

Körper- und Galoistheorie

Vorlesung 19

In dieser Vorlesung möchten wir zunächst nachweisen, dass es sich bei einem Kreisteilungskörper über \mathbb{Q} um eine Galoiserweiterung handelt, deren Galoisgruppe abelsch ist und eine Struktur besitzt, die unmittelbar mit den Einheitswurzeln zusammenhängt.

Kreisteilungskörper als Galoiserweiterung

Wir kommen nun zur Galoiseigenschaft der Kreisteilungskörper über \mathbb{Q} .

SATZ 19.1. *Es sei K_n der n -te Kreisteilungskörper. Dann ist $\mathbb{Q} \subseteq K_n$ eine Galoiserweiterung mit der Galoisgruppe*

$$\text{Gal}(K_n|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times.$$

Dabei entspricht der Einheit $a \in (\mathbb{Z}/(n))^\times$ derjenige Automorphismus $\varphi_a \in \text{Gal}(K_n|\mathbb{Q})$, der eine n -te Einheitswurzel ζ auf ζ^a abbildet.

Beweis. Nach Korollar 18.10 ist

$$K_n = \mathbb{Q}[X]/(\Phi_n),$$

wobei Φ_n das n -te Kreisteilungspolynom ist. Dieses ist das Produkt $\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i)$ über die $\varphi(n)$ primitiven Einheitswurzeln und damit vom Grad $\varphi(n)$. Da der Kreisteilungskörper all diese primitiven Einheitswurzeln enthält, zerfällt das Kreisteilungspolynom über K_n in Linearfaktoren und daher ist K_n der Zerfällungskörper des Kreisteilungspolynoms und somit nach Satz 15.6 eine Galoiserweiterung.

Es sei nun ζ eine primitive n -te Einheitswurzel, und zwar diejenige, die bei der obigen Restklassenidentifizierung der Variablen X entspricht. Zu $a \in (\mathbb{Z}/\mathbb{Z}n)^\times$ ist ζ^a ebenfalls eine primitive Einheitswurzel. Wir betrachten den Einsetzungshomomorphismus

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[X]/(\Phi_n), X \longmapsto \zeta^a.$$

Dieser ist surjektiv, da ζ^a den Kreisteilungskörper erzeugt. Wegen $\Phi_n(\zeta^a) = 0$ induziert dies einen Automorphismus

$$\mathbb{Q}[X]/(\Phi_n) \longrightarrow \mathbb{Q}[X]/(\Phi_n), \zeta \longmapsto \zeta^a.$$

Dadurch erhalten wir eine Zuordnung

$$(\mathbb{Z}/\mathbb{Z}n)^\times \longrightarrow \text{Gal}(K_n|\mathbb{Q}), a \longmapsto \varphi_a.$$

Für $a, a' \in (\mathbb{Z}/\mathbb{Z}n)^\times$ ist

$$\varphi_{aa'}(\zeta) = \zeta^{aa'} = (\zeta^a)^{a'} = \varphi_a(\zeta^{a'}) = \varphi_a(\varphi_{a'}(\zeta)) = (\varphi_a \circ \varphi_{a'}) (\zeta),$$

so dass $\varphi_{aa'} = \varphi_a \circ \varphi_{a'}$ gilt (da die Automorphismen auf dem Erzeuger ζ festgelegt sind). Die Zuordnung ist also ein Gruppenhomomorphismus. Für verschiedene Einheiten $a \neq a'$ ist $\zeta^a \neq \zeta^{a'}$ und somit $\varphi_a \neq \varphi_{a'}$. Die Abbildung ist also injektiv. Da es links und rechts $\varphi(n)$ Elemente gibt, ist die Abbildung eine Bijektion. \square

BEISPIEL 19.2. Wir betrachten den achten Kreisteilungskörper K_8 . Die Einheitengruppe $(\mathbb{Z}/(8))^\times$ ist $\{1, 3, 5, 7\}$, wobei 3, 5, 7 die Ordnung 2 besitzen. Die nach Satz 19.1 zugehörigen Körperautomorphismen sind neben der Identität die Abbildungen $\varphi_3, \varphi_5, \varphi_7$, die auf den Einheitswurzeln (ζ sei eine primitive achte Einheitswurzel) folgendermaßen wirken.

$$\varphi_3 : \zeta \longleftrightarrow \zeta^3, \zeta^2 = i \longleftrightarrow \zeta^6 = -i, \zeta^5 \longleftrightarrow \zeta^7,$$

$$\varphi_5 : \zeta \longleftrightarrow \zeta^5, i = \zeta^2 \longleftrightarrow \zeta^{10} = i, \zeta^3 \longleftrightarrow \zeta^7, -i \longleftrightarrow -i,$$

und

$$\varphi_7 : \zeta \longleftrightarrow \zeta^7, i = \zeta^2 \longleftrightarrow \zeta^{14} = -i, \zeta^3 \longleftrightarrow \zeta^5.$$

KOROLLAR 19.3. Zu jeder endlichen abelschen Gruppe G gibt es eine endliche Galoiserweiterung $\mathbb{Q} \subseteq L$, deren Galoisgruppe gleich G ist.

Beweis. Nach einem elementaren Satz, den wir hier nicht beweisen, lässt sich G als Restklassengruppe einer Einheitengruppe $(\mathbb{Z}/(n))^\times$ auffassen. Es sei

$$q : (\mathbb{Z}/(n))^\times \longrightarrow G$$

der zugehörige surjektive Restklassenhomomorphismus und H der Kern davon. Nach Satz 19.1 ist $(\mathbb{Z}/(n))^\times$ die Galoisgruppe der n -ten Kreisteilungserweiterung $\mathbb{Q} \subseteq K_n$. Es sei $M \subseteq K_n$ der Fixkörper zu H . Nach Satz 16.4 ist $\mathbb{Q} \subseteq M$ eine Galoiserweiterung mit Galoisgruppe G . \square

Es ist ein offenes Problem, ob jede endliche Gruppe als Galoisgruppe einer Galoiserweiterung von \mathbb{Q} auftritt. Diese Fragestellung gehört zur sogenannten *inversen Galoistheorie*.

Galoiseigenschaften des Kompositums

Wir betrachten eine wichtige Konstruktion, das sogenannte Kompositum.

DEFINITION 19.4. Sei $K \subseteq L$ eine Körpererweiterung und seien $K \subseteq M_1, M_2 \subseteq L$ zwei Zwischenkörper. Dann nennt man den von M_1 und M_2 erzeugten Unterkörper das *Kompositum* der beiden Körper (in L). Es wird mit $M_1 M_2$ bezeichnet.

LEMMA 19.5. *Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M , in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine endliche separable Körpererweiterung.*

Beweis. Es sei $K \subseteq L = K[x_1, \dots, x_n]$ separabel, und seien $F_i \in K[X]$ die zu x_i gehörigen (separablen) Minimalpolynome. Dann ist $L' = K'[x_1, \dots, x_n]$ und die Minimalpolynome G_i der x_i über K' sind in $K'[X]$ Teiler der F_i und daher selbst separabel. Nach Satz 12.7 ist $K' \subseteq L'$ eine separable Körpererweiterung. \square

LEMMA 19.6. *Es sei $K \subseteq L$ eine endliche normale Körpererweiterung und sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M , in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine normale Körpererweiterung.*

Beweis. Wir können $L = K[x_1, \dots, x_n]$ schreiben, und wir wissen, dass es zugehörige Polynome $F_i \in K[X]$ mit $F_i(x_i) = 0$ gibt, die über L zerfallen. Daher ist $L' = K'[x_1, \dots, x_n]$ und dieselben Polynome, aufgefasst in $K'[X]$, erfüllen die gleichen Eigenschaften. Aus Satz 14.3 ergibt sich die Normalität. \square

Aus diesen zwei Lemmata ergibt sich der folgende Satz, der für die Charakterisierung der auflösbaren Körpererweiterungen wichtig ist.

SATZ 19.7. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung, und es sei $K \subseteq K'$ eine weitere Körpererweiterung mit dem gemeinsamen Oberkörper M , in dem das Kompositum $L' = LK'$ gebildet sei. Dann ist $K' \subseteq L'$ ebenfalls eine endliche Galoiserweiterung, und für ihre Galoisgruppe gilt die natürliche Isomorphie*

$$\text{Gal}(L'|K') \cong \text{Gal}(L|L \cap K').$$

Beweis. Die Erweiterung $K' \subseteq L'$ ist normal nach Lemma 19.6 und separabel nach Lemma 19.5, also eine Galoiserweiterung aufgrund von Satz 15.6. Zur Berechnung der Galoisgruppe gehen wir von der Einschränkungabbildung

$$\Psi : \text{Gal}(L'|K') \longrightarrow \text{Gal}(L|K), \varphi \longmapsto \varphi|_L,$$

aus, die wegen der Normalität von $K \subseteq L$ nach Satz 14.3 ein wohldefinierter Gruppenhomomorphismus ist. Es sei $\varphi \in \text{Gal}(L'|K')$ ein Automorphismus, dessen Bild unter diesem Homomorphismus trivial sei, also $\varphi|_L = \text{id}_L$. Da auch $\varphi|_{K'} = \text{id}_{K'}$ gilt, ist φ auf dem Kompositum $L' = LK'$ die Identität, also das neutrale Element. Daher ist Ψ nach Lemma 4.9 injektiv. Das Bild von Ψ ist eine Untergruppe $H = \text{bild } \Psi \subseteq \text{Gal}(L|K)$. Aufgrund der Galois-Korrespondenz gibt es einen Zwischenkörper Z , $K \subseteq Z \subseteq L$, mit $H = \text{Gal}(L|Z)$, und zwar ist Z der Fixkörper von H . Für jedes $\varphi \in \text{Gal}(L'|K')$ ist $\varphi|_{K'} = \text{id}_{K'}$, und daher ist auch $(\varphi|_L)|_{L \cap K'} = \text{id}_{L \cap K'}$. Also ist $L \cap K' \subseteq Z$.

Wenn $x \in Z$ ist, so bedeutet dies, dass für jedes $\varphi \in \text{Gal}(L'|K')$ die Gleichheit $(\varphi|_L)(x) = x$ gilt. Dann ist aber $x \in K'$, wegen Satz 15.6 und da eine Galoiserweiterung vorliegt, und somit ist $x \in L \cap K'$. Insgesamt ist also

$$\text{Gal}(L'|K') = \text{bild } \Psi = \text{Gal}(L|L \cap K').$$

□