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

12.Vorlesung

12 Juni 2017

Korollar 12.1
Sei R ein ganz abgeschlossener Integritätsbereich, $K := \text{Quot}(R)$, L/K eine endliche Körpererweiterung. Sei $\beta \in \overline{R}^L$; dann sind $N_{L/K}(\beta) \in R$ und $Sp_{L/K}(\beta) \in R$.

Beweis. $\beta \in \overline{R}^L, \beta_1, \dots, \beta_m$ die Nullstellen von $\text{MinPol}_K(\beta) \in R[x] \Rightarrow \beta_1, \dots, \beta_m \in \overline{R}^L$. Nun ist außerdem $K \ni N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K} = r \sum \beta_i \in K$, also $N_{L/K}(\beta) \in \overline{R}^L$ und $Sp_{L/K} \in \overline{R}^L$. Nun ist aber R ganz abgeschlossen, also folgt die Behauptung. □

Satz 12.2
Sei L/K separabel, $[L : K] = n$, Ω die normale Hülle von L/K. Dann gelten:

1. $\exists \sigma_1, \dots, \sigma_n$ verschiedene Einbettungen von L/K in Ω.
2. Für $\beta \in L$ mit $[K(\beta) : K] = m = \frac{n}{r}$ und $[L : K(\beta)] = r$ und $\sigma \in \{\sigma_1, \dots, \sigma_n\}$ kommt $\sigma(\beta)$ genau r mal in der Folge $(\sigma_1(\beta), \dots, \sigma_n(\beta))$ vor.

Beweis. (1) Sei $L = K(\gamma)$, $\text{MinPol}_K(\gamma) = g$ und $\gamma_1, \dots, \gamma_n$ die n verschiedenen Nullstellen von g in Ω.

$$\begin{array}{ccc} L & \overset{\sigma_k}{\hookrightarrow} & \Omega \\ \gamma & \mapsto & \gamma_k \\ K & \underset{= Id}{\xrightarrow{\sigma_k \restriction K}} & K \end{array} \quad \text{(Isomorphismus } K(\gamma) \cong K[x]/ < g(x) > \cong K(\gamma_k) \text{ aus Algebra BIII)}$$

(2) $L/K(\beta)$ und $K(\beta)/K$ sind separabel, also liefert (1) m Einbettungen von $K(\beta)$ über K in Ω' (Ω' :=normale Hülle von $L/K(\beta)$, $\Omega' \supseteq \Omega$), und r Einbettungen von L über $K(\beta)$ in Ω'; zusammengefasst:

$\exists m$ Einbettungen von $K(\beta)$ über K in Ω'

$\exists r$ Einbettungen von L über $K(\beta)$ in Ω',

$\exists mr = n$ Einbettungen von L über K in Ω'.

$$L \underset{K(\beta)}{\overset{\lambda_1, \dots, \lambda_r}{\hookrightarrow}} \Omega'$$

$$K(\beta) \underset{K}{\overset{\mu_1, \dots, \mu_m}{\hookrightarrow}} \Omega'$$

Betrachte:

$L \xrightarrow{\sim} \lambda_i(L) \subseteq \Omega'$ und schreibe $L = K(\beta)(\gamma)$, also $\lambda_i(L) = K(\beta)(\lambda_i(\gamma))$.

Definiere $K(\beta)(\lambda_i(\gamma)) \xrightarrow{\tilde{\mu}_j} \Omega'$ durch: $\tilde{\mu}_j \restriction K(\beta) = \mu_j$ und $\lambda_i(\gamma) \mapsto \lambda_i(\gamma)$.

Betrachte nun $L \xrightarrow[\sim]{\lambda_i} \lambda_i(L) \xrightarrow{\tilde{\mu}_j} \Omega'$.

Es ist klar, daß $(\tilde{\mu}_j \circ \lambda_i)$ Einbettung von L über Kin Ω' ist für alle $j = 1, \ldots, m$ und $i = 1, \ldots, r$. Also ist $\{\tilde{\mu}_j \circ \lambda_i, j = 1, \ldots, m, i = 1, \ldots, r\} \subseteq \{\sigma_1, \ldots, \sigma_n\}$.

Außerdem ist $\tilde{\mu}_j \circ \lambda_i$ eindeutig durch ihre Bilder für γ und β bestimmt. Nun ist

$(\tilde{\mu}_j \circ \lambda_i)(\gamma) = \tilde{\mu}_j(\lambda_i(\gamma)) = \lambda_i(\gamma)$ und

$$(\tilde{\mu}_j \circ \lambda_i)(\beta) = \mu_j(\beta) \tag{$*$}$$

Es folgt $\{\tilde{\mu}_j \circ \lambda_i \mid j = 1, \ldots, m, i = 1, \ldots, r\} = \{\sigma_1, \ldots, \sigma_n\}$ und $\forall \sigma \in \{\sigma_1, \ldots \sigma_n\}$ ist $\sigma(\beta)$ r mal wiederholt wie in $(*)$.

□

Korollar 12.3
Sei $K \subseteq E \subseteq L$ mit L/K endlich separabel, $[L : K] = n$, und $\alpha \in L$. Dann gelten:

(i) $N_{L/K}(\alpha) = N_{E/K}(N_{L/E}(\alpha))$ und

(ii) $Sp_{L/K}(\alpha) = Sp_{E/K}(Sp_{L/E}(\alpha))$

Beweis. (i) $N_{L/K}(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)$ wobei $\{\sigma_1, \ldots, \sigma_n\}$ die Einbettungen von L/K in Ω sind. Nun $\forall k, \exists i, \exists j$, so daß $\sigma_k = \tilde{\mu}_j \circ \lambda_i$ (Bezeichnung wie im letzten Beweis). Also

$N_{L/K}(\alpha) \overset{\text{Hom}}{=} \prod_{j=1}^{m} \tilde{\mu}_j(\prod_{i=1}^{r} \lambda_i(\alpha))$. Nun folgt aus dem letzten Beweis, daß

$\prod_{i=1}^{r} \lambda_i(\alpha) = N_{L/E}(\alpha) \in E$ (insbesondere ist

$\tilde{\mu}_j(\prod_{i=1}^{r} \lambda_i(\alpha)) = \mu_j(\prod_{i=1}^{r} \lambda_i(\alpha)))$,

also $N_{L/K}(\alpha) = \prod_{j=1}^{m} \mu_j(N_{L/E}(\alpha)) = N_{E/K}(N_{L/E}(\alpha))$.

□

§Erinnerung: Bilineare Formen

Definition 1. Sei V ein endlichdimensionaler Vektorraum über K, $\dim_K V = n$ und $B : V \times V \to K$ eine bilineare Form.

2. B ist symmetrisch$\Leftrightarrow B(x, y) = B(y, x) \forall x, y \in V$.

3. Die Matrix-Darstellung von B bezüglich der Basis $\{v_i \mid i = 1, \ldots, n\} = \mathcal{B}$ ist definiert durch:

   $\mathbb{B}_{ij} = B(v_i, v_j)$

   Es gilt $\forall x, y \in V, [y]_{\mathcal{B}}^t \mathbb{B} [x]_{\mathcal{B}} = B(x, y)$

4. $\mathbb{B}' = P^t \mathbb{B} P$, wobei $\mathbb{B}'$ die Darstellung von B bezüglich einer Basis $\{v_i' \mid i = 1, \ldots, n\}$ und P die Basiswechselmatrix ist.