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

Körper- und Galoistheorie

Vorlesung 16

Die Galoiskorrespondenz

Der folgende Satz heißt auch *Hauptsatz der Galoistheorie* oder *Satz über die Galoiskorrespondenz*. Er stiftet eine unmittelbare Beziehung zwischen den Zwischenkörpern einer endlichen Galoiserweiterung und Untergruppen der Galoisgruppe. Er bildet die Grundlage dafür, gruppentheoretische Aussagen auf Körpererweiterungen anzuwenden.

Satz 16.1. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit der Galoisgruppe $G = \mathrm{Gal}\,(L|K)$. Dann sind die Zuordnungen*

$$M \longmapsto \mathrm{Gal}\,(L|M) \text{ und } H \longmapsto \mathrm{Fix}\,(H)$$

zueinander inverse Abbildungen zwischen der Menge der Zwischenkörper M, $K \subseteq M \subseteq L$, und der Menge der Untergruppen von G. Bei dieser Korrespondenz werden die Inklusionen umgekehrt.

Beweis. Diese Abbildungen sind wohldefiniert und kehren nach Lemma 15.2 die Inklusion um. Sei M ein Zwischenkörper. Nach Korollar 15.7 ist $M \subseteq L$ eine Galoiserweiterung, also ist $\mathrm{Fix}\,(\mathrm{Gal}\,(L|M)) = M$ nach Satz 15.6. Sei nun H vorgegeben mit dem Fixkörper $M = \mathrm{Fix}\,(H)$. Nach dem Satz von Artin ist $M \subseteq L$ eine Galoiserweiterung mit Galoisgruppe $H = \mathrm{Gal}\,(L|M)$. □

Für einen Automorphismus $\varphi \in \mathrm{Gal}\,(L|K)$ und einen Zwischenkörper M, $K \subseteq M \subseteq L$, ist $M' = \varphi(M)$ wieder ein Zwischenkörper, der zu M K-isomorph ist. Zwischen den zugehörigen Galoisgruppen $\mathrm{Gal}\,(L|M)$ und $\mathrm{Gal}\,(L|M')$ gilt die folgende Beziehung.

Satz 16.2. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Es sei $\psi \in G = \mathrm{Gal}\,(L|K)$ und $M' = \psi(M)$. Dann gilt in der Galoisgruppe G die Beziehung*

$$\mathrm{Gal}\,(L|M') \;=\; \psi\,\mathrm{Gal}\,(L|M)\psi^{-1}.$$

Beweis. Sei $\varphi \in \mathrm{Gal}\,(L|M')$. Wir schreiben $\varphi = \psi(\psi^{-1}\varphi\psi)\psi^{-1}$ und müssen zeigen, dass $\psi^{-1}\varphi\psi$ zu $\mathrm{Gal}\,(L|M)$ gehört. Sei dazu $x \in M$. Dann ist

$$(\psi^{-1}\varphi\psi)(x) \;=\; \psi^{-1}(\varphi(\psi(x))).$$

Dabei gehört $\psi(x) \in M'$ und somit ist $\varphi(\psi(x)) = \psi(x)$. Also ist

$$\psi^{-1}(\varphi(\psi(x))) \;=\; \psi^{-1}(\psi(x)) \;=\; x.$$

Die umgekehrte Inklusion ergibt sich genauso bzw. folgt direkt daraus, dass beide Gruppen die gleiche Anzahl besitzen. □

Korollar 16.3. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und sei M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann sind folgende Aussagen äquivalent.*

(1) *Für alle $\psi \in \mathrm{Gal}\,(L|K)$ ist $\psi(M) = M$.*
(2) *Die Untergruppe $\mathrm{Gal}\,(L|M) \subseteq \mathrm{Gal}\,(L|K)$ ist nur zu sich selbst konjugiert.*

Beweis. Siehe Aufgabe 16.12. □

Wir wissen bereits, dass bei einer Galoiserweiterung $K \subseteq L$ und einen Zwischenkörper $K \subseteq M \subseteq L$ auch die hintere Erweiterung $M \subseteq L$ galoissch ist. Die Erweiterung $K \subseteq M$ muss hingegen nicht galoisch sein, vielmehr liefert die folgende Aussage ein Kriterium.

Satz 16.4. *Es sei $K \subseteq L$ eine endliche Galoiserweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann gelten folgende Aussagen.*

(1) *Die Körpererweiterung $K \subseteq M$ ist genau dann eine Galoiserweiterung, wenn die Untergruppe $\mathrm{Gal}\,(L|M) \subseteq \mathrm{Gal}\,(L|K)$ ein Normalteiler ist.*
(2) *Sei $K \subseteq M$ eine Galoiserweiterung. Dann besteht zwischen den Galoisgruppen die natürliche Restklassenbeziehung*

$$\mathrm{Gal}\,(M|K) \;=\; \mathrm{Gal}\,(L|K)/\,\mathrm{Gal}\,(L|M).$$

Bei dieser Zuordnung wird ein Automorphismus $\varphi \in \mathrm{Gal}\,(L|K)$ auf M eingeschränkt.

Beweis. (1). Da die Körpererweiterung $K \subseteq M$ separabel ist, muss aufgrund von Satz 15.6 nur die Normalität betrachtet werden. Nach Satz 14.3 ist die Körpererweiterung $K \subseteq M$ genau dann normal, wenn jeder K-Automorphismus von L den Unterkörper M in sich selbst überführt. Dies ist wegen Korollar 16.3 genau dann der Fall, wenn $\mathrm{Gal}\,(L|M)$ unter jeder Konjugation auf sich selbst abgebildet wird, also ein Normalteiler ist. (2). Sei nun $K \subseteq M$ normal. Dann ist $\varphi(M) = M$ für jedes $\varphi \in \mathrm{Gal}\,(L|K)$ und somit gibt es eine natürliche Abbildung

$$\mathrm{Gal}\,(L|K) \longrightarrow \mathrm{Gal}\,(M|K),\ \varphi \longmapsto \varphi|_M.$$

Diese ist offensichtlich ein Gruppenhomomorphismus. Aufgrund von Satz 14.3 gibt es für einen Automorphismus $\psi \in \mathrm{Gal}\,(M|K)$ eine Fortsetzung zu einem Automorphismus $\tilde{\psi} \in \mathrm{Gal}\,(L|K)$. Daher ist der Gruppenhomomorphismus surjektiv. Der Kern davon ist offenbar $\mathrm{Gal}\,(L|M)$, so dass sich die behauptete Isomorphie aus Korollar 5.10 ergibt. □

Beispiele zur Galoiskorrespondenz

Die zuletzt genannte Aussage ist natürlich im Fall, dass eine Galoiserweiterung mit abelscher Galoisgruppe vorliegt, unmittelbar anwendbar. In dieser Situation ist also jeder Zwischenkörper über dem Grundkörper galoissch.

Beispiel 16.5. Es sei $\mathbb{F}_p \subseteq \mathbb{F}_q$ mit $q = p^n$ eine Körpererweiterung endlicher Körper. Nach Satz 15.10 ist dies eine Galoiserweiterung mit zyklischer Galoisgruppe der Ordnung m, die vom Frobenius-Homomorphismus Φ erzeugt wird. Die Galoisgruppe ist also isomorph zu $\mathbb{Z}/(n)$. Die Untergruppen von $\mathbb{Z}/(n)$ sind von der Form

$$H = \langle m \rangle = \{0, m, 2m, \ldots, (k-1)m\}$$

mit einem Teiler m von n, wobei $k = \frac{n}{m}$ die Ordnung der Untergruppe ist. Der zugehörige Fixkörper ist der Fixkörper zu Φ^m, der nach Korollar 15.11 isomorph zu $\mathbb{F}_{p^m}$ ist, und H ist die Galoisgruppe von $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$.

Zu jeder Untergruppe $H = \langle m \rangle$ gibt es die Restklassenabbildung

$$\mathbb{Z}/(n) \longrightarrow (\mathbb{Z}/(n))/H \cong \mathbb{Z}/(m).$$

Gemäß Satz 16.4 ist die Restklassengruppe dabei die Galoisgruppe von $\mathbb{F}_p \subseteq \mathbb{F}_{p^m}$, und der Frobenius Φ von $\mathbb{F}_{p^n}$ wird dabei auf den Frobenius von $\mathbb{F}_{p^m}$ eingeschränkt.

Insbesondere hängen die Anzahl und die Inklusionsbeziehungen der Zwischenkörper von $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ nur von n und nicht von der Primzahl ab.

Proposition 16.6. *Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Der Körper K enthalte eine m-te primitive Einheitswurzel, wobei m der Exponent von D sei. Dann ist jeder Zwischenkörper M, $K \subseteq M \subseteq L$, von der Form $M = \bigoplus_{d \in E} L_d$ mit einer eindeutig bestimmten Untergruppe $E \subseteq D$.*

Beweis. Die Körpererweiterung $K \subseteq L$ ist nach Satz 13.9 eine Galoiserweiterung mit Galoisgruppe $G = \mathrm{Char}\,(D, K)$. Da K hinreichend viele Einheitswurzeln besitzt, entsprechen sich die Untergruppen von D und von G über die Charakter-Korrespondenz

$$E \longmapsto E^\perp = \{\chi \in G |\, \chi(d) = 1 \text{ für alle } d \in E\}$$

und

$$H \longmapsto H^\perp = \{d \in D |\, \chi(d) = 1 \text{ für alle } \chi \in H\}\,.$$

Zu jeder Untergruppe $E \subseteq D$ ist $\bigoplus_{d \in E} L_d$ ein Zwischenkörper. Da wegen der Galoiskorrespondenz die Anzahl der Zwischenkörper mit der Anzahl der Untergruppen der Galoisgruppe, und diese mit der Anzahl der Untergruppen in D übereinstimmt, ist jeder Zwischenkörper graduiert. □

Zu einer Untergruppe $H \subseteq G$ ist dabei

$$\mathrm{Fix}\,(H) \;=\; \bigoplus_{d \in H^\perp} L_d,$$

und zu einem Unterkörper $M = L_E = \bigoplus_{d \in E} L_d$ ist

$$\mathrm{Gal}\,(L|M) \;=\; E^\perp \;=\; \{\chi \in D^\vee |\, \chi(d) = 1 \text{ für alle } d \in E\}.$$

Die Galoisgruppe von $M = L_E$ über K ist gleich

$$\mathrm{Gal}\,(M|K) \;=\; E^\vee \;=\; D^\vee / E^\perp.$$

Die bijektive Beziehung zwischen Zwischenkörpern und Untergruppen der graduierenden Gruppe im Galoisfall wird manchmal auch als *Kogaloiskorrespondenz* bezeichnet. Bei ihr werden Inklusionen erhalten und drehen sich nicht wie bei der Galoiskorrespondenz um (bei der Bijektion zwischen Untergruppen und ihrem Charakterdual drehen sich die Inklusionen um).

Beispiel 16.7. Wir knüpfen an Beispiel 9.14 an. Aufgrund von Satz 13.9 liegt eine Galoiserweiterung vor. Die graduierende Gruppe ist $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Neben der trivialen Untergruppe und D selbst gibt es noch die drei Untergruppen $\{(0,0),(1,0)\}$, $\{(0,0),(0,1)\}$, $\{(0,0),(1,1)\}$, die den Zwischenkörpern

$$\mathbb{Q},\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{6}),\ L$$

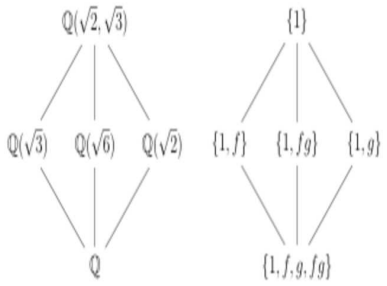
entsprechen. Wegen Proposition 16.6 gibt es keine weiteren Zwischenkörper. Die Galoisgruppe ist $G = D^\vee \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Zur Untergruppe $E = \{(0,0),(1,0)\} \subseteq D$ gehört dabei $E^\perp$ (das der Galoisgruppe $\mathrm{Gal}\,(E|L_E)$ entspricht), das aus dem konstanten Charakter und der Abbildung

$$\chi : D \longrightarrow \mathbb{Q}^\times$$

besteht, die E auf 1 und $D \setminus E$ auf -1 abbildet. Dazu gehört wiederum der durch

$$1 \longmapsto 1,\ \sqrt{2} \longmapsto \sqrt{2},\ \sqrt{3} \longmapsto -\sqrt{3},\ \sqrt{6} \longmapsto -\sqrt{6}$$

festgelegte $\mathbb{Q}$-Automorphismus φ.



Beispiel 16.8. Wir betrachten die $\mathbb{Z}/(6)$-graduierte Körpererweiterung

$$\mathbb{Q} \subseteq L = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}] = \mathbb{Q}[\sqrt[6]{-108}] = \mathbb{Q}[X]/(X^6 + 108)\,.$$

Die Graduierung ist durch $L_i = \mathbb{Q} \cdot x^i$ mit $x = \sqrt[6]{-108} = \sqrt[3]{2} \cdot \sqrt{-3}$ gegeben. Es ist $\sqrt{-3} = -\frac{1}{6}x^3$ und $\sqrt[3]{2} = \frac{1}{18}x^4$. Da es in $\mathbb{Q}$ keine primitive dritte Einheitswurzel gibt, ist $\mathrm{Char}\,(\mathbb{Z}/(6), \mathbb{Q}^\times) \cong \mathbb{Z}/(2)$ und daher gibt es nur zwei homogene Automorphismen (somit ist dies auch keine Kummererweiterung.[1]) Dennoch handelt es sich um eine Galoiserweiterung. Zunächst gehört

$$\zeta_3 = \frac{-1+\sqrt{-3}}{2} = \frac{-6-x^3}{12}$$

zu L, und es ist $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3}) = L_0 \oplus L_3$. Ein weiterer (mit der Graduierung verträglicher) Zwischenkörper ist $\mathbb{Q}(\sqrt[3]{2}) = L_0 \oplus L_2 \oplus L_4$. Die durch $x^i \mapsto (-1)^i x^i$ gegebene Abbildung ist ein homogener Automorphismus φ mit $\varphi^2 = \mathrm{id}$. Aber auch die Zuordnung $x^i \mapsto (\zeta_3)^i x^i$ definiert einen (nichthomogenen) Automorphismus ψ mit $\psi^3 = \mathrm{id}$. Es gibt also insgesamt 6 Automorphismen und daher liegt eine Galoiserweiterung vor. Dabei ist

$$(\varphi \circ \psi)(x) = \varphi(\psi(x)) = \varphi(\zeta_3 x) = \varphi(\frac{-6x-x^4}{12}) = \frac{6x-x^4}{12}$$

und

$$(\psi \circ \varphi)(x) = \psi(\varphi(x)) = \psi(-x) = -\psi(x) = -\frac{-6x-x^4}{12} = \frac{6x+x^4}{12}.$$

Daher ist die Galoisgruppe nicht kommutativ, und es muss $\mathrm{Gal}\,(L|\mathbb{Q}) = S_3$ sein.

[1] Siehe die nächste Vorlesung.

Abbildungsverzeichnis