Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 23

Weiteres zum Minimalpolynom

Satz 23.1. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Es sei P das Minimalpolynom von f. Dann gibt es eine kanonische K-Algebra-Isomorphie*

$$K[X]/(P) \longrightarrow K[f],\, X \longmapsto f.$$

Beweis. Die Einsetzung $X \mapsto f$ ergibt nach Satz 13.7 den kanonischen K-Algebra-Homomorphismus

$$K[X] \longrightarrow L,\, X \longmapsto f.$$

Das Bild davon ist genau $K[f]$, so dass ein surjektiver K-Algebra-Homomorphismus

$$K[X] \longrightarrow K[f]$$

vorliegt. Daher gibt es nach Korollar 14.5 eine Isomorphie zwischen $K[f]$ und dem Restklassenring von $K[X]$ modulo dem Kern der Abbildung. Der Kern ist aber nach Lemma 22.11 das vom Minimalpolynom erzeugte Hauptideal. □

Lemma 23.2. *Sei $K \subseteq L$ eine Körpererweiterung und sei $f \in L$ ein algebraisches Element. Dann gelten folgende Aussagen.*

(1) *Das Minimalpolynom P von f über K ist irreduzibel.*
(2) *Wenn $Q \in K[X]$ ein normiertes, irreduzibles Polynom mit $Q(f) = 0$ ist, so handelt es sich um das Minimalpolynom.*

Beweis. (1) Es sei $P = P_1P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(f) = P_1(f)P_2(f).$$

Da L ein Körper ist, muss ein Faktor 0 sein, sagen wir $P_1(f) = 0$. Da aber P unter allen Polynomen $\neq 0$, die f annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant ($\neq 0$), also eine Einheit sein.

(2) Wegen $Q(f) = 0$ ist Q aufgrund von Lemma 22.11 ein Vielfaches des Minimalpolynoms P, sagen wir $Q = GP$. Da Q nach Voraussetzung irreduzibel ist, und da P zumindest den Grad 1 besitzt, muss G konstant sein. Da schließlich sowohl P als auch Q normiert sind, ist $P = Q$.

□

Algebraische Körpererweiterung

Satz 23.3. *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. □

Satz 23.4. *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 23.1 liegt eine K-Algebra-Isomorphie $K[X]/(P) \cong K[f]$ vor, wobei P das Minimalpolynom zu f ist. Nach Lemma 23.2 (2) ist P irreduzibel, so dass wegen Satz 15.1 der Restklassenring $K[f]$ ein Körper ist. □

KOROLLAR 23.5. *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 23.4 der Unterring $K[f]$ schon ein Körper. □

BEMERKUNG 23.6. 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 8.3 und Korollar 8.6 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 $\overline{F} = z$.

Algebraischer Abschluss

DEFINITION 23.7. 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 23.8. *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 23.3 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 23.3 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 23.4 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 23.9. 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 23.10. 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 Lindemann 1882 gezeigt.

Abbildungsverzeichnis