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

13.Vorlesung

19 Juni 2017

Erinnerung: Bilineare Formen (Fortsetzung)
Definitionen und Bemerkungen: Sei V ein endlichdimensionaler Vektorraum über K. Sei $B : V \times V \to K$ bilinear symmetrisch. Für alle $x \in V$ definiere:
$B_x : V \to K$ durch $B_x(y) = B(x, y)$
(oder $B_y : V \to K$ durch $B_y(x) = B(x, y)$)
B heißt nicht ausgeartet, wenn: $\forall x \in V, x \neq 0 \Rightarrow Bx \neq 0$.
Bemerke, daß

(i) $B_x \in V^*$

(ii) B nicht ausgeartet$\Leftrightarrow \det \mathbb{B} \neq 0$ für eine (alle) Matrixdarstellungen $\mathbb{B}$ von B (ÜA).

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

$$\begin{array}{rccc} \phi_B : & V & \to & V^* \\ & x & \mapsto & B_x \end{array}$$

hat Kern $\{0\}$ (ÜA).

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

B nicht ausgeartet$\Leftrightarrow \phi_B$ ist eine Isomorphie

(v) Sei $\mathcal{B} := \{v_1, \ldots, v_n\}$ eine K-Basis für V, B nicht ausgeartet; setze $w_i := \phi_B^{-1}(v_i^*)$. Dann gilt $B(v_i, w_j) = \delta_{ij} \forall i, j$. Die Basis $\{w_i \mid i = 1, \ldots, n\}$ heißt die zu $\{v_1, \ldots, v_n\}$ B-duale Basis für V. Die B-duale Basis hat die folgende nützliche Eigenschaft:

$\forall v \in V$ mit $v = \sum c_i v_i$ ist $c_i = B(v, w_i)$ (ÜA).

§Die Spur bilineare Form

Fact 1: Sei L/K eine endliche separable Körpererweiterung; dann definiert die Abbildung

$$\begin{array}{rccc} B_{L/K} : & L \times L & \to & K \\ & (x, y) & \mapsto & Sp_{L/K}(xy) \end{array}$$

eine symmetrische bilineare Form (ÜA).

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

Beweis. (Satz vom Primitivelement) Sei $\gamma \in L$, so daß $L := K(\gamma)$; dann ist $\{\gamma^0, \ldots, \gamma^{n-1}\}$ eine K-Basis für L. Wir berechnen die Matrixdarstellung $\mathbb{B}$ der bilinearen Form bezüglich dieser Basis:

$\mathbb{B}_{ij} = Sp(\gamma^{i+j}) \overset{\text{Satz 11 Vor.}}{=} \sum_{k=1}^{n} \sigma_k(\gamma^{i+j}) \overset{\text{Hom}}{=} \sum_{k=1}^{n} \sigma_k(\gamma)^{i+j}$, wobei $\sigma_1, \ldots, \sigma_n$ die n verschiedenen Einbettungen von L in Ω sind.
Bezeichne $\gamma_1, \ldots, \gamma_n$ die n verschiedenen Nullstellen von $\operatorname{MinPol}_K(\gamma)$, 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 $\mathbb{B}$ ein Produkt von zwei Matrizen mit $\det \neq 0$ ist, nämlich $\mathbb{B} = \mathcal{V}^t\mathcal{V}$ und $\det \mathbb{B} = (\det \mathcal{V})^2$, wobei $\mathcal{V}$ die Vandermonde Matrix :

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

ist (In LA II haben wir gezeigt, daß $\det \mathcal{V} \neq 0$). Also ist $\det \mathbb{B} \neq 0$ und somit ist gezeigt, daß $B_{L/K}$ nicht ausgeartet ist.

□

Bemerkung (siehe ÜB)
Sei L/K endlich separabel, $[L : K] = n$. Wir können andere Basen betrachten (anstatt $\{\gamma^0, \ldots, \gamma^{n-1}\}$): Sei $\{v_1, \ldots, v_n\}$ eine beliebige Basis für L/K und wie zuvor $\{\sigma_1, \ldots, \sigma_n\}$ die n verschiedenen Einbettungen von L/K in Ω. Dann ist die Matrix $\mathbb{B}$ von $B_{L/K}$ bezüglich $\{v_1, \ldots, v_n\}$ $\mathcal{V}^t\mathcal{V}$, wobei $\mathcal{V}_{ij} := \sigma_i(v_j)$ für alle i, j, also ist $\det \mathbb{B} = (\det \mathcal{V})^2$.

Satz
Sei R ein ganz abgeschlossener Integritätsbereich, $K = \operatorname{Quot}(R)$, 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. später □

Korollar 13.1
Sei R ein ganz abgeschlossener Integritätsbereich, R noethersch, $K = \operatorname{Quot}(R)$. Dann ist $S := \overline{R}^L$ ein endlich erzeugter R-Modul.

Beweis. M' ist ein endlich erzeugter Modul über einem noetherschen Ring, also ist M' ein noetherscher R-Modul, und damit ist jeder Untermodul endlich erzeugt.

□

Korollar 13.2
Sei R ein HIR, L/K eine endliche separable Körpererweiterung und $n = [L : K]$. Dann ist $S := \overline{R}^L$ ein freier R-Modul der Dimension n.

Beweis. Ein Untermodul (von freiem Modul der Dimension $= n$ und über einem HIR) ist frei der Dimension $\leq n$, also:
$S \subseteq M' \Rightarrow S$ frei der Dimension $\leq n$
$M \subseteq S \Rightarrow \dim M = n \leq \dim S \leq n \Rightarrow \dim S = n$ □

Korollar 13.3
$R = \mathbb{Z}$. L ist ein Zahlkörper$\Rightarrow$ $\mathcal{O}_L$ ist ein freier $\mathbb{Z}$-Modul der Dimension $[L : K]$