Algebraische Zahlentheorie
Algebra B 4 - Sommersemester 2017
Prof'in Dr. Salma Kuhlmann

14.Vorlesung

22 Juni 2017

Beweis vom Satz. L/K endlich und separabel, $K = \text{Quot}(R)$, R ein ganz abgeschlossener Integritätsbereich, $S = \overline{R}^L$. $B_{L/K} : L \times L \to K$ $B_{L/K}(x, y) = Sp_{L/K}(xy)$. Die Einschränkung von $B_{L/K}$ auf $S \times S$ hat Werte in R. Sei $\{\nu_1, \ldots, \nu_n\}$ eine Basis für L/K (a fortiori linear unabhängig über R). Erinnerung: $\forall \alpha \in L \exists r \in R$ mit $r\alpha \in S$, also gilt o.E. $\{\nu_1, \ldots, \nu_n\} \subseteq S$. Sei $\{\mu_1, \ldots, \mu_n\}$ die $B_{L/K}$-duale Basis und setze $M := \bigoplus R\nu_i$ und $M' = \bigoplus R\mu_i$. Es ist klar, dass $M \subseteq S$. Wir zeigen $S \subseteq M'$. Sei $\alpha \in S$, $\alpha = \sum c_i\mu_i$ aber $c_i = B_{L/K}(\alpha, \nu_i) \in R$ □

Definition 14.1
Sei R ein HIR, $n = [L : K]$, L/K separable Erweiterung, $S = \overline{R}^L$ 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.

Bemerkung 14.1
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. „⇒" 13. Vorlesung.
„⇐"Sei $\{w_1, \ldots, w_n\}$ eine Basis und $v_i = \sum_j c_{ij}w_j$, $P := [c_{ij}]$, $P \in M_{n\times n}(K)$. 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 eine analogue Prozedur für R-Basen von S betrachten:

Diskriminante (einer Ringerweiterung)
Wir haben $B_{L/K} : S \times S \to R$. Für $\nu_1, \ldots, \nu_n \in S$ definiere
$D(\nu_1, \ldots, \nu_n) := \det(B_{L/K}(\nu_i, \nu_j)) \in R$.

Lemma 14.1
Seien $\{v_1, \ldots, v_n\}$ und $\{\mu_1, \ldots, \mu_n\}$ Basen für S als R-Modul. Dann ist $D(\nu_1, \ldots, \nu_n) = \pi^2 D(\mu_1, \ldots, \mu_n)$ mit $\pi \in R^\times$.

Beweis. 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 $\det P \in R^\times$. □

Wir definieren für $x, y \in R$:
$x \sim y \Leftrightarrow x = \pi^2 y$ für ein $\pi \in R^\times$.
Lemma 14.1 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 14.2
$D(S/R) := [D(\nu_1, \ldots, \nu_n)]_\sim$ für eine (alle) Basis $\{\nu_1, \ldots, \nu_n\} \subseteq S$ von S als R-Modul.

Bemerkung 14.2
$R = \mathbb{Z} \Rightarrow \mathbb{Z}^\times = \{\pm 1\}$, 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 14.2
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. „$\Rightarrow$“ folgt aus Lemma 14.1.
„$\Leftarrow$“ Sei $\mathcal{B} := \{\nu_1, \ldots, \nu_n\}$ eine Basis von S als R-Modul, so daß
$\det[B_{L/K}(\gamma_i, \gamma_j)] = D(\gamma_1, \ldots, \gamma_n) = \pi^2 D(\gamma_1, \ldots, \gamma_n) = \pi^2 \det[B_{L/K}(\nu_i, \nu_j)]$ mit $\pi \in R^\times$. Betrachte

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

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

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

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 C invertierbarer R-Homomorphismus, d.h $\{\gamma_1, \ldots, \gamma_n\}$ ist eine Basis. □

Ab jetzt: $R = \mathbb{Z}, L = \mathbb{Q}(\alpha)$ Zahlkörper, α primitives Element. O.E.: $\alpha \in \mathcal{O}_L := \overline{\mathbb{Z}}^L$. $\mathcal{O}_L$ ist frei vom Rang $[L : \mathbb{Q}]$, $D(\mathcal{O}_L/\mathbb{Z})$ ist die Diskriminante des Zahlkörpers L.
Fragestellung: Sei $\mathcal{B}$ eine Basis für L/K, so daß $\mathcal{B} \subseteq \mathcal{O}_L$. Ist $\mathcal{B}$ für $\mathcal{O}_L$ eine Basis als $\mathbb{Z}$-Modul?
Insbesondere: $\{1, \alpha, \ldots, \alpha^{n-1}\} \subseteq \mathcal{O}_L$ ist eine Basis für L über $\mathbb{Q}$ (also sicher $\mathbb{Z}$-linear unabhängig), aber wann ist $\{1, \alpha, \ldots, \alpha^{n-1}\}$ eine Basis für $\mathcal{O}_L$ über $\mathbb{Z}$?
Wir berechnen:

$$\begin{aligned} D(1, \alpha, \ldots, \alpha^{n-1}) &= \det[B_{L/\mathbb{Q}}(\alpha^i, \alpha^j)] \\ &\overset{\text{13. Vor}}{=} (\text{Vandermonde Determinante})^2 \\ &\overset{\text{LAII}}{=} [\prod_{i<j} (\alpha_i - \alpha_j)]^2 \end{aligned}$$

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

Definition 14.3
$D(f) := \prod_{i<j}(\alpha_i - \alpha_j)^2$ für ein irreduzibles $f \in \mathbb{Q}[x]$ und $\alpha_1, \ldots, \alpha_n$ alle Nullstellen von f. $D(f)$ ist die Diskriminante von f.

Bemerkung 14.3
Sei $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis (für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul) und P wie in $(*)$, dann ist

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

Aus (†) folgt:

(i) (aus (†) und Satz 14.2) 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 über R und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Ganzheitsbasis.

(iii) Wenn $D(f)$ nicht quadratfrei ist, benutzen wir Stickelberger's Satz

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

Beweis. Später (15. Vorlesung). □

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

Fall 1: $d \equiv 2, 3 \bmod 4$.

Behauptung: $\{1, \sqrt{d}\}$ ist eine Ganzheitsbasis un somit ist $\mathcal{O}_L = \mathbb{Z}[\sqrt{d}]$

Beweis. Setze $\alpha := \sqrt{d}$ primitives Element, $d \in \mathcal{O}_L$ und $\mathrm{MinPol}_{\mathbb{Q}}(\alpha) := f(x) = x^2 - d$. Seine Nullstellen sind
$x_{1,2} := \frac{-b \pm \sqrt{b^2-4ac}}{2a}$, also ist $D(f) = (x_1 - x_2)^2 = 4d$. Nun ist $4d = \underbrace{(\det P)^2}_{\in\mathbb{Z}} \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0,1 \bmod 4}$
$P \in M_{n\times n}(\mathbb{Z})$.

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 $\{1, d\}$ eine Ganzheitsbasis. □

Fall 2: $d \equiv 1 \bmod 4$

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

Beweis. $f = \mathrm{MinPol}_{\mathbb{Q}}(\omega) = x^2 - x + [\frac{1-d}{4}] \in \mathbb{Z}[x]$ und $D(f) = 1 - [4(\frac{1-d}{4})] = d$, d quadratfrei, also folgt nun unsere Behauptung aus Bemerkung 14.3(ii). □