

Körper- und Galoistheorie

Vorlesung 14

Normale Körpererweiterungen

DEFINITION 14.1. 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 14.2.

- (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. \square

SATZ 14.3. *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 -Algebra-Erzeugendensystem $x_i \in L$, $i \in I$, 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 -Algebra-Homomorphismus

$$\varphi : L \longrightarrow M$$

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) in Linearfaktoren zerfällt. (2) \Rightarrow (3). Die Familie aller Elemente mit ihren Minimalpolynomen besitzt diese Eigenschaft. (3) \Rightarrow (4). Seien $L \subseteq M$ und $\varphi : L \rightarrow M$ gegeben. Sei $x_i \in L$ ein Element aus der erzeugenden Familie und sei $F_i \neq 0$ das zugehörige zerfallende Polynom mit $F_i(x_i) = 0$, 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 Algebra-Erzeugendensystem 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 K -Algebra-Erzeugendensystem von L , sagen wir

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

Es seien $P_1 = P, P_2, \dots, P_n$ 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

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

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 11.5 ein kommutatives Diagramm

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

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

BEMERKUNG 14.4. Insbesondere die zweite Eigenschaft von

Satz 14.3 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 setzen weiterhin voraus, dass eine endliche Körpererweiterung vorliegt. Dann sind die normalen Körpererweiterungen genau die Zerfällungskörper von Polynomen.

SATZ 14.5. *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 $L = K[x_1, \dots, x_n]$. 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 wenden das Kriterium Satz 14.3 (4) an. Sei also $L \subseteq M$ eine Körpererweiterung und sei

$$\varphi : L \longrightarrow M$$

ein K -Algebra-Homomorphismus. Es ist dann

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

da sich die Koeffizienten von F nicht ändern (vergleiche Lemma 8.15), und somit gehört $\varphi(\alpha_i)$ zur Nullstellenmenge $\{\alpha_1, \dots, \alpha_n\}$ und damit insbesondere zu L . Daher gilt generell $\varphi(L) \subseteq L$. \square

KOROLLAR 14.6. *Sei $K \subseteq L$ eine endliche normale Körpererweiterung und M , $K \subseteq M \subseteq L$, ein Zwischenkörper. Es sei $\varphi : M \rightarrow L$ ein K -Algebra-Homomorphismus. Dann besitzt φ eine Fortsetzung zu einem Automorphismus auf L .*

Beweis. Aufgrund von Satz 14.5 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 11.5 einen Isomorphismus $\tilde{\varphi} : L \rightarrow L$, der mit den Abbildungen $M \rightarrow L$ und $M \xrightarrow{\varphi} M' \rightarrow L$ verträglich ist. \square

KOROLLAR 14.7. *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 $\varphi : L \rightarrow L$ mit $\varphi(\alpha) = \beta$ gibt.*

Beweis. Wenn es einen K -Automorphismus φ mit $\varphi(\alpha) = \beta$ gibt, so induziert dieser einen Isomorphismus $K[\alpha] \rightarrow K[\beta]$. 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 umgekehrt¹ die beiden Elemente konjugiert sind, so gibt es einen K -Isomorphismus $K[\alpha] \rightarrow K[\beta]$. Mit der Inklusion $K[\beta] \subseteq L$ führt dies zu einem K -Homomorphismus

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

den man nach Korollar 14.6 zu einem Automorphismus auf L fortsetzen kann. \square

KOROLLAR 14.8. *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 -Algebra-Automorphismus*

$$\varphi : L \longrightarrow L$$

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

Beweis. Wenn $K \subseteq M$ normal ist, so gilt die Homomorphismeigenschaft aufgrund von Satz 14.3. Zur Umkehrung verwenden wir das Kriterium Satz 14.3. 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 14.7 gibt es daher einen K -Automorphismus $\varphi : L \rightarrow L$ mit $\varphi(\alpha) = \beta$. Nach Voraussetzung ist $\beta \in M$. \square

BEISPIEL 14.9. 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 14.2 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

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

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.

¹Die Umkehrung folgt auch aus Satz 13.2.