Zahlentheorie IV

Klassenkörpertheorie

Do, 14-16 Uhr Übung

Literatur:

- J. Neukirch, Neuauflage von A. Schmidt, Klassenkörpertheorie
- J. Neukirch, Alg. Zahlentheorie
- J.P. Serre, Local fields
- P. Guillot, A gentle course in local class field theory

1. Überblick

1.1 Globale Klassenkörpertheorie (idealtheoretisch)

Ziel: Beschreibung aller abelschen endlichen Erweiterungen eines Zahlkp. k durch Daten in k.

Vorlage: Washington, Cyclotomic fields, Appendix

Grundkörper
$$\begin{tikzcd} k \arrow[d, dash, "<\infty"] \\ \mathbb{Q} \end{tikzcd}$$

<u>Definition:</u> Sei $\mathfrak{m}_0 \trianglelefteq \mathcal{O}_k$ ein Ideal und $\mathfrak{m}_\infty$ ein formales quadratfreies Produkt von reellen archimedischen Stellen. Dann nennt man $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ einen <u>Divisor</u> von k.

<u>Erläuterungen:</u>

Archimedische Stellen = unendliche Stellen sind reelle Einbettungen oder Paare komplexer Einbettungen.

$$\begin{tikzcd} k \arrow[r, hook, "\tau"] \arrow[d, dash, "<\infty"'] & \mathbb{R} \subseteq \mathbb{C} \\ \mathbb{Q} & \end{tikzcd} \qquad \begin{tikzcd} k \arrow[r, hook, "\sigma, \bar{\sigma}"] \arrow[d, dash] & \mathbb{C} \\ \mathbb{Q} & \end{tikzcd}$$

Jede unendliche Stelle definiert einen Betrag auf k durch

$$|\alpha|_\tau := |\tau(\alpha)| \qquad \alpha \in k$$

bzw. $$|\alpha|_\sigma := |\sigma(\alpha)| = |\bar{\sigma}(\alpha)|$$

<u>Bez:</u> $S_\infty = S_{k,\infty}$ = Menge der unendlichen Stellen auf k

<u>Anzahl:</u> $r_1 + r_2$ — # Paare kompl. Einbettungen

reellen Einbettungen

- Sei $\mathfrak{p} \triangleleft \mathcal{O}_k$ ein Primideal, $\neq (0)$.

Dann ist

$$|\alpha|_{\mathfrak{p}} := N_{k|\mathbb{Q}}(\mathfrak{p})^{-v_{\mathfrak{p}}(\alpha)} \qquad \alpha \in k$$

ein Betrag definiert. Hierbei

$$\alpha \mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\alpha)}$$

<u>Allgemein:</u> $\mathfrak{a}$ gebrochenes Ideal

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}, \quad v_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$$

fast alle gleich 0

<u>Beispiele von Divisoren:</u>

1) $k = \mathbb{Q}$

Es gibt genau eine unendliche Stelle ∞

Divisoren sind z.B.: $\mathfrak{m} = (1) = \mathcal{O}_k$

$\mathfrak{m} = \infty$

$\mathfrak{m} = 2^7 \cdot 3^5 \cdot 17$

$2^7 \cdot 3^5 \cdot 17 \cdot \infty$

(2) $k = \mathbb{Q}(\sqrt{d})$, $d < 0$, imag. quadr.

Hier gibt es keine reellen Einbettungen

Divisoren sind also (ganze) Ideale

(3) $k = \mathbb{Q}(\sqrt{d})$, $d > 0$, reell quad.

Zwei reelle Einbettungen:

$$a + b\sqrt{d} \xmapsto{id} a + b\sqrt{d} \in \mathbb{R} \quad \infty_1$$

$$\xmapsto{\tau} a - b\sqrt{d} \in \mathbb{R} \quad \infty_2$$

<u>Bspl:</u> $\mathfrak{m} = (1)$, $\infty_1 \infty_2$, ∞_1, $\mathfrak{m}_0 \cdot \infty_2$

<u>Def.:</u> Sei $\alpha \in k^\times$ und $\mathfrak{m} = \mathfrak{m}_0 \mathfrak{m}_\infty$ ein Divisor.

(1) Man schreibt $\alpha \equiv 1 \pmod{^* \mathfrak{m}}$, falls

(i) $v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0)$, $\forall \mathfrak{p} \mid \mathfrak{m}_0$

(falls $\alpha \in \mathcal{O}_k$ ist dies äquivalent zu $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$)

(ii) $\sigma(\alpha) > 0$ für alle $\sigma \in \mathfrak{m}_\infty$

(2) Die Gruppe

$$P_k(\mathfrak{m}) := \{ \alpha \mathcal{O}_k \mid \alpha \equiv 1 \ (\mathrm{mod}^* \mathfrak{m}) \}$$

heißt <u>Strahl modulo $\mathfrak{m}$</u>.

(3) Sei $I_k(\mathfrak{m}) = I_k(\mathfrak{m}_0)$ die Untergruppe von I_k der zu $\mathfrak{m}_0$ primen gebrochenen Ideale. Dann is $P_k(\mathfrak{m})$ eine Untergruppe von $I_k(\mathfrak{m})$ und

$$Cl_k(\mathfrak{m}) := I_k(\mathfrak{m}) / P_k(\mathfrak{m})$$

heißt <u>Strahlklassengruppe modulo $\mathfrak{m}$</u>.

<u>Erläuterungen:</u>

- Es gilt:

$$\alpha \mathcal{O}_k \in P_k(\mathfrak{m}) \iff \exists\, \varepsilon \in \mathcal{O}_k^\times \text{ mit } \varepsilon\alpha \equiv 1 \ (\mathrm{mod}^* \mathfrak{m})$$

- $\mathfrak{a} \in I_k(\mathfrak{m}) \iff \exists\, \mathfrak{b}, \mathfrak{c}$ ganze Ideale mit $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$, $\mathfrak{b} + \mathfrak{c} = \mathcal{O}_k$, $\mathfrak{b} + \mathfrak{m}_0 = \mathcal{O}_k$, $\mathfrak{c} + \mathfrak{m}_0 = \mathcal{O}_k$

Beispiel: Sei $\mathfrak{m} = (1)$. Dann:

$$\mathcal{C}\ell_k(\mathfrak{m}) = \mathcal{C}\ell_k$$

Beispiel: $k = \mathbb{Q}$

(1) Sei $\mathfrak{m} = (n) = n\mathbb{Z}$, $n \in \mathbb{Z}_{\geq 1}$.

Betrachte

$$\pi : \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \longrightarrow \mathcal{C}\ell_{\mathbb{Q}}((n))$$

induziert von $\quad \bar{a} \longmapsto a\mathbb{Z} = (a)$

Beh: Dies ist wohldefiniert

Bew: Sei $a \equiv b \pmod n$

Es gilt:

$$(a) \equiv (b) \;\left(\operatorname{mod} P_{\mathbb{Q}}(n)\right) \Leftrightarrow \left(\frac{a}{b}\right) \in P_{\mathbb{Q}}((n))$$

$$\Leftrightarrow \exists\, \varepsilon \in \mathbb{Z}^\times \;\forall p \mid n : \; v_p\!\left(\varepsilon \frac{a}{b} - 1\right) \geq v_p(n)$$

Man sieht: $\quad v_p\!\left(\varepsilon \frac{a}{b} - 1\right) = v_p(\varepsilon a - b)$

Dies liefert die Wohldefiniertheit.

Beh: π ist surjektiv

Bew: Sei $\left(\frac{a_1}{a_2}\right) \in I_{\mathbb{Q}}(n)$ mit $a_1, a_2 \in \mathbb{Z}$

$(a_1, a_2) = 1$, $(a_1 a_2, n) = 1$.

Dann ist $\pi\left(\overline{a_1}\,\overline{a_2}^{-1}\right) = \left(\frac{a_1}{a_2}\right)P_{\mathbb{Q}}(n)$.

Weiter gilt:

$\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ist im Kern

$\Longleftrightarrow \quad a \equiv \pm 1 \pmod{n}$

Zusammenfassung:

$$0 \to \{\pm \bar{1}\} \to (\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\pi} \mathcal{C}l_{\mathbb{Q}}(n) \to 0$$

ist exakt

(2) Sei $\mathfrak{m} = (n)\infty$. Betrachte

$$\pi : (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \mathcal{C}l_{\mathbb{Q}}((n)\infty)$$
$$\bar{a} \longrightarrow (a)P_{\mathbb{Q}}((n)\infty)$$

mit $a > 0$.

π ist wohldefinierter Epimorphismus mit $\ker(\pi) = \{\bar{1}\}$, d.h. π ist ein Iso.

Vorgriff:

$$
\begin{tikzcd}
 & \mathbb{Q}(\zeta_n) \arrow[d, no head, "{2,\ \langle\tau\rangle}"] & \\
P_{\mathbb{Q}}(n\infty) \arrow[ur, leftrightarrow] & \mathbb{Q}(\zeta_n)^+ \arrow[dd, no head] & (\mathbb{Z}/n\mathbb{Z})^\times \\
 & & \\
P_{\mathbb{Q}}(n) \arrow[uur, leftrightarrow] & \mathbb{Q} &
\end{tikzcd}
$$

$\tau =$ komplexe Konjugation

Notation:

- Man schreibt

$$k_{\mathfrak{m}}^\times := \{\alpha \in k^\times \mid \alpha \equiv 1 \bmod^\times \mathfrak{m}\}$$

Dann ist $P_k(\mathfrak{m}) = \{\alpha \mathcal{O}_k \mid \alpha \in k_{\mathfrak{m}}^\times\}$

- Definiere

$$\left(\mathcal{O}_k/\mathfrak{m}\right)^\times := \left(\mathcal{O}_k/\mathfrak{m}_0\right)^\times \times \underbrace{\{\pm 1\} \times \dots \times \{\pm 1\}}_{\text{einen Faktor für jedes } \sigma \text{ in } \mathfrak{m}_\infty}$$

- Sei $\alpha \in k^\times$ prim zu $\mathfrak{m}_0$. Dann gibt $\beta, \gamma \in \mathcal{O}_k$, beide prim zu $\mathfrak{m}_0$, mit
$$\alpha = \beta/\gamma.$$

Definiere
$$\overline{\alpha} := \overline{\beta}\,\overline{\gamma}^{-1} \qquad \in \left(\mathcal{O}_k/\mathfrak{m}_0\right)^\times$$
Dies ist unabhängig von der Wahl von β und γ. (Leicht!)

<u>Existenz:</u> $\alpha\mathcal{O}_k = \mathfrak{b}/\mathfrak{c}$ mit

$\mathfrak{b}, \mathfrak{c} \trianglelefteq \mathcal{O}_k$, $\mathfrak{b} + \mathfrak{c} = \mathcal{O}_k$.

<u>Klar:</u> $[\mathfrak{b}] = [\mathfrak{c}] =: c \in \mathcal{C}\ell_k$

Wähle $\mathfrak{c}_1 \trianglelefteq \mathcal{O}_k$, teilerfremd zu $\mathfrak{m}_0$ mit $\mathfrak{c}_1 \in c^{-1}$. Dann gilt:
$$\alpha\mathcal{O}_k = \frac{\mathfrak{b}\mathfrak{c}_1}{\mathfrak{c}\mathfrak{c}_1} = \beta'/\gamma\ \mathcal{O}_k$$
$$\Rightarrow \exists\ \varepsilon \in \mathcal{O}_k^\times \quad \text{mit} \quad \alpha = \frac{\beta'\varepsilon}{\gamma}.$$
Nimm also: $\beta = \beta'\varepsilon$.

Betrachte

$$\rho : \{\alpha \in k^\times \mid (\alpha, \mathfrak{m}_0) = 1\} \longrightarrow (\mathcal{O}_k/\mathfrak{m})^\times$$

$$\alpha \longmapsto \Big(\underset{\substack{\cap \\ (\mathcal{O}_k/\mathfrak{m}_0)^\times}}{\bar{\alpha}},\ \underbrace{(\mathrm{sgn}(\sigma(\alpha)))_{\sigma \in \mathfrak{m}_\infty}}_{\in \{\pm 1\}^{\cdots}}\Big)$$

Starke Approximationssatz $\Longrightarrow$

ρ ist surjektiv

$\rightsquigarrow$

$$0 \to \mathcal{O}_k^\times \cap k_\mathfrak{m}^\times \to \mathcal{O}_k^\times \to (\mathcal{O}_k/\mathfrak{m})^\times \longrightarrow Cl_k(\mathfrak{m}) \to Cl_k \to 0$$

$$u \mapsto (\bar{u}, (\mathrm{sgn}(\sigma(u)))) \qquad \mathfrak{a}\mathcal{P}_k(\mathfrak{m}) \mapsto \mathfrak{a}\mathcal{P}_k$$

$$\rho(\alpha) \longmapsto (\alpha)\mathcal{P}_k(\mathfrak{m})$$

ist exakt.

$\Longrightarrow \quad |Cl_k(\mathfrak{m})| < \infty$