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

Körper- und Galoistheorie

Vorlesung 15

Fixkörper

DEFINITION 14.1. Es sei L ein Körper und $H \subseteq \operatorname{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Dann heißt

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

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

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

Beweis. Siehe Aufgabe 15.3. □

BEMERKUNG 14.3. Zur trivialen Untergruppe $\{\mathrm{id}\} \subseteq \operatorname{Aut}(L)$ 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 Galoiserweiterungen

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

LEMMA 14.4. *Es sei L ein Körper und sei $H \subseteq \operatorname{Aut}(L)$ eine endliche Untergruppe der Automorphismengruppe von L. Es sei $K = \operatorname{Fix}(H)$. 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

$$M = \{\varphi(x) | \, \varphi \in H\} = \{x_1, \ldots, x_n\},$$

wobei $x_1 = x$ sei. Wir setzen

$$F = (X-x_1)(X-x_2)\cdots(X-x_n) = a_0+a_1X+a_2X^2+\ldots+a_{n-1}X^{n-1}+X^n$$

($\in L[X]$). 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 $K = \mathrm{Fix}\,(H)$ und daher ist $F \in K[X]$. Dies bedeutet, dass x algebraisch über K ist, und dass sein Minimalpolynom einen Grad

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

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

Der folgende Satz heißt *Satz von Artin.*

Satz 14.5. *Es sei L ein Körper und sei $H \subseteq \mathrm{Aut}\,(L)$ eine endliche Untergruppe der Automorphismengruppe von L. Es sei $K = \mathrm{Fix}\,(H)$. Dann ist*

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

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

Beweis. Nehmen wir an, dass $\#(H) < \mathrm{grad}_K\, L$ ist. Wir können annehmen, dass L endlich über K ist, da wir L durch einen (über K endlichen) Zwischenkörper der Form $K[\varphi(x_i), \varphi \in H,\, i = 1, \ldots, n]$ 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 $\#(H) \geq \mathrm{grad}_K\, L$. Nach Satz 13.5 muss hierbei Gleichheit gelten. Die Inklusion $H \subseteq \mathrm{Gal}\,(L|K)$ ist trivial. Da H nach Satz 13.5 schon die maximal mögliche Anzahl von Automorphismen enthält, gilt hier Gleichheit. □

Der nächste Satz fasst die verschiedenen Charakterisierungen einer Galoiserweiterung zusammen.

Satz 14.6. *Sei $K \subseteq L$ eine endliche Körpererweiterung und sei $G = \mathrm{Gal}\,(L|K)$ die Galoisgruppe. Dann sind folgende Eigenschaften äquivalent.*

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

(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 $K \subseteq \operatorname{Fix}(G) \subseteq L$. Nach der Gradformel und da eine Galoiserweiterung vorliegt ist

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

Nach dem Satz von Artin ist $\operatorname{grad}_{\operatorname{Fix}(G)} L = \#(G)$, also ist $\operatorname{grad}_K \operatorname{Fix}(G) = 1$ und somit $K = \operatorname{Fix}(G)$. 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 $L = K[x_1, \ldots, x_m]$. 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 $n = \operatorname{grad}_K L$ Einbettungen von L nach L (über K), und somit besitzt die Galoisgruppe n Elemente. □

Korollar 14.7. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist auch $M \subseteq L$ eine Galoiserweiterung.*

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 Galoiserweiterung. □

Endliche Körper als Galoiserweiterung

Wir besprechen zuerst endliche Körper im Rahmen der Galoistheorie.

Definition 14.8. 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 14.9. *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. □

Satz 14.10. *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 Φ^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 $\Phi^m = \mathrm{id}$. Für $k < m$ kann Φ^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. □

Korollar 14.11. *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 Φ^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 $M = \mathrm{Fix}\,(H) \subseteq L$ 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. □