Algebraische Zahlentheorie

SS 2012 - 2013

- Algebra B4 -

- Kuhlmann -

12. Vorlesung
am 03. 06. 2013

<u>Korollar 1</u> Sei R ganz abg. Integritätsbereich, $K = \mathrm{Quot}(R)$, $L|K$ endl. Körpererw. Sei $\beta \in \overline{R}^L$, dann sind

$$N_{L/K}(\beta) \in R \quad \text{und} \quad Sp_{L/K}(\beta) \in R.$$

<u>Beweis.</u> $\beta \in \overline{R}_L$, $\beta_1, \dots, \beta_m$ die NS von $\mathrm{Min\,Pol}_K \beta \in R[x]$

$\Rightarrow \beta_1, \dots, \beta_m \in \overline{R}_L$. Nun ist außerdem

$$K \ni N_{L/K}(\beta) = \left(\prod \beta_i\right)^r \text{ und } Sp_{L/K} = r \sum \beta_i \in K,$$

also $N_{L/K}(\beta) \in \overline{R}_L$ und $Sp_{L/K} \in \overline{R}_L$.

Nun ist aber R ganz abg; also folgt die Behauptung. $\blacksquare$

Satz 2: Sei L/K separabel, $[L:K] \cancel{=} n$, Ω die normale Hülle von L/K. Dann gelten:

1. $\exists\ \sigma_1, \dots, \sigma_n$ versiedene Einbettungen von L/K in Ω.

2. Für $\beta \in L$ mit $[K(\beta) : K] = m = n/r$
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 $L = K(\gamma)$ Min Pol$_K\,\gamma := g$

$\gamma_1, \dots, \gamma_n$ die n verschieden NS von g in Ω

$$\begin{array}{ccc} L & \xhookrightarrow{\sigma_k} & \Omega \\ \gamma & \longmapsto & \gamma_k \end{array} \qquad k = 1, \dots, n$$

$$K \xrightarrow{\sigma_k \restriction K} K$$
$$= \mathrm{Id}$$

(Isomorphismus $K(\gamma) \simeq K[x]/_{\langle g(x) \rangle} \simeq K(\gamma_k)$ aus Algebra B III).

2. $L/K(\beta)$ und $K(\beta)/K$ sind auch separabel.

Also 1. liefert m Einbettungen von $K(\beta)$ über K in Ω' [$\Omega' :=$ normale Hülle von $L/K(\beta)$; $\Omega' \supset \Omega$]; und r Einbettungen von L über $K(\beta)$ in Ω'; zusammengefasst:

$\exists\, m$ Einbett. von $K(\beta)$ über K in Ω'

$\exists\, r$ " " L " $K(\beta)$ " "

$\exists\, mr = n$ " " L " K " ".

$$L \xrightarrow[K(\beta)]{\lambda_1, \dots, \lambda_r} \Omega'$$

$$K(\beta) \xrightarrow[K]{\mu_1, \dots, \mu_m} \Omega'$$

Betrachte:

$L \xrightarrow{\sim} \lambda_i(L) \subset \Omega'$ und schreibe

$L = K(\beta)(\gamma)$ so $\lambda_i(L) = K(\beta)(\lambda_i(\gamma))$.

Definiere $K(\beta)(\lambda_i(\gamma)) \xrightarrow{\tilde{\mu}_j} \Omega'$

durch: $\tilde{\mu}_j \restriction_{K(\beta)} = \mu_j$ und

$$\lambda_i(\gamma) \longmapsto \lambda_i(\gamma) .$$

Betrachte nun

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

es ist klar daß $(\tilde{\mu}_j \circ \lambda_i)$ eine Einbettung von L über K in Ω' ist, für alle $j = 1, \dots, m$ und $i = 1, \dots, r$.

Also ist $\left\{ \tilde{\mu}_j \circ \lambda_i \ ; \ \begin{matrix} j = 1, \dots, m, \\ i = 1, \dots, r \end{matrix} \right\} \subseteq \{ 6_1, \dots, 6_n \}$.

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

Nun ist

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

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

Es folgt: $\{\tilde{\mu}_j \circ \lambda_i \,;\, j=1,\dots,m,\ i=1,\dots,r\} = \{\sigma_1,\dots,\sigma_n\}$

und $\forall \sigma \in \{\sigma_1,\dots,\sigma_n\}$ ist

$\sigma(\beta)$ r mal wiederholt wie in $(*)$. ∎

<u>**Korollar 3.**</u> Sei $K \subset E \subset L$ mit L/K endl. separabel, $[L:K]=n$ und $\alpha \in L$. Dann gelten

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

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

<u>Beweis:</u> (i) $N_{L/K}(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)$

wobei $\{\sigma_1,\dots,\sigma_n\}$ die Einbettungen von L/K in Ω.

Nun $\forall k\ \exists i, \exists j$ s.d. $\sigma_k = \tilde{\mu}_j \circ \lambda_i$ (Bezeichnung wie in letztem Beweis). Also

$$N_{L/K}(\alpha) \overset{\text{Hom.}}{=} \prod_{j=1}^{m} \tilde{\mu}_j \left(\prod_{i=1}^{r} \lambda_i(\alpha) \right).$$

Nun folgt aus dem letztem Beweis daß

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

[insbesondere ist $\tilde{\mu}_j\left(\prod_{i=1}^{r} \lambda_i(\alpha)\right) = \mu_j\left(\prod_{i=1}^{r} \lambda_i(\alpha)\right)$]

So $N_{L/K}(\alpha) = \prod_{j}^{m} \mu_j\left(N_{L/E}(\alpha)\right) = N_{E/K}\left(N_{L/E}(\alpha)\right)$. ∎

§ Erinnerung: Bilineare Forme.

Definition:

(i) Sei V endl. dim V.R über K ; $\dim_K V := n$

und $$B : V \times V \longrightarrow K$$

eine bilineare Form.

(ii) B ist symmetrisch $\Leftrightarrow$ $B(x,y) = B(y,x) \quad \forall x, y \in V$

(iii) Die Matrix Darstellung von B bzgl. der Basis $\{v_i \,;\, i = 1, \dots, n\} = \mathcal{B}$ ist definiert durch:

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

Es gilt $\forall x, y \in V$

$$[y]_{\mathcal{B}}^t \quad \mathbb{B} \quad [x]_{\mathcal{B}} = B(x,y)$$

(iv) und

$$\mathbb{B}' = P^t \; \mathbb{B} \; P$$

wobei $\mathbb{B}'$ die Darstellung bzgl einer Basis $\{v_i' \,;\, i = 1, \dots, n\}$ und P die Basiswechsel Matrix.