Vorlesung 3

27.4.2020

Wiederholung:

$\mathfrak{P} \mid \mathfrak{p}$ $K \mid k$ $\Big)$ G ab.

$\mathfrak{p} \longmapsto \sigma_{\mathfrak{p}}$ induziert

$$I_k(m) \longrightarrow G$$
$$\mathfrak{a} \longmapsto \sigma_{\mathfrak{a}} = \left(\frac{\mathfrak{a}, K|k}{\cdot}\right)$$

Artinsymbol

Hierbei:

- $m = m_0 m_\infty$ hat folgende Eigenschaft:

  $\mathfrak{p}$ verzweigt in $K|k \implies \mathfrak{p} \mid m$

- $\sigma_{\mathfrak{p}} \in Z(\mathfrak{p}) \leq G$ ist eindeutig bestimmt durch

$$\sigma_{\mathfrak{p}}(\alpha) \equiv \alpha^{N\mathfrak{p}} \pmod{\mathfrak{P}}, \quad \forall \alpha \in \mathcal{O}_K$$

  Beachte auch: $Z(\mathfrak{p}) = \langle \sigma_{\mathfrak{p}} \rangle$

  $\operatorname{ord}(\sigma_{\mathfrak{p}}) = |Z(\mathfrak{p})| = f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{p})$.

- Falls $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{z_i}$, so gilt:

$$\left(\frac{\mathfrak{a}, K|k}{\cdot}\right) = \prod_i \sigma_{\mathfrak{p}_i}^{z_i}.$$

SATZ 1: Sei $K|k$ gegeben. Dann gibt es einen minimalen Divisor $f_{K|k} = f$ mit

(1) $\mathfrak{p}$ verzweigt $\Leftrightarrow \mathfrak{p} \mid f$

(2) $\forall\, \mathfrak{m}$ mit $f \mid \mathfrak{m}$ $\exists!\ P_k(\mathfrak{m}) \subseteq H \subseteq I_k(\mathfrak{m})$ mit

$$I_k(\mathfrak{m})/H \xrightarrow{\simeq} \mathrm{Gal}(K|k)$$

$$\mathfrak{a}H \longmapsto (\mathfrak{a}, K|k)$$

M.a.W. $H = \ker\big((-, K|k)\big) \subseteq I_k(\mathfrak{m})$

Genauer:

$$H = P_k(\mathfrak{m})\, N_{K|k}\big(I_K(\mathfrak{m}_0)\big) \qquad \text{(mit } \mathfrak{m}_0 \mathcal{O}_K\text{)}$$

$$= \ker\big((-, K|k)\big).$$

SATZ 2 Sei $\mathfrak{m}$ ein Divisor und $P_k(\mathfrak{m}) \subseteq H \subseteq I_k(\mathfrak{m})$. Dann gibt es eine eindeutige abelsche Erweiterung $K|k$ mit

(1) $\mathfrak{p}$ verzweigt $\Rightarrow \mathfrak{p} \mid \mathfrak{m}$.

(2) $H = P_k(m)\, N_{K|k}(I_K(m_0))$ und

$$I_k(m)/H \simeq \mathrm{Gal}(K|k)$$
$$\sigma H \longmapsto (\sigma, K|k)$$

Def.: K heißt **Klassenkörper** zu H (bzw. zu (H, m))

Erläuterung:

diese ist endlich

- $I_k(m)$ ⟶ $\mathcal{U}_k(m)$
- H ⟶ $\overline{H}$
- $P_k(m)$ ⟶ 1

- Die Zuordnung $(H, m) \longmapsto K$ kann man zu einer 1-1 Korrespondenz machen zwischen Äquivalenzklassen von (H, m) $\overset{1\text{-}1}{\longleftrightarrow}$ endliche ab. $K|k$

Hierbei:

$(H_1, m_1) \sim (H_2, m_2) :\Leftrightarrow$ es gibt

Divisor m mit $m_i \mid m$ mit

$$H_1 \cap I_k(m) = H_2 \cap I_k(m)$$

SATZ 3 Seien $K_1 | k$ und $K_2 | k$ zwei abelsche Erweiterungen mit $f_1 = f_{K_1|k}$ und $f_2 = f_{K_2|k}$. Sei m ein gemeinsames Vielfaches von f_1 und f_2 und seien $H_1, H_2 \leq I_k(m)$ gemäß Satz 1.

$\mathfrak{P}_k(m)$

Dann gilt: $K_1 \subseteq K_2 \Leftrightarrow H_1 \supseteq H_2$

Beispiel: $k = \mathbb{Q}$, $K = \mathbb{Q}(\zeta_n)$. Sei p prim mit $p \nmid n$. Dann ist p unverzweigt und es gilt:

$$\sigma_{pZ} = (\zeta_n \longmapsto \zeta_n^p)$$

Bemerke: $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$

$$
\begin{array}{l}
K = \mathbb{Q}(\zeta_n) \\
\quad\quad | 2 \\
K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}) \\
\quad\quad | \\
k = \mathbb{Q}
\end{array}
\quad \Big) \langle \sigma_{-1} \rangle \quad \uparrow \text{komplexe Konjugation}
$$

$$
\left.
\begin{array}{l}
G \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \\
\sigma_a \longleftrightarrow \bar{a} \\
\sigma_a(\zeta_n) = \zeta_n^a
\end{array}
\right)
$$

Zur Artinabbildung:

$$
\begin{array}{ccc}
I_{\mathbb{Q}}(n) & \longrightarrow & Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \\
a\mathbb{Z} & \longmapsto & \sigma_{|a|}
\end{array}
$$

ZIEL: Finde $H \leq I_{\mathbb{Q}}(n)$ gemäß Satz 1

Es gilt: $H = kv((\_, K|k))$. Sei

$r\mathbb{Z} \in I_{\mathbb{Q}}(n)$, $r = \frac{r_1}{r_2}$, $r_1, r_2 \in \mathbb{Z}$, $(r_1 r_2, n) = 1$

Dann: $(r\mathbb{Z}, K|k) = id$

$\Leftrightarrow \zeta_n^{|r_1|} = \zeta_n^{|r_2|} \Leftrightarrow |r_1| \equiv |r_2| \pmod n$

$\Leftrightarrow v_p\left(\left|\frac{r_1}{r_2}\right| - 1\right) \geq v_p(n)$, $\forall p \mid n$

$\Leftrightarrow r\mathbb{Z} \in \mathcal{P}_{\mathbb{Q}}(n\infty)$

Fazit: $\mathbb{Q}(\zeta_n)$ ist der Klassenkörper zu

$$H = P_{\mathbb{Q}}(n\infty).$$

Zweite Frage: Wie sieht das H zu $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ aus? Dazu:

$$(r\mathbb{Z},\ K^+/k) = \mathrm{id} \iff \sigma_{|r|} \in \{\sigma_{\pm 1}\}$$

$$\iff \zeta_n^{|r_1|} = \zeta_n^{|r_2|} \text{ oder } \zeta_n^{|r_1|} = \zeta_n^{-|r_2|}$$

$$\iff |r_1| \equiv \pm |r_2| \pmod{n}$$

$$\iff v_p\left(\pm\left|\frac{r_1}{r_2}\right| - 1\right) \geq v_p(n),\ p \mid n$$

$$\iff r\mathbb{Z} \in P_{\mathbb{Q}}(n)$$

$$\updownarrow$$

$$K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$$

Dies ist ein Beispiel für Satz 3:

$$\begin{array}{ccccc} P_{\mathbb{Q}}(n\infty) & \subseteq & P_{\mathbb{Q}}(n) & \subseteq & I_{\mathbb{Q}}(n) \\ \updownarrow & & \updownarrow & & \updownarrow \\ \mathbb{Q}(\zeta_n) & \supseteq & \mathbb{Q}(\zeta_n)^+ & \supseteq & k = \mathbb{Q} \end{array}$$

Konsequenzen:

Sei $m = (1)$ und $H = P_k((1)) = P_k$.
Sei $k(1)$ der zugehörige Klassenkörper gemäß Satz 2.

Satz: $k(1)$ ist die maximal unverzweigte abelsche Erweiterung von k. Insbesondere gilt für jede unverzweigte abelsche Erweiterung $K|k$:

(1) $[K:k] \leq h_k < \infty$

(2) $K \subseteq k(1)$

Ferner gilt: $\mathrm{Gal}(k(1)|k) \simeq cl_k$

Def.: $k(1)$ heißt Hilbertscher Klassenkörper.

Beweis: Falls $K|k$ endlich, abelsch und überall unverzweigt, so folgt mit Satz 1, daß $K|k$ modulo $f_{K|k} = (1)$ definiert ist. Insbesondere korrespondiert $K|k$ zu $P_k \subseteq H \subseteq I_k$

$P_k((1)) \overset{=}{\underset{\mathrm{Gal}(k(1)|k)}{\supseteq}} \overset{\updownarrow}{K} \supseteq \overset{\updownarrow}{k}$

Nach Satz 3 folgt also $K \subseteq k(1)$. ∎

$\updownarrow P_{k(1)}$

Satz: Sei $\mathfrak{p}$ ein Primideal in k. Dann gilt:

$\mathfrak{p}$ ist voll zerlegt in $k(1)/k$

$\Leftrightarrow$ $\mathfrak{p}$ ist ein Hauptideal.

Beweis: $\mathfrak{p}$ ist voll zerlegt, falls:

$k(1)$ $\mathfrak{P}_0$ $\quad \mathfrak{p}\mathcal{O}_{k(1)} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$

G (| | $\quad r = [k(1) : k]$

k $\mathfrak{p}$ $\mathfrak{p}$

Betrachte: $G/Z(\mathfrak{p}) \xrightarrow{\simeq} \{\mathfrak{P} \mid \mathfrak{p}\}$

$g \longmapsto g\mathfrak{P}_0$

Dann gilt:

$\mathfrak{p}$ ist voll zerlegt $\Leftrightarrow |Z(\mathfrak{p})| = 1$

$\Leftrightarrow \sigma_{\mathfrak{p}} = id \Leftrightarrow (\mathfrak{p}, k(1)|k) = id \Leftrightarrow \mathfrak{p} \in H = P_k$

∎

Verallgemeinerung:

Satz: Sei $K|k$ der Klassenkörper zu $H \leq I_k(m)$. Sei $\mathfrak{p} \lhd \mathcal{O}_k$ ein Primideal mit $(\mathfrak{p}, m) = 1$. Sei

$$f_{\mathfrak{p}} = \left[\mathcal{O}_K / \mathfrak{P} : \mathcal{O}_k / \mathfrak{p} \right].$$

Dann gilt:

$$f_{\mathfrak{p}} = \operatorname{ord}_{I_k(m)/H}(\mathfrak{p}H)$$

Beweis:

$$f_{\mathfrak{p}} = |Z(\mathfrak{p})| = \operatorname{ord}(\sigma_{\mathfrak{p}}) = \operatorname{ord}_{\dots}(\mathfrak{p}H)$$

$$I_k(m)/H \simeq \mathrm{Gal}(K|k)$$

$$\mathfrak{p}H \longmapsto \left(\mathfrak{p}, K|k\right) = \sigma_{\mathfrak{p}}$$

Def.: Falls $H = P_k(m)$, so heißt der zugehörige Klassenkörp. (gemäß Satz 2) Strahlklassenkörp. mod m. **Bez:** $k(m)$ ∎

Bemerkung: $m \mid n \Rightarrow k(m) \subseteq k(n)$

Beweis: $k(m)$ kann auch modulo n definiert werden. Dann korrespondiert $k(m)$ nach Satz 1 zu

$$\begin{array}{ccccc} P_k(n) & N_{k(m)/k} & \left(I_{k(m)}(n)\right) & \hookrightarrow & k(m) \\ \| & & \text{Satz 3} & & \cap \| \\ P_k(n) & & & \longleftrightarrow & k(n) \end{array}$$

∎

Beispiele:

(1) $k = \mathbb{Q}$ und $n \equiv 2 \pmod 4$, d.h. $n = 2n_1$, $2 \nmid n_1$. Dann:

$$\begin{array}{ccc} \mathbb{Q}(n\infty) = \mathbb{Q}(\zeta_n) & & \text{Es gilt:} \\ \Big| \qquad\qquad \Big) \varphi(n) & & n_1\infty \mid n\infty \\ & & \Rightarrow \mathbb{Q}(n_1\infty) \subseteq \mathbb{Q}(n\infty) \\ \mathbb{Q} & & \| \qquad\qquad \| \\ & & \mathbb{Q}(\zeta_{n_1}) \qquad \mathbb{Q}(\zeta_n) \end{array}$$

$$\left[\mathbb{Q}(\zeta_{n_1}) : \mathbb{Q}\right] = \varphi(n_1) = \varphi(n) = \left[\mathbb{Q}(\zeta_n) : \mathbb{Q}\right].$$

(2) Sei k imag.-quad.. Sei $\mathfrak{m} = m_0$ ein Divisor. Definiere

$$w(1) := |\mu_k| \in \{2, 4, 6\}$$

$$w(\mathfrak{m}) := \#\{\zeta \in \mu_k \mid \zeta \equiv 1 \pmod{\mathfrak{m}}\}$$

Übung: $[k(\mathfrak{m}) : k] = \# \ell_k(\mathfrak{m})$

$$= h_k \frac{w(1)}{w(\mathfrak{m})} \varphi_k(\mathfrak{m})$$

↑ Eulersche Fkt. von $\mathcal{O}_k$

Dann gilt für $d_k \neq -3, -4$:

$$[k(2) : k] = h_k \frac{2}{2} \varphi_k(2) = \begin{cases} h_k, & 2 = \mathfrak{p}\bar{\mathfrak{p}} \\ 3h_k, & 2 = \mathfrak{p}_2 \\ 2h_k, & 2 = \mathfrak{p} \end{cases}$$

Falls 2 zerlegt, so gilt:

$$k(1) = k(2)$$