

Norma na tělese K

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

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

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

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

Ostrovski: Existují (ať už ekvivalentně)

ještě normy na \mathbb{Q}

① 'triviální' ($\alpha \in \mathbb{Q}, \alpha \neq 0 \Rightarrow |\alpha| = 1$)

② absolutní hodnota

③ p -adická norma vhlédem
k libovolnému prvočíslu p

$$\alpha \in \mathbb{Q}, \alpha \neq 0 \quad \alpha = p^m \cdot \frac{r}{s} \quad \left(\begin{array}{l} r \in \mathbb{Z}, s \in \mathbb{N} \\ (r, s) = 1 \\ p \nmid r, s \end{array} \right)$$
$$|\alpha|_p = p^{-m}$$

zápleť \mathbb{Q} vhlédem k $|\cdot|_p$

dostaneme těleso \mathbb{Q}_p p -adicky úpl.

neardim. norma:

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

(to zplni uspr. 1.0.1p)

$\{ \alpha \in K ; |\alpha| \leq 1 \}$ je podobuh vK

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

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

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

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

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

L	$\mathcal{O}_L \cong \mathcal{O}$	$\mathcal{O}_L/\mathcal{O}$	L/\mathcal{O}
$ $	$ $	$ f$	$ ef$
K	$\mathcal{O}_K \cong \mathfrak{p}$	$\mathcal{O}_K/\mathfrak{p}$	K/\mathfrak{p}
$ $	$ $	$ f_0$	$ ef_0$
\mathbb{Q}	$\mathbb{Z} \cong p\mathbb{Z}$	$\mathbb{Z}/p\mathbb{Z}$	\mathbb{Q}_p

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

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

filosa
zlystia

zúplnení

$$\mathcal{O} \text{ se v\u011etr\u00e1 med } \mathfrak{p} \stackrel{\text{def.}}{\Leftrightarrow} \mathcal{O}^2 \mid \mathfrak{p}\mathcal{O}_L \Leftrightarrow e > 1 \Leftrightarrow$$

$$\Leftrightarrow [L/\mathcal{O} : K/\mathfrak{p}] > [\mathcal{O}_L/\mathcal{O} : \mathcal{O}_K/\mathfrak{p}]$$

$$\mathcal{O}_L/\mathcal{O} \cong \frac{\{\alpha \in L \mid |\alpha|_{\mathcal{O}} \leq 1\}}{\{\alpha \in L \mid |\alpha|_{\mathcal{O}} < 1\}}$$

$$\sigma : L \rightarrow \mathbb{C}$$

$$|\alpha|_{\mathcal{O}} = |\sigma(\alpha)|$$

L	L_{σ}	\mathbb{R}	\mathbb{C}	\mathbb{C}	σ se v\u011etr\u00e1 do K \updownarrow def.
$ $	$ $	$ 1$	$ 2$	$ 1$	
K	K_{σ}	\mathbb{R}	\mathbb{R}	\mathbb{C}	$[L_{\sigma} : K_{\sigma}] > 1$
$ $	$ $	$ 1$	$ 1$	$ 2$	
\mathbb{Q}	$\mathbb{Q}_{\sigma} = \mathbb{R}$	\mathbb{R}	\mathbb{R}	\mathbb{R}	

$$K = \mathbb{Q}(\sqrt{-m})$$

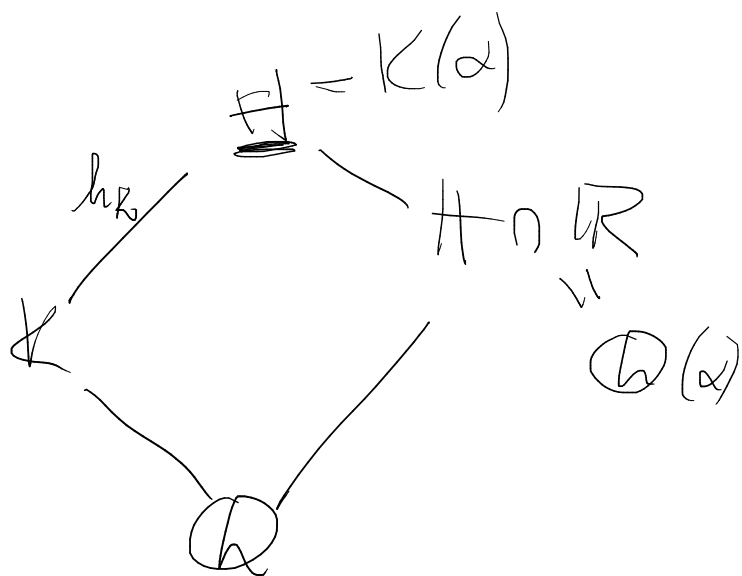
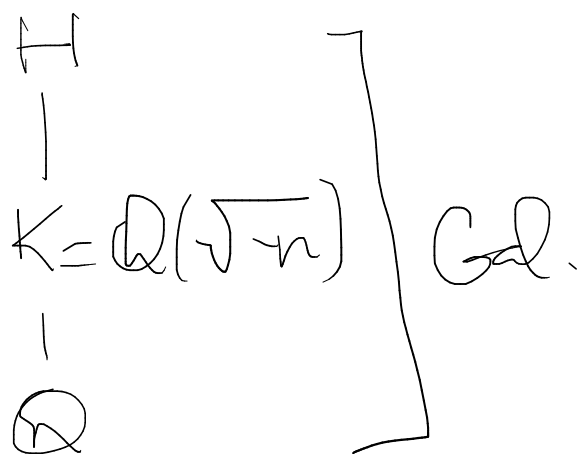
$$m \in \mathbb{N}, \quad \square \nmid m$$

$$d_K = \begin{cases} -m \\ -4m \end{cases}$$

$$m \equiv 3 \pmod{4}$$

$$m \not\equiv 3 \pmod{4}$$

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



$$1 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 1$$

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

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

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

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

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

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

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

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

$$khk^{-1} = h$$

$$\begin{array}{ccc} G & \rightarrow & G \\ \cup & & \cup \\ H & \rightarrow & H \end{array} \quad k$$

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

conjugation automorphisms

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

$$\sigma_k : H \rightarrow H$$

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

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

$$\sigma : K \rightarrow \text{Aut}(H)$$

$$\psi \quad \psi \\ k \mapsto \sigma_k$$

je homomorfisma grup

Maka grup H, K , homomorfisma grup

$\sigma : K \rightarrow \text{Aut}(H)$. Definisi grup

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

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

\mathbb{D}_n grup sym. perov. n -lateral.

r rotasi $\frac{2\pi}{n}$ | s osok osok.

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

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

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

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

M

K

label.

\mathbb{Q}

M... Gauss field

největší rozšíření K

které je normální

abelské nad \mathbb{Q}
