Algebraische Zahlentheorie
B IV
Kuhlmann
14. Vorlesung am 10.06.2013

Beweis vom Satz (13. Vorlesung)

L/K endl. sep ; $K = \mathrm{Quot}(R)$; R ganz abg.

Integritätsbereich. $S := \overline{R}^L$

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

Es ist: die Einschränkung auf $S \times S$ hat Werte in R:

$$B_{L/K}\big|_{S\times S} : S \times S \longrightarrow R .$$

Sei $\{v_1, \dots, v_n\}$ eine Basis für L/K (a fortiori lin. unab. über R). Erinnerung: $\forall \alpha \in L \; \exists r \in R$ mit $r\alpha \in S$.

Also OE $\{v_1, \dots, v_n\} \subseteq S$.

Sei $\{\mu_1, \dots, \mu_n\}$ die $B_{L/K}$ - duale Basis

und setze:

$$M := \bigoplus R v_i \text{ und } M' := \bigoplus R\mu_i$$

Es ist klar daß $M \subseteq S$.
Wir zeigen: $S \subseteq M'$. Sei $\alpha \in S$, $\alpha = \sum c_i \mu_i$ aber

$c_i = B_{L/K}(\alpha, v_i) \in R.$ ∎

Definition 1. [Sei R HIR; $[L:K] = n$; L separable Erweiterung; $S := \overline{R}^L$ ist freies R-Modul der Dimension n].

$\{\mu_1, \dots, \mu_n\} \subseteq S$ Basis von S über R heißt Ganzheitsbasis.

Wir wollen nun Ganzheitsbasen finden.

Bemk 1. Sei V endl. dim. K VR, B nicht ausgeartete bilineare Form; $\mathcal{B} = \{v_1, \dots, v_n\} \subseteq V$.

Dann ist $\mathcal{B}$ Basis für V über $K \Leftrightarrow$

$$\det(B(v_i, v_j)) \neq 0$$

Beweis "$\Rightarrow$" 13. Vor.

"$\Leftarrow$" sei $\{w_1, \dots, w_n\}$ eine Basis

und $w_i = \sum_j c_{ij} w_j$ $\quad P := [c_{ij}]$

$P \in M_{n \times n}(k)$.

es ist $\quad B(v_i, v_j) = P^t \left[B(w_i, w_j)\right] P$

und $\det P \neq 0 \Leftrightarrow \{v_1, \dots, v_n\}$ linear unabhängig ist. Außerdem ist

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

Also $\det\left[B(v_i, v_j)\right] \neq 0 \Leftrightarrow \{v_1, \dots, v_n\}$ lin. unab. $\boxtimes$

Wir werden analogue Prozedur für R-Basen von S betrachten:

<u>Diskriminante (einer Ringerweiterung)</u>

Wir haben

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

Für $\nu_1, \dots, \nu_n \in S$ definiere

$$D(\nu_1, \dots, \nu_n) := \det\left(B_{L/K}(\nu_i, \nu_j)\right) \in R.$$

<u>Lemma 1:</u> Seien $\underbrace{\{\nu_1, \dots, \nu_n\}}_{\subseteq S}$ und $\underbrace{\{\mu_1, \dots, \mu_n\}}_{\subseteq S}$

Basen für S als R-Modul.

Dann ist $\quad D(\nu_1, \dots, \nu_n) = \pi^2 \, D(\mu_1, \dots, \mu_n)$

mit $\pi \in R^{\times}$.

<u>Beweis</u>. Wir haben

$$D(v_1, \dots, v_n) = [\det P]^2 \, D(\mu_1, \dots, \mu_n)$$

wobei $P \in M_{n \times n}(R)$ und P invertierbar (weil P Basis Wechsel Matrix ist);

also folgt aus Cramer's Formel daß $\det P \in R^{\times}$. ∎

Wir definieren für $x, y \in R$:

$$x \sim y \iff x = \pi^2 y \quad \text{für ein } \pi \in R^{\times}$$

<u>Lemma 1 besagt</u>: für alle Basen $\{v_1, \dots, v_n\}$ von S als R-Modul liegen $D(v_1, \dots, v_n)$ in der gleichen Äquivalenzklasse.

<u>Definition 2</u> $\quad D(S/R) := [D(v_1, \dots, v_n)]_{\sim}$

für eine (alle) Basis $\{v_1, \dots, v_n\} \subseteq S$ von S als R-Modul.

<u>Bmk 2</u> $R = \mathbb{Z} \Rightarrow \mathbb{Z}^\times = \{\pm 1\}$

also hier haben wir

$$D(\nu_1, \ldots, \nu_n) \sim D(\mu_1, \ldots, \mu_n) \Leftrightarrow$$

$$D(\nu_1, \ldots, \nu_n) = D(\mu_1, \ldots, \mu_n).$$

<u>Satz 1.</u> Sei $\{\gamma_1, \ldots, \gamma_n\} \subset S$.

Dann ist $\{\gamma_1, \ldots, \gamma_n\}$ eine Basis von S über R $\Leftrightarrow$

$$[D(\gamma_1, \ldots, \gamma_n)]_\sim = D(S/R)$$

<u>Beweis:</u> "$\Rightarrow$" folgt aus Lemma 1.

"$\Leftarrow$" Sei $\mathcal{B} := \{\nu_1, \ldots, \nu_n\} \subseteq S$ eine Basis für S als R-Modul

so daß

$$\det\left[B_{L/K}(\gamma_i, \gamma_j)\right] = D(\gamma_1, \ldots, \gamma_n) = \pi^2 \, D(\nu_1, \ldots, \nu_n)$$

$= \pi^2 \det[B_{L/K}(\nu_i, \nu_j)]$; mit $\pi \in R^\times$.

Betrachte $C: S \to S$, $\nu_i \mapsto \gamma_i$ R-Modul Hom-

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

(**) so $[B_{L/K}(r_i, r_j)] = P^t [B_{L/K}(v_i, v_j)] P$

also

(* **) $(\det P)^2 = \pi^2$ und somit ist

$\det P \in R^\times$ (weil $\det P = \pm \pi$);

also ist P invertierbar (über R);

also ist C invertierbar R-Hom. i.e

$\{r_1, \ldots, r_n\}$ ist eine Basis. $\square$

Rahmen: Ab jetzt: $R = \mathbb{Z}$ $\quad L = \mathbb{Q}(\alpha)$

Zahlkörper; α Primitiveselement:

OE: $\alpha \in \mathcal{O}_L := \overline{\mathbb{Z}}^L$

$\mathcal{O}_L$ ist frei vom rank $[L : \mathbb{Q}]$

$D(\mathcal{O}_L / \mathbb{Z})$ 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?

14. Vor. $\qquad$ 10.06.2013

Insbesondere: $\{1, \alpha, \dots, \alpha^{n-1}\} \subseteq \mathcal{O}_L$ ist eine Basis für L über $\mathbb{Q}$ (also sicherlich $\mathbb{Z}$-lin. unab); aber wann ist $\{1, \alpha, \dots, \alpha^{n-1}\}$ eine Basis für $\mathcal{O}_L$ über $\mathbb{Z}$?

(i.e. erzeugt es $\mathcal{O}_L$ als $\mathbb{Z}$-Modul?).

Wir berechnen:

$$D(1, \alpha, \dots, \alpha^{n-1}) = \det\left[B_{L/\mathbb{Q}}(\alpha^i, \alpha^j)\right]$$

$$\overset{\text{13. Vor}}{=} (\text{Vandermonde Determinante})^2$$

$$\overset{\text{LA II}}{=} \left[\prod_{i<j} (\alpha_i - \alpha_j)\right]^2$$

wobei $\alpha_1 := \alpha, \alpha_2, \dots, \alpha_n$ die verschiedene NS von $f := \mathrm{MinPol}_{\mathbb{Q}}\, \alpha$.

Definition 3. $D(f) := \prod_{i<j} (\alpha_i - \alpha_j)^2$

für ein irreduzibles $f \in \mathbb{Q}[x]$ und $\alpha_1, \dots, \alpha_n$ alle NS von f.

16. Vor $\quad$ 7 - $\quad$ 10.06.2013

$D(f)$ ist die <u>Diskriminante von f.</u>

<u>Bmk 3</u> Sei $\{\beta_1, \ldots, \beta_n\}$ eine Ganzheitsbasis (für $\mathcal{O}_L$ als $\mathbb{Z}$-Modul) und P wie in ⊛ Seite 5; dann ist

$$\mathbb{Z} \ni D(f) = D(1, \alpha, \ldots, \alpha^{n-1}) \underset{S.5}{\overset{(**)}{=\!=}}$$

$$(\det P)^2 \; D(\beta_1, \ldots, \beta_n)$$

$$= (\det P)^2 \; D(\mathcal{O}_L / \mathbb{Z}) \qquad (\dagger)$$

Aus $(\dagger)$ folgt:

(i) Aus $(\dagger)$ und Satz 1 S. 5: 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 $\det P = \pm 1$, so P ist invertierbar über R und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Ganzheitsbasis.

(iii) wenn $D(f)$ ist nicht quadratfrei,

dann benutzen wir Stickelberger's Satz.

<u>Satz von Stickelberger</u>

$$D(\mathcal{O}_L / \mathbb{Z}) \equiv 0, 1 \mod 4$$

(also is Quadrat mod 4).

<u>Beweis</u>: später (15. Vorlesung).

<u>Anwendung</u>: sei L quadratischer Zahlkörper

(siehe Vor. 1 & 2); $[L : \mathbb{Q}] = 2$

$L = \mathbb{Q}(\sqrt{d})$; $d \in \mathbb{Z}$ quadratfrei.

<u>Fall 1.</u> $d \equiv 2, 3 \mod 4$. Beh. $\{1, \sqrt{d}\}$

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

Beweis. Setze $\alpha := \sqrt{d}$ primitives Element;

$\alpha \in \mathcal{O}_L$ und $\text{Min Pol}_{\mathbb{Q}}\, \alpha := f(x) = x^2 - d$.

Seine NS sind

$$\left[x_{1,2} := \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \right]$$

Also ist $D(f) = (x_1 - x_2)^2 = 4d$

Nun ist

$$4d = \underset{\in \mathbb{Z}}{(\det P)}^2 \underbrace{D(\mathcal{O}_L/\mathbb{Z})}_{\equiv 0,1 \bmod 4}$$

$$P \in M_{n\times n}(\mathbb{Z})$$

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

Bew: wenn $D(\mathcal{O}_L/\mathbb{Z}) \equiv 1 \bmod 4$ wäre

dann ist $(\det P)^2 \equiv 0 \bmod 4$; aber dann

$$\underset{2,3 \bmod 4}{\underset{\equiv}{d}} = \underset{0,1 \bmod 4}{\underset{\equiv}{l^2}} \; \underset{1 \bmod 4}{\underset{\equiv}{D(\mathcal{O}_L/\mathbb{Z})}} \quad \lightning$$

Also

$$4d = (\det P)^2 \underset{0 \bmod 4}{\underset{\equiv}{D(\mathcal{O}_L/\mathbb{Z})}}$$

4 auf beiden Seiten kürzen ergibt nun:

$$d = (\det P)^2 w$$

und d quadratfrei $\Rightarrow (\det P)^2 = 1$

also ist $\det P = \pm 1$ so $\{1, d\}$

ist eine Ganzheitsbasis.

<u>Fall 2</u>. $d \equiv 1 \mod 4$ Behauptung: $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$

ist eine Ganzheitsbasis, also ist

$$\mathcal{O}_L = \mathbb{Z}[\omega] \quad \text{wobei} \quad \omega := \tfrac{1}{2}\left(1 + \sqrt{d}\right).$$

Bew: $f = \mathrm{MinPol}_{\mathbb{Q}}\, \omega =$

$$x^2 - x + \left[\frac{1-d}{4}\right] \in \mathbb{Z}[x]$$

und

$$D(f) = 1 - \left[4\left(\frac{1-d}{4}\right)\right] = 1 - 1 + d = d;$$

d quadratfrei, also folgt nun unsere

Beh. aus Bmk 3 (ii) S. 8.