Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Vorlesung 15

Normale Körpererweiterungen

Ein irreduzibles Polynom $F \in K[X]$ hat in dem Erweiterungskörper

$$K \subseteq L := K[X]/(F)$$

eine Nullstelle, nämlich die Restklasse x von X und damit in $L[X]$ auch den Linearfaktor $X - x$. Es besteht aber kein Grund, warum das Polynom F über L in Linearfaktoren zerfallen sollte. Vielmehr handelt es sich um eine erweiterungstheoretische Besonderheit, wenn mit einer Nullstelle bereits schon alle Nullstellen vollzählig vorhanden sind.

Definition 15.1. Eine Körpererweiterung $K \subseteq L$ heißt *normal*, wenn es zu jedem $x \in L$ ein Polynom $F \in K[X]$, $F \neq 0$, mit $F(x) = 0$ gibt, das über L zerfällt.

Eine normale Körpererweiterung ist insbesondere algebraisch. Wir werden gleich noch dazu äquivalente Eigenschaften kennenlernen. Einfache Eigenschaften von normalen Erweiterungen werden im folgenden Lemma zusammengefasst.

Lemma 15.2. (1) *Die Identität ist eine normale Körpererweiterung.*
(2) *Jede quadratische Körpererweiterung ist normal.*
(3) *Wenn $K \subseteq L$ eine normale Körpererweiterung ist und $K \subseteq M \subseteq L$ ein Zwischenkörper, so ist auch $M \subseteq L$ normal.*
(4) *Eine Erweiterung von endlichen Körpern ist normal.*

Beweis. (1) ist trivial. (2). Sei $x \in L$ mit dem Minimalpolynom F, das den Grad 1 oder 2 besitzt. In $L[X]$ besitzt F einen Linearfaktor, der andere Faktor ist wegen der Gradbedingung konstant oder auch ein Linearfaktor. (3). Zu jedem $x \in L$ gibt es ein Polynom $F \in K[X]$, $F \neq 0$, mit $F(x) = 0$, das über $L[X]$ zerfällt. Wegen $K[X] \subseteq M[X]$ gilt diese Eigenschaft auch für $M \subseteq L$. (4). Nach (3) können wir sofort eine Körpererweiterung $\mathbb{Z}/(p) \subseteq \mathbb{F}_q$ mit einer Primzahl p und einer Primzahlpotenz $q = p^e$ betrachten. Jedes Element $x \in \mathbb{F}_q$ ist nach dem Satz von Lagrange eine Nullstelle des Polynoms $X^q - X$, so dass dieses Polynom über $\mathbb{F}_q$ zerfällt. □

Beispiel 15.3. Das Polynom $X^3 - 3X + 1 \in \mathbb{Q}[X]$ ist irreduzibel nach Aufgabe 3.16 und definiert daher eine Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[X]/\left(X^3 - 3X + 1\right) =: L$$

vom Grad 3. Die Restklasse von X in L sei mit α bezeichnet. Nach Aufgabe 11.7 sind auch die Elemente aus L

$$\beta = \alpha^2 - 2$$

und

$$\gamma = -\alpha^2 - \alpha + 2$$

Nullstellen der definierenden Gleichung und daher zerfällt das Polynom bereits über L. Daher ist die Körpererweiterung normal nach Satz 15.4 (3).

SATZ 15.4. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann sind folgende Aussagen äquivalent.*

(1) *Die Körpererweiterung ist normal.*
(2) *Wenn ein irreduzibles Polynom $P \in K[X]$ eine Nullstelle in L besitzt, so zerfällt es in $L[X]$.*
(3) *Es gibt ein K-Algebraerzeugendensystem $x_i \in L$, $i \in I$, von L und über L zerfallende Polynome $F_i \in K[X]$, $F_i \neq 0$, $i \in I$, mit $F_i(x_i) = 0$.*
(4) *Für jede Körpererweiterung $L \subseteq M$ und jeden K-Algebrahomomorphismus*
$$\varphi\colon L \longrightarrow M$$
ist $\varphi(L) \subseteq L$.

Beweis. (1) $\Rightarrow$ (2). Sei $P \in K[X]$ irreduzibel und $P(x) = 0$. Dann ist P nach Lemma 7.12 das Minimalpolynom zu x. Nach (1) gibt es ein über L zerfallendes Polynom F mit $F(x) = 0$. Da F ein Vielfaches von P ist, muss auch P über L zerfallen. (2) $\Rightarrow$ (1). Zu $x \in L$ gehört das Minimalpolynom P, das nach Lemma 7.12 irreduzibel ist und nach Voraussetzung (2) über L in Linearfaktoren zerfällt. (2) $\Rightarrow$ (3). Die Familie aller Elemente mit ihren Minimalpolynomen besitzt diese Eigenschaft. (3) $\Rightarrow$ (4). Seien $L \subseteq M$ und $\varphi\colon L \to M$ gegeben. Sei $x_i \in L$ ein Element aus der erzeugenden Familie und sei $F_i \neq 0$ das zugehörige zerfallende Polynom mit $F_i(x) = 0$, das wir als irreduzibel annehmen dürfen. Es ist

$$F_i(\varphi(x_i)) = \varphi(F_i(x_i)) = \varphi(0) = 0,$$

daher ist $\varphi(x_i) \in M$ eine Nullstelle des über L zerfallenden Polynoms F_i. Das heißt aber, dass $\varphi(x_i) \in L$ ist. Diese Zugehörigkeit gilt dann für alle $x \in L$, da sie für ein Algebraerzeugendensystem gilt. (4) $\Rightarrow$ (2). Sei $P \in K[X]$ irreduzibel und sei $x \in L$ mit $P(x) = 0$. Wir können nach Lemma 7.12 annehmen, dass P das Minimalpolynom von x ist. Wir setzen $x_1 = x$ und ergänzen dies zu einem endlichen K-Algebraerzeugendensystem von L, sagen wir

$$L = K[x_1, \ldots, x_n].$$

Es seien $P_1 = P, P_2, \ldots, P_n$ die Minimalpolynome von x_i über K. Wir betrachten das Produkt $F = P_1 \cdots P_n$ und den Zerfällungskörper M von F

über L, der zugleich der Zerfällungskörper über K ist. Sei $y \in M$ eine Nullstelle von P. Wir müssen $y \in L$ zeigen. Es gibt einen K-Isomorphismus

$$\varphi\colon\ K[x] \cong K[X]/(P) \longrightarrow K[y]$$

mit $\varphi(x) = y$. Der Körper M ist der Zerfällungskörper von F über $K[x]$ als auch über $K[y]$. Daher gibt es nach Satz 11.6 ein kommutatives Diagramm

$$\begin{array}{ccc} K[x] & \stackrel{\varphi}{\longrightarrow} & K[y] \\ \downarrow & & \downarrow \\ M & \stackrel{\tilde{\varphi}}{\longrightarrow} & M \end{array}$$

mit einem K-Isomorphismus $\tilde{\varphi}$. Nach Voraussetzung ist dabei $\tilde{\varphi}(L) \subseteq L$, also ist $y = \varphi(x) \in L$. □

Bemerkung 15.5. Insbesondere die zweite Eigenschaft von Satz 15.4 zeigt, dass es sich hierbei um eine recht starke Eigenschaft handelt. Wenn man mit einem Primpolynom $P \in K[X]$ startet und sich den Restklassenkörper $L = K[X]/(P)$ anschaut, so besitzt P in L eine Nullstelle, nämlich die Restklasse x von X. Daher gilt in $L[X]$ die Beziehung $P = (X - x)Q$ mit einem Polynom $Q \in L[X]$. Es gibt aber keinen allgemeinen Grund, warum Q über L in Linearfaktoren zerfallen sollte.

Wir geben ein Beispiel, das zeigt, dass die Verkettung von normalen Körpererweiterungen nicht normal sein muss.

Beispiel 15.6. Wir betrachten die Körperkette $\mathbb{Q} \subseteq M \subseteq L$, wobei $M = \mathbb{Q}(\sqrt{3})$ und $L = M(\sqrt{1+\sqrt{3}})$ ist. Das sind zwei quadratische Körpererweiterungen, die beide nach Lemma 15.2 (2) normal sind. Wir setzen $u = \sqrt{1+\sqrt{3}}$, und dieses Element erzeugt L über $\mathbb{Q}$. Wir können L als einen Unterkörper von $\mathbb{R}$ auffassen, indem wir für $\sqrt{3}$ und dann für $\sqrt{1+\sqrt{3}}$ die positiven reellen Wurzeln wählen. Wir haben

$$u^4 - 2u^2 - 2 = (u^2-1)^2 - 3 = 0,$$

d.h. das Polynom $X^4 - 2X^2 - 2$ wird von u annulliert. Dieses Polynom besitzt über L die Zerlegung

$$\begin{aligned} X^4 - 2X^2 - 2 &= \left(X^2-1\right)^2 - 3 \\ &= \left(X^2 - 1 - \sqrt{3}\right)\left(X^2 - 1 + \sqrt{3}\right) \\ &= \left(X^2 - u^2\right)\left(X^2 - 1 + \sqrt{3}\right) \\ &= (X-u)(X+u)\left(X^2 - 1 + \sqrt{3}\right). \end{aligned}$$

Wegen $L \subseteq \mathbb{R}$ und $\sqrt{3} - 1 > 0$ ist das hintere quadratische Polynom über L unzerlegbar. Dieses Polynom zerfällt also über L nicht in Linearfaktoren und somit ist $\mathbb{Q} \subseteq L$ nicht normal.

Wir setzen weiterhin voraus, dass eine endliche Körpererweiterung vorliegt. Dann sind die normalen Körpererweiterungen genau die Zerfällungskörper von Polynomen.

SATZ 15.7. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine normale Körpererweiterung, wenn L Zerfällungskörper eines Polynoms $F \in K[X]$ ist.*

Beweis. Sei $K \subseteq L$ normal. Wegen der vorausgesetzten Endlichkeit ist $L = K[x_1, \ldots, x_n]$. Zu x_i sei $F_i \in K[X]$ das Minimalpolynom. Wegen der Normalität zerfällt jedes F_i in $L[X]$ in Linearfaktoren. Daher ist L der Zerfällungskörper des Produktes $F = F_1 \cdots F_n$. Sei nun $L = Z(F)$ ein Zerfällungskörper, und sei $F = (X - \alpha_1) \cdots (X - \alpha_n)$ die Faktorzerlegung zu den Nullstellen $\alpha_i \in L$, die den Körper L erzeugen. Wir werden das Kriterium Satz 15.4 (4) anwenden. Sei also $L \subseteq M$ eine Körpererweiterung und sei

$$\varphi \colon L \longrightarrow M$$

ein K-Algebrahomomorphismus. Es ist dann

$$F(\varphi(\alpha_i)) = \varphi(F(\alpha_i)) = 0,$$

da sich die Koeffizienten von F nicht ändern (vergleiche Lemma 10.15), und somit gehört $\varphi(\alpha_i)$ zur Nullstellenmenge $\{\alpha_1, \ldots, \alpha_n\}$ und damit insbesondere zu L. Daher gilt generell $\varphi(L) \subseteq L$. □

KOROLLAR 15.8. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Es sei $\varphi \colon M \to L$ ein K-Algebrahomomorphismus. Dann besitzt φ eine Fortsetzung zu einem Automorphismus auf L.*

Beweis. Aufgrund von Satz 15.7 wissen wir, dass L der Zerfällungskörper eines Polynoms $F \in K[X]$ ist. L ist auch der Zerfällungskörper von $F \in M[X]$. Sei $M' = \varphi(M)$ das isomorphe Bild von M in L unter φ. Somit ist L auch der Zerfällungskörper von $F \in M'[X]$. Daher gibt es nach Satz 11.6 einen Isomorphismus $\tilde{\varphi} \colon L \to L$, der mit den Abbildungen $M \to L$ und $M \xrightarrow{\varphi} M' \to L$ verträglich ist. □

KOROLLAR 15.9. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und es seien $\alpha, \beta \in L$. Dann sind α und β genau dann konjugiert, wenn es einen K-Automorphismus $\varphi \colon L \to L$ mit $\varphi(\alpha) = \beta$ gibt.*

Beweis. Wenn es einen K-Automorphismus φ mit $\varphi(\alpha) = \beta$ gibt, so induziert dieser einen Isomorphismus $K[\alpha] \to K[\beta]$. Da diese erzeugten Unterkörper jeweils durch die Minimalpolynome von α bzw. β festgelegt sind, müssen die Minimalpolynome übereinstimmen. Also sind α und β konjugiert. Wenn umgekehrt[1] die beiden Elemente konjugiert sind, so gibt es einen K-Isomorphismus $K[\alpha] \to K[\beta]$. Mit der Inklusion $K[\beta] \subseteq L$ führt dies zu

[1] Die Umkehrung folgt auch aus Satz 14.5.

einem K-Homomorphismus

$$K[\alpha] \longrightarrow L,$$

den man nach Korollar 15.8 zu einem Automorphismus auf L fortsetzen kann. □

In der nichtnormalen Erweiterung $\mathbb{Q} \subseteq L$ aus Beispiel 15.6 sind $\sqrt{3}$ und $-\sqrt{3}$ zueinander konjugiert (und es gibt einen Automorphismus $\mathbb{Q}[\sqrt{3}] \to \mathbb{Q}[\sqrt{3}] = \mathbb{Q}[-\sqrt{3}]$, der $\sqrt{3}$ in $-\sqrt{3}$ überführt), es gibt aber keinen Automorphismus $L \to L$, der $\sqrt{3}$ in $-\sqrt{3}$ überführt. Aufgrund der Faktorzerlegung des Minimalpolynoms zu u sind die Identität und die durch $u \mapsto -u$ festgelegte Abbildung die einzigen Automorphismen, und beide sind eingeschränkt auf $\mathbb{Q}[\sqrt{3}]$ die Identität.

Korollar 15.10. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist $K \subseteq M$ genau dann normal, wenn für jeden K-Algebraautomorphismus*

$$\varphi\colon L \longrightarrow L$$

die Beziehung $\varphi(M) \subseteq M$ gilt.

Beweis. Wenn $K \subseteq M$ normal ist, so gilt die Homomorphismuseigenschaft aufgrund von Satz 15.4 (4). Zur Umkehrung verwenden wir das Kriterium Satz 15.4 (2). Sei also $P \in K[X]$ ein irreduzibles (normiertes) Polynom, das in M eine Nullstelle, sagen wir α, besitzt. Dieses Polynom zerfällt über L in Linearfaktoren, und wir müssen zeigen, dass die zugehörigen Nullstellen zu M gehören. Sei $\beta \in L$ eine weitere Nullstelle von P. Wegen der Irreduzibilität und Lemma 7.12 ist P das Minimalpolynom von α und auch von β, d.h. die beiden Elemente sind konjugiert. Nach Korollar 15.9 gibt es daher einen K-Automorphismus $\varphi\colon L \to L$ mit $\varphi(\alpha) = \beta$. Nach Voraussetzung ist $\beta \in M$. □

Beispiel 15.11. Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}, \sqrt{-3}] = \mathbb{Q}[\sqrt[3]{7}, \eta] =: L,$$

wobei

$$\eta = \frac{-1+\sqrt{3}\mathrm{i}}{2}$$

die dritte primitive Einheitswurzel ist und wobei wir mit $\sqrt[3]{7}$ die reelle Zahl meinen. Dies ist eine Erweiterung vom Grad 6, wie die Kette

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{7}] =: M \subseteq L$$

zeigt. Die Erweiterung $\mathbb{Q} \subseteq M$ ist nicht normal, da die beiden anderen dritten Wurzeln der 7, nämlich $\sqrt[3]{7}\eta$ und $\sqrt[3]{7}\eta^2$, nicht zu M gehören, weil sie nicht reell sind. Sie gehören aber zu L und da mit $\sqrt{-3}$ auch $-\sqrt{-3}$ zu L gehört ist nach Satz 15.4 (3) die Gesamterweiterung $\mathbb{Q} \subseteq L$ normal. Nach Korollar 15.10 muss es $\mathbb{Q}$-Automorphismen $\varphi\colon L \to L$ mit $\varphi(M) \neq M$

geben. In der Tat gibt es einen Automorphismus φ auf L, der η auf sich selbst und $\sqrt[3]{7}$ auf $\sqrt[3]{7}\eta$ abbildet. Dabei ist

$$M' = \varphi(M) = \mathbb{Q}[\sqrt[3]{7}\eta] \neq M.$$

Abbildungsverzeichnis