B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

18.Vorlesung

22. Juni 2021

In diesem Skript werden wir unsere bisherige Ergebnisse anwenden, um Ganzheitsbasen für Zahlkörper zu berechnen. Wir fassen zusammen hier unseren ***Ansatz*** *aus Skript 16 und 17:*

- $R = \mathbb{Z}$, $L/\mathbb{Q}$ *ist ein Zahlkörper,* α *ist ein primitives Element für die Erweiterung, so daß* $L = \mathbb{Q}(\alpha)$, $f :=$ *MinPol*$_{\mathbb{Q}}(\alpha)$, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ *die verschiedene Nullstellen von* f.
- $\mathcal{O}_L = \overline{\mathbb{Z}}^L$, *ohne Einschränkung* $\alpha \in \mathcal{O}_L$, $\mathcal{O}_L$ *ist frei vom Rang* $n = [L : \mathbb{Q}]$, *und* $D(\mathcal{O}_L/\mathbb{Z}) \in \mathbb{Z}$ *ist die Diskriminante des Zahlkörpers* L .
- *Unsere Fragestellung: Sei* $\mathcal{B}$ *eine Basis für* $L/\mathbb{Q}$, *so daß* $\mathcal{B} \subseteq \mathcal{O}_L$. *Wann ist* $\mathcal{B}$ *eine Basis (eine Ganzheitsbasis) für* $\mathcal{O}_L$ *als* $\mathbb{Z}$*-Modul?*

Wir benutzen weiterhin die Kurzbezeichnung die wir in der 17. Vorlesung eingeführt haben: Sei V *ein* n*-dimensionaler* K*-Vektorraum,* B *eine bilinerare Form,* $\mathcal{B} = \{v_1, \ldots, v_n\} \subseteq V$, *wir bezeichnen hierunten mit* $B(v_i, v_j)$ *die* $n \times n$ *Matrix Darstellung von* B *bzgl* $\mathcal{B}$.

Besondere Fragestellung: Betrachte die Basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ für $L/\mathbb{Q}$. Dann ist $\{1, \alpha, \ldots, \alpha^{n-1}\} \subseteq \mathcal{O}_L$, und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist insbesondere $\mathbb{Z}$-linear unabhängig. Wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ sogar erzeugend für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul? Also wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ sogar eine *Basis* (eine Ganzheitsbasis) für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul?

Um diese Frage zu beantworten, wollen wir Satz 17.2 anwenden. Dafür müssen wir zunächst berechnen:

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \det[B_{L/\mathbb{Q}}(\alpha^i, \alpha^j)] \\ &\overset{\text{Bem. } 16.2}{=} (\text{Vandermonde Determinante})^2 \\ &\overset{\text{Bem. } 17.1}{=} [\prod_{i<j}(\alpha_i - \alpha_j)]^2 \end{aligned}$$

(wobei $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ die verschiedene Nullstellen von $f =$ MinPol$_{\mathbb{Q}}(\alpha)$ sind).

Diese Berechnung motiviert die folgende allgemeine Definition:

Definition 18.1
Sei $g \in \mathbb{Q}[x]$ irreduzibel und $\alpha_1, \ldots, \alpha_n$ alle Nullstellen von g. Die Diskriminante von g ist $D(g) := \prod_{i<j}(\alpha_i - \alpha_j)^2$.

Bemerkung 18.1
Sei $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul. Sei P wie in $(*)$ im Beweis vom Satz 17.2. Wir berechnen $D(f) \in \mathbb{Z}$ mithilfe der $(**)$ im Beweis vom Satz 17.2:

$$\begin{aligned} D(f) &= D(1, \alpha, \ldots, \alpha^{n-1}) \\ &\overset{(**)}{=} (\det P)^2 D(\beta_1, \ldots, \beta_n) \\ (\dagger) \qquad &= (\det P)^2 D(\mathcal{O}_L/\mathbb{Z}) \end{aligned}$$

Diese Gleichung (†) ist sehr hilfreich weil:

(i) Aus (†) und Satz 17.2 folgt daß wenn wir $D(\mathcal{O}_L/\mathbb{Z})$ berechnen können, dann können wir auch entscheiden, ob $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Ganzheitsbasis ist.

(ii) Ist $D(f)$ quadratfrei, dann ist $\det P = \pm 1$, also ist P invertierbar und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Ganzheitsbasis.

(iii) Wenn $D(f)$ nicht quadratfrei ist, benutzen wir den **Satz von Stickelberger**.

Satz 18.1 (Satz von Stickelberger)
$D(\mathcal{O}_L/\mathbb{Z}) \equiv 0, 1 \bmod 4$, also ist $D(\mathcal{O}_L/\mathbb{Z})$ ein Quadrat mod 4.

Bevor wir den Satz von Stickelberger beweisen, wollen wir eine Anwendung der Bemerkung 18.1 auf die Berechnung von Ganzheitsbasen für quadratische Zahlkörper bringen (vgl. Algebra 2; Kapitel 1).

Beispiel [Quadratische Zahlkörper.]
Sei L quadratischer Zahlkörper, $[L : \mathbb{Q}] = 2$, $L = \mathbb{Q}(\sqrt{d}), d \in \mathbb{Z}$ quadratfrei.

Fall 1: Wenn $d \equiv 2, 3 \bmod 4$, dann ist $\{1, \sqrt{d}\}$ ist eine Ganzheitsbasis

(und somit ist $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$).

Hier haben wir $\alpha = \sqrt{d}$ das primitive Element, $d \in \mathcal{O}_L$ und $f(x) = \text{ MinPol}_{\mathbb{Q}}(\alpha) = x^2 - d$. Die Nullstellen von f sind

$$x_{1,2} := \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} .$$

Also ist $D(f) = (x_1 - x_2)^2 = 4d$. Nun ist $4d = \underbrace{(\det P)^2}_{\in \mathbb{Z}} \quad \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0,1 \bmod 4 (s.\ Satz\ 18.1)}$

Behauptung: $D(\mathcal{O}_L/\mathbb{Z}) \equiv 0 \bmod 4$

Beweis. wenn $D(\mathcal{O}_L/\mathbb{Z}) \equiv 1$ wäre, wäre dann $(\det P)^2 \equiv 0$, aber dann $\underbrace{d}_{\equiv 2,3} = \underbrace{l^2}_{\equiv 0,1} \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 1}$: Widerspruch. □

Es gilt also $4d = (\det P)^2 \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0 \bmod 4}$. 4 auf beiden Seiten kürzen ergibt: $d = (\det P)^2 w$ und d quadratfrei$\Rightarrow (\det P)^2 = 1$, also ist $\det P = \pm 1$, also ist $\{1, \sqrt{d}\}$ eine Ganzheitsbasis.

Fall 2: Wenn $d \equiv 1 \bmod 4$, dann ist $\{1, \frac{1+\sqrt{d}}{2}\}$ ist eine Ganzheitsbasis

(also ist $\mathcal{O}_L = \mathbb{Z}[\omega]$, wobei $\omega = \frac{1}{2}(1 + \sqrt{d})$).

Beweis. $f = \text{ MinPol}_{\mathbb{Q}}(\omega) = x^2 - x + [\frac{1-d}{4}] \in \mathbb{Z}[x]$ und $D(f) = 1 - [4(\frac{1-d}{4})] = d$, d quadratfrei, also folgt nun unsere Behauptung aus Bemerkung 18.1(ii). □