrm{LO}_K(x_0^{i_0} \ldots x_n^{i_n} \mid \sum_{j=0}^n i_j = d)$. O každém polynomu $F \in \mathcal{H}_d$ řekneme, že je to *homogenní polynom* stupně d a $K[X_0, \ldots, X_n] = \bigcup_{d \geq 0} \mathcal{H}_d$ značí množinu všech homogenních polynomů. Položme

$$K(\mathbb{P}^n) := \{\frac{G}{H} \mid H, G \in K[X_0, \ldots, X_n] \setminus \{0\} : \deg H = \deg G\} \cup \{0\}.$$

Množinu (racionálních) homogenních nul polynomu F značíme

$$V_F = \{(a_0 : a_1 : \cdots : a_n) \in \mathbb{P}^n \mid F(a_0, \ldots, a_n) = 0\} \quad (V_F(K) = V_F \cap \mathbb{P}^n(K)).$$

Jestliže $F \in K[X_0, \ldots, X_n]$ a $a \in V_F$, řekneme, že je F *hladký* v bodě $a \in V_F$, pokud $\exists j$ splňující $\frac{\partial F}{\partial x_i}(a_0, \ldots, a_n) \neq 0$, v opačném případě je F v bodě a *singulární*.

Je-li F ireducibilní, nazýváme V_F *projektivní ireducibilní křivka* její funkční těleso je

$$K(V_F) := \{\frac{G + (F)}{H + (F)} \mid H, G \in K[X_0, \ldots, X_n] \setminus (F) : \deg H = \deg G\} \cup \{0\}.$$

Pozorování. Nechť $d \geq 0$, $i_0, \ldots, i_n \geq 0$ a $F \in \mathcal{H}_d \subseteq K[X_0, X_1, \ldots, X_n]$. Potom

(1) $\sum_{j=0}^{n} i_j = d \Rightarrow \sum_{j=0}^{n} \frac{\partial(\prod x_j^{i_j})}{\partial x_j} x_j = d \prod_{j=0}^{n} x_j^{i_j}$,
(2) $\sum_{j=0}^{n} \frac{\partial F}{\partial x_j} x_j = dF$,
(3) $K(\mathbb{P}^n)$ je podtěleso $K(x_0, \ldots, x_n)$,
(4) je-li F ireducibilní, pak je $K(V_F)$ podtěleso podílového tělesa oboru $K[x_0, \ldots, x_n]/(F)$.

T&N. Nechť $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ a $a = (a_1, \ldots, a_n) \in \mathbb{A}^n$. Definujme

$$\overline{f} := X_0^{\deg f} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}),$$

$$\overline{0} := 0 \in K[X_0, X_1, \ldots, X_n], \quad \overline{a} := (1 : a_1 : \cdots : a_n) \in \mathbb{P}^n$$

Dále $\forall j$ značme $p_j : \mathbb{P}^n \to \mathbb{A}^n$ parciální zobrazení dané vztahem

$$p_j(a_0 : a_1 : \cdots : a_n) = (\frac{a_0}{a_j}, \ldots, \frac{a_{j-1}}{a_j}, \frac{a_{j+1}}{a_j}, \ldots, \frac{a_n}{a_j})$$

pro $a_j \neq 0$ a zobrazení $\pi_j : K[X_0, X_1, \ldots, X_n] \to K[x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n]$ dané vztahem

$$\pi_j(F) = F(x_1, \ldots, x_{j-1}, 1, x_{j+1}, \ldots, x_n).$$

Pozorování. Nechť $f, g \in K[x_1, \ldots, x_n]$, $k = \deg f$, $l = \deg g$ a $s = k + l - (\deg(f + g))$.
(5) $\overline{f} \in K[X_0, X_1, \ldots, X_n]$, $\overline{fg} = \overline{f} \cdot \overline{g}$ a $\pi_0(\overline{f}) = f$,
(6) $0 \notin \{f, g, f + g\} \Rightarrow X_0^l \overline{f} + X_0^k \overline{g} = X_0^s \overline{(f + g)}$,
(7) f je ireducibilní $\Leftrightarrow$ $\overline{f}$ je ireducibilní,
(8) $a \in V_f \Leftrightarrow \overline{a} \in V_{\overline{f}}$,
(9) $p_0(V_{X_0^t \overline{f}}) = V_f \ \forall t \geq 0$.

Poznámka 15.1. Nechť $f \in K[x_1, \ldots, x_n] \setminus \{0\}$ a $a \in V_f$. Potom f je hladký v $a \Leftrightarrow \overline{f}$ je hladký v $\overline{a}$.

Tvrzení 15.2. Nechť $f \in K[x_1, x_2]$ je ireducibilní a $F = \overline{f}$. Definujme zobrazení $\epsilon_f : K(V_f) \to K(V_F)$ a $\epsilon : K(x) \to K(\mathbb{P}^1)$ pravidly $\epsilon_f(0) = \epsilon(0) = 0$ a

$$\epsilon_f\left(\frac{g + (f)}{h + (f)}\right) = \frac{X_0^{\deg(h)} \overline{g} + (F)}{X_0^{\deg(g)} \overline{h} + (F)} \quad \text{a} \quad \epsilon\left(\frac{g}{h}\right) = \frac{X_0^{\deg(h)} \overline{g}}{X_0^{\deg(g)} \overline{h}}.$$

pak ϵ_f a ϵ jsou K-izomorfismy těles.

Důsledek 15.3. $K(\mathbb{P}^1)$ a $K(V_{\overline{f}})$ jsou AFF nad K pro každý ireducibilní polynom $f \in K[x_1, x_2]$.

T&N. Pro $A, B, G \in K[X_0, X_1] \setminus \{0\}$ definujme

$$\nu_G(A) := \max\{e \geq 0 \mid G^e \text{ dělí } A\}, \quad \nu_G\left(\frac{A}{B}\right) := \nu_G(A) - \nu_G(B), \quad \nu_G(0) = \infty.$$

Důsledek 15.4. Nechť ν je normalizovaná diskrétní valuace na AFF $K(\mathbb{P}^1)$ nad K. Potom
(1) existuje ireducibilní polynom $G \in K[X_0, X_1]$ splňující $\nu = \nu_G$,
(2) stupeň místa $\{U \in K(\mathbb{P}^1) \mid \nu_G(U) > 0\}$ je roven $\deg G$,

(3) zobrazení $(a_0 : a_1) \to \{U \in K(\mathbb{P}^1) \mid \nu_{a_0X_1 - a_1X_0}(U) > 0\}$ je bijekce $\mathbb{P}^1(K) \to \mathbb{P}^1_{K(\mathbb{P}^1)/K}$.

T&N. Pro $F \in K[X_0, X_1, X_2]$ ireducibilní a $a \in V_F \subseteq \mathbb{P}^2$ definujme

$$\mathcal{O}_a = \{\frac{G + (F)}{H + (F)} \in K(V_F) \mid H(a) \neq 0\}$$

$$P_a = \{\frac{G + (F)}{H + (F)} \in \mathcal{O}_a \mid G(a) = 0\}$$

Pozorování. Nechť $a = (a_0 : a_1 : a_2)$ a $F \in K[X_0, X_1, X_2]$ je ireducibilní.

(1) pokud $\exists f \in K[x_1, x_2]$ a $\exists \gamma \in \mathbb{A}^2$ splňující $F = \overline{f}$ a $\frac{g+(f)}{h+(f)} \in K(V_f)$, pak $h(\gamma) \neq 0 \Leftrightarrow \overline{h}X_0^{\deg g}(\overline{\gamma}) \neq 0$ a dále $g(\gamma) = 0 \Leftrightarrow \overline{g}X_0^{\deg h}(\overline{\gamma}) = 0$, proto podle 15.2 $\epsilon_f(P_\gamma) = P_{\overline{\gamma}}$,
(2) jestliže $F \neq \overline{f}$ pro žádné $f \in K[x_1, x_2] \Rightarrow F = \lambda X_0$ pro nějaké $\lambda \in K^* \Rightarrow K(V_F) = K(V_{X^0}) \cong K(V_{x_2}) \cong K(\mathbb{P}^1)$ díky 15.2.

Věta 15.5. Nechť $F \in K[X_0, X_1, X_2]$, je ireducibilní, $a \in V_F$ a $P \in \mathbb{P}_{K(V_F)/K}$. Potom

(1) existuje $b \in V_F$ tak, že $P_b \subseteq P$,
(2) jestliže $\deg P = 1$ a $P_a \subseteq P$, pak $a \in V_F(K)$,
(3) jestliže F je hladký v $a \in V_F(K)$ a $P_a \subseteq P$, pak $P_a = P$ a $\deg P_a = 1$.