**Prof. Dr. H. Brenner** **Osnabrück SS 2011**

# Körper- und Galoistheorie

## Vorlesung 8

### Erzeugte Algebra und erzeugter Körper

Satz 8.1. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann ist die von $f$ erzeugte $K$-Algebra $K[f] \subseteq L$ ein Körper.*

*Beweis.* Nach Satz 7.11 liegt eine $K$-Algebra-Isomorphie $K[X]/(P) \cong K[f]$ vor, wobei $P$ das Minimalpolynom zu $f$ ist. Nach Lemma 7.12 ist $P$ irreduzibel, so dass wegen Korollar 7.7 der Restklassenring $K[f]$ ein Körper ist. □

Korollar 8.2. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann stimmen die von $f$ über $K$ erzeugte Unteralgebra und der von $f$ über $K$ erzeugte Unterkörper überein. Es gilt also $K[f] = K(f)$.*

*Beweis.* Die Inklusion $K[f] \subseteq K(f)$ gilt immer, und nach Vorraussetzung ist aufgrund von Satz 8.1 der Unterring $K[f]$ schon ein Körper. □

Bemerkung 8.3. Sei $K$ ein Körper, $P \in K[X]$ ein irreduzibles Polynom und $K \subseteq L = K[X]/(P)$ die zugehörige Körpererweiterung. Dann kann man zu $z = F(x)$, $z \neq 0$, (mit $F \in K[X]$, $x = \overline{X}$) auf folgende Art das Inverse $z^{-1}$ bestimmen. Es sind $P$ und $F$ teilerfremde Polynome in $K[X]$ und daher gibt es nach Satz 3.15 und Lemma 3.16 eine Darstellung der 1, die man mit Hilfe des euklidischen Algorithmus finden kann. Wenn $RF + SP = 1$ ist, so ist die Restklasse von $R$, also $\overline{R} = R(x)$, das Inverse zu $\overline{F} = z$.

### Charakterisierung von algebraischen Elementen

Satz 8.4. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein Element. Dann sind folgende Aussagen äquivalent.*

(1) *$f$ ist algebraisch über $K$.*
(2) *Es gibt ein normiertes Polynom $P \in K[X]$ mit $P(f) = 0$.*
(3) *Es besteht eine lineare Abhängigkeit zwischen den Potenzen*
$$f^0 = 1, f^1 = f, f^2, f^3, \ldots .$$
(4) *Die von $f$ über $K$ erzeugte $K$-Algebra $K[f]$ hat endliche $K$-Dimension.*
(5) *$f$ liegt in einer endlich-dimensionalen $K$-Algebra $M \subseteq L$.*

*Beweis.* (1) $\Rightarrow$ (2). Das ist trivial, da man ein von null verschiedenes Polynom stets normieren kann, indem man durch den Leitkoeffizienten durchdividiert. (2) $\Rightarrow$ (3). Nach (2) gibt es ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(f) = 0$. Sei

$$P = \sum_{i=0}^{n} c_i X^i \, .$$

Dann ist

$$P(f) = \sum_{i=0}^{n} c_i f^i = 0$$

eine lineare Abhängigkeit zwischen den Potenzen. (3) $\Rightarrow$ (1). Umgekehrt bedeutet die lineare Abhängigkeit, dass es Elemente $c_i$ gibt, die nicht alle null sind mit $\sum_{i=0}^{n} c_i f^i = 0$. Dies ist aber die Einsetzung $P(f)$ für das Polynom $P = \sum_{i=0}^{n} c_i X^i$, und dieses ist nicht das Nullpolynom. (2) $\Rightarrow$ (4). Sei $P = \sum_{i=0}^{n} c_i X^i$ ein normiertes Polynom mit $P(f) = 0$, also mit $c_n = 1$. Dann kann man umstellen

$$f^n = -\sum_{i=0}^{n-1} c_i f^i \, .$$

D.h. $f^n$ kann man durch kleinere Potenzen ausdrücken. Durch Multiplikation dieser Gleichung mit weiteren Potenzen von $f$ ergibt sich, dass man auch die höheren Potenzen durch die Potenzen $f^i$, $i \leq n-1$, ausdrücken kann. (4) $\Rightarrow$ (5). Das ist trivial. (5) $\Rightarrow$ (3). Wenn $f$ in einer endlich-dimensionalen Algebra $M \subseteq L$ liegt, so liegen darin auch alle Potenzen von $f$. Da es in einem endlich-dimensionalen Vektorraum keine unendliche Folge von linear unabhängigen Elementen geben kann, müssen diese Potenzen linear abhängig sein. $\square$

Mit dieser Charakterisierung können wir noch einen zweiten Beweis von Satz 8.1 geben, der unabhängig von der Restklassenbildung ist und der zugleich zeigt, wie man aus dem Minimalpolynom eines algebraischen Elementes das inverse Element beschreiben kann.

Nach Satz 8.4 ist $M = K[f]$ eine endlich-dimensionale $K$-Algebra. Wir müssen zeigen, dass $M$ ein Körper ist. Sei dazu $g \in M$ ein von null verschiedenes Element. Damit ist auch $K[g] \subseteq M = K[f]$, so dass $K[g]$ wieder eine endlich-dimensionale Algebra ist. Daher ist, wiederum nach Satz 8.4, das Element $g$ algebraisch über $K$ und es gibt ein Polynom $P \in K[X]$, $P \neq 0$, mit $P(g) = 0$. Wir ziehen aus diesem Polynom die höchste Potenz von $X$ heraus und schreiben

$$P = QX^k \, ,$$

wobei der konstante Term von $Q$ von null verschieden sei. Die Ersetzung von $X$ durch $g$ ergibt

$$0 \, = \, P(g) \, = \, Q(g)g^k .$$

Da $g \neq 0$ ist und sich alles im Körper $L$ abspielt, folgt $Q(g) = 0$. Wir können durch den konstanten Term von $Q$ dividieren und erhalten die Gleichung

$$1 + c_1 g + \ldots + c_d g^d = 0\,.$$

Umstellen ergibt

$$g(-c_1 g^0 - \ldots - c_d g^{d-1}) = 1\,.$$

Das heißt, dass das Inverse zu $g$ sich als Polynom in $g$ schreiben lässt und daher zu $K[g]$ und erst recht zu $K[f]$ gehört.

## Algebraischer Abschluss

Definition 8.5. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Menge

$$M = \{x \in L |\, x \text{ ist algebraisch über } K\}$$

den *algebraischen Abschluss* von $K$ in $L$.

Satz 8.6. *Sei $K \subseteq L$ eine Körpererweiterung und sei $M$ der algebraische Abschluss von $K$ in $L$. Dann ist $M$ ein Unterkörper von $L$.*

*Beweis.* Wir müssen zeigen, dass $M$ bzgl. der Addition, der Multiplikation, des Negativen und des Inversen abgeschlossen ist. Seien $x, y \in M$. Wir betrachten die von $x$ und $y$ erzeugte $K$-Unteralgebra $U = K[x, y]$, die aus allen $K$-Linearkombinationen der $x^i y^j$, $i, j \in \mathbb{N}$, besteht. Da sowohl $x$ als auch $y$ algebraisch sind, kann man gewisse Potenzen $x^n$ und $y^m$ durch kleinere Potenzen ersetzen. Daher kann man alle Linearkombinationen mit den Monomen $x^i y^j$, $i < n$, $j < m$, ausdrücken. D.h. alle Operationen spielen sich in dieser endlich-dimensionalen Unteralgebra ab. Daher sind Summe, Produkt und das Negative nach Satz 8.4 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 8.1 ein Körper von endlicher Dimension. Daher ist $z^{-1} \in K[z]$ selbst algebraisch. □

## Algebraische Zahlen

Die über den rationalen Zahlen $\mathbb{Q}$ algebraischen komplexen Zahlen erhalten einen speziellen Namen.

Definition 8.7. Eine komplexe Zahl $z$ heißt *algebraisch* oder *algebraische Zahl*, wenn sie algebraisch über den rationalen Zahlen $\mathbb{Q}$ ist. Andernfalls heißt sie *transzendent*.

Die Menge der algebraischen Zahlen wird mit $\mathbb{A}$ bezeichnet.

Ferdinand von Lindemann (1852-1939)

BEMERKUNG 8.8. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von null verschiedenes Polynom $P$ mit rationalen Koeffizienten gibt mit $P(z) = 0$. Durch Multiplikation mit einem Hauptnenner kann man für eine algebraische Zahl auch ein annullierendes Polynom mit ganzzahligen Koeffizienten finden (das allerdings nicht mehr normiert ist). Eine rationale Zahl $q$ ist trivialerweise algebraisch, da sie Nullstelle des linearen rationalen Polynoms $X - q$ ist. Weiterhin sind die reellen Zahlen $\sqrt{q}$ und $q^{1/n}$ für $q \in \mathbb{Q}$ algebraisch. Dagegen sind die Zahlen $e$ und $\pi$ nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von $\pi$ wurde beispielsweise von Lindemann 1882 gezeigt.

## Algebra-Automorphismen

Die folgenden Definitionen werden wir vor allem für eine Körpererweiterung $K \subseteq L$ anwenden.

DEFINITION 8.9. Es sei $K$ ein kommutativer Ring und $A$ eine kommutative $K$-Algebra. Ein bijektiver $K$-Algebra-Homomorphismus

$$\varphi : A \longrightarrow A$$

heißt *$K$-Algebra-Automorphismus.*

LEMMA 8.10. *Es sei $K$ ein kommutativer Ring und $A$ eine kommutative $K$-Algebra. Dann gelten folgende Aussagen.*

(1) *Die Identität ist ein $K$-Algebra-Automorphismus.*
(2) *Die Verknüpfung $\varphi \circ \psi$ von zwei $K$-Algebra-Automorphismen $\varphi$ und $\psi$ ist wieder ein Automorphismus.*
(3) *Die Umkehrabbildung $\varphi^{-1}$ zu einem $K$-Algebra-Automorphismus $\varphi$ ist wieder ein Automorphismus.*
(4) *Die Menge der $K$-Algebra-Automorphismen bilden mit der Hintereinanderschaltung als Verknüpfung eine Gruppe.*

*Beweis.* Siehe Aufgabe 8.5. □

Definition 8.11. Es sei $K$ ein kommutativer Ring und $A$ eine kommutative $K$-Algebra. Die Menge der $K$-Algebra-Automorphismen

$$\varphi : A \longrightarrow A$$

mit der Hintereinanderschaltung als Verknüpfung heißt *Automorphismengruppe* der Algebra. Sie wird mit $\mathrm{Aut}_K(A)$ bezeichnet.

Beispiel 8.12. Es sei $K$ ein Körper und $K[X_1, \ldots, X_n]$ der Polynomring über $K$ in $n$ Variablen. Es sei

$$\alpha : K^n \longrightarrow K^n$$

ein linearer Automorphismus, der durch eine invertierbare Matrix

$$\alpha = (a_{ij})_{1 \leq i,j \leq n}$$

gegeben ist. Wir definieren dazu direkt einen $K$-Algebra-Automorphismus, nämlich den durch

$$X_i \longmapsto a_{i1}X_1 + \ldots + a_{in}X_n$$

definierten Einsetzungshomomorphismus (in mehreren Variablen), den wir mit $\varphi_\alpha$ bezeichnen. Dabei handelt es sich in der Tat um einen Algebra-Automorphismus: Der inverse lineare Automorphismus $\alpha^{-1}$ definiert in der gleichen Weise einen Algebra-Homomorphismus $\varphi_{\alpha^{-1}}$, und es gilt $\varphi_{\alpha^{-1}} \circ \varphi_\alpha = \mathrm{id}$, da diese Hintereinanderschaltung jede Variable auf sich selbst abbildet.

Bei einem Polynomring in einer Variablen über einem Körper $K$ ist jeder $K$-Automorphismus ein linearer Automorphismus, also durch die Zuordnung $X \mapsto aX + b$ mit $a \neq 0$ gegeben. Dies ist in mehreren Variablen nicht der Fall, in der Tat ist schon die Automorphismengruppe von $K[X, Y]$ nicht vollständig verstanden. Ein wichtiges offenes Problem ist hierbei das Jacobiproblem.

## Die Galoisgruppe einer Körpererweiterung

Definition 8.13. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Automorphismengruppe

$$\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$$

die *Galoisgruppe* der Körpererweiterung.

Lemma 8.14. *Sei $K \subseteq L$ eine Körpererweiterung und es sei $x_i \in L$, $i \in I$, ein Erzeugendensystem (als Körper) von $L$ über $K$. Es sei $\varphi \in \mathrm{Gal}(L|K)$ mit $\varphi(x_i) = x_i$ für alle $i \in I$. Dann ist $\varphi = \mathrm{id}$.*

*Beweis.* Wir zeigen, dass die Teilmenge

$$M = \{x \in L | \, \varphi(x) = x\}$$

gleich $L$ ist. Sei $E = \{x_i | \, i \in I\}$ das Erzeugendensystem und sei $P(x_1, \ldots, x_n)$ ein $K$-Polynom in einer endlichen Teilmenge $\{x_1, \ldots, x_n\} \subseteq E$. Dann ist

$$\varphi(P(x_1, \ldots, x_n)) \; = \; P(\varphi(x_1), \ldots, \varphi(x_n)) \; = \; P(x_1, \ldots, x_n),$$

da ja $\varphi$ ein $K$-Algebra-Automorphismus ist, und somit gehört $P \in M$. Das bedeutet, dass die von $E$ über $K$ erzeugte Algebra zu $M$ gehört. Da $L$ der von $E$ erzeugte Körper ist, gibt es für $x \in L$, $x \neq 0$, eine Darstellung $x = y/z$ mit $y, z \in M$. Daher ist auch $x \in M$. □

Es ist eine grundlegende Frage, welche Eigenschaften eines Elementes $x \in L$ unter einem $K$-Algebra-Automorphismus erhalten bleiben und welche nicht.

LEMMA 8.15. *Sei $K \subseteq L$ eine Körpererweiterung, $x \in L$, $F \in K[X]$ ein Polynom mit $F(x) = 0$ und sei $\varphi \in \mathrm{Gal}\,(L|K)$. Dann ist auch $F(\varphi(x)) = 0$.*

*Beweis.* Sei $F = a_0 + a_1 X + \ldots + a_n X^n$ mit $a_i \in K$. Dann ist

$$F(\varphi(x)) \; = \; a_0 + a_1\varphi(x) + \ldots + a_n(\varphi(x))^n \; = \; \varphi(F(x)) \; = \; \varphi(0) \; = \; 0.$$

□

SATZ 8.16. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Galoisgruppe $\mathrm{Gal}\,(L|K)$ endlich.*

*Beweis.* Die Körpererweiterung besitzt ein endliches $K$-Algebra-Erzeugendensystem, also $L = K[x_1, \ldots, x_n]$. Nach Lemma 8.14 ist ein $K$-Algebra-Automorphismus

$$\varphi : L \longrightarrow L$$

durch $\varphi(x_i)$, $i = 1, \ldots, n$, eindeutig festgelegt. Da jedes $x_i$ nach Satz 8.4 algebraisch ist, gibt es Polynome $F_i \neq 0$ mit $F_i(x_i) = 0$. Nach Lemma 8.15 ist auch $F_i(\varphi(x_i)) = 0$. Die Polynome $F_i$ besitzen aber nach Korollar Anhang 1.5 jeweils nur endlich viele Nullstellen, so dass nur endlich viele Werte für $\varphi(x_i)$ in Frage kommen. □

# Abbildungsverzeichnis