– Algebraische Zahlentheorie –

– B4 – SS 2012/2013

– Kuhlmann –

13. Vorlesung am 06. 06. 2013

__Erinnerung__: Bilineare Formen (Fortsetzung)

__Definitionen und Bemerkungen__: Sei V endl. dim. VR über K.

Sei $B : V \times V \longrightarrow K$ bilinear symmetrisch

$\forall x \in V$ definiere:

$$B_x : V \longrightarrow K \quad \text{durch } B_x(y) := B(x,y)$$

[oder $B_y : V \longrightarrow K$ durch $B_y(x) := B(x,y)$].

B heißt __nicht ausgeartet__ wenn:

$$\forall_{x \in V} \; x \neq 0 \Rightarrow B_x \neq 0.$$

Bemerke daß

(i) $B_x \in V^*$

(ii) B ist nicht ausgeartet $\Leftrightarrow$ $\det \mathbb{B} \neq 0$

(üA) für eine (alle) matrix Darstellung $\mathbb{B}$ für B.

(iii) B ist nicht ausgeartet $\Leftrightarrow$ die lineare Abbildung

(üA) $$\varphi_B : V \longrightarrow V^*$$
$$x \longmapsto B_x$$

hat kernel $\{0\}$ $(\ker \varphi_B = \{0\})$.

(iv) Da $\dim V = \dim V^*$ gilt also:

B nichtausgeartet $\Leftrightarrow$ φ_B eine Isomorphie ist.

(v) Sei $\mathcal{B} := \{v_1, \ldots, v_n\}$ K-Basis für V, B nicht ausgeartet; setze

$$w_i := \varphi_B^{-1}(v_i^*)$$

dann gilt: $B(v_i, w_j) = \delta_{ij} \quad \forall i, j$.

Die Basis $\{w_i ; i = 1, \ldots, n\}$ heißt die zu $\{v_1, \ldots, v_n\}$ <u>B- duale Basis</u> für V.

üA. Die B- duale Basis hat die folgende nützliche Eigenschaft: $\forall v \in V$ mit $v = \sum c_i v_i$ ist $c_i = B(v, w_i)$.

Die Spur Bilineare Form:

Fact 1: Sei L/K endl. separable Körpererw., dann definiert die Abbildung

$$B_{L/K} : L \times L \longrightarrow K$$

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

eine symmetrische bilineare Form (ÜA).

Fact 2. $B_{L/K}$ ist nicht ausgeartet.

Beweis. (Satz vom Primitivenelement) sei $\gamma \in L$ so daß $L := K(\gamma)$; dann ist

$\{\gamma^0, \dots, \gamma^{n-1}\}$ eine K-Basis für L.

Wir berechnen die matrix Darstellung $\mathbb{B}$ der bilinearen Form bezüglich dieser Basis:

$$\mathbb{B}_{ij} = sp(\gamma^{i+j}) \underset{11.\,Vor.}{\overset{satz}{=}} \sum_{k=1}^{n} \sigma_k(\gamma^{i+j})$$

$i = 0, \dots, n-1$
$j = 0, \dots, n-1$

wobei $\sigma_1, \dots, \sigma_n$ die n-verschiedene Einbettungen von L in Ω

$\underline{\underline{\text{Hom.}}}$ $\sum_{k=1}^{n} \sigma_k(\gamma)^{i+j}$.

Bezeichne $\gamma_1, \ldots, \gamma_n$ die n verschiedene NS vom $\text{MinPol}_K \gamma$, also ist

$\{\gamma_1, \ldots, \gamma_n\} = \{\sigma_1(\gamma), \ldots, \sigma_n(\gamma)\}$.

Wir schreiben um:

$$\mathbb{B}_{ij} = \sum_{k=1}^{n} \gamma_k^{i+j}$$

Daraus sehen wir daß $\mathbb{B}$ Produkt ist von zwei Matrizen mit $\det \neq 0$ nämlich

$$\mathbb{B} = \mathcal{V}^t \mathcal{V} \quad \text{und}$$

$$\det \mathbb{B} = (\det \mathcal{V})^2$$ wobei $\mathcal{V}$ die Vandermonde Matrix

$$\mathcal{V} := \begin{pmatrix} \gamma_1^0 & \cdots & \gamma_1^{n-1} \\ \gamma_2^0 & \cdots & \gamma_2^{n-1} \\ \vdots & & \vdots \\ \gamma_n^0 & \cdots & \gamma_n^{n-1} \end{pmatrix}$$

In LA II haben wir gezeigt

$\det \mathcal{V} \neq 0$.

Also ist $\det \mathbb{B} \neq 0$ und somit ist gezeigt

daß $B_{L/K}$ nicht ausgeartet ist. $\boxed{}$

Bemerkung (siehe ÜB).

Sei L/K endlich separabel; $[L:K] = n$;

wir können andere Basen betrachten

(anstatt $\{\gamma^0, \dots, \gamma^{n-1}\}$) wie folgend:

Sei $\{\nu_1, \dots, \nu_n\}$ eine beliebige Basis für

L/K und wie zuvor $\{\sigma_1, \dots, \sigma_n\}$ die n

verschiedene Einbettungen von L in Ω.

Dann ist die Matrix $\mathbb{B}$ von $B_{L/K}$ bezüglich

$\{\nu_1, \dots, \nu_n\}$ $\quad V^t V \quad$ wobei

$V_{ij} := \sigma_i(\nu_j) \quad \forall\, i, j$.

Also ist $\det \mathbb{B} = (\det V)^2$. $\boxed{}$

Satz: sei R ganz abgeschlossen Integritätsb.

$k := \mathrm{Quot}(R)$

L/k end. sep. $[L:k] = n$

$S := \bar{R}^L$

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: später

Korollar 1: Sei R ganz abgeschlossen Integritätsb, R noethersch; $k = \mathrm{Quot}(R)$.

Dann ist $S := \bar{R}^L$ ein endl. erz. R-Modul.

Beweis: M' ist endl. erz. Modul über ein noethersch'en Ring; also M' is noethersch R-Modul; und damit ist jeder Untermodul endl. erzeugt. □

Korollar 2: Sei R ein HIR; L/K endl. separable Erweiterung, $[L:K] = n$.
Dann ist $S := \bar{R}^L$ frei R-Modul der Dimension n.

Beweis: Ein Untermodul (über ein HIR) (vom freiem Modul der Dimension $\leq n$) ist frei der Dimension $\leq n$.

Also: $S \subseteq M' \Rightarrow S$ frei der Dimension $\leq n$

$M \subseteq S \Rightarrow \dim M = n \leq \dim S \leq n$

$\Rightarrow \dim S = n$. $\square$

Korollar 3 $R: \mathbb{Z}$ L Zahlkörper

$\Rightarrow \mathcal{O}_L$ is frei $\mathbb{Z}$-Modul der Dimension $\deg L/K$. $\square$