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

17.Vorlesung

17. Juni 2021

In diesem Skript werden wir den folgenden Anstaz studieren:

R ganz abgeschloßen Integer Ring , $K = QuotR, L/K$ eine endliche separable Körpererweiterung .

Wir werden den ganzen Abschluß $\overline{R}^L$ beschreiben und wie (in der Algebra II Vorlesung) vorangekündigt Satz 13.4 (Satz 17.1 hier) beweisen. Wir wollen schließlich in Korollar 17.4 diese Ergebnisse auf

$$R = \mathbb{Z}, L/\mathbb{Q} \text{ ein Zahlkörper, und } \overline{\mathbb{Z}}^L = \mathcal{O}_L$$

anwenden. Danach werden wir die Diskriminante einführen, um Ganzheitbasen zu berechnen.

Ansatz und Bezeichnungen weiterhin wie im Skript 16.

Bemerkung 17.1 (ÜA)
Im Beweis von Bemerkung 16.2 können wir andere Basen betrachten (anstatt $\{\gamma^0, \dots, \gamma^{n-1}\}$): Sei $\{v_1, \dots, v_n\}$ eine beliebige Basis für L/K und wie zuvor $\{\sigma_1, \dots, \sigma_n\}$ die n verschiedenen Einbettungen von L/K in Ω. Sei $\mathcal{V}_{ij} := \sigma_i(v_j)$ für alle i, j, und $\mathbb{B}$ die Matrix von $B_{L/K}$ bezüglich $\{v_1, \dots, v_n\}$. Dann ist $\mathbb{B} = \mathcal{V}^t\mathcal{V}$, also ist $\det \mathbb{B} = (\det \mathcal{V})^2$.

Satz 17.1
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \mathrm{Quot}(R)$, L/K eine endliche separable Erweiterung, $n = [L : K]$ und $S = \overline{R}^L$. Dann gibt es $M \subseteq L, M' \subseteq L$ R-Untermoduln von L, beide frei von Dimension n, so daß $M \subseteq S \subseteq M'$.

Beweis. • Betrachte

$$B_{L/K} : L \times L \to K \ , \ B_{L/K}(x, y) = Sp_{L/K}(xy).$$

Bemerke daß die Einschränkung von $B_{L/K}$ auf $S \times S$ hat Werte in R (Korollar 15.2).

• Sei $\{\nu_1, \dots, \nu_n\}$ eine Basis für L/K. O.E. $\{\nu_1, \dots, \nu_n\} \subseteq S$ (weil $\forall \alpha \in L \, \exists r \in R$ mit $r\alpha \in S$, s. Proposition 9.4).

• Sei $\{\mu_1, \dots, \mu_n\}$ die $B_{L/K}$-duale Basis ($B_{L/K}(\nu_i, \mu_j) = \delta_{ij}$) wie im Bemerkung 16.1.
Setze

$$M := \bigoplus R\nu_i \text{ und } M' = \bigoplus R\mu_i \, .$$

M und M' sind frei und haben Dimension gleich n (da $\{\nu_1, \dots, \nu_n\}$ und $\{\mu_1, \dots, \mu_n\}$ a fortiori linear unabhängig über R sind). Es ist klar, dass $M \subseteq S$. Wir zeigen $S \subseteq M'$. Sei $\alpha \in S$, schreibe $\alpha = \sum c_i\mu_i$. Aber $c_i = B_{L/K}(\alpha, \nu_i) \in R$ (Bemerkung 16.1 und Korollar 15.2). □

Korollar 17.2
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \mathrm{Quot}(R)$, L/K eine endliche separable Erweiterung. Wenn R noethersch ist, dann ist $\overline{R}^L$ ein endlich erzeugter R-Modul.

Beweis. Sei M' wie in Satz 17.1, M' ist ein endlich erzeugter Modul über einem noetherschen Ring, also ist M' ein noetherscher R-Modul (s. Korollar 8.3), und damit ist jeder Untermodul endlich erzeugt.

□

Korollar 17.3
Sei R ein Hauptidealbereich, L/K eine endliche separable Körpererweiterung und $n = [L : K]$. Dann ist $\overline{R}^L$ ein freier R-Modul der Dimension n.

Beweis. Ein Untermodul (über einem HIR) von einem freiem Modul der Dimension $= n$ ist frei der Dimension $\leq n$ (s. Satz 5.1). Sei M' wie in Satz 17.1. Es gelten:

$$S \subseteq M' \Rightarrow S \text{ frei der Dimension } \leq n$$

und

$$M \subseteq S \Rightarrow \dim_R M = n \leq \dim_R S \leq n \Rightarrow \dim_R S = n\,.$$

□

Korollar 17.4
$R = \mathbb{Z}$. L ist ein Zahlkörper $\Rightarrow \mathcal{O}_L$ ist ein freier $\mathbb{Z}$-Modul der Dimension $[L : K]$.

§Ganzheitsbasen

Definition 17.1
Sei R ein Hauptidealbereich, $K = \mathrm{Quot}(R)$, L/K separable Erweiterung, $n = [L : K]$. Dann ist $S = \overline{R}^L$ ist ein freier R-Modul der Dimension n. Eine Basis $\{\mu_1, \ldots, \mu_n\}$ von S über R heißt Ganzheitsbasis.

Wir wollen nun Ganzheitsbasen finden.

Kurzbezeichnung: 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 $\mathcal{B}$.

Bemerkung 17.2
Sei V ein endlichdimensionaler K-Vektorraum, B eine nicht ausgeartete bilineare Form, $\mathcal{B} = \{v_1, \ldots, v_n\} \subseteq V$. Dann ist $\mathcal{B}$ genau dann eine Basis für V über K, wenn $\det(B(v_i, v_j)) \neq 0$.

Beweis. „⇒“ Siehe Bemerkung 16.1.
„⇐“Sei $\{w_1, \ldots, w_n\}$ eine Basis für V über K. Setze $v_i = \sum_j c_{ij} w_j$, $P := [c_{ij}]$, $P \in M_{n\times n}(K)$. Es ist
$B(v_i, v_j) = P^t[B(w_i, w_j)]P$ und $\det P \neq 0 \Leftrightarrow \{v_1 \ldots, v_n\}$ linear unabhängig. Außerdem ist

$$\det[B(v_i, v_j)] = (\det P)^2 \underbrace{\det[B(w_i, w_j)]}_{\neq 0}$$

also $\det[B(v_i, v_j)] \neq 0 \Leftrightarrow \{v_1, \ldots, v_n\}$ linear unabhängig. □

Wir werden nun analog vorgehen wie in Bemerkung 17.2 um R-Basen von S zu bestimmen:

Ansatz wie oben.

Diskriminante der Ringerweiterung S/R:
Wir haben (wegen Korollar 15.2)

$$B_{L/K} : S \times S \to R\,.$$

Für $\{\nu_1, \ldots, \nu_n\} \subseteq S$ definiere $D(\nu_1, \ldots, \nu_n) := \det(B_{L/K}(\nu_i, \nu_j))$. Es ist: $D(\nu_1, \ldots, \nu_n) \in R$.

Lemma 17.1
Seien $\{v_1, \ldots, v_n\}$ und $\{\mu_1, \ldots, \mu_n\}$ Basen für S als R-Modul. Dann ist

$$D(\nu_1, \ldots, \nu_n) = \pi^2 D(\mu_1, \ldots, \mu_n)$$

für ein geeignetes $\pi \in R^\times$.

Beweis. Wir argumentieren wie im Beweis von Bemerkung 17.2. Wir haben $D(\nu_1, \ldots, \nu_n) = (\det P)^2 D(\mu_1, \ldots, \mu_n)$, wobei $P \in M_{n\times n}(R)$ und P invertierbar (weil P Basiswechselmatrix ist), also folgt aus Cramer's Formel, daß $\pi := \det P \in R^\times$. □

Bevor wir die Diskriminante der Ringerweiterung S/R definieren können, müssen wir noch eine Äquivalenzrelation einführen. Wir definieren für $x, y \in R : x \sim y \Leftrightarrow x = \pi^2 y$ für ein $\pi \in R^\times$. Lemma 17.1 besagt:

Für alle Basen $\{\nu_1, \ldots, \nu_n\}$ von S als R-Modul liegen $D(\nu_1, \ldots, \nu_n)$ in der gleichen Äquivalenzklasse.

Definition 17.2
$D(S/R) := [D(\nu_1, \ldots, \nu_n)]_\sim$ für eine (alle) Basis $\{\nu_1, \ldots, \nu_n\} \subseteq S$ von S als R-Modul.

Bemerkung 17.3
$R = \mathbb{Z} \Rightarrow \mathbb{Z}^\times = \{\pm 1\}$, also hier haben wir $D(\nu_1, \ldots, \nu_n) \sim D(\mu_1, \ldots, \mu_n) \Leftrightarrow D(\nu_1, \ldots, \nu_n) = D(\mu_1, \ldots, \mu_n)$

Satz 17.2
Sei $\{\gamma_1, \ldots, \gamma_n\} \subseteq S$. Dann ist $\{\gamma_1, \ldots, \gamma_n\}$ genau dann eine Basis von S über R, wenn $[D(\gamma_1, \ldots, \gamma_n)]_\sim = D(S/R)$.

Beweis. „⇒“ folgt aus Lemma 17.1.
„⇐“ Sei $\mathcal{B} := \{\nu_1, \ldots, \nu_n\}$ eine Basis von S als R-Modul, so daß
$\det[B_{L/K}(\gamma_i, \gamma_j)] = D(\gamma_1, \ldots, \gamma_n) = \pi^2 D(\nu_1, \ldots, \nu_n) = \pi^2 \det[B_{L/K}(\nu_i, \nu_j)]$ mit $\pi \in R^\times$. Betrachte

$$C : \begin{array}{ccc} S & \to & S \\ \nu_i & \mapsto & \gamma_i \end{array} \qquad C \text{ definiert ein } R\text{-Modul Homomorphismus.}$$

$$(*) \qquad \text{Sei } P = [C]_{\mathcal{B}} \in M_{n\times n}(R)$$

$$(**) \qquad \text{also } [B_{L/K}(\gamma_i, \gamma_j)] = P^t [B_{L/K}(\nu_i, \nu_j)] P$$

also

$$(***) \qquad (\det P)^2 = \pi^2$$

und somit ist $\det P \in R^\times$ (weil $\det P = \pm\pi$), also ist P invertierbar (über R), also ist auch ein C invertierbarer R-Homomorphismus, d.h $\{\gamma_1, \ldots, \gamma_n\}$ ist eine Basis. □