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

11.Vorlesung

8. Juni 2017

§Norm, Spur, Diskriminante

Sei L/K eine endliche Körpererweiterung.

Definition und Notation
Sei $\alpha \in L$ und betrachte die Abbildung

$$\begin{array}{rccc} \mu_{\alpha,L}: & L & \to & L \\ & x & \mapsto & \alpha x \end{array}$$

Es ist $\mu_{\alpha,L} \in \mathcal{L}_K(L,L)$ (d.h ein linearer Operator). Setze
$\chi_{\alpha,L} :=$ CharPol von $\mu_{\alpha,L}$
$f_{\alpha,L} :=$ MinPol von $\mu_{\alpha,L}$
$N_{L/K}(\alpha) := \det(\mu_{\alpha,L}) \in K$ heißt die (L/K)-Norm von α.
$Sp_{L/K}(\alpha) := \mathrm{Spur}(\mu_{\alpha,L}) \in K$ ist die (L/K)-Spur von α

Lemma 11.1 (i) $f_{\alpha,L} =$ MinPol$_K(\alpha)$; Insbesondere ist $f_\alpha := f_{\alpha,K(\alpha)} = \chi_{\alpha,K(\alpha)} =$ MinPol$_K(\alpha)$ (weil $\deg \chi_{\alpha,K(\alpha)} = [K(\alpha) : K] = \deg$ MinPol$_K(\alpha) = \deg f_{\alpha,K(\alpha)}$, und damit sind sie gleich).

(ii) $\chi_{\alpha,L} = f^m_{\alpha,L}$, wobei $m := [L : K(\alpha)]$.

Beweis. (i) Es ist leicht zu prüfen, daß $f(\mu_{\alpha,L}) = 0 \Leftrightarrow f(\alpha) = 0 \forall f \in K[x]$. Die Aussage folgt nun unmittelbar aus der Definition.

(ii) Sei $\{\lambda_1, \dots, \lambda_m\}$ eine Basis für $L/K(\alpha)$, also

$$(*) \qquad L = \bigoplus_{i=1}^m K(\alpha)\lambda_i$$

Setze $W_i := K(\alpha)\lambda_i$; die W_i sind (prüfe!) $\mu_{\alpha,L}$-invariante K-Unterräume und

$$(**) \qquad L = \bigoplus_{i=1}^m W_i \text{ als } K\text{-Vektorraum},$$

d.h $\mu_{\alpha,L} : L \to L$

$\mu_{\alpha,K(\alpha)} : K(\alpha) \to K(\alpha)$

und $\begin{array}{ccc} K(\alpha) & \overset{\omega_i}{\tilde{\to}} & W_i \\ x & \mapsto & x\lambda_i \end{array}$ als K-Vektorräume, wobei ω_i die folgende Eingenschaft hat:

$\omega_i \circ \mu_{\alpha,K(\alpha)} = \mu_{\alpha,L} \circ \omega_i$ auf $K(\alpha)$, d.h $\mu_{\alpha,L} = \bigoplus_{i=1}^m \mu_{\alpha,K(\alpha)}$

und $\underbrace{\mu_{\alpha,L} \restriction W_i = \omega_i \circ (\mu_{\alpha,K(\alpha)}) \circ \omega_i^{-1}}_{\text{ähnliche lineare Transformationen}}$ (prüfe!)

$(**)$ liefet nun (LA I+II), daß

$$\begin{aligned}
\chi_{\alpha,L} &= \mathrm{CharPol}(\mu_{\alpha,L}) \\
&= \prod_{i=1}^{m} \mathrm{CharPol}(\mu_{\alpha,L} \restriction_{W_i}) \\
&= \prod_{i=1}^{m} \mathrm{CharPol}(\omega_i \circ \mu_{\alpha,K(\alpha)} \circ \omega_i^{-1}) \\
&= \prod_{i=1}^{m} \mathrm{CharPol}(\mu_{\alpha,K(\alpha)}) \\
&= \prod_{i=1}^{m} \chi_{\alpha,K(\alpha)} \\
&\overset{(i)}{=} \prod_{i=1}^{m} f_\alpha
\end{aligned}$$

□

Lemma 11.2
Seien $\alpha, \beta \in L$, $\lambda \in K$ und $n = [L : K]$. Es gilt:

1. $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) N_{L/K}(\beta)$
2. $Sp_{L/K}(\lambda\alpha + \beta) = \lambda Sp_{L/K}(\alpha) + Sp_{L/K}(\beta)$
3. $N_{L/K}(\lambda) = \lambda^n, Sp_{L/K}(\lambda) = n\lambda$
4. Sei $f_{\alpha,L} = x^\nu + a_{\nu-1}x^{\nu-1} + \cdots + a_0, \quad a_i \in K$.

Setze $\mu := [L : K(\alpha)] = \frac{n}{\nu}$. Es gilt:

(i) $N_{L/K}(\alpha) = (-1)^n a_0^\mu$

(ii) $Sp_{L/K}(\alpha) = -\mu a_{\nu-1}$

Beweis. 1. $\mu_{\alpha\beta,L} = \mu_{\alpha,L} \circ \mu_{\beta,L}$ und die Determinante ist multiplikativ (LA II).

2. $\mu_{\lambda\alpha+\beta,L} = \lambda\mu_{\alpha,L} + \mu_{\beta,L}$ und die Spur ist additiv (LA II).

3. $N_{L/K}(\lambda) = \det(\mu_{\lambda,L}) = \det(\lambda \,\mathrm{Id}_L) = \lambda^n$.
   Analog $Sp_{L/K}(\lambda) = \mathrm{Spur}(\lambda \,\mathrm{Id}_L) = n\lambda$.

4. **Erinnerung**(LA I+II): $A \in M_{n\times n}(K)$, setze $\mathrm{CharPol}(A) = \det(xI - A) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$. Es ist $b_0 = (-1)^n \det A$ und $b_{n-1} = -\mathrm{Spur}(A)$.

(i) $\nu = [K(\alpha) : K], \quad \mu = [L : K(\alpha)], \quad n = \nu\mu$. $N_{L/K}(\alpha) = \det(\mu_{\alpha,L})$ und

$$(\dagger) \qquad \chi_{\alpha,L} = x^n + b_{n-1}x^{n-1} + \cdots + b_0 = (f_\alpha)^\mu$$

also gilt $(-1)^n \det(\mu_{\alpha,L}) = b_0$ und Koeffizientenvergleich in $(\dagger)$ ergibt $b_0 = a_0^\mu$.

(ii) $b_{n-1} = -Sp_{L/K}(\alpha)$, Koeffizientenvergleich in (†) ergibt: links ist Koeffizient von x^{n-1}, gleich Koeffizient von $x^{\nu\mu-1}$ rechts, also ist gleich $\mu a_{\nu-1}$ (ÜA).

$\square$

Proposition 11.3
Sei $n = [L : K]$, $\beta \in L$, $f(x) = \operatorname{MinPol}_K(\beta)$ und $\deg f := m = [K(\beta) : K]$. Seien $\beta = \beta_1, \beta_2, \dots, \beta_m$ alle Nullstellen von f. Es ist $N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K}(\beta) = r \sum \beta_i$, wobei $r := \frac{n}{m} = [L : K(\beta)]$

Beweis. (Lemma 11.2 4-(i) und 4-(ii) anwenden) Sei $f_{\beta,L} = \operatorname{MinPol}_K(\beta) = x^m + a_{m-1}x^{m-1} + \dots + a_0$, $a_i \in K$. Nun ist $\prod \beta_i = (-1)^m a_0$ und $\sum \beta_i = -a_{m-1}$ (Algebra BIII), also ist $(\prod \beta_i)^r = (-1)^{mr} a_0^r \overset{(i)}{=} N_{L/K}(\beta)$ und $r \sum \beta_i = -r a_{m-1} \overset{(ii)}{=} Sp_{L/K}(\beta)$. $\square$

Satz 11.4
Sei L/K separabel, $[L : K] = n$ und $\{\sigma_1, \dots, \sigma_n\}$ die Menge der verschiedenen K-Einbettungen von L (in der normalen Abschluss Ω von L/K). Sei $\beta \in L$. Es ist $N_{L/K}(\beta) = \prod_{k=1}^n \sigma_k(\beta)$ und $Sp_{L/K}(\beta) = \sum_{k=1}^n \sigma_k(\beta)$

Beweis. (Wir zeigen in der 12. Vorlesung, daß $\sigma_1, \dots \sigma_n$ existieren) Sei $f(x) := \operatorname{MinPol}_K(\beta)$, $[K(\beta) : K] = m = \deg f$ und setze $r := [L : K(\beta)]$, und
$\beta = \beta_1, \beta_2, \dots, \beta_m$ die verschiedene Nullstellen von f.

Behauptung: Für $i = 1, \dots, m$ gibt es genau r Einbettungen von L in Ω, die β auf β_i absenden (d.h β_i erscheint genau r mal in $\{\sigma_k(\beta)\}_k$) (Diese Behauptung wird auch in der 12. Vorlesung bewiesen).

Nun folgt aus Prop 11.3, daß
$N_{L/K}(\beta) = (\prod_{i=1}^m \beta_i)^r = \prod_{i=1}^n \sigma_i(\beta)$ und $Sp_{L/K}(\beta) = r(\sum_{i=1}^m \beta_i) = \sum_{i=1}^n \sigma_i(\beta)$. $\square$

12