Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 22

Algebraische Körpererweiterung

Satz 22.1. *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. □

Satz 22.2. *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 22.1 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 22.1, 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. □

Korollar 22.3. *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 22.1 der Unterring $K[f]$ schon ein Körper. □

Bemerkung 22.4. 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 16.11 und Satz 17.12 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 22.5. 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 22.6. *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 22.1 wieder algebraisch. Für das Inverse sei $z \neq 0$ algebraisch. Dann ist $K[z]$ nach Satz 22.1 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 22.7. 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 22.8. 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 π nicht algebraisch. Diese Aussagen sind keineswegs selbstverständlich, die Transzendenz von π wurde beispielsweise von Lindemann 1882 gezeigt.

Quadratische Körpererweiterungen

Die aller einfachste Körpererweiterung ist die *identische Körpererweiterung* $K = K$, die den Grad 1 besitzt. Die nächst einfachsten sind die vom Grad zwei.

Definition 22.9. Eine endliche Körpererweiterung $K \subset L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Lemma 22.10. *Es sei K ein Körper mit einer Charakteristik $\neq 2$ und es sei $K \subset L$ eine quadratische Körpererweiterung. Dann gibt es ein $x \in L$, $x \notin K$ und $x^2 \in K$.*

Beweis. Nach Voraussetzung ist L ein zweidimensionaler Vektorraum über K, und darin ist $K = K1$ ein eindimensionaler Untervektorraum. Nach dem Basisergänzungssatz gibt es ein Element $y \in L$ derart, dass 1 und y eine K-Basis von L bilden. Wir können schreiben

$$y^2 = a + by$$

bzw. (da 2 eine Einheit ist)

$$0 \;=\; y^2 - by - a \;=\; (y - \frac{b}{2})^2 - \frac{b^2}{4} - a.$$

Mit $x = y - \frac{b}{2}$ gilt also $x^2 = \frac{b^2}{4} + a \in K$ und 1 und x bilden ebenfalls eine K-Basis von L. $\square$

Satz 22.11. *Sei $\mathbb{R} \subseteq K$ eine endliche Körpererweiterung der reellen Zahlen. Dann ist K isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$.*

Beweis. Das reelle normierte Polynom $P \in \mathbb{R}[X]$ zerfällt über den komplexen Zahlen $\mathbb{C}$ nach dem Fundamentalsatz der Algebra in Linearfaktoren, d.h. es ist

$$P = \prod_j (X - \lambda_j)$$

mit $\lambda_j = a_j + b_j i \in \mathbb{C}$. Das P reelle Koeffizienten hat, stimmt es mit seinem komplex-konjugierten überein, d.h. es ist insgesamt

$$\prod_j (X - \lambda_j) \,=\, P \,=\, \overline{P} \,=\, \prod_j (X - \overline{\lambda_j}).$$

Wegen der Eindeutigkeit der Primfaktorzerlegung gibt es zu jedem j ein k mit $\overline{\lambda_j} = \lambda_k$. D.h. entweder, dass $\lambda_j \in \mathbb{R}$ ist, und dann liegt ein reeller Linearfaktor vor, oder aber $j \neq k$ und dann ist

$$(X - \lambda_j)(X - \overline{\lambda_j}) \,=\, (X - a_j - b_j i))(X - a_j + b_j i) \,=\, X^2 - 2a_j X + a_j^2 + b_j^2$$

ein reelles Polynom. In der reellen Primfaktorzerlegung von P kommen also nur lineare und quadratische Faktoren vor, und insbesondere haben im Reellen alle irreduziblen Polynome den Grad eins oder zwei.

Sei nun $\mathbb{R} \subseteq L$ eine endliche Körpererweiterung. Sei $\mathbb{R} \subset L$ und $x \in L$, $x \notin \mathbb{R}$. Dann ist x algebraisch über $\mathbb{R}$ und Satz 21.12 ist $\mathbb{R}[x] \cong \mathbb{R}[X]/(P)$ mit einem irreduziblen Polynom P (dem Minimalpolynom zu x). Das Polynom P besitzt in $\mathbb{C}$ Nullstellen, so dass es einen $\mathbb{R}$-Algebra-Homomorphismus $\mathbb{R}[X]/(P) \to \mathbb{C}$ gibt. Da beides reell-zweidimensionale Körper sind, muss eine Isomorphie vorliegen. Wir erhalten also eine endliche Körpererweiterung $\mathbb{C} \subseteq L$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, muss $\mathbb{C} = L$ sein. $\square$

Das Irreduzibilitätskriterium von Eisenstein

Lemma 22.12. *(Eisenstein Irreduzibilitätskriterium)*

Sei R ein Integritätsbereich und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann besitzt F keine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$.

Beweis. Sei angenommen, dass es eine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$ gäbe, und sei $G = \sum_{i=0}^{k} a_i X^i$ und $H = \sum_{j=0}^{m} b_j X^j$. Dann ist $c_0 = a_0 b_0$ und dies ist ein Vielfaches von p, aber nicht von p^2. Da p prim ist, teilt es einen der Faktoren, sagen wir a_0, aber nicht den anderen. Es ist nicht jeder Koeffizient von G ein Vielfaches von p, da sonst G und damit auch F ein Vielfaches von p wäre, was aber aufgrund der Bedingung an den Leitkoeffizienten ausgeschlossen ist. Es sei r der kleinste Index derart, dass a_r kein Vielfaches von p ist. Es ist $r \leq \operatorname{grad}(G) < \operatorname{grad}(F)$, da H nicht konstant ist. Wir betrachten den Koeffizienten c_r, für den

$$c_r = a_0 b_r + a_1 b_{r-1} + \ldots + a_{r-1} b_1 + a_r b_0$$

gilt. Hierbei sind c_r und alle Summanden $a_i b_{r-i}$, $i = 0, \ldots, r-1$, Vielfache von p. Daher muss auch der letzte Summand $a_r b_0$ ein Vielfaches von p sein. Dies ist aber ein Widerspruch, da $p \nmid a_r$ und $p \nmid b_0$. $\square$

Satz 22.13. *Sei R ein faktorieller Bereich mit Quotientenkörper $K = Q(R)$ und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, aber alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann ist F irreduzibel in $K[X]$.*

Beweis. Dies folgt aus Lemma 22.12 und Lemma 20.13. □

Korollar 22.14. *Sei p eine Primzahl und $n \geq 1$. Dann sind die Polynome $X^n - p$ irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Dies folgt direkt aus Satz 22.13 angewendet mit der Primzahl p. □

Korollar 22.15. *Es gibt endliche Körpererweiterungen von $\mathbb{Q}$ von beliebigem Grad.*

Beweis. Aufgrund von Satz 22.13 sind zu einer Primzahl p die Polynome $X^n - p \in \mathbb{Q}[X]$ irreduzibel und nach Satz 17.15 auch prim. Aufgrund von Satz 18.5 sind dann die Restklassenringe $\mathbb{Q}[X]/(X^n - p)$ Körper. Diese haben den Grad n nach Proposition 21.3. □

Abbildungsverzeichnis