

## Körper- und Galoistheorie

### Vorlesung 15

#### Fixkörper

DEFINITION 15.1. Es sei  $L$  ein Körper und  $H \subseteq \text{Aut}(L)$  eine Untergruppe der Automorphismengruppe von  $L$ . Dann heißt

$$\text{Fix}(H) = \{x \in L \mid \varphi(x) = x \text{ für alle } \varphi \in H\}$$

der *Fixkörper* zu  $H$ .

Es ist unmittelbar klar, dass es sich dabei um einen Unterkörper von  $L$  handelt. Dies gilt auch dann, wenn  $H$  eine beliebige Menge von Ringhomomorphismen ist, die nicht notwendigerweise bijektiv sein müssen.

LEMMA 15.2. *Es sei  $L$  ein Körper und  $G = \text{Aut}(L)$  die Automorphismengruppe von  $L$ . Dann gelten folgende Eigenschaften.*

- (1) *Für Untergruppen  $H_1 \subseteq H_2 \subseteq G$  ist  $\text{Fix}(H_1) \supseteq \text{Fix}(H_2)$ .*
- (2) *Für Unterkörper  $M_1 \subseteq M_2 \subseteq L$  ist  $\text{Gal}(L|M_1) \supseteq \text{Gal}(L|M_2)$ .*
- (3) *Für eine Untergruppe  $H \subseteq G$  ist  $H \subseteq \text{Gal}(L|\text{Fix}(H))$ .*
- (4) *Für einen Unterkörper  $M \subseteq L$  ist  $M \subseteq \text{Fix}(\text{Gal}(L|M))$ .*

*Beweis.* Siehe Aufgabe 15.3. □

BEMERKUNG 15.3. Zur trivialen Untergruppe  $\{\text{id}\} \subseteq \text{Aut}(L)$  gehört der Fixkörper  $L$ , und für jede andere Untergruppe ist der Fixkörper ein echter Unterkörper. Den Fixkörper zur gesamten Automorphismengruppe kann man dagegen nicht einfach charakterisieren (es ist nicht immer der Primkörper).

### Charakterisierung von Galoisweiterungen

Wir streben eine umfassende Charakterisierung von Galoisweiterungen an, was einige Vorbereitungen erfordert.

LEMMA 15.4. *Es sei  $L$  ein Körper und sei  $H \subseteq \text{Aut}(L)$  eine endliche Untergruppe der Automorphismengruppe von  $L$ . Es sei  $K = \text{Fix}(H)$ . Dann ist  $K \subseteq L$  eine algebraische Körpererweiterung, die normal und separabel ist. Für jedes  $x \in L$  ist der Grad des Minimalpolynoms von  $x$  maximal gleich  $\#(H)$ .*

*Beweis.* Sei  $x \in L$  fixiert. Wir betrachten die endliche Menge

$$M = \{\varphi(x) \mid \varphi \in H\} = \{x_1, \dots, x_n\},$$

wobei  $x_1 = x$  sei. Wir setzen

$F = (X - x_1)(X - x_2) \cdots (X - x_n) = a_0 + a_1X + a_2X^2 + \dots + a_{n-1}X^{n-1} + X^n$   
 ( $\in L[X]$ ). Es ist  $F(x) = 0$ . Wir zeigen zuerst, dass die Koeffizienten  $a_i$  dieses Polynoms zu  $K$  gehören. Sei dazu  $\varphi \in H$ . Dann ist

$$\sum_{i=0}^n \varphi(a_i)X^i = \prod_{i=1}^n (X - \varphi(x_i)) = \prod_{i=1}^n (X - x_i) = \sum_{i=0}^n a_i X^i.$$

Daher ist  $\varphi(a_i) = a_i$ . Somit gehören die Koeffizienten zum Fixkörper  $K = \text{Fix}(H)$  und daher ist  $F \in K[X]$ . Dies bedeutet, dass  $x$  algebraisch über  $K$  ist, und dass sein Minimalpolynom einen Grad

$$\leq \text{Grad}(F) = n = \#(M) \leq \#(H)$$

besitzt. Da  $F$  über  $L$  in Linearfaktoren zerfällt, und da alle Nullstellen von  $F$  einfach sind, ist die Erweiterung normal und separabel.  $\square$

Der folgende Satz heißt *Satz von Artin*.

**SATZ 15.5.** *Es sei  $L$  ein Körper und sei  $H \subseteq \text{Aut}(L)$  eine endliche Untergruppe der Automorphismengruppe von  $L$ . Es sei  $K = \text{Fix}(H)$ . Dann ist*

$$\text{grad}_K L = \#(H).$$

*Insbesondere ist  $K \subseteq L$  eine Galoiserweiterung mit Galoisgruppe  $H$ .*

*Beweis.* Nehmen wir an, dass  $\#(H) < \text{grad}_K L$  ist. Wir können annehmen, dass  $L$  endlich über  $K$  ist, da wir  $L$  durch einen (über  $K$  endlichen) Zwischenkörper der Form  $K[\varphi(x_i), \varphi \in H, i = 1, \dots, n]$  mit beliebig hohem Grad ersetzen können. Nach Lemma 15.4 ist die Körpererweiterung separabel und nach dem Satz vom primitiven Element kann man  $L = K[x]$  schreiben. Dabei ist der Grad des Minimalpolynoms von  $x$  gleich dem Grad der Körpererweiterung, so dass sich ein Widerspruch zu Lemma 15.4 ergibt. Also ist  $K \subseteq L$  eine endliche Körpererweiterung mit  $\#(H) \geq \text{grad}_K L$ . Nach Satz 13.5 muss hierbei Gleichheit gelten. Die Inklusion  $H \subseteq \text{Gal}(L|K)$  ist trivial. Da  $H$  nach Satz 13.5 schon die maximal mögliche Anzahl von Automorphismen enthält, gilt hier Gleichheit.  $\square$

Der nächste Satz fasst die verschiedenen Charakterisierungen einer Galoiserweiterung zusammen.

**SATZ 15.6.** *Sei  $K \subseteq L$  eine endliche Körpererweiterung und sei  $G = \text{Gal}(L|K)$  die Galoisgruppe. Dann sind folgende Eigenschaften äquivalent.*

- (1) *Die Körpererweiterung  $K \subseteq L$  ist eine Galoiserweiterung.*
- (2) *Es ist  $\text{Fix}(G) = K$ .*

- (3) Die Körpererweiterung  $K \subseteq L$  ist normal und separabel.  
 (4)  $L$  ist Zerfällungskörper eines separablen Polynoms  $F \in K[X]$ .

*Beweis.* Zum Beweis der Implikation von (1) nach (2) betrachten wir die Körperkette  $K \subseteq \text{Fix}(G) \subseteq L$ . Nach der Gradformel und da eine Galoisweiterung vorliegt ist

$$\text{grad}_K \text{Fix}(G) \cdot \text{grad}_{\text{Fix}(G)} L = \text{grad}_K L = \#(G).$$

Nach dem Satz von Artin ist  $\text{grad}_{\text{Fix}(G)} L = \#(G)$ , also ist  $\text{grad}_K \text{Fix}(G) = 1$  und somit  $K = \text{Fix}(G)$ . Die Implikation von (2) nach (3) folgt aus Lemma 15.4. Die Äquivalenz von (3) und (4) ergibt sich sofort aus Satz 14.5. Sei nun (3) erfüllt. Wir schreiben  $L = K[x_1, \dots, x_m]$ . Die Minimalpolynome  $F_i \in K[X]$  der  $x_i$  zerfallen wegen der Normalität in  $L[X]$  in Linearfaktoren. Daher können wir Lemma 12.6 mit  $M = L$  anwenden und erhalten  $n = \text{grad}_K L$  Einbettungen von  $L$  nach  $L$  (über  $K$ ), und somit besitzt die Galoisgruppe  $n$  Elemente.  $\square$

**KOROLLAR 15.7.** *Es sei  $K \subseteq L$  eine endliche Galoisweiterung und  $M$ ,  $K \subseteq M \subseteq L$ , ein Zwischenkörper. Dann ist auch  $M \subseteq L$  eine Galoisweiterung.*

*Beweis.* Nach Lemma 14.2 ist  $M \subseteq L$  eine normale Körpererweiterung. Nach Lemma 12.4 ist sie auch separabel. Somit handelt es sich aufgrund von Satz 15.6 um eine Galoisweiterung.  $\square$

## Endliche Körper als Galoisweiterung

Wir besprechen zuerst endliche Körper im Rahmen der Galoistheorie.

**DEFINITION 15.8.** Sei  $R$  ein kommutativer Ring, der einen Körper der positiven Charakteristik  $p > 0$  enthalte. Der *Frobenius-Homomorphismus* ist der Ringhomomorphismus

$$R \longrightarrow R, f \longmapsto f^p.$$

Zu jeder Primzahl  $p$  und jedem Exponenten  $m$  gibt es nach Satz 11.9 einen eindeutig bestimmten endlichen Körper mit  $p^m$  Elementen.

**LEMMA 15.9.** *Sei  $L$  ein endlicher Körper der Charakteristik  $p$ . Dann ist der Frobenius-Homomorphismus*

$$\Phi : L \longrightarrow L, x \longmapsto x^p,$$

*ein Automorphismus, dessen Fixkörper  $\mathbb{Z}/(p)$  ist.*

*Beweis.* Der Frobenius-Homomorphismus ist stets ein Ringhomomorphismus. Die Injektivität ergibt sich aus Korollar 13.17, und daraus ergibt sich die Surjektivität wegen der Endlichkeit aus Lemma 3.14 (Mathematik (Osnabrück 2009-2011)). Wegen  $\Phi(1) = 1$  werden die Elemente aus  $\mathbb{Z}/(p)$  auf sich selbst

abgebildet. Daher gibt es  $p$  Elemente in  $K$  mit  $x^p = x$ . Mehr kann es wegen Korollar Anhang 1.5 nicht geben.  $\square$

**SATZ 15.10.** *Es sei  $p$  eine Primzahl und  $m \in \mathbb{N}$ ,  $q = p^m$ . Dann ist die Körpererweiterung  $\mathbb{F}_p \subseteq \mathbb{F}_q$  eine Galoiserweiterung mit einer zyklischen Galoisgruppe der Ordnung  $m$ , die vom Frobenius-Homomorphismus erzeugt wird.*

*Beweis.* Es sei

$$\Phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$$

der Frobenius-Homomorphismus, der nach Lemma 15.9 ein  $\mathbb{F}_p$ -Automorphismus ist. Daher sind auch die Iterationen  $\Phi^k$  Automorphismen, und zwar gilt

$$\Phi^k(x) = x^{p^k}.$$

Bei  $k = m$  ist nach Korollar 4.17  $x^{p^m} = x$  für alle  $x \in \mathbb{F}_q$ , also ist  $\Phi^m = \text{id}$ . Für  $k < m$  kann  $\Phi^k$  nicht die Identität sein, da dies sofort Korollar Anhang 1.5 widersprechen würde. Also gibt es  $m$  verschiedene Potenzen des Frobenius-Automorphismus. Nach Satz 13.5 kann es keine weiteren Automorphismen geben und die Körpererweiterung ist galoissch mit der vom Frobenius erzeugten Gruppe als Galoisgruppe.  $\square$

**KOROLLAR 15.11.** *Es sei  $p$  eine Primzahl und  $m, n \in \mathbb{N}_+$ . Es seien  $K$  und  $L$  endliche Körper mit  $p^m$  bzw.  $p^n$  Elementen. Dann ist  $K$  genau dann ein Unterkörper von  $L$ , wenn  $m$  ein Teiler von  $n$  ist. In diesem Fall ist  $K \subseteq L$  eine Galoiserweiterung vom Grad  $n/m$  mit einer zyklischen Galoisgruppe der Ordnung  $n/m$ , die von der  $m$ -ten Iteration des Frobenius erzeugt wird.*

*Beweis.* Sei  $q = p^m$ . Wenn  $K$  ein Unterkörper von  $L$  ist, so ist  $L$  ein  $K$ -Vektorraum einer gewissen endlichen Dimension. Daher muss die Elementanzahl eine Potenz von  $q$  sein. Aus

$$p^n = q^k = (p^m)^k = p^{mk}$$

ergibt sich sofort, dass  $n$  ein Vielfaches von  $m$  ist. Sei umgekehrt  $m$  ein Teiler von  $n$ . Die Frobeniusiteration  $\Phi^m$  auf  $L$  erzeugt eine Untergruppe  $H$  der nach Satz 15.10 zyklischen Galoisgruppe von  $\mathbb{F}_p \subseteq L$ . Die Ordnung von  $H$  ist  $n/m$ . Es sei  $M = \text{Fix}(H) \subseteq L$  der zugehörige Fixkörper. Dann besitzt die Körpererweiterung  $M \subseteq L$  nach Korollar 15.7 den Grad  $n/m$  und somit besitzt  $\mathbb{F}_p \subseteq M$  den Grad  $m$ . Daher besitzt  $M$  gerade  $p^m$  Elemente und ist daher wegen Satz 11.9 isomorph zu  $K$ .  $\square$