Norma na tělese K

$$|\cdot| : K \to \mathbb{R}$$

$|0| = 0$, $\forall \alpha \in K \quad \alpha \neq 0 \Rightarrow |\alpha| > 0$

$\forall \alpha, \beta \in K : \quad |\alpha\beta| = |\alpha| \cdot |\beta|$

$\forall \alpha, \beta \in K : \quad \underline{|\alpha + \beta| \leq |\alpha| + |\beta|}$

Ostrowski: Existují (až na ekvivalenci) jen tyto normy na $\mathbb{Q}$

1. „triviální" ($\alpha \in \mathbb{Q}, \alpha \neq 0 \Rightarrow |\alpha| = 1$)
2. absolutní hodnota
3. p-adická norma vzhledem k libovolnému prvočíslu p

$\alpha \in \mathbb{Q}, \alpha \neq 0 \qquad \alpha = p^m \cdot \frac{r}{s}$, $r \in \mathbb{Z}, s \in \mathbb{N}$, $(r,s) = 1$, $p \nmid r, s$

$$|\alpha|_p = p^{-m}$$

zúplnění $\mathbb{Q}$ vzhledem k $|\cdot|_p$ dostaneme těleso $\mathbb{Q}_p$ p-adických čísel.

nearchim. norma:

$$|\alpha+\beta| \leq \max\{|\alpha|, |\beta|\}$$

(to splní např. $|\cdot|_p$)

$\{\alpha \in K ; |\alpha| \leq 1\}$ je podokruh v K

$$\mathbb{Z}_p = \{\alpha \in \mathbb{Q}_p ; |\alpha|_p \leq 1\}$$

$$\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

$$\mathbb{Z}/p\mathbb{Z} \twoheadleftarrow \mathbb{Z}/p^2\mathbb{Z} \twoheadleftarrow \dots \quad \mathbb{Z}/p^n\mathbb{Z} \twoheadleftarrow \mathbb{Z}/p^{n+1}\mathbb{Z} \dots$$

každé nenulové $\alpha \in \mathbb{Q}_p$ je tvaru

$$p^m \cdot \sum_{i=0}^{\infty} a_i p^i, \quad a_i \in \{0, 1, \dots, p-1\}, \quad a_0 \neq 0$$

$$|p^i| = \frac{1}{p^i}$$

$$\begin{array}{cccc}
L & \mathcal{O}_L \supseteq \mathfrak{P} & \mathcal{O}_L/\mathfrak{P} & L_{\mathfrak{P}} \\
| & | & |\,f & |\,ef \\
K & \mathcal{O}_K \supseteq \mathfrak{p} & \mathcal{O}_K/\mathfrak{p} & K_{\mathfrak{p}} \\
| & | & |\,f_0 & |\,e_0 f_0 \\
\mathbb{Q} & \mathbb{Z} \supseteq p\mathbb{Z} & \mathbb{Z}/p\mathbb{Z} & \mathbb{Q}_p \\
 & & \text{tělesa zbytků} & \text{zúplnění}
\end{array}$$

$\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$

$\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$

$\mathfrak{P}$ se <u>větví</u> nad $\mathfrak{p}$ $\overset{\text{def.}}{\Longleftrightarrow}$ $\mathfrak{P}^2 \mid \mathfrak{p}\mathcal{O}_L \Longleftrightarrow e > 1 \Longleftrightarrow$

$$\Longleftrightarrow [L_{\mathfrak{P}} : K_{\mathfrak{p}}] > [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$$

$$\mathcal{O}_L/\mathfrak{P} \cong \underline{\{\alpha \in L;\ |\alpha|_{\mathfrak{P}} \le 1\}} \,/\, \underline{\{\alpha \in L;\ |\alpha|_{\mathfrak{P}} < 1\}}$$

$\sigma : L \to \mathbb{C}$ $\qquad |\alpha|_\sigma = |\sigma(\alpha)|$

$$\begin{array}{cc|ccc}
L & L_\sigma & \mathbb{R} & \mathbb{C} & \mathbb{C} \\
| & | & 1| & 2| & 1| \\
K & K_\sigma & \mathbb{R} & \mathbb{R} & \mathbb{C} \\
| & | & 1| & 1| & 2| \\
\mathbb{Q} & \mathbb{Q}_\sigma = \mathbb{R} & \mathbb{R} & \mathbb{R} & \mathbb{R}
\end{array}$$

σ se větví v L/K

$\Updownarrow$ def.

$[L_\sigma : K_\sigma] > 1$

$K=\mathbb{Q}(\sqrt{-m})$ $\qquad m\in\mathbb{N},\ \square\nmid m$

$$d_K=\begin{cases}-m & m\equiv 3 \pmod 4\\ -4m & m\not\equiv 3 \pmod 4\end{cases}$$

(5.2) ... $-4n$ je telesový diskriminant $\mathbb{Q}(\sqrt{-n})$

$$\left.\begin{array}{c} H \\ | \\ K=\mathbb{Q}(\sqrt{-n}) \\ | \\ \mathbb{Q} \end{array}\right]\ \text{Gal.}$$

$$\begin{tikzcd}
 & H=K(\alpha) \arrow[dl, dash, "h_K"'] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & H\cap\mathbb{R} = \mathbb{Q}(\alpha) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

$$\begin{tikzcd} 1 \arrow[r] & H \arrow[r] & G \arrow[r] & G/H \arrow[r] \arrow[l, bend left, "\text{homom.}"] & 1 \end{tikzcd}$$

$$H,\quad K \leq G$$

$$H \trianglelefteq G,\quad \underline{H \cap K = \{1\}},\quad \langle H \cup K \rangle = G$$

$$\langle H \cup K \rangle = H \cdot K = \{h \cdot k;\ h \in H, k \in K\}$$

$$h_1 k_1 h_2 k_2 = \underbrace{h_1}_{\in H} \overbrace{\underbrace{k_1 h_2 k_1^{-1}}_{\in H}}^{H} \cdot \underbrace{k_1 k_2}_{\in K}$$

$$k_1 h_2 k_1^{-1} \in H$$

$$h_1 \cdot k_1 = h_2 \cdot k_2 \quad / \cdot k_2^{-1} \quad / h_1^{-1}$$

$$K \ni k_1 k_2^{-1} = h_1^{-1} h_2 \in H \Rightarrow h_1 = h_2,\ k_1 = k_2$$

$$k \cdot h = \underbrace{k h k^{-1}}_{\in H} \cdot \underbrace{k}_{\in K} \qquad k h k^{-1} = h^k$$

$$G \to G,\quad h \mapsto h^k$$

$$k \cdot h = \sigma_k(h) \cdot k$$

vnitřní automorfismus

pro lib. $k \in K$ mám $\sigma_k(h) = k h k^{-1}$

$$\sigma_k : H \to H$$

$k_1, k_2 \in K$ $\quad \sigma_{k_1 k_2}(h) = k_1 k_2 h k_2^{-1} k_1^{-1} =$

$$= \sigma_{k_1}(\sigma_{k_2}(h))$$

$$\begin{array}{cccc} \sigma_\bullet : & K & \longrightarrow & \mathrm{Aut}(H) \\ & \psi & & \psi \\ & k & \longmapsto & \sigma_k \end{array}$$

je homomorfismus grup

Mám grupy H, K, homomorfismus grup $\sigma_\bullet : K \longrightarrow \mathrm{Aut}(H)$. Definujeme ~~grupu~~

$$H \rtimes K = \{(h, k);\ h \in H,\ k \in K\}$$

$$(h_1, k_1)(h_2, k_2) = (h_1 \cdot \sigma_{k_1}(h_2), k_1 \cdot k_2)$$

$\mathbb{D}_n$ grupa sym. prav. n-úhel.

r rotace o $\frac{2\pi}{n}$, s osová soum.

$\langle r \rangle \leq \mathbb{D}_n$ $\quad \{id, s\}$

$$\sigma_s(r) = r^{-1}$$

$$\mathbb{D}_n = \langle r \rangle \rtimes \langle s \rangle$$

$s \circ r \circ s = r^{-1} \Rightarrow s r = r^{-1} s$

M

K

label

Q

M ... Galois field

největší rozšíření K

které je nerozv. nad K

abelovské nad Q