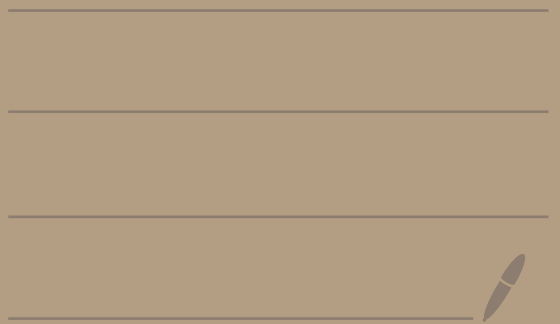


Zth II

2. Vorlesung

22.4.2020



$$\begin{array}{l}
 k \\
 | \\
 \mathbb{Q}
 \end{array}
 \quad
 \begin{array}{l}
 \mathbb{F} \\
 | \\
 \mathbb{P}
 \end{array}
 \quad
 \begin{array}{l}
 N_{\mathbb{F}} = N_{k|\mathbb{Q}}(\mathbb{F}) = |\mathcal{O}_k/\mathbb{F}| \\
 N_{\mathbb{P}} = |\mathcal{O}_k/\mathfrak{p}| \\
 N(\alpha \mathcal{O}_k) = |N_{k|\mathbb{Q}}(\alpha)|
 \end{array}$$

Wiederholung

$$m = m_0 m_{\infty} \quad \text{Divisor, } m_0 \triangleleft \mathcal{O}_k$$

$\hat{=}$ quadratfreies Produkt
von reellen unendlichen Stellen



$$\tau: k \hookrightarrow \mathbb{R} \subseteq \mathbb{C}$$

$$k_m^* = \{ \alpha \in k^* \mid \alpha \equiv 1 \pmod{m} \}$$

$$\left\{ \begin{array}{l} v_{\mathfrak{p}}(\alpha - 1) \geq v_{\mathfrak{p}}(m_0), \forall \mathfrak{p} \mid m_0 \\ \sigma(\alpha) > 0, \forall \sigma \mid m_{\infty} \end{array} \right.$$

$$P_k(m) := \{ \alpha \mathcal{O}_k \mid \alpha \in k_m^* \} \leq P_k$$

$$d_k(m) := \frac{I_k(m)}{P_k(m)}$$

Strahlklassen-
gruppe mod m

Bem: • $d_k(1) = d_k$

• $d_k(m) \rightarrow d_k, \quad \alpha P_k(m) \mapsto \alpha P_k$

$$(\mathcal{O}_k/m)^{\times} := (\mathcal{O}_k/m_0)^{\times} \times \underbrace{\{\pm 1\} \times \dots \times \{\pm 1\}}_{\text{ein Faktor pro } \mathfrak{p} \in \mathfrak{p} \mid m_0}$$

↑
S

$$(\bar{\alpha} = \bar{\alpha}_1 \bar{\alpha}_2^{-1}, (\text{sgn}(\sigma(\alpha)))_{\mathfrak{p} \mid m_0})$$

↑

$$\{\alpha \in k^{\times} \mid (\alpha, m_0) = 1\}$$

$$\alpha = \frac{\alpha_1}{\alpha_2}$$

$$\alpha_1, \alpha_2 \in \mathcal{O}_k$$

$$\alpha_i \mathcal{O}_k + m_0 = \mathcal{O}_k$$

Erinnerung an den Approximationsatz:

Gegeben: • $\|\cdot\|_1, \dots, \|\cdot\|_n$ paarweise inäquivalente
Bewertungen von k

• $a_1, \dots, a_n \in k$

• $\varepsilon > 0$

Dann gibt es $\alpha \in k$ mit $|\alpha - a_i|_i < \varepsilon$
für $i = 1, \dots, n$.

Surjektivität von S:

Sei $(\bar{\alpha}, (\varepsilon_1, \dots, \varepsilon_s)) \in (\mathcal{O}_k/m)^{\times}$, d.h.
 $\bar{\alpha} \in (\mathcal{O}_k/m_0)^{\times}$, $\varepsilon_i \in \{\pm 1\}$, $m_0 = \mathfrak{p}_1 \dots \mathfrak{p}_s$

Approximationssatz liefert $\alpha \in k^x$ mit

$$|\alpha - a|_f < \varepsilon \quad \text{für } f | m_0$$

$$|\alpha - \varepsilon_i|_i < \varepsilon \quad \text{für } i=1, \dots, s$$

Wähle ε klein genug, d.h. es sollte gelten $\varepsilon < \frac{1}{2}$. Ferner sollte gelten:

$$\alpha \equiv a \pmod{m_0}$$

$$\Leftrightarrow \alpha \equiv a \pmod{f^{v_f(m_0)}}, \quad \forall f | m_0$$

$$\Leftrightarrow v_f(\alpha - a) \geq v_f(m_0), \quad \forall f | m_0$$

$$\Leftrightarrow N_f^{-v_f(\alpha - a)} \leq N_f^{-v_f(m_0)} \quad m_0 = \prod_{f|m_0} f^{v_f(m_0)}$$

$$\Leftrightarrow |\alpha - a|_f \leq N_f^{-v_f(m_0)}, \quad \forall f | m_0$$

Satz: Die folgende Sequenz ist exakt

$$0 \rightarrow \mathcal{O}_k^x \cap k_m^x \rightarrow \mathcal{O}_k^x \rightarrow (\mathcal{O}_k/m)^x \rightarrow d_k(m) \rightarrow d_k \rightarrow 0$$

$$\zeta(\alpha) \mapsto (\alpha) \mathcal{P}_k(m)$$

$$u \mapsto (\bar{u}, (\text{sgn}(\zeta(u)))_{f|m_0})$$

Beweis: Übung. ▣

Folgerung: Es gilt: $|d_k(m)| < \infty$

Genauer:

$$|d_k(m)| = h_k \cdot \frac{\#(\mathcal{O}_k/m)^x}{\#(\mathcal{O}_k / (\mathcal{O}_k \cap \mathfrak{m}^x))}$$

Beweis:

$$0 \rightarrow \frac{\mathcal{O}_k^x}{\mathcal{O}_k \cap \mathfrak{m}^x} \rightarrow (\mathcal{O}_k/m)^x \rightarrow d_k(m) \rightarrow d_k \rightarrow 0$$

\uparrow ist exakt.

Beh: Dies ist endlich

Bew: Übung □

$$\#(\mathcal{O}_k/m_0)^x = \prod_{\mathfrak{p} | m_0} \varphi \left(\frac{N_{\mathfrak{p}}^{v_{\mathfrak{p}}(m_0)}}{\mathfrak{p}} \right)$$

$\varphi(a) = \#(\mathcal{O}_k/a)^x$ Eulerische Funktion

$$\varphi(\mathfrak{p}^e) := (N_{\mathfrak{p}} - 1) N_{\mathfrak{p}}^{e-1}$$

ZIEL: Definition der Artinabbildung

Erinnerung an Frobenius-elemente:

$$G \begin{pmatrix} K \supseteq \mathcal{O}_K \supseteq \mathfrak{p} \\ k \supseteq \mathcal{O}_k \supseteq \mathfrak{q} \end{pmatrix} \quad \begin{array}{l} \text{Zahlkop.} \\ \bar{K} = \mathbb{R}(\mathfrak{p}) := \mathcal{O}_K/\mathfrak{p} \\ |) f = f(\mathfrak{p}|\mathfrak{q}) \\ \bar{k} = \mathbb{R}(\mathfrak{q}) := \mathcal{O}_k/\mathfrak{q} \end{array}$$

\bar{K}/\bar{k} ist zyklische Galois-erweiterung vom Grad f . $\text{Gal}(\bar{K}/\bar{k}) = \langle f \rangle$,

f = Frobenius, wobei

$$f(x) = x^q, \quad \forall x \in \bar{K}$$

wobei $q = |\bar{k}| = N_{\mathfrak{q}} = N_{\mathfrak{p}|\mathfrak{q}}$.

Sei $Z = Z(\mathfrak{p}|\mathfrak{q}) := \{ \sigma \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p} \}$
die Zerlegungsgruppe.

Sei $T = T(\mathfrak{p}|\mathfrak{q}) := \{ \sigma \in Z \mid \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{p}}, \forall \alpha \in \mathcal{O}_K \}$
die Verzweigungsgruppe.

Die Sequenz

$$0 \rightarrow T \rightarrow Z \rightarrow \text{Gal}(\bar{k}|\bar{k}) \rightarrow 0$$
$$\sigma \mapsto (\bar{\alpha} \mapsto \overline{\sigma(\alpha)})$$

ist exakt.

$$\bar{\alpha} \in \mathcal{O}_K/\mathfrak{p} = \bar{k}$$

Bekannt: $|T(\mathfrak{p}|\mathfrak{y})| = e(\mathfrak{p}|\mathfrak{y})$

Also: $\mathfrak{p}|\mathfrak{y}$ ist unverzweigt

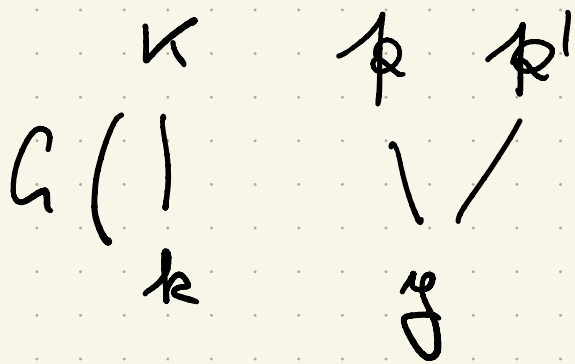
$$\Leftrightarrow |T(\mathfrak{p}|\mathfrak{y})| = 1$$

$$\Leftrightarrow Z \simeq \text{Gal}(\bar{k}|\bar{k})$$

Sei $\mathfrak{p}|\mathfrak{y}$ unverzweigt.

"$\langle \varphi \rangle$"

Also gibt es einen (globalen) Frobenius $\sigma_{\mathfrak{p}}$
mit $\sigma_{\mathfrak{p}} \in Z \subseteq G$. $\sigma_{\mathfrak{p}}$ ist eindeutig
bestimmt durch $N_{\mathfrak{y}}$
$$\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{N_{\mathfrak{y}}} \pmod{\mathfrak{p}}, \quad \forall \alpha \in \mathcal{O}_K$$



Dann gibt es $\tau \in G$
mit $\tau(\mathfrak{p}) = \mathfrak{p}'$

Es gilt:

$$Z(\mathfrak{p}'/k) = \tau Z(\mathfrak{p}/k) \tau^{-1}$$

$$T(\mathfrak{p}'/k) = \tau T(\mathfrak{p}/k) \tau^{-1}$$

Weiter gilt:

$$\sigma_{\mathfrak{p}'}(\tau^{-1}(\alpha)) \equiv \tau^{-1}(\alpha)^{N_{\mathfrak{f}}} \pmod{\mathfrak{p}'}, \quad \forall \alpha \in \mathcal{O}_K$$

$$\Leftrightarrow (\tau \sigma_{\mathfrak{p}} \tau^{-1})(\alpha) \equiv \alpha^{N_{\mathfrak{f}}} \pmod{\mathfrak{p}'}$$

$$\Rightarrow \boxed{\sigma_{\mathfrak{p}'} = \tau \sigma_{\mathfrak{p}} \tau^{-1}}$$

Falls $K|k$ abelsch ist, so ist $\sigma_{\mathfrak{p}'} = \sigma_{\mathfrak{p}}$

und wir schreiben $\underline{\underline{\sigma_{\mathfrak{f}} = \sigma_{\mathfrak{p}} = \sigma_{\mathfrak{p}'}}}}$.

Definition (Artinabbildung)

Sei $K|k$ abelsch. Dann induziert

$$\mathfrak{f} \mapsto \sigma_{\mathfrak{f}}$$

einen Homomorphismus

$$\mathbb{I}_k(\mathcal{O}_{K|k}) \longrightarrow \text{Gal}(K|k)$$

$$\mathfrak{a} \mapsto (\mathfrak{a}, K|k) = \sigma_{\mathfrak{a}}$$

durch multiplikative Fortsetzung.

Erklärung:

- $\mathfrak{f} \in \mathbb{I}_k(\mathcal{O}_{K|k}) \Rightarrow \mathfrak{f}$ unverzweigt in $K|k$
 \uparrow Relativdiskriminante

- Explizit: Falls $\mathfrak{a} = \prod_{\mathfrak{f}} \mathfrak{f}^{v_{\mathfrak{f}}(\mathfrak{a})}$
 $v_{\mathfrak{f}}(\mathfrak{a}) \in \mathbb{Z}$, fast alle gleich 0

so ist

$$(\mathfrak{a}, K|k) = \prod_{\mathfrak{f}} \sigma_{\mathfrak{f}}^{v_{\mathfrak{f}}(\mathfrak{a})}$$

Dies ist wohldefiniert, weil $I_k(f)$, $f \in \mathcal{O}_k$, frei erzeugt ist von den Primidealen \mathfrak{p} mit $\mathfrak{p} \nmid f$.

SATZ 1: Sei $K|k$ abelsch. Dann gibt es einen Divisor $f = f_0 f_\infty$ von k mit:

(1) \mathfrak{p} ist verzweigt in $K|k$

$$\Leftrightarrow \mathfrak{p} \mid f$$

(2) Zu jedem Divisor m mit $f \mid m$ gibt es eine eindeutige Untergruppe H von $I_k(m)$ mit $P_k(m) \subseteq H$, so daß

$$\begin{array}{ccc} I_k(m)/H & \longrightarrow & \text{Gal}(K|k) \\ \text{or } H & \longmapsto & (\sigma, K|k) \end{array}$$

ein Isomorphismus ist

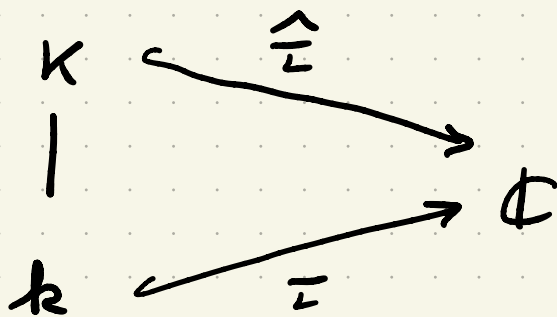
Genauer gilt:

$$H = P_k(m) \cdot N_{K|k}(I_k(m)_0 \mathcal{O}_k)$$

Erläuterungen:

1) Wann ist $\pi: k \rightarrow \mathbb{C}$ verzweigt?

Es gilt:



$\hat{\pi}$ definiert
Stelle über π ,
falls $\hat{\pi}|_k = \pi$.

Def.: π heißt verzweigt

$\Leftrightarrow \pi$ reell & $\hat{\pi}$ komplex.

Definition:

(1) Es gibt ein minimales f mit den Eigenschaften in Satz 1. Dieses heißt Führer oder Kondukt ν von $K|k$.

Man schreibt: $f_{K|k} = f(K|k)$.

(2) Jedes m mit $f_{K|k} | m$ nennt man Erklärungsmodul von $K|k$.

SATZ 2 (Existenzsatz)

Sei m ein Divisor von k und $H \leq I_k(m)$ mit $P_k(m) \leq H$. Dann gibt es eine eindeutig bestimmte abelsche Erweiterung $K|k$ mit:

- (1) Falls \mathfrak{y} in $K|k$ verzweigt, so folgt $\mathfrak{y} | m$.
- (2) Es gilt

$$H = P_k(m) \cdot N_{K|k} (I_K(m, \mathcal{O}_K))$$

und

$$\begin{array}{ccc} I_k(m) / H & \xrightarrow{\cong} & \text{Gal}(K|k) \\ \alpha \in H & \longmapsto & (\alpha, K|k) \end{array}$$

ist ein Iso. (mit anderen Worten:

$I_k(m) \rightarrow \text{Gal}(K|k), \alpha \mapsto (\alpha, K|k),$
ist surjektiv und hat Kern H .)