1. DISKRÉTNY VALUAČNÝ OBOR

Def: LOKÁLNY OKRUH R

$\Leftrightarrow$ má práve jeden nenulový maximálny ideál

$\Leftrightarrow$ $R \setminus R^*$ je ideál

- $R \setminus R^*$ je ideál $\Rightarrow$ je maximálny, pretože pridaním invertibilného prvku dostaneme R
- $a \in R \setminus R^* \Rightarrow aR \neq R \Rightarrow$ (?ZBN) $aR \subseteq M$, M maximálny $\Rightarrow$ je jediný $\Rightarrow a \in M$ $\forall R \setminus R^*$.

Def: LOMENÝ IDEÁL: R okruh, F jeho podielové ~~nadteleso~~ teleso. Lomený ideál je R-modul v ňom (prenásobíme ľubovoľným na ľavo a $\cdot R$)

1.2 T: R lokálny OIHI, F podielové nadteleso, $M = aR = R \setminus R^*$. Potom $\dots a^{-1}R \supsetneq a^{-1}R \supsetneq R \supsetneq aR \supsetneq \dots$ sú práve všetky lomené ideály F.

Navyše $a^{i-1}R \setminus a^iR = a^{i-1}R^*$ a $\forall b \in F \; \exists! i: b \in a^iR^*$.

1 ⊇: $a^iR \supseteq a^{i-1}R$ triviálne ($\supseteq$ aS)

$\not\subseteq$: $a^iR = a^{i-1}R \overset{\cdot F}{\Rightarrow} R = aR$ ↯

$a^{i-1}R = a^{i-1}R^* \cup a^{i-1}M = a^{i-1}R^* \cup a^iR$

$\not\supseteq$: $a^{i-1}R^* \cap a^iR \neq 0 \Rightarrow R^* \cap aR \neq \emptyset$ ↯ $b(ar-1)=0$

$\forall$: $\exists$: $\bigcap_{i \in \mathbb{N}_0} a^iR = I \neq 0 \Rightarrow aI = I \overset{\text{OIHI}}{\Rightarrow} abR = bR \Rightarrow ab = b \Rightarrow ar = 1$ ↯

$\Rightarrow \forall r \in R \; \exists! i \geq 0: r \in a^iR$. $b = \frac{k}{s} = \frac{a^i r_1}{a^j s_1} = a^{(i-j)} t_1$, $t_1 \in R^*$.

Def Zobrazenie $v: F \to \mathbb{Z}_\infty$, F teleso sa nazýva <u>diskrétna valuácia</u>, ak

(i) $v(xy) = v(x) + v(y)$

(ii) $v(x+y) \geq \min(v(x), v(y))$

(iii) $v(x) = \infty \Leftrightarrow x = 0$

1.3. C: Zobrazenie $v: F \to \mathbb{Z}_\infty$, F podielové nadteleso R (ide. OIHI), definované ako $v(x) = i$, kde $x \in a^iR^*$, $aR = R \setminus R^*$, je diskrétna valuácia.

1 $x \in a^iR^*$, $y \in a^jR^*$. $xy \in a^{(i+j)}R^* \Rightarrow v(xy) = i+j$, $x+y \in a^{\min(i,j)}R \Rightarrow$ (ii)

1.4. L: Ak $aR = R \setminus R^* = bR$, tak pre $x \in a^iR^* \Rightarrow x \in b^iR^*$ platí $i = j$.

1 $\cdot an = br \Rightarrow a^iR = b^ir^iR = b^iR$

~~1.5 T: F teleso, v diskr. valuácia R okruh celých prvkov, b~~ ... ~~dôkaz~~

1.5.L: F teleso, v dis. valuácia. Potom $R = \{a \in F \mid v(a) \geq 0\}$ je obsah, pre ktorý platí $R^* = \{a \in F \mid v(a) = 0\}$.

$v(a) \geq 0,\ v(b) \geq 0 \Rightarrow v(ab) = v(a) + v(b) \geq 0,\quad v(a+b) \geq \min\{v(a), v(b)\} \geq 0$

$\overset{\text{def}}{a|b} = 1 \Leftrightarrow v(a) + v(b) = 0 \Leftrightarrow v(a) = v(b) = 0 \Rightarrow a, b \in R \setminus R^*$

Def:
- F teleso. Obsah R je <u>valuačným obsahom F</u>, ak $\forall a \in F^*$ $a \in R \vee a^{-1} \in R$.
- Obsah R je <u>valuačný</u>, ak je val. obsahom svojho podtelesa nadtelesa.
- Obsah R je <u>diskrétny valuačný (DVR)</u>, ak je to obor integrity, pre ktorého pod. nadteleso F existuje disk. val. v taká, že $R = \{a \in F \mid v(a) \geq 0\}$.

DVR $\Rightarrow$ valuačný

1.6.L: R valuačný obor F. Potom pre $a \in F^*$ platí:
- práve jedna z možností $a \in R^*$, $a \in R$, $a^{-1} \in R$
- $R \setminus R^*$ je ideál R ($\Rightarrow R$ je lokálny obsah)
- Pre $I, J \subseteq F$ vlastné ideály platí $I \subseteq J$ alebo $J \subseteq I$.

i) triviálne z definície

ii) $R \setminus R^*$ uzavretá na $\cdot$: $ab \in R^* \Rightarrow a \in R^* \wedge b \in R^*$

uzavretá na $+$: $a+b \in R^* \Rightarrow \frac{a}{b} \vee \frac{b}{a} \in R \Rightarrow B \cup N \overset{i)}{\Rightarrow} \frac{b}{a} \in R \Rightarrow (\frac{b}{a}+1)b \in R^* \Rightarrow b \in R^*$

iii) 

$\not\exists$: $a \in I \setminus J$, $b \in J \setminus I \Rightarrow B \cup N \overset{i)}{\Rightarrow} \frac{a}{b} \in R \Rightarrow a = (\frac{a}{b})b \in J$ $\not\in$.

1.7.T: R je DVR $\Leftrightarrow R$ je lokálny OIHI

"$\Leftarrow$" 1.3.L

"$\Rightarrow$" R DVR $\Rightarrow R$ valuačný obor $\overset{1.6.L}{\Rightarrow} R$ lokálny.

Zostáva OIHI: $\not\exists$

Nech $I \subseteq R$ nie je hlavný ideál, $a \in I$ taký, že $v(a)$ je najmenšia možná.

Potom $aR \subseteq I$, vieme $b \in I \setminus aR$. 1.6 (iii) $\Rightarrow$ (b ∈ aR ⇒ aR ⊆ bR)

$\Rightarrow a = br \Rightarrow v(a) = v(b) + v(r) \Rightarrow v(r) = 0 \Rightarrow r \in R^* \Rightarrow aR = bR$ $\not\in$.

DVR je lok OIHI $\Rightarrow \forall b \in F^*$ sa dá napísať ako $a^i r$, $aR = RR^*$, $r \in R^*$ jednoznačne

$\Rightarrow v(b) = iv(a) + v(r) = iv(a) \Rightarrow$ valuácia je jednoznačne určená už na násobok

Def: Diskrétna valuácia sa nazýva <u>normalizovaná</u>, ak spĺňa
(iv) $\exists a \in R$: $v(a) = 1$

1.8.L: Nech $I \subsetneq R \setminus R^*$ je nějaký ideál lokálního oboru R, nech $a_0 \in I$.
Potom $\exists a_1, \dots, a_n \in I$, $r_1, \dots, r_n \in R \setminus R^*$ takové že $a_{i-1} = a_i r_i \quad \forall i \in \hat{1} \dots n$.

Indukcí, nech platí pro $n-1$: $a_{n-1} \in I$, $a_{n-1} = a_0 \underbrace{r_1 \cdots r_{n-2}}_{\in R \setminus R^*}$.
Vezmu $a_n \in I \setminus a_{n-1}R \Rightarrow a_n R \subsetneq a_{n-1} R \overset{1.6.(iii)}{\Rightarrow} a_{n-1} R \subseteq a_n R \Rightarrow a_{n-1} = a_n r$.
Potom $r \notin R^*$, protože $\not\downarrow$ potom $a_{n-1} R = a_n R$.

1.9.L: Nech $R \subseteq S \subseteq F$, kde F je podtěleso tělesa oborů R a S je obor.
Ať je R DVR, tak $R = S$ anebo $S = F$.

Dům. $aR = R \setminus R^*$. S je třeba nějaký ideál F, tzn. ať $S \neq R$, tak $S = a^{-k} R^* \Rightarrow$
$a^{-1} \in S \Rightarrow$ (S je obor) $a^i \in S \quad \forall i \in \mathbb{Z} \Rightarrow S = F$.

1.10.D: Nech R je DVR a $M = R \setminus R^*$. Potom

$$R^* = \{a^{-1} b \mid a, b \in M \setminus M^2\} = \{r \in R \mid \exists a, b \in R : aR = bR = M \wedge br = a\}$$

(R určuje $R \setminus R^*$ a naopak)

1.11.T: Nech R_i jsou DVR tělesa F a $M_i = R_i \setminus R_i^*$, $i \in \{1, 2\}$.
Ať $R_1 \subseteq R_2$ anebo $M_1 \subseteq M_2$, tak $R_1 = R_2$.

$M_1 \subseteq M_2 \overset{1.10.D}{\Rightarrow} R_1^* \subseteq R_2^* \Rightarrow R_1 \subseteq R_2$
$R_1 \subseteq R_2 \overset{1.9.L}{\Rightarrow} R_1 = R_2$

Def:
- $R \subseteq S$, R ideál v I. Ideál v S generovaný I značíme IS:
$$IS := \{\textstyle\sum a_i s_i \mid a_i \in I, s_i \in S\}$$
- $a \in S \setminus R$. Nejmenší podokruh S obsahující $R \cup \{a\}$ značíme $R[a]$:
$$R[a] := \{\textstyle\sum r_i a^i \mid r_i \in R\}$$

Pozn:
- Může za stat $I \subsetneq R$ a $IS = S$ ($\Leftrightarrow 1 \in IS$)
- $I \cdot R[a] = I[a] = \{\sum r_i a^i \mid r_i \in I\}$
- $R[a] = \operatorname{Im} \eta_a$, $\eta_a : R[x] \to R[a]$
$r \mapsto r$
$x \mapsto a$
- Může za stat $I \subsetneq R$ a $I[a] = R[a]$

1.12.T: Nech F je teleso obsahujúce obor R a I vlastný ideál v R. Potom existuje valuačný obor $\mathcal{O}$ telesa F taký, že

$$R \subseteq \mathcal{O} \subsetneq F \quad a \quad I\mathcal{O} \subseteq \mathcal{O} \setminus \mathcal{O}^*$$

Nech $\mathcal{Y}$ je množina všetkých obrubov S takých, že $R \subseteq S \subsetneq F$ a $IS \neq S$.

- $R \in \mathcal{Y} \Rightarrow \mathcal{Y} \neq \emptyset$
- $\mathcal{Y}$ je usporiadaná inklúziami
- $(S_\alpha)_{\alpha \in A}$ reťazec $\Rightarrow \bigcup S_\alpha$ obrub, označme S. Ak $IS = S \Rightarrow 1 \in IS \Rightarrow$

$\Rightarrow 1 \in IS_\alpha \Rightarrow IS_\alpha = S_\alpha$ ↯. Tj. $(S_\alpha)_{\alpha \in A}$ má horné ohraničenie.

ZORN: existuje maximálny prvok $\mathcal{O}$. Ukážeme, že je to hľadaný val. obor:

↯: Nech pre $a \in F^*$ $a \notin \mathcal{O}$ a $a^{-1} \notin \mathcal{O}$

Potom $\mathcal{O}[a]$, $\mathcal{O}[a^{-1}] \notin \mathcal{Y}$, pretože $\mathcal{O}$ je maximálny $\Rightarrow$

$\Rightarrow I\mathcal{O}[a] = \mathcal{O}[a] \Rightarrow 1 \in I\mathcal{O}[a]$ a (analogicky) $1 \in I\mathcal{O}[a^{-1}]$

$$\Rightarrow 1 = g_0 + \dots + g_m a^m = h_0 + \dots + h_n a^{-n}, \quad g_i, h_j \in I\mathcal{O}, \ 1 \notin I\mathcal{O}$$

Vezmime minimálne m a n, BUNV $n \leq m$. Potom ale

$$(1 - h_0) = (g_0 - h_0) g_0 + \dots + (g_0 h_0) g_m a^m, \quad (1 - h_0) = h_n a^{-1} + \dots + h_n a^{-n}$$

Takto dosadením sem dostaneme polynóm nenulového stupňa v a ⇒ ↯.

1.13.L: Nech $F \to \mathbb{Z}_\infty$ je diskrétna valuácia a $a, b \in F$ také, že $\nu(a) < \nu(b)$. Potom $\nu(a+b) = \nu(a)$.

$\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$

↯: $\nu(a+b) > \nu(a)$

$\nu(a) = \nu((a+b)-b) \geq \min\{\nu(a+b), \nu(-b)\} \Rightarrow \nu(a) \geq \nu(-b) = \nu(-1) + \nu(b)$ ↯.

2. ALGEBRAICKÉ FUNKČNÉ TELESO

Def: $K \leq F$ telesá. Prvok $\alpha \in F$ je *algebraický nad K*, ak $\exists p \in K[x]: p(\alpha) = 0$. Inak je *transcendentný*. V tom prípade $K[x] \simeq K[\alpha]$, $K(x) \simeq K(\alpha)$.

x, y, z budú označovať transcendentné prvky. Budeme skúmať $K \subseteq L \leq F$.

2.1.L: Nech $x \in F$ je transcendentné nad K. Prvky $f_i \in F$, $i \in \{1, \dots, n\}$ sú LZ nad $K(x) \iff$ sú LZ nad $K[x] \iff \exists p_i \in K[x]: \sum p_i f_i = 0$, kde $\exists j: x \nmid p_j$.

"$\Leftarrow$" vždy platí

"$\Rightarrow$" $\sum \frac{a_i}{b_i} f_i = 0$, $a_i, b_i \in K[x] \Rightarrow \sum q_i f_i = 0$, $p_i = \frac{a_i}{b_i} \prod_{j \neq i} b_j \Rightarrow \sum p_i f_i = 0$, vydelíme $\max_i x \mid f_i$

$x, y \in F$, obe transc. nad K.

$K[x] \simeq K[x_1]$ ale nemusí byť $K(x, y] \simeq K[x_1, x_2]$

$K[y] \simeq K[x_2]$ dtto nemusí byť y transc. nad $K(x)$

2.7.L: Nech $x, y \in F$ sú transc. nad K. PNTSE:

(i) $[K(x,y) : K(x)] < \infty$, t.j. y je algebraický nad $K(x)$

(ii) $[K(x,y) : K(y)] < \infty$, t.j. x — " — $K(y)$

(iii) $\exists p \in K[x_1, x_2]^{\#}: p(x, y) = 0$

(i) $\Leftrightarrow$ (iii):

"$\Rightarrow$" $1, y, y^2, \dots, y^n$ LZ nad $K(x) \overset{2.1}{\Rightarrow} \exists p_i \in K[x]: \sum p_i(x) y^i = 0$

stačí položiť $p(x_1, x_2) = \sum p_i(x_1) x_2^i$

"$\Leftarrow$" opačným postupom: $p(x, y) = 0 \Rightarrow \sum p_i(x) y^i = 0 \Rightarrow 1, \dots, y^n$ sú LZ nad $K(x) \Rightarrow K(x)$.

(ii) $\Leftrightarrow$ (iii) analogicky.

Def: Nech $K \leq F$ spĺňajú že $\exists x \in F$ transc. nad K, že $[F : K(x)] < \infty$.

Potom (K, F) nazývame *algebrickým funkčným telesom* a značíme F/K, príp. F.

Algebrický uzáver K v F značíme $\tilde{K}$ a nazývame ho *teleso konštánt*.

2.3.T: Nech F/k je alg. funkčné teleso. Potom pre $a \in F$ platí

$$a \notin \hat{k} \Leftrightarrow [F:k(a)] < \infty$$

$[F:k(k)] < \infty \Rightarrow [F:k(a,x)][k(a,x):k(x)] < \infty \Rightarrow [F:k(a,x)] < \infty \wedge [k(a,x):k(x)] < \infty.$

a transcendentné $\overset{7.7.}{\Rightarrow} [k(a,x):k(a)] < \infty \Rightarrow [F:k(a,x)][k(a,x):k(a)] = [F:k(a)] < \infty$

a algebrické $\Rightarrow [k(a):k] < \infty \Rightarrow [F:k] = [F:k(a)][k(a):k] = \infty$

$\Rightarrow [F:k(a)] = \infty$

Def: Valuačný obor F/k je každý valuačný obor $\mathcal{O}$ telesa F, ktorý spĺňa $k \subseteq \mathcal{O}$.

2.4.L: Nech $\mathcal{O}$ je valuačný obor F/k. Potom $\hat{k} \subseteq \mathcal{O}$.

Nech a je algebrické. Ak $a \in \mathcal{O}$, sme hotoví. Inak $a^{-1} \in \mathcal{O}$. Lenže

$$\gamma_0 + \dots + \gamma_k a^k = 0 \Rightarrow \underbrace{\gamma_0 a^{-k} + \dots + \gamma_{k-1} a^{-1}}_{\in \mathcal{O}} + \gamma_k = 0 \Rightarrow a \in \mathcal{O}$$

2.5.T: Každý valuačný obor F/k je diskrétny.

$\mathcal{O}$ valuačný $\overset{1.6}{\Rightarrow}$ $\mathcal{O}$ lokálny $\overset{1.7}{\Rightarrow}$ potrebujeme $\mathcal{O}$ OIHI

Nech I nie je hlavný ideál. Voľme $\alpha \in I^{\#}$ a nech $M = \mathcal{O} \setminus \mathcal{O}^*$, $n = [F:k(x)]$.

$1.5 \Rightarrow \exists a_1, \dots, a_{n+1} \in I$, $r_1, \dots, r_n \in M$: $a_0 = r_1 r_2 \dots r_k a_k$ pre $k \in \{1, \dots, n\}$.

Ukážeme, že $M \cap k^* \neq \emptyset$. To bude spor, pretože $M = \mathcal{O} \setminus \mathcal{O}^*$ neobsahuje invertibilné prvky (t.j. ani prvky k^*).

$a_0, \dots, a_n$ sú LZ nad $k(x)$ (je ich $n+1$) $\Rightarrow$ 2.1:

$\exists \varphi_i = \alpha_i + x\psi_i$, $\alpha_i \in k$, $\psi_i \in k[x]$, $\exists j$: $\alpha_j \neq 0$ tak, že $\sum \varphi_i a_i = 0$

Vezmime j najväčšie také, že $\alpha_j \neq 0$. Potom

$$\varphi_j a_j = -\sum_{i<j} \varphi_i a_i - \sum_{j<i} \varphi_i a_i$$

$$\psi_j = -\sum_{i<j} \varphi_i \frac{a_i}{a_j} - \sum \frac{a_0}{a_j} \psi_i a_i \Rightarrow \psi_j \in M[x]$$

$= r_{i+1} \cdots r_j \in M$ $\quad \in M$

Lenže $\alpha_j = \underset{\in M}{\varphi_j} - x \underset{\in I^{\#} \subseteq M}{\psi_j} \Rightarrow \alpha_j \in k^* \cap M$ ↯.

7

Def: Místo F/k je každá množina P, pro kterou existuje valuační obor $\mathcal{O}$ v F/k, že $P = \mathcal{O} \setminus \mathcal{O}^*$. 1.10 $\Rightarrow$ P jednoznačně určuje tento obor, značíme $\mathcal{O}_P$.

Množinu všech míst značíme $\mathbb{P} = \mathbb{P}_{F/k}$.

$\mathcal{O}_P$ je DVR (2.5), jednoznačně (nim) určená normalizovanou valuací značíme v_P.

$t \in F$ je uniformizující prvek $\Leftrightarrow v_P(t) = 1 \Leftrightarrow P = t\mathcal{O}_P$

• 1.11: $P_1 \subseteq P_2 \Rightarrow P_1 = P_2$, $\mathcal{O}_{P_1} \subseteq \mathcal{O}_{P_2} \Rightarrow \mathcal{O}_{P_1} = \mathcal{O}_{P_2}$

2.6. L: Pro každý $x \in F$ transc. $\exists P \in \mathbb{P}_{F/k}$ takové, že $v_P(x) > 0$ (t.j. $x \in P$).
Speciálně $\mathbb{P}_{F/k} \neq \emptyset$.

$xK[x]$ je ideál $K[x]$, což je obor F. 1.12 $\Rightarrow \exists \mathcal{O}$ valuační obor takový, že $K[x] \subseteq \mathcal{O}$ a $I\mathcal{O} = xK[x] \subseteq \mathcal{O} \setminus \mathcal{O}^* = P$. Tedy $x \in P$.

$P = \mathcal{O} \setminus \mathcal{O}^*$ ... P neobsahuje invertibilní prvky ... $P \cap K = \{0\}$

$\Rightarrow {}^{(K+P)}/_{P} \simeq K$ ... prvky $k + P$, $k \in K$ ($k + P = 0 + P \Leftrightarrow k \in P \Leftrightarrow k = 0$).

$\Rightarrow$ stotožňujeme K s ${}^{(K+P)}/_{P}$

Def: Stupeň místa: $\deg P = [{}^{\mathcal{O}_P}/_{P} : K]$

2.7. T: Nech $x \in P^{\#}$. Potom x je transc. nad K a $\deg P \leq [F : K(x)] < \infty$.

Ak je x algebraický, tak (2.4). x aj $x^{-1} \in \mathcal{O}_P \Rightarrow x \notin P$. Tedy x je transcend. a z (2.3) platí $[F : K(x)] < \infty$.

Pre zvyšok stačí ukázať, že ak $a_1 + P, \ldots, a_n + P$ sú LNZ nad K v ${}^{\mathcal{O}_P}/_{P}$, tak $a_1, \ldots, a_n$ sú LNZ nad $K(x)$ v F.

Nech $a_1, \ldots, a_n$ LZ nad $K(x) \overset{2.1}{\Rightarrow} \exists a_i \in K, \psi_i \in K[x]$: $\sum (a_i + x\psi_i) a_i = 0$

$\Rightarrow \sum a_i a_i + x \sum \psi_i a_i \in P \Rightarrow \sum x_i a_i \in P \Rightarrow a_i + P$ sú LZ nad K.
($x \in P$)

2.8. L: $\deg P = [{}^{\mathcal{O}_P}/_{P} : \tilde{K}][\tilde{K} : k]$. Špeciálne $[\tilde{K} : k] < \infty$.

Nechť F/k konečné rozšíření, $\tilde{k}/k$:

- x je k transc. nad k, pak je transc. nad $\tilde{k}$
- $[F:\tilde{k}(x)] \leq [F:k(x)] < \infty$
- $F/\tilde{k}$ splňuje definiční obl. konečné těleso

Navíc $x \in F \setminus \tilde{k}$ je transc. nad $\tilde{k}$

- $\mathbb{P}_{F/k} \simeq \mathbb{P}_{F/\tilde{k}}$ (2.4)
- $\deg_{F/k} P = \deg_{F/\tilde{k}} P \cdot [\tilde{k}:k]$

2.3.L: Nechť $k \subseteq k' \subseteq F$ jsou tělesa, $x \in F$ transc. nad k.
Potom $[k':k] \leq [k'(x):k(x)]$ a $[k':k] < \infty$, právě když je konečné normální.

Pro $\leq$ stačí, že pokud $a_1, \dots, a_n \in k'$ jsou LNZ nad k, tak $a_1, \dots, a_n \in k'(x)$ jsou LNZ nad $k(x)$.
Nepřímo: $a_1, \dots, a_n$ LZ nad $k(x) \overset{2.1}{\Rightarrow} \exists \alpha_i \in k, \psi_i \in k[x]$: $\sum \alpha_i a_i + x \sum \psi_i a_i = 0$
$\Rightarrow$ (k je transc.) $\sum \alpha_i a_i = 0 \Rightarrow a_1, \dots, a_n$ LZ nad k.

Nechť $[k':k] < \infty$ a $a_1, \dots, a_n$ je báze k' nad k. Def.
$S := \{ \sum c_i a_i \mid c_i \in k(x) \} \subseteq k'(x)$, je to VP nad $k(x)$ dimenze n.
Je-li pole $k'(x)$ generované $k(x) \cup \{a_1, \dots, a_n\} \Rightarrow$
$\Rightarrow S = k(x)[a_1, \dots, a_n]$. S je těleso, protože jsme k o konečný adjungovali algebraické prvky $\Rightarrow$ $S = k(x)(a_1, \dots, a_n)$. $x \in S$, $k' \subseteq S \Rightarrow S = k'(x)$.

3. VALUÁCIE

F/k alg. funkčné teleso

Valuácie $v_p(x)$ sú normalé pre F/k aj $F/\tilde{k}$

Odteraz predpokladáme $k = \tilde{k}$.

3.1.L: Nech $a, b \in F$, $P \in \mathbb{P}$, $v_p(a) \neq 0$ alebo $v_p(b) \neq 0$. Potom existuje nanajvýš jedno $k \in \mathbb{Z}$, pre ktoré $v(a+b^k) \neq \min\{v_p(a), k v_p(b)\}$

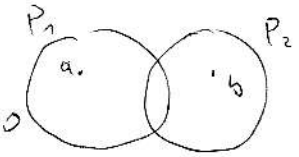
Z (1.13) vieme, že ak $v_p(a) \neq k v_p(b)$, tak $v(a+b^k) = \min\{\dots\}$.
Pre $v_p(b) \neq 0$ je to zrejmé, inak to máme z predpokladu
(že rovnosť nastane pre nanajvýš jedno k)

3.2.T: WAT (Weak Approximation Theorem)

Nech $P_1, \dots, P_n \in \mathbb{P}$ po dvoch rôzne, $r_1, \dots, r_n \in \mathbb{Z}$ a $x_1, \dots, x_n \in F$.
Píšme $v_i = v_{P_i}$. Potom $\exists x \in F$, že $v_i(x - x_i) = r_i$.

$n=1$ ľahko: $v_1(t) = 1 \Rightarrow v_1(t^{r_1}) = r_1 \Rightarrow x = t^{r_1} + x_1$

(W1) $\exists c \in F: v_1(c) > 0$ a $v_2(c) < 0$.



Vol' $a \in P_1 \setminus P_2$, $b \in P_2 \setminus P_1$

$v_1(a) > 0$, $v_2(a) \leq 0$, $v_1(b) \leq 0$, $v_2(b) > 0$ $\Rightarrow$ $v_1(a/b) = v_1(a) - v_1(b) > 0$, $v_2(a/b) = v_2(a) - v_2(b) < 0$

(W2) $\exists c \in F: v_1(c) > 0$ a $v_2(c), \dots, v_n(c) < 0$

Indukcia. Nech platí pre $n-1$. Ak $v_n(c) < 0$, hotovo.
Inak $v_n(c) \geq 0$. Z (W1) $\Rightarrow \exists d: v_1(d) > 0$, $v_n(d) < 0$.
Uvažujme $c' = c + d^k$, $k \in \mathbb{N}$.

$v_1(c + d^k) \geq \min(v_1(c), k v_1(d)) > 0$

$v_i(c + d^k) \overset{*}{=} \min(v_1(c), k v_1(d)) < 0$ (* – až na jedno k; $v_1(c) > 0$)

$v_n(c + d^k) \overset{*}{=} \min(v_n(c), k v_n(d)) < 0$ ($v_n(d) < 0$)

Zakrúžkované k je konečne, vieme vybrať vyhovujúce.

(W3) $\exists d \in F: v_1(1-d) > r_1$, $v_2(d) > r_2, \dots, v_n(d) > r_n$.

Pre c z (W2) položme $d = \frac{1}{1+c^k}$, $k \in \mathbb{N}$. ($v_i(c) < 0$, $v_1(c) > 0$)

$v_i\left(\frac{1}{1+c^k}\right) = -v(1+c^k) \overset{*}{=} -\{v(1), k v(c)\} \geq +k$

$v_1\left(\frac{c^k}{1+c^k}\right) = k v(c) + v(1+c^k) \overset{*}{=} k v(c) - \min\{v(1), k v(c)\} \geq k$

Zakrúžkované k je konečne, stačí vybrať dostatočne veľké.

(W4) $\exists x \in F:\ v_i(x-x_i) > r_i$.

z (W3) vieme nájsť $\forall j:\ d_j$ tak, aby $v_j(1-d_j)$, $v_{i\neq j}(d_j)$ boli dostatočne veľké. Hľadajme x v tvare $d = \sum x_i d_i$. Potom:

$$v_j\Big(\sum x_i d_i\Big) \geq \min\Big\{v_j(d_j - x_j),\ \min_{i\neq j} v_j(x_i d_i)\Big\} = \min\{v_j(x_j) + v_j(d_j - 1),\ v_j(x_i) + v_j(d_i)\}.$$

(W5) WAT.

$x - x_i = y_i + (z - y_i) + (x - z - x_i)$

Budeme hľadať y_i, x, z tak, aby

- $v_i(y_i) = r_i$
- $v_i(z - y_i) > r_i$
- $v_i(x - z - x_i) > r_i$

Potom $v_i(x - x_i) \geq \min\{v_i(y_i), v_i(z-y_i), v_i(x-z-x_i)\} = r_i$, (rovnosť pretože $v_i(y_i) \neq \min\{v_i(z-y_i), -\}$)

Voľme

- $y_i = t_i^{r_i}$, kde t_i je uniformizujúci prvok P_i
- z a následne x dostaneme z (W4).

3.3.D: **Množina $\mathbb{P}_{F/k}$ je nekonečná.**

Ak by bola $\mathbb{P}_{F/k}$ konečná, mohli by sme predpísať $v_i(x) = \max_i - 1$.
Lenže pre $x \in \tilde{k}^*$ je $v_i(x) = 0$, a pre $x \in F \setminus \tilde{k} \Rightarrow x$ transc $\overset{7.6}{\Rightarrow}$ ∃ miesto
je $v_i(x) > 0$. ($x = 0$ triv.)

3.4.T: **Nech F/k je teleso, $P_1, \dots, P_n \in \mathbb{P}$ po dvoch rôzne a $x \in F/k$ taký, že $v_i(x) > 0$ $(v_i = v_{P_i})$. Potom**

$$[F : k(x)] \geq \sum v_i(x) \deg P_i$$

A. Voľba bázy

bázu $\mathcal{O}_{F/P}$ nad $k+P/P \cong k$

$P = P_i$, $c_1, \dots, c_f$ báza $\mathcal{O}_P$ modulo P, $f = \deg P$.

Potom aj $b_1, \dots, b_f$ kde $b_i \in c_i + P$ je báza $\mathcal{O}_P$ modulo P. *

Nanajvýš ak $\exists \varphi_i \in \mathcal{O}_P$: $\sum \varphi_i b_i \in P$, tak $\varphi_i \in P$, pretože b_i sú lin. nezávislé nad P, a teda jediné ich triviálna kombinácia (t. j. s koeficientami z $\mathcal{O}+P$) padne do $\mathcal{O}+P$.

Pritom * nastane práve vtedy, keď $b_i - c_i \in P$, t. j. $v_P(b_i - c_i) > 0$.

B. Voľba parametrov

Označme $f_i = \deg P_i$ a zvoľme báziu $c_{i1}, \dots, c_{if_i}$ O_{P_i} modulo P_i.

Z WAT-u nájdime pre $\forall$ dvojicu (i,j): $1 \le i \le n$, $1 \le j \le f_i$ prvok b_{ij} taký, že

$$v_i(b_{ij} - c_{ij}) > 0 \quad a \quad v_{i'}(b_{ij}) \ge v_{i'}(x).$$
$$i' \neq i$$

Na dôkaz tvrdenia chceme nájsť $\sum v_i(x) f_i$ LNZ prvkov F lin. nezávislých nad $k(x)$. Tipnem, že to budú

$$u_{ijk} := t_i^k b_{ij} \qquad 1 \le i \le n,\ 1 \le j \le f_i,\ 0 \le k < v_i(x)$$

kde t_i je uniform. prvok P_i.

C. Dôkaz

Sporom, nech u_{ijk} sú LZ nad $k(x)$ $\overset{2.1}{\Rightarrow} \exists\, \varphi_{ijk} \in k[x]$:

$\sum \varphi_{ijk} u_{ijk} = 0$ a niektoré φ_{ijk} má abs. člen nenulový.

Označím (i',j',k') taký trojicu že pre dané (i',j') je k' najmenšie také, že $\varphi_{i'j'k'}$ má nenulový voľný člen.

$v' = v_{i'}$, $P' = P_{i'}$, $O' = O_{P_{i'}}$, $f' = f_{i'}$, $t' = t_{i'}$

C. Podmienka a spor

Platí: **Pre $(i,k) \neq (i',k')$ je $\varphi_{ijk} u_{ijk} t'^{\,-k'} \in P'$.**

Potom $\sum_{ijk} u_{ijk} \varphi_{ijk} = 0$

$$\Rightarrow \sum_{ijk} u_{ijk} \varphi_{ijk} t'^{-k'} = 0$$

$$\Rightarrow \sum_{j} u_{i'jk'} \varphi_{i'jk'} t'^{-k'} \in P'$$

$$\Rightarrow \sum_{j} b_{i'j} \varphi_{i'jk'} \in P'$$

$\overset{(A)}{\Rightarrow} \varphi_{i'jk'} \in P'$. Lenže $\varphi_{i'jk'}$ má nenulový konštantný člen $\alpha \in k^*$, a teda

$$\varphi_{i'jk'} = \alpha + \underset{\in P}{x}\,\underset{\in P}{\psi} \quad \Rightarrow \alpha \in P \quad \lightning \quad (P \cap k^* = \emptyset).$$
$$\in P \qquad \in P \ (v_i(x) > 0)$$

D. Dôkaz podmienky

Podmienka pre $(i,k) \neq (i',k')$ hovorí

$$v'(\varphi_{ijk}) + v'(u_{ijk}) > +k'$$
$$v'(\varphi_{ijk}) + v'(b_{ij}) + k\, v'(t_i) > +k'$$

- $\varphi_{ijk} \in k[x] \le O_i$ $(v_i(x) > 0)$ $\Rightarrow v'(\varphi_{ijk}) \ge 0$.
- $v'(b_{ij}) \ge v'(x) > k'$ (pretože $0 \le k' < v'(x)$)
- $v'(t_i) = 0$ (z definície, pripadnosť prvku t_i do $P_{i'}$ závisí na výbere t_i)

$\Rightarrow$ nerovnosť platí.

4. DIVIZORY

Def: • $\mathrm{Div}\, F/k = \mathrm{Div}\, F = \{ \sum a_P P \mid a_P \in \mathbb{Z},\ P \in \mathbb{P},\ a_P \neq 0 \text{ len pre konečne mnoho} \}$,
t.j. voľná abelovská grupa nad $\mathbb{P}$ sa nazýva grupa <u>divizorov</u>.

- Divizor je <u>kladný</u> (efektívny), ak $\forall P \in \mathbb{P}: a_P \geq 0$.
- $A \in \mathrm{Div}\, F/k$ je <u>prvodivizor</u> ak $A = P$ pre nejaké $P \in \mathbb{P}$.

Pr $P_1 + 2P_2 - 4P_3 \in \mathrm{Div}\, F$

Def: • Každé $A \in \mathrm{Div}\, F/k$ vieme zapísať ako rozdiel kladných divizorov $A_+ - A_- = A$:

$$A_+ = \sum_{a_P \geq 0} a_P P \qquad A_- = \sum_{a_P \leq 0} -a_P P$$

- <u>Stupeň</u> divizora $A = \sum a_P P$ je definovaný ako $\deg P = \sum a_P \deg P$
- Pre $x \in F^*$ definujeme <u>hlavný</u> divizor $(x) = \sum a_P P$, kde $a_P = \nu_P(x)$.
Podľa (3.4) je $\sum \nu_P(x) \deg P$ konečné číslo, takže $\nu_P(x) \neq 0$ pre kon. veľa P.

4.1.L: $\forall x, y \in F^*$: $(xy) = (x) + (y)$, $(x^{-1}) = -(x)$, $(x) = 0 \Leftrightarrow x \in k^*$ a $(\alpha x) = x$ pre $\alpha \in k^*$.

$\nu_P(xy) = \nu_P(x) + \nu_P(y)$, $\nu_P(x^{-1}) = -\nu_P(x)$, $x \in k^* \Rightarrow \nu_P(x) = 0$,
$x \notin k^* \Rightarrow \exists P: \nu_P(x) > 0$ (2.6)

4.2.D: Hlavné divizory tvoria podgrupu $\mathrm{Div}\, F/k$.

Def: Grupa hlavných divizorov značíme <u>Princ F/k</u>. Faktor

$$Cl(F/k) = \frac{\mathrm{Div}(F/k)}{\mathrm{Princ}(F/k)}$$

nazývame <u>class group</u> (triedová grupa).

4.3.L: Nech $x \in F^*$. Potom

$$\deg (x)_+ \leq [F : k(x)] \quad \text{a} \quad \deg (x)_- \leq [F : k(x)]$$

$(x)_+ = \sum a_{P_i} P_i$ kde $a_{P_i} > 0$. Aplikujeme (3.4) na tieto miesta $P_i \Rightarrow \deg (x)_+ \leq [F : k(x)]$.
$(x)_- = +(x^{-1})_+ \Rightarrow \deg (x)_- = \deg (x^{-1})_+ \leq [F : k(x)]$.

Cieľ: dokázať rovnosť

Def: Riemann-Rochov priestor

- def. $A \geq B$ ak $a_P \geq b_P \ \forall P$. Je $\leq$ čiast. usporiadanie na divizoroch
- Riemann-Rochov priestor prislušný divizoru A:

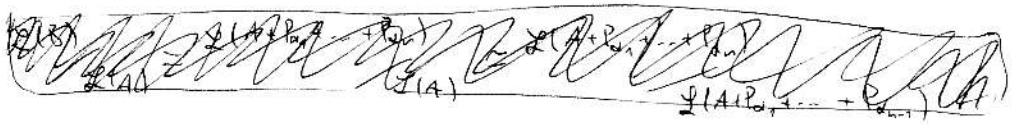
$$\mathcal{L}(A) = \{x \in F^* \mid (x) + A \geq 0\} \cup \{0\}$$

- $x \in \mathcal{L}(A) \Leftrightarrow \forall P: \nu_P(x) + a_P \geq 0 \Leftrightarrow \forall P: \nu_P(x) \geq -a_P$
- $(x) + A \geq 0, \ B \geq A \Rightarrow (x) + B \geq 0 \Rightarrow \mathcal{L}(A) \subseteq \mathcal{L}(B)$
- $x, y \in \mathcal{L}(A) \Rightarrow \nu_P(x), \nu_P(y) \geq -a_P \Rightarrow \nu_P(x) + \nu_P(y) = \nu_P(x+y) \geq -a_P \Rightarrow x+y \in \mathcal{L}(A)$
  ($\mathcal{L}(A)$ je uzavretý na súčet)
- $\nu_P(x) = \nu_P(\alpha x)$ pre $\alpha \in K^* \ldots \ x \in \mathcal{L}(A) \Rightarrow \alpha x \in \mathcal{L}(A)$ (uzavretý na násobenie K)

$\Rightarrow \mathcal{L}(A)$ je vektorový priestor nad K

4.4.L: $A \leq B$ divizory. Potom $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ a $\dim \mathcal{L}(B)/\mathcal{L}(A) \leq \deg(B-A)$

$\mathcal{L}(A) \subseteq \mathcal{L}(B)$ je v úvahe vyššie. Nech $B - A = \sum P_{\alpha_i}$ ($B-A$ je kladný), t.j. $B = A + P_{\alpha_1} + \ldots + P_{\alpha_n}$. Potom $\mathcal{L}(A) \subseteq \mathcal{L}(A+P_{\alpha_1}) \subseteq \ldots \subseteq \mathcal{L}(A + P_{\alpha_1} + \ldots + P_{\alpha_n})$ a



$$\dim \mathcal{L}(B)/\mathcal{L}(A) = \dim \mathcal{L}(B)/\mathcal{L}(A+\ldots+P_{\alpha_{n-1}}) + \dim \mathcal{L}(A+\ldots+P_{\alpha_{n-1}})/\mathcal{L}(A+\ldots+P_{\alpha_{n-2}}) + \ldots + \dim \mathcal{L}(A+P_{\alpha_1})/\mathcal{L}(A).$$

Stačí dokázať $\dim \mathcal{L}(C+P)/\mathcal{L}(C) \leq \deg P$, dokážeme indukciou.

Uvažujme zobrazenie $\varphi: \mathcal{L}(C+P) \to \mathcal{O}_P/P : x \mapsto x t_P^{c_P+1}$

To je homomorfizmus

$x \in \mathcal{L}(C+P) \Rightarrow \nu_P(x) \geq -c_P - 1 \Rightarrow \nu_P(x t_P^{c_P+1}) = \nu_P(x) + c_P + 1 \geq 0$, t.j. $\varphi(x) \in \mathcal{O}_P$

a navyše $\varphi(x) \in P \Leftrightarrow$

$\nu_P(x) + c_P + 1 > 0 \Leftrightarrow \nu_P(x) > -c_P - 1 \Leftrightarrow \nu_P(x) \geq -c_P \Leftrightarrow x \in \mathcal{L}(C)$

t.j. $\ker \varphi = \mathcal{L}(C) \Rightarrow \mathcal{L}(C+P)/\ker\varphi \cong \operatorname{Im}\varphi \Rightarrow \dim \mathcal{L}(C+P)/\mathcal{L}(C) \leq \dim \mathcal{O}_P/P = \deg P$.

4.4.D: Nech $A \leq B$ sú divizory. Potom $\deg A \leq \ell(A) \leq \deg A + 1$

- dokážeme $A = 0$: $\mathcal{L}(0) = \{x \in F \mid \forall P \ \nu_P(x) \geq 0\} = K$

  (ak $x \notin K \Rightarrow x$ je transc. $\Rightarrow x^{-1}$ transc $\Rightarrow$ (7.6) $\exists P: \nu_P(x^{-1}) > 0 \Rightarrow \nu_P(x) < 0$)

  $\Rightarrow \dim \mathcal{L}(B)/K \leq \deg B \Rightarrow \dim \mathcal{L}(B) \leq \deg B + 1$ pre $B \geq 0$

  špeciálne $\ell(B) < \infty$:

  $B \leq B_+ \Rightarrow \ell(B) \leq \ell(B_+) \leq \deg B + 1$

(14) • $\ell(A)$, $\ell(B) < \infty$, $A \le B \Rightarrow$

$$\ell(B) - \ell(A) = \dim \mathcal{L}(B)/\mathcal{L}(A) \le \deg(B-A) = \deg B - \deg A$$

$$\Rightarrow \deg A - \ell(A) \le \deg B - \ell(B)$$

4.5 D: Nech $A \le B$ sú divizory. Potom $\deg A - \ell(A) \le \deg B - \ell(B)$.
Ak je $A \ge 0$, tak $\ell(A) \le \deg A + 1$.

Viď vyššie.

4.6.L: Nech F/k teleso, x transc. nad k. Potom $f_1, \dots, f_k \in F$ sú lin. nezávislé nad $k(x) \Leftrightarrow \{f_i x^j \mid 1 \le i \le k,\ j \ge 0\}$ je LNZ nad k.

f_i LZ nad $k(x) \overset{(2.1)}{\Leftrightarrow} \exists \varphi_i \in k[x]$: $\sum f_i \varphi_i = \sum_i \sum_j a_{ij} x^j = 0 \Leftrightarrow \{f_i x^j\}$ LZ nad k

4.7.L: Pre každé $x \in F \setminus k$ $\exists$ kladný divisor C, že pre $\forall k \ge 1$:

$$(k+1)[F:k(x)] \le \ell(k(x)_\infty + C)$$

Nech $e_1, \dots, e_m$ je báza F nad $k(x)$. Vieme, že $\{e_j x^r \mid 1 \le j \le m,\ r \ge 0\}$ je LNZ nad k. Ak vhodne c tak, že $e_j x^r \in \mathcal{L}(k(x)_\infty + C)$ pre $0 \le r \le k$, tak $\dim \mathcal{L}(k(x)_\infty + C) \ge m \cdot (k+1) = (k+1)[F:k(x)]$.

Označme $(x)_\infty = \sum a_p P$, $C = \sum c_p P$. Chceme teda pre $0 \le r \le k$:

$$v_p(e_j x^r) \ge -k a_p - c_p$$

$$v_p(e_j) + r\, v_p(x) \ge -k a_p - c_p \qquad a_p \ge 0$$

- $v_p(x) \ge 0 \Rightarrow a_p = 0$
  A teda $v_p(e_j) + r\, v_p(x) \ge -c_p \Leftrightarrow v_p(e_j) \ge -c_p$
- $v_p(x) < 0 \Rightarrow a_p = -v_p(x)$
  A teda $v_p(e_j) + r\, v_p(x) \ge +k v_p(x) - c_p \Leftrightarrow v_p(e_j) + (r+k) v_p(x) \ge -c_p \Leftrightarrow v_p(e_j) \ge -c_p$

Stačí teda voliť c_p tak, aby $c_p \ge \max\{0, -v_p(e_j)\}$.
$v_p(e_j)$ je nenulové iba pre konečne P, takže $\sum c_p P$ bude kladný divizor.

4.9.D: $\forall x \in F \setminus k$ platí $\deg(x)_+ = \deg(x)_- = [F : k(x)]$ a $\deg(x) = 0$.

(4.3) $\Rightarrow \deg(x)_- \le [F:k(x)]$, $m := [F:k(x)]$, $\mathcal{B} := (x)_-$.

(4.7) $\Rightarrow \exists C: \forall k: \quad (k+1)m \le \ell(k\mathcal{B}+C) \le \deg(k\mathcal{B}+C)+1 = k\deg\mathcal{B} + \deg C + 1$

$\Rightarrow k(m - \deg\mathcal{B}) \le \deg C + 1 - m \quad \forall k$

$\Rightarrow m - \deg\mathcal{B} \le 0 \Rightarrow m \le \deg\mathcal{B} \le m.$

Tvrzení pro $(x)_+$ získáme z $(x)_+ = (x^{-1})_-$.

4.9.D: Nech $x \in F \setminus k$ a nech $\mathcal{B} = (x)_-$. Potom $\exists$ kladný dělitel C takový, že $\forall k \ge 1$: $\deg(k\mathcal{B}) - \ell(k\mathcal{B}) \le \deg(C - \mathcal{B})$

(4.4) $\Rightarrow \ell(k\mathcal{B}+C) - \ell(k\mathcal{B}) \le \deg C$

(4.7) $\Rightarrow (k+1)m \le \ell(k\mathcal{B}+C) \le \deg C + \ell(k\mathcal{B})$

$\Rightarrow km = k\deg\mathcal{B} = \deg k\mathcal{B} \le \deg C + \ell(k\mathcal{B}) - m = \deg C + \ell(k\mathcal{B}) - \deg\mathcal{B}.$

Def: Definujme ekvivalenci na děliteloch:

$$\mathcal{A} \sim \mathcal{B} \iff \exists x \in F: \quad \mathcal{A} = \mathcal{B} + (x)$$

je to ekvivalence, neboť $\mathcal{B} = \mathcal{C} + (y) \Rightarrow \mathcal{A} = \mathcal{C} + (y) + (x) = \mathcal{C} + (xy)$

4.10.T: $\mathcal{A} \sim \mathcal{B} \Rightarrow \ell(\mathcal{A}) = \ell(\mathcal{B}),\ \deg(\mathcal{A}) = \deg(\mathcal{B})$

$\deg(\mathcal{B} + (x)) = \deg\mathcal{B} + \deg(x) = \deg\mathcal{B}$

~~$\ell(\mathcal{A}) - \ell(\mathcal{B}) = \dim \mathcal{L}(\mathcal{B}) \le \deg(x) \Rightarrow \ell(\mathcal{A}) = \ell(\mathcal{B})$~~

Ukážeme $\mathcal{L}(\mathcal{A}) \cong \mathcal{L}(\mathcal{A}+(x))$: isomorfismus $\varphi(y) = xy$

- je k-lineární: $\varphi(y+z) = \varphi(y) + \varphi(z)$, $\varphi(\alpha y) = \alpha\varphi(y)$
- je prosté a na: má inverz: $\varphi^{-1}(z) = x^{-1}z$

4.11.L: Nech $\mathcal{A}, \mathcal{B} \in \mathrm{Div}\, F$. Potom $\ell(\mathcal{B}-\mathcal{A}) \ge 1 \iff \exists \mathcal{A}' \sim \mathcal{A}: \quad \mathcal{A}' \le \mathcal{B}$

$\ell(\mathcal{B}-\mathcal{A}) \ge 1 \iff \exists x \in F^*: x \in \mathcal{L}(\mathcal{B}-\mathcal{A}) \iff \exists x \in F^*: \mathcal{B} - \mathcal{A} + (x) \ge 0 \iff \mathcal{B} \ge \mathcal{A} - (x) = \mathcal{A} + (x^{-1})$

4.12.T: Nech $F \setminus k$ je alg. konečné těleso. Potom $\exists \gamma > 0$, že $\forall \mathcal{A} \in \mathrm{Div}\, F \setminus k$ je

$$\deg(\mathcal{A}) - \ell(\mathcal{A}) < \gamma.$$

(Připomínka věty)

$x \in F \setminus k$, $\mathcal{B} = (x)_-$, (4.9) $\Rightarrow \exists \gamma$: $\deg(k\mathcal{B}) - \ell(k\mathcal{B}) < \gamma$.

Ukážeme ukázali, že $\forall \mathcal{A} \in \mathrm{Div}\, F\ \exists \mathcal{A}' \sim \mathcal{A}$ takové, že $\mathcal{A}' \le k\mathcal{B}$: (pro vhodné k)

$$\deg\mathcal{A} - \ell(\mathcal{A}) \overset{4.10}{=} \deg\mathcal{A}' - \ell(\mathcal{A}') \overset{4.5}{\le} \deg(k\mathcal{B}) - \ell(k\mathcal{B}) < \gamma.$$

(4.11) $\Rightarrow \mathcal{A}' \le k\mathcal{B} \iff \ell(k\mathcal{B} - \mathcal{A}') \ge 1$

(16)

$A_+ \geq A$, $\Rightarrow \ell(kB - A_+) \leq \ell(kB - A)$, stačí tedy $\ell(kB - A_+) \geq 1$.

$$\deg(kB - A_+) - \ell(kB - A_+) \leq \deg(kB) - \ell(kB) < g$$

$$\Rightarrow k \underbrace{\deg B}_{\Sigma_{P \in F:k(x)}} - \deg A_+ < g + \ell(kB - A_+)$$

$$\Rightarrow \exists k: \; 0 < \ell(kB - A_+).$$

$\forall A: \quad \deg A - \ell(A) < g$

$A = 0: \quad \deg 0 - \ell(0) = 0 - \dim k = -1 < g$

Def: $g \in \mathbb{Z}$ nejmenší takový, že $\deg A - \ell(A) < g$ se nazývá <u>nod (genus)</u> F/k, značíme g. Z předchozího $g \geq 0$.

$$g = \max\{\deg A - \ell(A) + 1 \mid A \in \mathrm{Div}\, F/k\},$$

4.13.T: Nech F/k je alg. funkční těleso rodu g. Nech $D \in \mathrm{Div}\, F/k$ je takový, že $\deg D - \ell(D) = g - 1$. Potom nk platí jedna z podmínek

- $\deg A \geq \deg D + g$
- $\ell(A - D) \geq 1$
- $A \geq D$,

tak tedy $\deg A - \ell(A) = g - 1$.

$\deg A \geq \deg D + g$

$\deg(A - D) - \ell(A - D) \leq g - 1 \Rightarrow \ell(A - D) \geq \underbrace{\deg(A - D)}_{\deg A - \deg D \geq g} - g + 1 \geq 1.$

$\ell(A - D) \geq 1 \overset{4.11}{\Rightarrow} \exists D' \sim D: \; D' \leq A$

$D \leq A \Rightarrow g - 1 = \deg D - \ell(D) \leq \deg A - \ell(A) \leq g - 1$

4.14.T: Nech F/k je alg. fun. těleso, $A, B \in \mathrm{Div}\, F$. Potom:

(P1) $A \sim B \Rightarrow \ell(A) = \ell(B) \wedge \deg A = \deg B$

(P2) $\ell(A) \geq 1 \Leftrightarrow \exists x \in F^*: \; A + (x) \geq 0 \Leftrightarrow \exists A \sim A': \; A' \geq 0$

(P3) $A \leq B \Rightarrow \deg A - \ell(A) \leq \deg B - \ell(B)$

(P4) $A < 0 \Rightarrow \deg A < 0 \Rightarrow \ell(A) = 0$

| První $\Rightarrow$ triv.; druhá: $\ell(A) \geq 1 \Rightarrow \exists A' \sim A: \; A' \geq 0 \Rightarrow \deg A' \geq 0 \Rightarrow \deg A \geq 0$ ↯.

(P5) $\forall x \in F: \; \mathcal{L}((x)) = k \cdot x^{-1}, \quad \ell((x)) = 1 \quad a \quad \deg((x)) = 0$

| $y \in \mathcal{L}((x)) \Leftrightarrow (y) + (x) \geq 0 \Leftrightarrow (xy) \geq 0 \Leftrightarrow$ (hint, 4.1) $xy \in k$

(P6) Nech $\deg A = 0$. Potom $\ell(A) \geq 1 \Rightarrow \ell(A) = 1 \Leftrightarrow A = (x)$ pre nejaké $x \in F^*$.

| "$\Leftarrow$" P5. $\ell(A) \geq 1 \overset{P2}{\Rightarrow} \exists x: \; A' = A + (x) \geq 0$. $\deg A' = \deg A = 0 \Rightarrow A' = 0 \Rightarrow A = (x)$.

5. ADÈLE

5.1.L: Nech V je v.p. nad K a $U_2 \subseteq U_1$, W jeho podpriestory. Potom $U_2 + (U_1 \cap W) = (U_2 + W) \cap U_1$.

Zväzový dôkaz:

"$\subseteq$" $U_2 \subseteq U_2 + W_1$, $U_2 \subseteq U_1 \Rightarrow U_2 \subseteq P.S.$

$U_1 \cap W \subseteq W \subseteq U_2 + W_1$, $U_1 \cap W \subseteq U_1 \Rightarrow U_1 \cap W_2 \subseteq P.S.$ $\Big\}\ \subseteq$

"$\supseteq$" $u_2 + w \in U_1 \Rightarrow w \in U_1 \Rightarrow w \in U_1 \cap W \Rightarrow U_2 + w \in U_2 + (U_1 \cap W)$

$\Uparrow$

$(U_2 + W) \cap U_1$

5.2.L: Nech V je v.p. nad K a $U_2 \subseteq U_1$, W jeho podpriestory také, že $\dim (U_1/U_2) < \infty$. Potom

$$\dim \left(\frac{U_1 + W}{U_2 + W} \right) = \dim \left(U_1/U_2 \right) - \dim \left(\frac{U_1 \cap W}{U_2 \cap W} \right)$$

I To snáď vymyslím...

Def: $\mathbb{P} = \mathbb{P}_{Flk}$ množina miest, Flk alg. funkčné teleso

$F^{\mathbb{P}}$ ... algebra na kartézskom súčine

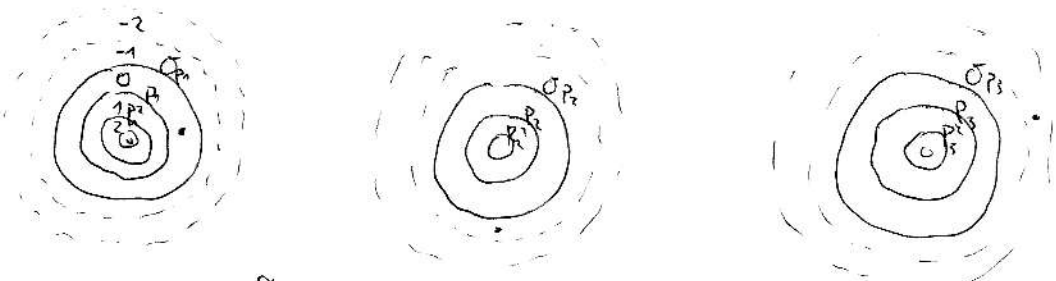
$\underline{\text{Adèle}(F|k)} = \text{Adèle } F = \{ f \in F^{\mathbb{P}} \mid f(P) \in \mathcal{O}_P$ nanajvýš pre konečne mnoho $P \in \mathbb{P} \}$

$\underline{\vartheta(f)} \in \mathbb{Z}_\infty^{\mathbb{P}}$, $\vartheta(f)(P) := v_P(f(P))$

$\underline{c_x}(P) = x$ pre $x \in F$ ... $c_x \in F^{\mathbb{P}}$ ... budeme stotožňovať s F

$\underline{\mathcal{A}(A)} = \{ f \in \text{Adèle } F \mid \vartheta(f) + A \geq 0 \} \subseteq \text{Adèle } F$ pre $A \in \text{Div } F$

Pozn: $F^{\mathbb{P}}$ si predstavujeme ako terče; v každom z nich jeden šíp



Adèle ... terče $\mathcal{O}_P$ môžem len konečne veľa kaziť

$\vartheta(f)$ ... obdobný zápisnáhor $f \in \text{Adèle } F \Rightarrow \vartheta(f)(P) \leq 0$ pre konečne veľa P.

$\vartheta(c_x)$ ... odpovedá hlavnému divízoru x:

$$\vartheta(c_x)(P) = v_P(c_x(P)) = v_P(x)$$

$\mathcal{A}(A)$ ... odpovedá Riemann-Rochovmu priestoru. Dá sa predstaviť tak, že terčíl oválom (na hraniciach $-a_P$) a musím sa trafiť.

Pozn: $\vartheta(f) \in \mathbb{Z}_\infty^{\mathbb{P}}$ nemusí byť divizor, môže byť nenulové na do nekonečne mnohých miestach

Prvky $\mathbb{Z}_\infty^{\mathbb{P}}$ sú prirodzene čiastočne usporiadané:

Určíme dohodnuté $c = \min\{a,b\}$ ... $c(p) = \min\{a(p), b(p)\}$.

5.3.L: $f, g \in F^{\mathbb{P}}$, $x \in F$. Potom

(i) $\vartheta(f+g) \geq \min\{\vartheta(f), \vartheta(g)\}$, $\quad \vartheta(fg) = \vartheta(f) + \vartheta(g)$

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

Ľahké, ~~analogické~~

5.4.D: $Adèle(F/k)$ je podalgebra F-algebry $F^{\mathbb{P}}$. $\forall x \in F$ je $c_x \in Adèle(F/k)$.

$\vartheta(f)$ je záporné iba na konečne veľa miestach, nanajvýš $\vartheta(g)$.

Preto $\vartheta(f+g) \geq \min\{\vartheta(f), \vartheta(g)\}$ aj $\vartheta(fg) = \vartheta(f) + \vartheta(g)$ tiež.

Napokon $\vartheta(c_x) = (x)$ je nenulové (dokonca) len pre konečne veľa $P \Rightarrow c_x \in Adèle\, F$.

5.5.L: $a(A)$ je v.p. nad k a spĺňa $a(A) \cap F = \mathcal{L}(A)$.

$f, g \in a(A)$, $\lambda \in k^\times$

$\vartheta(\lambda f) = (\lambda) + \vartheta(f) = \vartheta(f)$, $\quad \vartheta(f+g) \geq \min\{\vartheta(f), \vartheta(g)\} \geq -A$

$c_x \in a(A) \Leftrightarrow \vartheta(c_x) + A \geq 0 \Leftrightarrow (x) + A \geq 0 \Leftrightarrow x \in \mathcal{L}(A)$

5.6.L: Nech $A, B \in Div\, F$, $A \leq B$. Potom $a(A) \subseteq a(B)$ a platí

$$\dim a(B)/a(A) = \deg(B - A)$$

Indukciou: stačí $\dim a(A+P)/a(A) = \deg P$.

Uvažujme $\varphi: a(A+P) \to \mathcal{O}_P/P$, $\quad \varphi(f) = f(P)\, t_P^{a_P+1}$

- $f \in a(A+P) \Rightarrow v_P(f(P)) \geq -a_P - 1 \Rightarrow v_P(\varphi(f)) = v_P(f(P)) + a_P + 1 \geq 0 \Rightarrow \varphi(f) \in \mathcal{O}_P$
- Ďalej $f \in a(A) \Leftrightarrow v_P(f(P)) \geq -a_P \Leftrightarrow v_P(\varphi(f)) = v_P(f(P)) + a_P > 0 \Leftrightarrow \varphi(f) \in P$
- pre $x \in \mathcal{O}_P$ voľbou $f(P) = x\, t_P^{-a_P-1}$; $f(Q) = 0$ pre $Q \neq P$

  dostávame $f \in a(A+P)$: $v_Q(f(Q)) = \infty \geq -A_Q$, $v_P(f(P)) = v_P(x) - a_P - 1 \geq -a_P - 1$

  A pritom $\varphi(f) = x \Rightarrow \varphi$ je na.

Jadro a izomorfizmus: $a(A+P)/a(A) \simeq \mathcal{O}_P/P \Rightarrow \dim a(A+P)/a(A) = \deg P$

Def: $i(A) = g - 1 - (\deg A - \ell(A))$ ... index špecializácie

$i(A) \geq 0$, $\quad i(A) = 0$ pre $\deg(A)$ dostatočne veľké (4.13).

5.7.L: Nech $A \le B$. Potom $a(A)+F \subseteq a(B)+F$ a

$$\dim\left(\frac{a(B)+F}{a(A)+F}\right) = (\deg B - \ell B) - (\deg A - \ell A) = i(A) - i(B)$$

(5.2) $\Rightarrow$ $U_2 = a(A)$, $U_1 = a(B)$, $W = F$

$$\Rightarrow \dim\left(\frac{a(B)+F}{a(A)+F}\right) = \dim\left(\frac{a(B)}{a(A)}\right) - \dim\left(\frac{a(B)\cap F}{a(A)\cap F}\right) =$$

$$\overset{5.5,\,5.6}{=} \deg(B-A) - \dim\left(\frac{\mathcal{L}(B)}{\mathcal{L}(A)}\right) \Rightarrow \deg B - \deg A - \ell B + \ell A$$

5.8.L: Nech $i(D) = 0$, $D \in \mathrm{Div}\, F/k$. Potom $a(D)+F = \mathrm{Adele}\ F/k$.

$f \in \mathrm{Adele}\ F/k$. $\vartheta(f)(P) < \infty$ pre konečne veľa P $\Rightarrow$ $\exists B \ge 0$ (dívizor): $\vartheta(f) + B \ge 0$.

$f \in a(B) \subseteq a(D+B)$. $\dim\left(\frac{a(D+B)+F}{a(D)+F}\right) = i(D) - i(D+B) \ge 0$ $\Rightarrow$

($i(D) = 0$, $i(D+B) = 0$)

$\Rightarrow \dim(\dots) = 0 \Rightarrow a(D+B)+F = a(D)+F \Rightarrow f \in a(D)+F$.

5.9.D: $\forall A \in \mathrm{Div}\, F/k$ je $i(A) = \dim\left(\frac{\mathrm{Adele}\ F/k}{a(A)+F}\right)$

(5.8) .. dosadíme $B = D$.

5.10.L: Nech $A \in \mathrm{Div}\, F/k$ a $x \in F^*$. Potom $x\,a(A) = a(A - (x))$

$g \in \mathrm{Adele}\ F$: $\vartheta(x^{-1}g) = \vartheta(g) - (x)$

$g \in x\,a(A) \Leftrightarrow x^{-1}g \in a(A) \Leftrightarrow \vartheta(x^{-1}g) \ge -A \Leftrightarrow \vartheta(g) - (x) \ge -A \Leftrightarrow \vartheta(g) \ge -A + (x)$ ✓.

5.11.L: Nech $A, B \in \mathrm{Div}\, F/k$. Potom $a(A) + a(B) = a(\max\{A, B\})$.

$A = \sum a_P P$, $B = \sum b_P P$, $C = \max\{A,B\} = \sum c_P P$, $c_P = \max\{a_P, b_P\}$

$A \le C$, $B \le C$ $\Rightarrow$ $a(A) \subseteq a(C)$, $a(B) \subseteq a(C)$ $\Rightarrow$ $a(A) + a(B) \subseteq a(C)$.

"$\supseteq$": Nech $f \in a(C)$, chceme $f = f_1 + f_2$, $f_1 \in a(A)$, $f_2 \in a(B)$:

- $v_P(f(P)) \ge -a_P \Rightarrow f_1(P) = f(P)$, $f_2(P) = 0$
- $v_P(f(P)) < -a_P \Rightarrow f_1(P) = 0$, $f_2(P) = f(P)$

zvyšné $f_1 \in a(A)$, zostáva $f_2 \in a(B)$, t.j. $\vartheta(f_2) \ge -B$:

- $v_P(f(P)) \ge -a_P \Rightarrow f_2(P) = 0 \Rightarrow v_P(f_2(P)) = \infty \ge -B$ ✓
- $v_P(f(P)) < -a_P \Rightarrow v_P(f_2(P)) = v_P(f(P)) < -a_P$

(ešte $v_P(f(P)) \ge -\max\{a_P, b_P\} \Rightarrow v_P(f(P)) \ge -b_P$ ✓

6. WEILOVE DIFERENCIÁLY

$\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim U_1 + \dim U_2$ ... lingebra

6.1.L: Nech $\dim V = n$. Ak $U_1 \leq V$, $U_2 \leq V$ takej, že $\dim U_1 + \dim U_2 > n$, tak $\dim(U_1 \cap U_2) \geq 1$.

$V^* = \mathrm{Hom}(V, k)$ -- lineárne formy na V

$\sigma: V \to U$ indukuje $\sigma^*: U^* \to V^*$, $\psi \mapsto \psi \circ \sigma$

$\pi: V \to V/W$ projekcia

Def: $\mathrm{Ann}_V(W) = \{\varphi \in V^* \mid W \leq \ker \varphi\}$ $\quad W \leq V$

Anihilátor -- lin. formy na V, ktoré sú nulové na W.

👁: $\mathrm{Ann}_V(W) \simeq (V/W)^*$

π^* je izomorfizmus: $\varphi \in V/W^*$ [illegible] $\Rightarrow \varphi \circ \pi(W) = \varphi(0) = 0$

$\psi \in \mathrm{Ann}_V W \Rightarrow \pi^{*-1}(\psi)(v+W) := \psi(v)$ je korektné a je to inverz



6.2.L: Nech V je v.p. nad K, W a W' jeho podpriestory.

(i) $\mathrm{Ann}_V W \simeq (V/W)^*$. Ak je V/W kon. dim, platí $\dim \mathrm{Ann}_V(W) = \dim V/W$.

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

(iii) $W' \leq W \Rightarrow \mathrm{Ann}_V W' \geq \mathrm{Ann}_V W$

Ľahké

Nech V^* je v.p. nieleen nad K, ale aj nad F.

6.3.L: Pre $x \in F$ a $\varphi \in V^*$ definujme $x\varphi: V \to K$ tak, že $\forall v \in V$ je $(x\varphi)(v) = \varphi(xv)$. Potom $x\varphi \in V^*$. Takto definované násobenie vyhovuje V^* v.p. nad F.

Ak je $W \leq V$ podpriestor a $x \in F^*$, tak $\mathrm{Ann}_V(x \cdot W) = x \,\mathrm{Ann}_V(W)$.

↓

Určete $x\varphi \in V^*$.

V^* je v.p. nad F, ale platí $\begin{cases} x(\varphi_1+\varphi_2) = x\varphi_1 + x\varphi_2 & \checkmark \\ 1\cdot\varphi = \varphi \qquad (x+y)\varphi = x\varphi + y\varphi & \checkmark \\ x(y\varphi) = (xy)\varphi & \checkmark \end{cases}$

$\varphi \in Ann(x^{-1}W) \Leftrightarrow \forall w\in W: \ \varphi(x^{-1}w) = (x^{-1}\varphi)(w) = 0 \Leftrightarrow x^{-1}\varphi \in Ann(W)$

$\Leftrightarrow \varphi \in x\,Ann(W)$

Def: Pro $A \in Div\ F/k$ definujme

$$\Omega(A) = \Omega_{F/k}(A) = Ann_{Adèle\ F/k}(a(A)+F)$$

$$\Omega = \Omega(F/k) = \bigcup_{A\in Div F/k} \Omega(A)$$

Množinu $\Omega(F/k)$ nazýváme množinou Weilových diferenciálů.

Pozn:
- Adèle F/k je vekt. prostor nad F aj k
- $\Omega(A) = \{\omega \in (Adèle\ F/k)^* \mid \omega(f)=0 \ \forall f\in a(A),\ \omega(c_x)=0 \ \forall x\in F\}$
  $\leq (Adèle\ F/k)^*$

$Div\ F/k$	$\leq F$	$\leq$ Adèle F	$\leq (Adèle\ F)^*$
B	$\mathcal{L}(B)$	$a(B)$	$\Omega(B)$
$\vee$	$\cup$	$\cup$	$\cap$
A	$\mathcal{L}(A)$	$a(A)$	$\Omega(A)$

6.4.L: Nech $A, B, C \in Div\ F/k$ a nech $x \in F^*$. Potom

(i) $\dim \Omega(A) = \dim {}^{Adèle\ F/k}\!/_{a(A)+F} = i(A)$

(ii) $C = \max\{A,B\}$: $\Omega(A)\cap\Omega(B) = Ann_{Adèle\ F}(a(A)+a(B)+F) = Ann_{..}(a(C)+F)$

$= \Omega(C)$

(iii) $A \leq B \Rightarrow a(A)+F \leq a(B)+F \Rightarrow Ann(a(A)+F) \geq Ann(a(B)+F) \Rightarrow \Omega(A) \supseteq \Omega(B)$

(iv) $C \leq A,\ C \leq B \Rightarrow \Omega(C) \supseteq \Omega(A)+\Omega(B)$

(v) $\Omega(A+(x)) = x\,\Omega(A) \quad \forall x \in F^*$

Už do důsledky předtím:

(i): $Ann_{Adèle}(a(A)+F) \simeq \left({}^{Adèle\ F}\!/_{a(A)+F}\right)^*$

(iv): $\Omega(C)$ je vekt. prostor, $\Omega(B) \supseteq \Omega(A)$, $\Omega(C) \supseteq \Omega(B)$

(v): $x\,Ann(a(A)+F) \overset{6.3}{=} Ann(x^{-1}a(A)+F) \overset{5.10}{=} Ann(a(A+(x))+F) = \Omega(A+(x))$

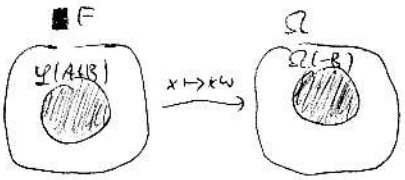
6.5.D: $\Omega(F/k)$ je podpriestor $(\mathbb{A}_F)^*$ chápaním ako v.p. nad F.

6.6.L: Nech $\omega \in \Omega(F/k)$, $\omega \neq 0$ a nech $A, B \in \mathrm{Div}\, F/k$. Ak $\omega \in \Omega(A)$ a $x \in \mathcal{L}(A+B)$, tak $x\omega \in \Omega(-B)$.

$x\omega \in \Omega(-B) \Leftrightarrow \omega \in x^{-1}\Omega(-B) = \Omega(-(x)-B)$

$x \in \mathcal{L}(A+B) \Leftrightarrow A+B+(x) \geq 0 \Leftrightarrow A \geq -(x)-B$

$\omega \in \Omega(A) = \omega \in \Omega(-(x)-B)$ ... □

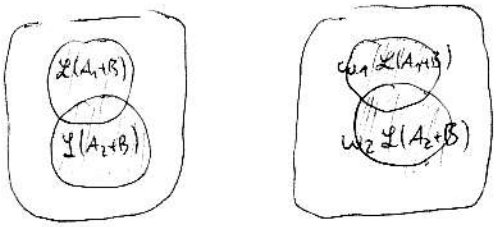


6.7.T: $\Omega(F/k)$ má ako v.p. nad F dimenziu 1.

Vezmime $\omega_1, \omega_2 \in \Omega$, $\omega_1 \neq 0 \neq \omega_2$.

Chceme nájsť $x \in F^*$ takej, že $\omega_2 = x\omega_1$.

Na to stačí, že $\exists x_1, x_2 \in F^*$ takej, že $x_1\omega_1 = x_2\omega_2$



Označme $\omega_1 \in \Omega(A_1)$, $\omega_2 \in \Omega(A_2)$.

Uvažujme B takej, že $\omega_1\mathcal{L}(A_1+B)$ a $\omega_2\mathcal{L}(A_2+B)$ majú nenulový prienik (existencia neskôr), $B \geq 0$.

Nech $y \in \omega_1\mathcal{L}(A_1+B) \cap \omega_2\mathcal{L}(A_2+B)$, $y \neq 0$.

(6.6) $\Rightarrow \frac{1}{y}\omega_1 \in \Omega(-B)$, $\frac{1}{y}\omega_2 \in \Omega(-B)$. Teda $\dim \Omega(-B) = i(-B) \geq$

$\geq \deg(-B) + \ell(-B) \overset{4.14.\text{PL}}{=} \deg B$ (pretože $\deg(-B) < 0$, $\ell(-B) = 0$)

Potom buď $\omega_1 x_1 = \omega_2 x_2$.

(6.6) $\Rightarrow$ vieme, že $\omega_1\mathcal{L}(A_1+B) \subseteq \Omega(-B)$ aj $\omega_2\mathcal{L}(A_2+B) \subseteq \Omega(-B)$

(6.1) $\Rightarrow$ stačí $\dim(\omega_1\mathcal{L}(A_1+B)) + \dim(\omega_2\mathcal{L}(A_2+B)) > \dim\Omega(-B)$

$\Leftrightarrow \ell(A_1+B) + \ell(A_2+B) > i(-B)$

$i(-B) = g-1-\deg(-B)+\ell(-B) \overset{4.14.\text{PL}}{=} g-1+\deg B$

(4.13) $\Rightarrow$ pre B dostatočne veľkého stupňa

$\deg(A_i+B) - \ell(A_i+B) = g-1 \Rightarrow \ell(A_i+B) = \deg A_i + \deg B - g + 1$

$\Rightarrow \ell(A_1+B) + \ell(A_2+B) = g-1+\deg B + (\deg A_1 + \deg A_2 + \deg B - 2g - 2)$. ($\deg B \to \infty$)

Def: Nech $\omega \in \Omega(A)$ definujme

$$M(\omega) = \{B \in \mathrm{Div}\, F/k \mid \omega \in \Omega(B)\}$$

$B \leq A \Rightarrow \Omega(B) \supseteq \Omega(A) \Rightarrow B \in M(\omega) \Rightarrow M(\omega)$ tvorí ideál

6.8.T: $\forall w \in \Omega^{\#}\ \exists! W \in M(w)$, že $A \le W\ \forall A \in M(w)$ ($M(w)$ má max. prvok)

Def: Také W značíme (w)

(4.13) $\Rightarrow$ pre $\deg A$ dostatočne veľké je $i(A) = 0 = \dim \Omega(A) \Rightarrow w \notin \Omega(A) \Rightarrow A \notin M(w)$.

Preto $\{\deg B \mid B \in M(w)\}$ je zhora obmedzená. Voľme $W \in M(w)$, ktorý $\deg W$ bolo maximálne možné.

$A \in M(w) \Rightarrow w \in \Omega(A) \cap \Omega(W) \Rightarrow w \in \Omega(\max\{A, W\}) \Rightarrow \max\{A, W\} \in M(w)$

Keby nerovnalo $A \le W$, tak $\deg \max\{A, W\} > \deg W$ spor.

6.9.D: $A \in \mathrm{Div}\, F/k$, $w \in \Omega(F/k)$, $w \neq 0$. Potom $A \le (w) \Leftrightarrow w \in \Omega(A)$.

6.10.D: $w \in \Omega(F/k)$, $w \neq 0$ a $x \in F^*$. Potom $(xw) = (x) + (w)$

$A \le (xw) \Leftrightarrow xw \in \Omega(A) \Leftrightarrow w \in x^{-1}\Omega(A) \Leftrightarrow w \in \Omega(A - (x)) \Leftrightarrow A - (x) \le (w)$
$\Leftrightarrow A \le (x) + (w)$
$\Leftrightarrow A \in \Omega((x) + (w))$

Def: Divizor sa nazýva kanonický, ak ho vieme vyjadriť ako (w), $w \in \Omega^{\#}$.

6.11.D: Všetky kanonické divizory tvoria v $\mathrm{Div}\, F/k$ presne jednu rozkladovú triedu modulo $\mathrm{Princ}\, F/k$.

$(w_1), (w_2)$ kanonické divizory $\overset{6.7}{\Rightarrow} \exists x: w_1 = x w_2 \overset{6.10}{\Rightarrow} (w_1) = (x) + (w_2)$

6.12.T: Nech $B \in \mathrm{Div}\, F/k$ a $w \in \Omega(F/k)$, $w \neq 0$. Potom $x \mapsto xw$ je izomorfizmus $\mathcal{L}((w) - B) \simeq \Omega(B)$ vekt. priestorov nad k.

$w \in \Omega((w))$, $x \in \mathcal{L}((w) - B) \overset{6.6}{\Rightarrow} xw \in \Omega(B)$. Zostáva surjekcia.

(6.7) $w_1 \in \Omega \Rightarrow w_1 = xw$. Chceme $xw \in \Omega(B) \Rightarrow x \in \mathcal{L}((w) - B)$.

(6.7), (6.10): $xw \in \Omega(B) \Leftrightarrow B \le (xw) \Leftrightarrow B \le (x) + (w) \Leftrightarrow (x) + ((w) - B) \ge 0 \Leftrightarrow x \in \mathcal{L}((w) - B)$

6.13. V: (Riemann-Roch)

Nech W je kanonický divizor. Potom $\forall B \in \mathrm{Div}\, F/k$ platí

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

Víme $i(B) = g - 1 - (\deg B - l(B)) \Rightarrow l(B) = \deg B + i(B) + 1 - g$.
Chceme tedy $i(B) = l(W-B)$. Víme
$i(B) \overset{6.4}{=} \dim \Omega(B) \overset{6.13}{=} \dim \mathcal{L}(W-B) = l(W-B)$.

6.14. D: $B = W$: $l(W) = \deg W + 2 - g$
$B = 0$: $1 = 0 + l(W) + 1 - g$

$l(W) = g$ $\qquad i(W) = 1$
$\deg W = 2g - 2$

6.15. V: (Riemann-Roch)

Ať $A \in \mathrm{Div}\, F/k$ splňuje, že $\deg A \geq 2g-1$, tak $i(A) = 0$, t.j.

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

$\deg(W-A) \leq 2g-2-(2g-1) = -1 < 0$
$\overset{6.14.\,P4}{\Rightarrow} l(W-A) = 0 \overset{6.13}{=} i(A)$

7. ELIPTICKÉ FUNKČNÉ TELESO

$\mathbb{P}$ .. miesta, g ... rod

7.1.L: Pre $n \geq 1$, $x \in F$ a $P \in \mathbb{P}$ platí $x \in \mathcal{L}(nP) \Leftrightarrow \exists i \in \{0, \dots, n\}$, že $(x)_\infty = iP$.
Pritom $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P) \Leftrightarrow (x)_\infty = nP$.
V tom prípade je $[F : K(x)] = n \deg P$.

$x \in \mathcal{L}(nP) \Leftrightarrow (x) + nP \geq 0 \Leftrightarrow (x)_\infty = iP$, $i \in \{0, \dots, n\}$
$\Rightarrow x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P) \Leftrightarrow (x)_\infty = nP$; $[F : k(x)] \overset{4.8}{=} \deg (x)_\infty = n \deg P$

7.2.L: Nech $(n-1) \deg P \geq 2g-1$, kde $P \in \mathbb{P}$, $n \in \mathbb{Z}$. Potom $\exists x \in F$, že $(x)_\infty = nP$.

(7.1).. chceme $\ell(nP) > \ell((n-1)P)$
(RR).. Riemann-Roch (6.15).. $\deg (n-1)P \geq 2g-1 \Rightarrow \ell((n-1)P) = \deg (n-1)P - g + 1$
$\deg nP = \deg P + \deg (n-1)P \geq 2g-1 \Rightarrow \ell(nP) = \deg P + \deg (n-1)P - g + 1$

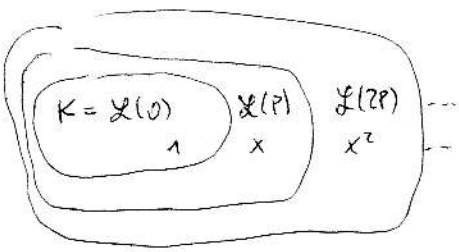
7.3.D: Nech $g = 0$ a $\exists P \in \mathbb{P}$ stupňa 1. Potom $\exists x$, že $F = K(x)$.

(7.2): $n = 1 \Rightarrow (n-1)\deg P = 0 \geq 2g-1 = -1$ ✓
$\Rightarrow \exists x$: $(x)_\infty = P \Rightarrow [F : K(x)] = \deg P = 1 \Rightarrow F = K(x)$

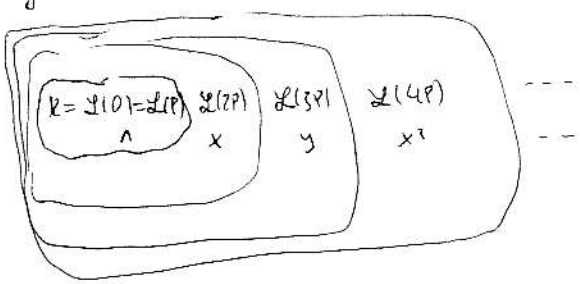
7.4.L: Nech $g = 1$ a $P \in \mathbb{P}$ stupňa 1. Potom $\mathcal{L}(P) = \mathcal{L}(0)$ a $\ell(kP) = k$ $\forall k \geq 1$.

$\mathcal{L}(0) \simeq K$, $\ell(0) = 1$. Pre $k \geq 1$ platí $\deg (kP) = k \geq 1 = 2g-1$.
RR $\Rightarrow \ell(kP) = \deg(kP) - g + 1 = \deg(kP) = k$

$g = 0$



$g = 1$



7.5.L: Nech n, m sú nesúdeliteľné, n prirodzené. Ak $[F : k(x)] = n$ a $[F : k(y)] = m$, tak $F = k(x, y)$.

$m = 1$ triviálne: [redacted]

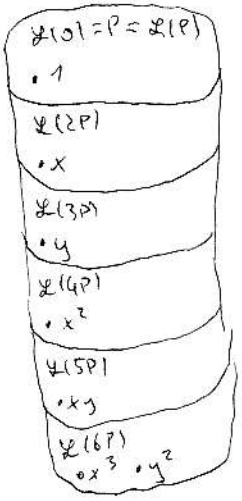
$1 = [F : k(y)] = [F : k(x,y)]\,[k(x,y) : k(y)] = 1 \Rightarrow F = k(x,y)$.
($[F : k(x,y)] = 1$, $[k(x,y) : k(y)] = m$)

$[F : K(x)] = [F : k(x,y)]\,[k(x,y) : k(x)] = n$ (prirodzené)
- $[F : k(x,y)] = 1$, $[k(x,y) : k(x)] = n \Rightarrow F = k(x,y)$ ✓
- $[F : k(x,y)] = n$, $[k(x,y) : k(x)] = 1 \Rightarrow k(x,y) = k(x) \Rightarrow k(x) \geq k(y)$
  $[F : k(x,y)]\,[k(x,y) : k(y)] = [F : k(y)]$ ↯
  (n, m)

7.6. V: Nech $g=1$ a $P \in \mathbb{P}$ je stupňa 1. Potom existujú $x, y \in F$ také, 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 pre vhodné $a_i \in k$ platí

(WR) $y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$

(7.4) $\Rightarrow$ x, y existujú (množiny, z ktorých sú x, y nepriazdne)
(7.1) $\Rightarrow$ $[F:k(x)] = 2 \deg P = 2$, $[F:k(y)] = 3 \deg P = 3$
(7.5) $\Rightarrow$ $F = k(x,y)$
(7.1) $\Rightarrow$ $(x)_\infty = 2P \Rightarrow v_P(x) = -2$, $(y)_\infty = 3P \Rightarrow v_P(y) = -3$



$v_P(x) = -2$ $\quad$ $v_P(xy) = -5$
$v_P(y) = -3$ $\quad$ $v_P(x^3) = -6$
$v_P(x^2) = -4$ $\quad$ $v_P(y^2) = -6$

(7.4) $\Rightarrow$ $\dim \mathcal{L}(kP) = k \Rightarrow \dim \mathcal{L}(6P) = 6 \Rightarrow$
$\Rightarrow \{1, x, y, xy, x^2, x^3, y^2\}$ sú LZ $\Rightarrow \exists u_i, v_j \in k$:

$$u_1 y^2 + u_2 xy + u_3 y = v_1 x^3 + v_2 x^2 + v_3 x + v_4$$

Pritom $\{1, x, y, x^2, xy\}$ sú LNZ, pretože tvoria bázu $\mathcal{L}(5P) \Rightarrow$
$\Rightarrow u_1 \neq 0 \wedge v_1 \neq 0$ (ak obe nulové, tak $\{\dots\}$ LZ; ak jedno, tak BUNV $x^2 \in \mathcal{L}(5P)$ (!).
Rovnicu zo zadania dostaneme vynásobením $u_1^3 v_1^2$ a substitúciou
$\tilde{y} = u_1^2 v_1 y$, $\tilde{x} = u_1 v_1 x$.

7.7. T: Nech $F = k(x)$. Potom $y = 0$, $k[x]$ je valuačný obor, x jeho uniformizujúci prvok a $\deg(x k[x]) = 1$.

$[F:k(x)] = 1 \Rightarrow \deg(x)_\infty = 1 \Rightarrow \exists! P : (x)_\infty = P \Rightarrow (x^k)_\infty = kP$.
(7.1) $\Rightarrow x^k \in \mathcal{L}(kP) \setminus \mathcal{L}((k-1)P)$, $\{1, x, \dots, x^k\} \in \mathcal{L}(kP)$ LNZ $\Rightarrow \underline{\ell(kP) \geq k+1}$
$k \geq 2g-1 \Rightarrow \deg kP \geq 2g-1$
(RR) $\Rightarrow$ $k+1 \leq \ell(kP) = \deg kP - g + 1 = k - g + 1 \Rightarrow g \leq 0 \Rightarrow \underline{g = 0}$.
$(x)_\infty = P \Rightarrow v_P(x^{-1}) = 1 \Rightarrow x^{-1}$ je uniformizujúci prvok,
$\mathcal{O}_P = k[x^{-1}]$ a $P = x^{-1} k[x^{-1}]$.
Uvažovaním ob zvyšných $x \in x^{-1}$ $(F = k(x) \Leftrightarrow F = k(x^{-1}))$ dostaneme tvrdenie.

(27)

Ako vyzerajú všetky miesta?

$p \in K[x]$ ireducibilný

$v_p\left(\frac{f}{g}\right) = v_p(f) - v_p(g)$ $\qquad v_p(f) = \max\{i \mid p^i | f\}$

-- miesta zodpovedajúce valuáciam (nulovosky polynómu p)

--- chýba miesto zodpovedajúce nevlastnej priamke (miesto v ∞)

$v_\infty\left(\frac{f}{g}\right) = \deg g - \deg f$

$v_\infty\left(\frac{1}{x}\right) = 1 - 0 = 1$ $\qquad v_\infty\left(\frac{1}{x^k}\right) = k$

$v_\infty(a_0 + \dots + a_k x^k) = v_\infty\left(x^k\left(\frac{a_0}{x^k} + \dots + \frac{a_k}{x^0}\right)\right) = -k + 0 = -k$

($a_k \neq 0$; $-k$; $\min = 0$)

$v_\infty\left(\sum a_i x^i\right) = -k$ -- $v_\infty(f) = -\deg f$

stupeň miesta = stupeň polynómu

Weierstrassova rovnica (WR)

$$\underbrace{y^2 + a_1 xy + a_3 y}_{L} = \underbrace{x^3 + a_2 x^2 + a_4 x + a_6}_{R}$$

$V = \mathbb{V}(I)$, pravidelná $I = (f)$, $f = R - L$

$\tilde{V} = \mathbb{V}(v_i^{-1}(I)) \overset{\text{dekomp.}}{=} L(\mathfrak{v}_0^*(f))$ ... nepreniesteme rovnicou: (homogenizáciu)

$$Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3$$

graf prechádza miestom P

hľadáme body -- $Z = 0 \Rightarrow X = 0$ a Y nenulové $\qquad k(V) \ni \frac{f+I}{y+I}$ $\qquad f(P) = 0,\ g(P) \neq 0$



- miesto zodpovedá všetkým vac. funkciám, ktoré sú $\dots$ v bode P determinant
- Je nutné overiť, že vo funkčnom telese, ktoré zodpovedá nejakej krivke, zodpovedajúce body tejto krivky $\S$?!
  a uniformizujúce prvky nedolyčíriam

$F = k(x,y)$ -- vždy sa dá urobiť pomocou dvoch generátorov

$[F : k(x)] < \infty$ separabilné kon. stupňa $\Rightarrow$ jednoduché

$F = (k(x))[y]$ pre nejaké $y \in F$ -- y hovorí nejakého polynómu $a_0 + \dots + a_k t^k = 0$,

$a_i \in k(x)$ -- $a_i = \frac{b_i(x)}{c_i(x)}$ --- po rozšírení nenulovými $a_i \in k[x]$ .. polynóm $f(x,y)$

$F = k(\mathbb{V}(f))$

$\rightsquigarrow$ eliptické funkčné teleso ($g = 1$) je alg. funkčným telesom WR.