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

Körper- und Galoistheorie

Vorlesung 2

Körpererweiterungen

In der letzten Vorlesung haben wir gesehen, dass es sinnvoll sein kann, das Studium der Nullstellen eines Polynoms $F \in \mathbb{Q}[X]$ nicht in $\mathbb{C}$, sondern in einem kleineren Körper, der $\mathbb{Q}$ umfasst, durchzuführen. Wir stellen dazu die nötige Terminologie zusammen.

Definition 2.1. Es sei K ein Körper. Ein Unterring $M \subseteq K$, der zugleich ein Körper ist, heißt *Unterkörper* von K.

Wenn ein Unterring $R \subseteq K$ in einem Körper vorliegt, so muss man nur noch schauen, ob R mit jedem von null verschiedenen Element x auch das Inverse x^{-1} (das in K existiert) enthält. Bei einem Unterring $R \subseteq S$, wobei R ein Körper ist, aber S nicht, spricht man nicht von einem Unterkörper. Die Situation, wo ein Körper in einem anderen Körper liegt, wird als Körpererweiterung bezeichnet.

Definition 2.2. Sei L ein Körper und $K \subseteq L$ ein Unterkörper von L. Dann heißt L ein *Erweiterungskörper* (oder *Oberkörper*) von K und die Inklusion $K \subseteq L$ heißt eine *Körpererweiterung*.

Für eine Körpererweiterung gilt stets folgende wichtige Beobachtung.

Lemma 2.3. *Sei $K \subseteq L$ eine Körpererweiterung. Dann ist L in natürlicher Weise ein K-Vektorraum.*

Beweis. Die Skalarmultiplikation

$$K \times L \longrightarrow L,\ (\lambda, x) \longmapsto \lambda x,$$

wird einfach durch die Multiplikation in L gegeben. Die Vektorraumaxiome folgen dann direkt aus den Ringaxiomen. □

Definition 2.4. Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlich-dimensionaler Vektorraum über K ist.

Definition 2.5. Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.

Der Grad einer endlichen Körpererweiterung $K \subseteq L$ wird mit

$$\operatorname{grad}_K L$$

bezeichnet. Dass man hier von Grad spricht und nicht einfach von Dimension hat seinen Grund darin, dass dieser Grad mit dem Grad von gewissen Polynomen zusammenhängt, worauf wir ausführlich zu sprechen kommen werden. Da bei einer Körpererweiterung $K \subseteq L$ sofort eine K-Vektorraumstruktur auf L zur Verfügung steht, ist es naheliegend, für das Studium der Körpererweiterungen die lineare Algebra einzusetzen. Dies ist besonders bei endlichen Körpererweiterungen ein schlagkräftiges Mittel. Durch diesen Apparat wird unter Anderem die additive Struktur auf L einfach beschreibbar, und man kann sich ganz auf die Multiplikation konzentrieren. Aber auch für diese ist die Vektorraumstruktur reich an Konsequenzen. Um ein typisches Beispiel für die lineare Argumentationsweise zu geben, betrachten wir eine endliche Körpererweiterung $K \subseteq L$ und ein beliebiges Element $x \in L$. Die Potenzen von x, also

$$x^0 = 1, x^1 = x, x^2, x^3, \ldots$$

bilden eine unendliche Familie (auch wenn es unter den Potenzen Wiederholungen geben kann). Da diese Potenzen alle zu L gehören und L ein endlichdimensionaler K-Vektorraum ist, kann diese unendliche Familie nicht linear unabhängig sein, sondern es muss eine Beziehung der Form

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0$$

geben, bei der nicht alle Koeffizienten $a_i \in K$ gleich 0 sind. Diese Beobachtung führt zu den Begriffen *algebraisches Element* und *Minimalpolynom*.

Die einzige Körpererweiterung vom Grad 1 ist die Identität $K \subseteq K$. Die Körpererweiterungen vom Grad zwei sind aber schon eine umfangreiche Beispielklasse und bekommen einen eigenen Namen. Zu ihnen gehören die beiden letzten Beispiele der ersten Vorlesung.

Definition 2.6. Eine endliche Körpererweiterung $K \subset L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Lemma 2.7. *Es sei K ein Körper mit einer Charakteristik $\neq 2$[1] und es sei $K \subset L$ eine quadratische Körpererweiterung. Dann gibt es ein $x \in L$ mit $x^2 \in K$.*

Beweis. Siehe Aufgabe 2.4. □

Die Gradformel

Häufig studiert man Körpererweiterungen $K \subseteq M$ dadurch, dass man Zwischenkörper L, $K \subseteq L \subseteq M$, betrachtet, und die beiden einzelnen (häufig einfacheren) Körpererweiterungen $K \subseteq L$ und $L \subseteq M$ untersucht. Man spricht von einem *Körperturm* oder einer *Körperkette*. In dieser Situation gilt die folgende wichtige *Gradformel*.

[1] Diese Bedingung bedeutet, dass $0 \neq 2 = 1 + 1$ ist. Wir werden die Charakteristik eines Körpers bald einführen.

SATZ 2.8. *Seien $K \subseteq L$ und $L \subseteq M$ endliche Körperweiterungen. Dann ist auch $K \subseteq M$ eine endliche Körpererweiterung und es gilt*

$$\operatorname{grad}_K M = \operatorname{grad}_K L \cdot \operatorname{grad}_L M\,.$$

Beweis. Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j, 1 \leq i \leq n, 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j}x_1 + \ldots + a_{nj}x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= (a_{11}x_1 + \ldots + a_{n1}x_n)y_1 + \ldots + (a_{1m}x_1 + \ldots + a_{nm}x_n)y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören, folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist, folgt, dass $c_{ij} = 0$ ist für alle i, j. □

Reine Gleichungen

Die Lösungsformel von Cardano für ein kubisches Polynom zeigt, dass man die Nullstellen eines solchen Polynoms durch arithmetisch verschachtelte reine (zweite und dritte) Wurzeln ausdrücken kann. Solche reinen Wurzeln sind Nullstellen von sogenannten reinen Polynomen, also von Polynomen der Form

$$X^n - a\,,$$

wobei $a \in K$ ist und die Nullstelle in einem geeigneten Erweiterungskörper L von K liegen soll. Verglichen mit beliebigen Polynomen gelten solche reinen Polynome als vergleichsweise einfach, insbesondere wenn man an ein reelles positives a und seine reelle positive Wurzel $\sqrt[n]{a}$ denkt (und bei geradem n noch die zweite reelle Lösung $-\sqrt[n]{a}$ berücksichtigt). Allerdings zerfällt das Polynom $X^n - a$ über $\mathbb{C}$ in n Linearfaktoren, so dass bei $n \geq 3$ im Reellen

nicht alle komplexen Lösungen sichtbar sind. Ein extremes Beispiel ist dabei das Polynom

$$X^n - 1$$

bzw. die Gleichung $X^n = 1$. Dies führt zu den sogenannten Einheitswurzeln.

Einheitswurzeln

DEFINITION 2.9. Es sei K ein Körper und $n \in \mathbb{N}_+$. Dann heißen die Nullstellen des Polynoms

$$X^n - 1$$

in K die n-ten *Einheitswurzeln* in K.

Die 1 ist für jedes n eine n-te Einheitswurzel, und die -1 ist für jedes gerade n eine n-te Einheitswurzel. Es gibt maximal n n-te Einheitswurzel, da das Polynom $X^n - 1$ maximal n Nullstellen besitzt. Die Einheitswurzeln bilden eine endliche Untergruppe (mit $x^n = 1$ und $y^n = 1$ ist auch $(xy)^n = 1$, usw.) der Einheitengruppe $K^\times = K \setminus \{0\}$ des Körpers.

Im Reellen gibt es nur die Einheitswurzeln 1 oder 1 und -1, je nachdem, ob n gerade oder ungerade ist. Die komplexen Einheitswurzeln lassen sich einfach beschreiben und besitzen eine einfache geometrische Interpretation.

LEMMA 2.10. *Sei $n \in \mathbb{N}_+$. Die Nullstellen des Polynoms $X^n - 1$ über $\mathbb{C}$ sind*

$$e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, k = 0, 1, \ldots, n-1.$$

In $\mathbb{C}[X]$ gilt die Faktorisierung

$$X^n - 1 = (X-1)(X - e^{2\pi i/n})\cdots(X - e^{2\pi i(n-1)/n})$$

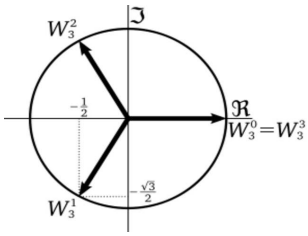
Beweis. Der Beweis verwendet einige Grundtatsachen über die *komplexe Exponentialfunktion*. Es ist

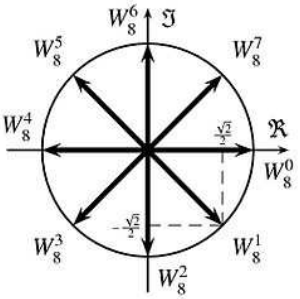
$$(e^{2\pi ik/n})^n = e^{2\pi ik} = (e^{2\pi i})^k = 1^k = 1.$$

Die angegebenen komplexen Zahlen sind also wirklich Nullstellen des Polynoms $X^n - 1$. Diese Nullstellen sind alle untereinander verschieden, da aus

$$e^{2\pi ik/n} = e^{2\pi i\ell/n}$$

mit $0 \le k \le \ell \le n-1$ sofort durch betrachten des Quotienten $e^{2\pi i(\ell-k)/n} = 1$ folgt, und daraus $\ell - k = 0$. Es gibt also n explizit angegebene Nullstellen und daher müssen dies alle Nullstellen des Polynoms sein. Die explizite Beschreibung in Koordinaten folgt aus der eulerschen Formel. □





KOROLLAR 2.11. *Es sei K ein Körper. Dann gilt in $K[X]$ die Beziehung*

$$X^n - 1 = (X-1) \cdot (X^{n-1} + X^{n-2} + \ldots + X + 1).$$

Für jede n-te Einheitswurzel $\zeta \neq 1$ gilt

$$\zeta^{n-1} + \zeta^{n-2} + \ldots + \zeta + 1 = 0$$

Beweis. Die erste Aussage ergibt sich durch Ausmultiplizieren der rechten Seite. Zum Beweis des Zusatzes sei eine n-te Einheitswurzel $\zeta \neq 1$ gegeben. Nach Definition ist $\zeta^n - 1 = 0$. Wegen $\zeta \neq 1$ muss also das rechte Polynom zu 0 werden, wenn man darin ζ einsetzt. □

Zu jedem $n \in \mathbb{N}$ gibt es einen kleinsten Unterkörper von $\mathbb{C}$, der alle n-ten Einheitswurzeln enthält, der sogenannte n-te *Kreisteilungskörper*. Wir werden bald sehen, dass der Kreisteilungskörper eine endliche Erweiterung von $\mathbb{Q}$ ist, und dass sein Grad maximal gleich $n-1$ ist. Genauere Gradberechnungen und weitere Strukturuntersuchungen dieser Körpererweiterungen werden im Laufe des Kurses noch folgen.

Mit den Einheitswurzeln lassen sich wiederum die Lösungen zu beliebigen reinen Gleichungen charakterisieren, insbesondere, wenn eine bekannt ist, wie das bei $X^n = a$ mit $a \in \mathbb{R}_+$ der Fall ist.

LEMMA 2.12. *Es sei K ein Körper, $a \in K$ und $n \in \mathbb{N}$. Dann gelten folgende Aussagen.*

(1) *Wenn $b_1, b_2 \in K$ zwei Lösungen der Gleichung $X^n = a$ sind und $b_2 \neq 0$, so ist ihr Quotient b_1/b_2 eine n-te Einheitswurzel.*
(2) *Wenn $b \in K$ eine Lösung der Gleichung $X^n = a$ und ζ eine n-te Einheitswurzel ist, so ist auch ζb eine Lösung der Gleichung $X^n = a$.*

Beweis. Siehe Aufgabe 2.9. □

Abbildungsverzeichnis