Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Vorlesung 8

Norm und Spur bei einer Körpererweiterung

Ein Element $f \in L$ einer Körpererweiterung (oder allgemeiner einer K-Algebra A) $K \subseteq L$ definiert durch Multiplikation eine K-lineare Abbildung

$$\mu_f \colon L \longrightarrow L, y \longmapsto fy.$$

Dies erlaubt es, Begriffe und Methoden der linearen Algebra anzuwenden. Zu einer K-Basis von L wird die Multiplikationsabbildung durch eine $(n \times n)$-Matrix beschrieben, wobei n den Grad der Körpererweiterung bezeichnet. Für $f \in K$ liegt bezüglich einer beliebigen Basis die Streckungsmatrix

$$\begin{pmatrix} f & 0 & 0 & \ldots & 0 \\ 0 & f & 0 & \ldots & 0 \\ 0 & 0 & f & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 & f \end{pmatrix}$$

vor, für beliebige Elemente $f \in L$ werden die Matrizen ziemlich kompliziert, was man teilweise durch Wahl einer geeigneten Basis korrigieren kann. Insbesondere sind Konzepte relevant, die nicht von der Wahl einer Basis abhängen.

Beispiel 8.1. Es sei $F = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 \in K[X]$ ein irreduzibles Polynom über einem Körper K und

$$K \subseteq K[X]/\left(X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0\right) =: L$$

die zugehörige endliche Körpererweiterung. Nach Proposition 7.9 bilden die Potenzen x^i, $0 \leq i \leq n-1$, (wobei x die Restklasse von X bezeichnet) eine K-Basis von L. Zu einem $g \in L$ wird die Multiplikationsabbildung

$$\mu_g \colon L \longrightarrow L, y \longmapsto gy,$$

bezüglich der gegebenen Basis durch die $(n \times n)$-Matrix beschrieben, deren Spalten aus den Koordinanten zu den Produkten $g \cdot x^i$, $0 \leq i \leq n-1$, bezüglich der Basis besteht. Wegen $x^0 = 1$ stehen in der ersten Spalte einfach die Koordinaten von g selbst. Zu x ist diese Matrix gleich

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix}$$

beschrieben. Zu einem beliebigen Element

$$g = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1} x^{n-1}$$

wird die Matrix schnell kompliziert, wir führen nur die ersten beiden Spalten an

$$\begin{pmatrix} b_0 & -a_0 b_{n-1} & \dots & * & * \\ b_1 & b_0 - a_1 b_{n-1} & \dots & * & * \\ b_2 & b_1 - a_2 b_{n-1} & \dots & * & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n-1} & b_{n-2} - a_{n-1} b_{n-1} & \dots & * & * \end{pmatrix}.$$

In der folgenden Aussage wird zu einem K-Vektorraum mit $\operatorname{End}_K(V)$ der (nichtkommutative) Ring bezeichnet, der aus allen K-linearen Abbildungen besteht und wobei die Multiplikations durch die Hintereinanderschaltung von Abbildungen gegeben ist.

LEMMA 8.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Abbildung*

$$L \longrightarrow \operatorname{End}_K(L),\ f \longmapsto \mu_f,$$

ein injektiver Ringhomomorphismus.

Beweis. Siehe Aufgabe 8.6. □

Über diese Konstruktion bzw. Zuordnung werden Norm und Spur von f erklärt.

BEMERKUNG 8.3. Zu einer linearen Abbildung

$$\varphi\colon V \longrightarrow V$$

eines endlichdimensionalen K-Vektorraumes V in sich wird die Determinante $\det(\varphi)$ und die Spur $S(\varphi)$ wie folgt berechnet. Man wählt eine K-Basis $v_1, \dots, v_n \in V$ und repräsentiert die lineare Abbildung bezüglich dieser Basis durch eine quadratische $n \times n$-Matrix

$$\begin{pmatrix} \lambda_{1,1} & \cdots & \lambda_{1,n} \\ \vdots & \ddots & \vdots \\ \lambda_{n,1} & \cdots & \lambda_{n,n} \end{pmatrix}$$

mit $\lambda_{ij} \in K$ und rechnet dann die Determinante aus. Es folgt aus dem Determinantenmultiplikationssatz, dass dies unabhängig von der Wahl der Basis ist. Die Spur ist durch

$$S(\varphi) = \lambda_{1,1} + \lambda_{2,2} + \cdots + \lambda_{n,n}$$

gegeben, und dies ist nach Aufgabe 8.17 ebenfalls unabhängig von der Wahl der Basis.

Definition 8.4. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Determinante der K-linearen Abbildung

$$\mu_f \colon L \longrightarrow L,\, y \longmapsto fy,$$

die *Norm* von f. Sie wird mit $N(f)$ bezeichnet.

Definition 8.5. Sei $K \subseteq L$ eine endliche Körpererweiterung. Zu einem Element $f \in L$ nennt man die Spur der K-linearen Abbildung

$$\varphi_f \colon L \longrightarrow L,\, y \longmapsto fy,$$

die *Spur* von f. Sie wird mit $S(f)$ bezeichnet.

Beispiel 8.6. Es sei $K \subseteq L = K[X]/(X^n - a)$ eine Körpererweiterung, die durch die Hinzunahme einer n-ten Wurzel aus einem Element $a \in K$ entstehe. Es sei x die Restklasse von X. Dann wird μ_x bezüglich der K-Basis $1, x, x^2, \ldots, x^{n-1}$ von L durch die Matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & a \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

beschrieben. Somit ist die Norm von x gleich $\pm a$ (das Vorzeichen hängt davon ab, ob n gerade oder ungerade ist) und die Spur ist 0.

Lemma 8.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann hat die Norm*

$$N \colon L \longrightarrow K,\, f \longmapsto N(f),$$

folgende Eigenschaften:

(1) *Es ist $N(fg) = N(f)N(g)$.*
(2) *Für $f \in K$ ist $N(f) = f^n$, wobei n den Grad der Körpererweiterung bezeichne.*
(3) *Es ist $N(f) = 0$ genau dann, wenn $f = 0$ ist.*

Beweis. (1) Dies folgt aus dem Determinantenmultiplikationssatz und Lemma 8.2.

(2) Zu einer beliebigen Basis von L wird die Multiplikation mit einen Element $f \in K$ durch die Diagonalmatrix beschrieben, bei der jeder Diagonaleintrag f ist. Die Determinante ist daher f^n nach Lemma 16.4 (Lineare Algebra (Osnabrück 2017-2018)).

(3) Die eine Richtung ist klar, sei also $f \neq 0$. Dann ist f eine Einheit in L und daher ist die Multiplikation mit f eine bijektive K-lineare Abbildung $L \to L$, und deren Determinante ist $\neq 0$ nach Satz 16.11 (Lineare Algebra (Osnabrück 2017-2018)).

□

LEMMA 8.8. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n. Dann hat die Spur*

$$S\colon L \longrightarrow K,\ f \longmapsto S(f),$$

folgende Eigenschaften:

(1) *Die Spur ist K-linear, also $S(f+g) = S(f)+S(g)$ und $S(\lambda f) = \lambda S(f)$ für $\lambda \in K$.*
(2) *Für $f \in K$ ist $S(f) = nf$.*

Beweis. Dies folgt aus den Definitionen. □

Norm und Spur sind Elemente aus K.

LEMMA 8.9. *Es sei $K \subseteq L$ eine endliche Körpererweiterung und $f \in L$ mit der zugehörigen K-linearen Abbildung*

$$\mu_f\colon L \longrightarrow L,\ x \longmapsto fx.$$

Dann stimmt das Minimalpolynom von f mit dem Minimalpolynom von μ_f überein.

Beweis. Dies folgt aus dem kommutativen Diagramm

$$\begin{array}{ccc} K[X] & \stackrel{X\mapsto f}{\longrightarrow} & L \\ & X \mapsto \mu_f \searrow & \downarrow \mu \\ & & \operatorname{End}(L) \end{array}$$

von Ringhomomorphismen, in dem horizontal die Einsetzungshomomorphismen stehen, und Lemma 8.2. □

Im Minimalpolynom zu $f \in L$ finden sich Norm und Spur in folgender Weise wieder.

SATZ 8.10. *Sei $K \subseteq L = K[f]$ eine einfache endliche Körpererweiterung vom Grad n. Dann hat das Minimalpolynom P von f die Gestalt*

$$P = X^n - S(f)X^{n-1} + \cdots + (-1)^n N(f).$$

Beweis. Das Minimalpolynom und das charakteristische Polynom der durch f definierten K-linearen Multiplikationsabbildung

$$\mu_f\colon L \longrightarrow L,\ y \longmapsto fy,$$

haben beide den Grad n. Nach dem Satz von Cayley-Hamilton annulliert das charakteristische Polynom die lineare Abbildung und ist somit ein Vielfaches des Minimalpolynoms, so dass sie übereinstimmen. Sei bezüglich einer Basis $v_1, \ldots, v_n$ von L diese lineare Abbildung μ_f durch die Matrix $(\lambda_{ij})_{ij}$ gegeben. Dann ist das charakteristische Polynom gleich

$$\chi_{\mu_f} = \det \begin{pmatrix} X-\lambda_{1,1} & \cdots & -\lambda_{1,n} \\ \vdots & \ddots & \vdots \\ -\lambda_{n,1} & \cdots & X-\lambda_{n,n} \end{pmatrix} = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Zum Koeffizienten a_{n-1} leisten (in der Leibniz-Formel zur Berechnung der Determinante) nur diejenigen Permutationen einen Beitrag, bei denen $(n-1)$-mal die Variable X vorkommt, und das ist nur bei der identischen Permutation (also der Diagonalen) der Fall. Multipliziert man die Diagonale distributiv aus, so ergibt sich $X^n - \sum_{i=1}^{n} \lambda_{i,i} X^{n-1} + \ldots$, so dass also $a_{n-1} = -S(f)$ gilt. Setzt man in der obigen Gleichung $X = 0$, so ergibt sich, dass a_0 die Determinante der negierten Matrix ist, woraus $a_0 = (-1)^n N(f)$ folgt. □

Weitere Beschreibungen des Minimalpolynoms und der Norm und der Spur finden sich in Korollar 13.9 und Korollar 13.10.

Diskriminante

Die Lösbarkeit einer quadratischen Gleichung $x^2 + px + q = 0$ über einem Körper K hängt im Wesentlichen davon ab, ob die „Diskriminante“ $p^2 - 4q$ eine Quadratwurzel in K besitzt. Für die Lösungen einer kubischen Gleichung $x^3 + px + q = 0$ spielt nach Satz 1.2 der Ausdruck $-4p^3 - 27q^2$ (bzw. das -3-fache davon) eine wichtige Rolle. Beide Terme fallen unter das allgemeine Konzept einer Diskriminante, das wir kurz vorstellen.

Definition 8.11. Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ Elemente in L. Dann wird die *Diskriminante* von $b_1, \ldots, b_n$ durch

$$\triangle(b_1, \ldots, b_n) = \det\left(S(b_i b_j)_{i,j}\right)$$

definiert.

Die Produkte $b_i b_j$, $1 \leq i, j \leq n$, sind dabei Elemente in L, von denen man jeweils die Spur nimmt, die in K liegt. Man erhält also eine quadratische $n \times n$-Matrix über K. Deren Determinante ist nach Definition die Diskriminante. Im folgenden werden wir vor allem an der Diskriminante von speziellen Basen interessiert sein.

Beispiel 8.12. Wir betrachten eine quadratische Gleichung $X^2 + pX + q = 0$ und (unter der Voraussetzung, dass das Polynom irreduzibel ist) die zugehörige quadratische Körpererweiterung $K \subseteq L = K[X]/(X^2 + pX + q)$. Wir bestimmen die Diskriminante dieser Erweiterung zur Basis $1, x$. Wir müssen also die Spuren der Elemente $1, x, x^2 = -px - q$ bestimmen. Die Matrizen dieser Elemente sind

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -q \\ 1 & -p \end{pmatrix} \text{ und } \begin{pmatrix} -q & pq \\ -p & p^2 - q \end{pmatrix}$$

und ihre Spuren sind 2, $-p$ und $p^2 - 2q$. Somit ist die Diskriminante gleich

$$\triangle(1, x) = \det \begin{pmatrix} 2 & -p \\ -p & p^2 - 2q \end{pmatrix} = 2\left(p^2 - 2q\right) - p^2 = p^2 - 4q.$$

Beispiel 8.13. Wir betrachten die kubische Gleichung

$$x^3 + px + q = 0$$

und (unter der Voraussetzung, dass das Polynom irreduzibel ist) die zugehörige kubische Körpererweiterung $K \subseteq L = K[X]/(X^3 + pX + q)$. Wir bestimmen die Diskriminante dieser Erweiterung zur Basis $1, x, x^2$. Die Matrix zu x ist $\begin{pmatrix} 0 & 0 & -q \\ 1 & 0 & -p \\ 0 & 1 & 0 \end{pmatrix}$, die Matrix zu x^2 ist $\begin{pmatrix} 0 & -q & 0 \\ 0 & -p & -q \\ 1 & 0 & -p \end{pmatrix}$, die Matrix zu $x^3 = -px - q$ ist $\begin{pmatrix} -q & 0 & pq \\ -p & -q & p^2 \\ 0 & -p & -q \end{pmatrix}$, die Matrix zu $x^4 = -px^2 - qx$ ist $\begin{pmatrix} 0 & pq & q^2 \\ -q & p^2 & 2pq \\ -p & -q & p^2 \end{pmatrix}$. Die Diskriminante ist daher die Determinante der Matrix

$$\begin{pmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{pmatrix},$$

also gleich

$$3\left(-4p^3 - 9q^2\right) - 2p(-4p^2) = -4p^3 - 27q^2.$$

Dies ist die Zahl D aus Satz 1.2.

Bei einem Basiswechsel verhält sich die Diskriminante wie folgt.

Lemma 8.14. *Sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und seien $b_1, \ldots, b_n$ und $c_1, \ldots, c_n$ zwei K-Basen von L. Der Basiswechsel werde durch $c = Tb$ mit der Übergangsmatrix $T = (t_{ij})_{ij}$ beschrieben. Dann gilt für die Diskriminanten die Beziehung*

$$\triangle(c_1, \ldots, c_n) = (\det(T))^2 \triangle(b_1, \ldots, b_n).$$

Beweis. Ausgeschrieben haben wir die Beziehungen $c_i = \sum_{j=1}^n t_{ij} b_j$. Damit gilt

$$c_i c_k = \left(\sum_{j=1}^n t_{ij} b_j\right)\left(\sum_{m=1}^n t_{km} b_m\right) = \sum_{j,m} t_{ij} t_{km} b_j b_m.$$

Wir schreiben $c_{ik} := S(c_i c_k)$ und $b_{jm} := S(b_j b_m)$. Wegen der K-Linearität der Spur gilt

$$c_{ik} = S(c_i c_k) = S\left(\sum_{j,m} t_{ij} t_{km} b_j b_m\right) = \sum_{j,m} t_{ij} t_{km} S(b_j b_m) = \sum_{j,m} t_{ij} t_{km} b_{jm}.$$

Wir schreiben diese Gleichung mit den Matrizen $C = (c_{ik})$, $B = (b_{jm})$ und $T = (t_{ij})$ als

$$C = T^{\text{transp}} B T$$

und die Behauptung folgt dann aus dem Determinantenmultiplikationssatz und Satz 17.5 (Lineare Algebra (Osnabrück 2017-2018)). □

Satz 8.15. *Sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine endliche Körpererweiterung vom Grad n und sei $b_1, \ldots, b_n$ eine K-Basis von L. Dann ist*

$$\triangle(b_1, \ldots, b_n) \neq 0.$$

Beweis. Siehe Aufgabe 8.22. □

Abbildungsverzeichnis