

Körper- und Galoistheorie

Vorlesung 10

Erzeugte Algebra und erzeugter Körper

SATZ 10.1. *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 -Algebraisomorphie $K[X]/(P) \cong K[f]$ vor, wobei P das Minimalpolynom zu f ist. Nach Lemma 7.12 (2) ist P irreduzibel, so dass wegen Korollar 7.7 der Restklassenring $K[f]$ ein Körper ist. \square

KOROLLAR 10.2. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann stimmen die von f über K erzeugte Unter algebra 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 Voraussetzung ist der Unterring $K[f]$ aufgrund von Satz 10.1 schon ein Körper. \square

BEMERKUNG 10.3. 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 $F \in K[X]$, $x = \bar{X}$) 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 $\bar{R} = R(x)$, das Inverse zu $\bar{F} = z$.

Charakterisierung von algebraischen Elementen

SATZ 10.4. *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

$$f^0 = 1, f^1 = f, f^2, f^3, \dots$$

- (4) Die von f über K erzeugte K -Algebra $K[f]$ hat endliche K -Dimension.

(5) f liegt in einer endlichdimensionalen K -Algebra $M \subseteq L$.

Beweis. (1) \Rightarrow (2). Das ist trivial, da man ein von 0 verschiedenes Polynom stets normieren kann, indem man durch den Leitkoeffizienten dividiert. (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 0 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 endlichdimensionalen Algebra $M \subseteq L$ liegt, so liegen darin auch alle Potenzen von f . Da es in einem endlichdimensionalen 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 10.1 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 10.4 ist $M = K[f]$ eine endlichdimensionale K -Algebra. Wir müssen zeigen, dass M ein Körper ist. Sei dazu $g \in M$ ein von 0 verschiedenes Element. Damit ist auch $K[g] \subseteq M = K[f]$, so dass $K[g]$ wieder eine endlichdimensionale Algebra ist. Daher ist, wiederum nach Satz 10.4, 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 0 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

$$1 + c_1g + \cdots + c_dg^d = 0.$$

Umstellen ergibt

$$g(-c_1g^0 - \cdots - c_dg^{d-1}) = 1.$$

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

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

den *algebraischen Abschluss* von K in L .

SATZ 10.6. 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 bezüglich 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 nach Satz 10.4 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 endlichdimensionalen Unteralgebra ab. Daher sind Summe, Produkt und das Negative nach Satz 10.4 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 10.1 ein Körper von endlicher Dimension. Daher ist $z^{-1} \in K[z]$ selbst algebraisch. \square

Algebraische Zahlen

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

DEFINITION 10.7. 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 10.8. Eine komplexe Zahl $z \in \mathbb{C}$ ist genau dann algebraisch, wenn es ein von 0 verschiedenes Polynom P mit rationalen Koeffizienten und mit $P(z) = 0$ gibt. 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 π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Ferdinand von Lindemann 1882 gezeigt.

Algebraautomorphismen

Wir beginnen nun mit der eigentlichen Galoistheorie. Die folgenden Definitionen werden wir vor allem für eine Körpererweiterung $K \subseteq L$ anwenden.

DEFINITION 10.9. Es sei K ein kommutativer Ring und A eine kommutative K -Algebra. Ein bijektiver K -Algebrahomomorphismus

$$\varphi: A \longrightarrow A$$

heißt K -Algebraautomorphismus.

LEMMA 10.10. *Es sei K ein kommutativer Ring und A eine kommutative K -Algebra. Dann gelten folgende Aussagen.*

- (1) *Die Identität ist ein K -Algebraautomorphismus.*
- (2) *Die Verknüpfung $\varphi \circ \psi$ von zwei K -Algebraautomorphismen φ und ψ ist wieder ein Automorphismus.*
- (3) *Die Umkehrabbildung φ^{-1} zu einem K -Algebraautomorphismus φ ist wieder ein Automorphismus.*

- (4) Die Menge der K -Algebraautomorphismen bilden mit der Hintereinanderschaltung als Verknüpfung eine Gruppe.

Beweis. Siehe Aufgabe 10.6. □

DEFINITION 10.11. 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 $\text{Aut}_K(A)$ bezeichnet.

BEISPIEL 10.12. Es sei K ein Körper und $K[X_1, \dots, X_n]$ 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 -Algebraautomorphismus, nämlich den durch

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

definierten Einsetzungshomomorphismus (in mehreren Variablen), den wir mit φ_α bezeichnen. Dabei handelt es sich in der Tat um einen Algebraautomorphismus: Der inverse lineare Automorphismus α^{-1} definiert in der gleichen Weise einen Algebrahomomorphismus $\varphi_{\alpha^{-1}}$, und es gilt $\varphi_{\alpha^{-1}} \circ \varphi_\alpha = \text{Id}$, 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 $X \mapsto aX$ 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 10.13. Sei $K \subseteq L$ eine Körpererweiterung. Dann nennt man die Automorphismengruppe

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

die *Galoisgruppe* der Körpererweiterung.

LEMMA 10.14. 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 $\varphi \in \text{Gal}(L|K)$ mit $\varphi(x_i) = x_i$ für alle $i \in I$. Dann ist $\varphi = \text{Id}$.

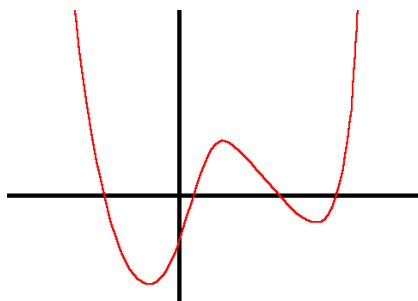
Beweis. Wir zeigen, dass die Teilmenge

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

gleich L ist. Da φ ein K -Algebrahomomorphismus ist, ist $K \subseteq M$ und nach Voraussetzung ist $x_i \in M$. Mit $x, y \in M$ ist wegen $\varphi(x+y) = \varphi(x) + \varphi(y) = x + y$ (und entsprechend für die Multiplikation) auch $x + y, xy \in M$. Ferner ist mit $x \in M, x \neq 0$, wegen

$$\varphi(x^{-1}) = (\varphi(x))^{-1} = x^{-1}$$

auch $x^{-1} \in M$. Also ist M ein Unterkörper, der K und das Körpererzeugendensystem x_i umfasst und daher ist $M = L$. \square



Unter einem K -Körperautomorphismus φ muss ein Element $x \in L$, das Nullstelle eines Polynoms F aus $K[X]$ ist, auf eine Nullstelle dieses Polynoms abgebildet werden. Das schränkt die Möglichkeiten wesentlich ein.

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

LEMMA 10.15. *Sei $K \subseteq L$ eine Körpererweiterung, $x \in L$, $F \in K[X]$ ein Polynom mit $F(x) = 0$ und sei $\varphi \in \text{Gal}(L|K)$. Dann ist auch $F(\varphi(x)) = 0$.*

Beweis. Sei $F = a_0 + a_1X + \dots + a_nX^n$ mit $a_i \in K$. Dann ist

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

\square

SATZ 10.16. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist die Galoisgruppe $\text{Gal}(L|K)$ endlich.*

Beweis. Die Körpererweiterung besitzt ein endliches K -Algebraerzeugendensystem, also $L = K[x_1, \dots, x_n]$. Nach Lemma 10.14 ist ein K -Algebraautomorphismus

$$\varphi: L \longrightarrow L$$

durch $\varphi(x_i), i = 1, \dots, n$, eindeutig festgelegt. Da jedes x_i nach Satz 10.4 algebraisch ist, gibt es Polynome

$$F_i \neq 0$$

mit $F_i(x_i) = 0$. Nach Lemma 10.15 ist auch $F_i(\varphi(x_i)) = 0$. Die Polynome F_i besitzen aber nach Korollar 19.9 (Lineare Algebra (Osnabrück 2017-2018)) jeweils nur endlich viele Nullstellen, so dass nur endlich viele Werte für $\varphi(x_i)$ in Frage kommen. \square

Abbildungsverzeichnis

- Quelle = Carl Louis Ferdinand von Lindemann.jpg , Autor = unbekannt
(hochgeladen von Benutzer JdH auf Commons), Lizenz = PD 4
- Quelle = Courbe quatrième degré 08.GIF , Autor = Benutzer Lydienoria
auf Commons, Lizenz = CC-by-sa 3.0 6
- Erläuterung: Die in diesem Text verwendeten Bilder stammen aus
Commons (also von <http://commons.wikimedia.org>) und haben eine
Lizenz, die die Verwendung hier erlaubt. Die Bilder werden mit ihren
Dateinamen auf Commons angeführt zusammen mit ihrem Autor
bzw. Hochlader und der Lizenz. 9
- Lizenzklärung: Diese Seite wurde von Holger Brenner alias
Bocardodarapti auf der deutschsprachigen Wikiversity erstellt und
unter die Lizenz CC-by-sa 3.0 gestellt. 9