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

Körper- und Galoistheorie

Vorlesung 20

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

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

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

Beweis. Nach Korollar 19.12 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 alle 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 16.6 eine Galoiserweiterung.

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

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

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

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

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. □

Beispiel 20.2. 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 20.1 zugehörigen Körperautomorphismen sind neben der Identität die Abbildungen φ_3, φ_5, φ_7, die auf den Einheitswurzeln (ζ sei eine primitive achte Einheitswurzel) folgendermaßen wirken.

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

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

und

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

Korollar 20.3. *Zu jeder endlichen abelschen Gruppe G gibt es eine endliche Galoiserweiterung $\mathbb{Q} \subseteq L$, deren Galoisgruppe gleich G ist.*

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

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

der zugehörige surjektive Restklassenhomomorphismus und H der Kern davon. Nach Satz 20.1 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 17.5 ist $\mathbb{Q} \subseteq M$ eine Galoiserweiterung mit Galoisgruppe G. □

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 20.4. 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_1M_2 bezeichnet.

Das Kompositum hängt vom Oberkörper ab. Wenn man von endlichen Körpererweiterungen $K \subseteq M_1$ und $K \subseteq M_2$ ausgeht, so sichert Aufgabe 10.11, dass es überhaupt einen gemeinsamen Oberkörper gibt.

LEMMA 20.5. *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 $K \subseteq L = K[x_1, \ldots, x_n]$ separabel, und seien $F_i \in K[X]$ die zu x_i gehörigen (separablen) Minimalpolynome. Dann ist $L' = K'[x_1, \ldots, x_n]$ und die Minimalpolynome G_i der x_i über K' sind in $K'[X]$ Teiler der F_i und daher selbst separabel. Nach Satz 13.11 ist $K' \subseteq L'$ eine separable Körpererweiterung. □

LEMMA 20.6. *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 $L = K[x_1, \ldots, x_n]$ 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 $L' = K'[x_1, \ldots, x_n]$ und dieselben Polynome, aufgefasst in $K'[X]$, erfüllen die gleichen Eigenschaften. Aus Satz 15.4 (3) ergibt sich die Normalität. □

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

SATZ 20.7. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung 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 Galoiserweiterung, und für ihre Galoisgruppe gilt die natürliche Isomorphie*

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

Beweis. Die Erweiterung $K' \subseteq L'$ ist normal nach Lemma 20.6 und separabel nach Lemma 20.5, also eine Galoiserweiterung aufgrund von Satz 16.6. Zur Berechnung der Galoisgruppe gehen wir von der Einschränkungsabbildung

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

aus, die wegen der Normalität von $K \subseteq L$ nach Satz 15.4 (4) ein wohldefinierter Gruppenhomomorphismus ist. Es sei $\varphi \in \mathrm{Gal}\,(L'|K')$ ein Automorphismus, dessen Bild unter diesem Homomorphismus trivial sei, also $\varphi|_L = \mathrm{Id}_L$. Da auch $\varphi|_{K'} = \mathrm{Id}_{K'}$ gilt, ist φ auf dem Kompositum $L' = LK'$ die Identität, also das neutrale Element. Daher ist Ψ nach dem Kernkriterium injektiv. Das Bild von Ψ ist eine Untergruppe $H = \mathrm{bild}\,\Psi \subseteq \mathrm{Gal}\,(L|K)$.

Aufgrund der Galoiskorrespondenz gibt es einen Zwischenkörper Z, $K \subseteq Z \subseteq L$, mit $H = \mathrm{Gal}\,(L|Z)$, und zwar ist Z der Fixkörper von H. Es liegt also insgesamt die Situation

$$\mathrm{Gal}\,(L'|K') \xrightarrow{\cong} \mathrm{bild}\,\Psi = H = \mathrm{Gal}\,(L|Z) \subseteq \mathrm{Gal}\,(L|K)$$

vor. Wir behaupten $L \cap K' = Z$. Für jedes $\varphi \in \mathrm{Gal}\,(L'|K')$ ist $\varphi|_{K'} = \mathrm{Id}_{K'}$, und daher ist auch $(\varphi|_L)|_{L\cap K'} = \mathrm{Id}_{L\cap K'}$. Also ist $L \cap K' \subseteq Z$. Wenn $x \in Z$ ist, so bedeutet dies, dass für jedes $\varphi \in \mathrm{Gal}\,(L'|K')$ die Gleichheit $(\varphi|_L)(x) = x$ gilt. Dann ist aber $x \in K'$ nach Satz 16.6, da $K' \subseteq L'$ eine Galoiserweiterung ist. Somit ist $x \in L \cap K'$. Insgesamt ist also

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

□

Abbildungsverzeichnis