# B4: Algebraische Zahlentheorie
Sommersemester 2021
Frau Prof. Dr. Salma Kuhlmann

# 15.Vorlesung

10. Juni 2021

*In diesem Skript werden wir die Eigenschaften von Norm und Spur weiter entwickeln. Dafür werden wir (hier sowie in die folgende Skripte) weitere Elemente der Galoistheorie einbauen, die wir in der Algebra I nicht fertig gebracht haben.*

Sei $L/K$ stets eine endliche Körpererweiterung (das heißt $\dim_K L < \infty$).

Wir fangen an mit dem Beweis von Lemma 14.2

*Beweis.* 1. Wir bemerken zunächst daß $\mu_{\alpha\beta,L} = \mu_{\alpha,L} \circ \mu_{\beta,L}$ per Definition (ÜA). Wir berechnen nun: $N_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta,L}) = \det(\mu_{\alpha,L} \circ \mu_{\beta,L}) = \det(\mu_{\alpha,L}) \det(\mu_{\beta,L})$ (weil die Determinante multiplikativ ist).

2. Wir bemerken zunächst daß $\mu_{\lambda\alpha+\beta,L} = \lambda\mu_{\alpha,L} + \mu_{\beta,L}$ per Definition (ÜA). Wir argumentieren (analog wie in 1, und die Tatsache daß die Spur additiv ist) (ÜA).

3. Wir bemerken zunächst daß $\mu_{\lambda,L} = \lambda \operatorname{Id}_L$ per Definition (ÜA). Wir berechnen nun: $N_{L/K}(\lambda) = \det(\mu_{\lambda,L}) = \det(\lambda \operatorname{Id}_L) = \lambda^n$. Analog $Sp_{L/K}(\lambda) = \operatorname{Spur}(\lambda \operatorname{Id}_L) = n\lambda$.

4. (i) Wir haben $\nu = [K(\alpha) : K], \quad \mu = [L : K(\alpha)], \quad n = \nu\mu$ . Setze

   (†) $$\chi_{\alpha,L} = x^n + b_{n-1}x^{n-1} + \cdots + b_0.$$

   Wir berechnen nun $N_{L/K}(\alpha) = \det(\mu_{\alpha,L})$. Wir wissen (Erinnerung LA I + LA II) daß $(-1)^n \det(\mu_{\alpha,L}) = b_0$ . Außerdem ist (wegen Lemma 14.1):

   (‡) $$\chi_{\alpha,L} = (f_\alpha)^\mu.$$

   Ein Koeffizientenvergleich in (†) und (‡) ergibt nun $b_0 = a_0^\mu$.

   (ii) Wir wissen (Erinnerung LA I + LA II) daß $b_{n-1} = -\operatorname{Spur}(\mu_{\alpha,L}) = -Sp_{L/K}(\alpha)$ per Definition. Wir berechnen: der Koeffizient von $x^{n-1}$ (das heißt der Koeffizient von $x^{\nu\mu-1}$) in $(f_\alpha)^\mu$ ist $\mu a_{\nu-1}$ (ÜA). Wir vergleichen nun die Koeffizienten in (†) und (‡) und bekommen $b_{n-1} = \mu a_{\nu-1}$.

□

**Proposition 15.1**
Setze $n = [L : K]$. Sei $\beta \in L, f(x) := \text{ MinPol}_K(\beta)$ , $\deg f := m = [K(\beta) : K]$. Setze $r := \frac{n}{m} = [L : K(\beta)]$ . Seien $\beta = \beta_1, \beta_2, \ldots, \beta_m$ alle Nullstellen von $f$ (in einem Zerfällungskörper). Es ist

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

*Beweis.* Setze $f(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_0$, $a_i \in K$. Wir wissen daß $\prod \beta_i = (-1)^m a_0$ und $\sum \beta_i = -a_{m-1}$ (siehe ÜB).
Wir berechnen (mit Anwendung von Lemma 14.2 4-(i) und 4-(ii)):

$$(\prod \beta_i)^r = (-1)^{mr} a_0^r \overset{(i)}{=} N_{L/K}(\beta)$$

und

$$r \sum \beta_i = -r a_{m-1} \overset{(ii)}{=} Sp_{L/K}(\beta) \, .$$

□

**Korollar 15.2**
Sei $R$ ein ganz abgeschlossener Integritätsbereich, $K := \text{Quot}(R)$, und $L/K$ 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.* Da $\beta \in \overline{R}^L$ wissen wir daß $\text{ MinPol}_K(\beta) \in R[x]$. Nun seien $\beta = \beta_1, \ldots, \beta_m$ seine Nullstellen. Es folgt daß auch $\beta_1, \ldots, \beta_m \in \overline{R}^L$. Setze $r := [L : K(\beta)]$ . Nun sind per Definition $N_{L/K}(\beta)$ , $Sp_{L/K}(\beta) \in K$. Außerdem wegen Proposition 15.1 sind $N_{L/K}(\beta) = (\prod \beta_i)^r$ und $Sp_{L/K}(\beta) = r \sum \beta_i$. Also sind $N_{L/K}(\beta) \in \overline{R}^L$ und $Sp_{L/K} \in \overline{R}^L$. Nun ist aber $R$ ganz abgeschlossen, also folgt die Behauptung. □

In Satz 15.4 führen wir eine genauere Berechnung wenn $L/K$ separabel ist. Dafür brauchen wir einen weiteren Satz der Galoistheorie:

**Satz 15.3**
Sei $L/K$ separabel, und $\Omega$ die normale Hülle von $L/K$. Setze $[L : K] = n$. Dann gelten:

1. $\exists \sigma_1, \ldots, \sigma_n$ verschiedene Einbettungen von $L/K$ in $\Omega$.
2. Sei $\beta \in L$ und setze $[K(\beta) : K] = m = \frac{n}{r}$ und $[L : K(\beta)] = r$. Dann gilt

$$\forall \sigma \in \{\sigma_1, \ldots, \sigma_n\} \, : \, \sigma(\beta) \text{ kommt genau } r \text{ mal in der Folge } (\sigma_1(\beta), \ldots, \sigma_n(\beta)) \text{ vor .}$$

*Beweis.* Da $L/K$ separabel ist, ist sie eine einfache Erweiterung, also

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

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

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

$\exists mr = n$ Einbettungen von $L$ über $K$ in $\Omega'$,

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

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

Im Zeichen:

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

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

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 $L \overset{\lambda_i}{\xrightarrow{\sim}} \lambda_i(L) \xrightarrow{\tilde{\mu}_j} \Omega'$.

Es ist klar, daß $(\tilde{\mu}_j \circ \lambda_i)$ Einbettung von $L$ über $K$ in $\Omega'$ 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 $\gamma$ und $\beta$ bestimmt. Nun ist

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

und

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

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

□

**Satz 15.4**
Setze $[L : K] = n$ . Sei $L/K$ separabel, und $\{\sigma_1, \ldots, \sigma_n\}$ die Menge der verschiedenen $K$-Einbettungen von $L$ (in der normalen Abschluss $\Omega$ von $L/K$). Sei $\beta \in L$. Es ist

$$N_{L/K}(\beta) = \prod_{k=1}^{n} \sigma_k(\beta) \text{ und } Sp_{L/K}(\beta) = \sum_{k=1}^{n} \sigma_k(\beta) \,.$$

*Beweis.* Seien $\sigma_1, \ldots \sigma_n$ wie in Satz 15.3. Sei $f(x) :=$ $\mathrm{MinPol}_K(\beta)$, $[K(\beta) : K] = m = \deg f$ und setze $r := [L : K(\beta)]$, und
$\beta = \beta_1, \beta_2, \ldots, \beta_m$ die verschiedene Nullstellen von $f$.

• Es folgt aus Satz 15.3 daß: Für $i = 1, \ldots, m$ gibt es genau $r$ Einbettungen von $L$ in $\Omega$, die $\beta$ auf $\beta_i$ absenden. Das heißt: $\beta_i$ erscheint genau $r$ mal in der Folge $(\sigma_k(\beta))_k$.

• Nun folgt aus Prop 15.1, daß
$N_{L/K}(\beta) = (\prod_{i=1}^{m} \beta_i)^r = \prod_{i=1}^{n} \sigma_i(\beta)$ und $Sp_{L/K}(\beta) = r(\sum_{i=1}^{m} \beta_i) = \sum_{i=1}^{n} \sigma_i(\beta)$. □