15.7 Definition einer Galoiserweiterung

Definition. Sei L eine endliche Körpererweiterung eines Körpers K, und sei $G := G(L/K)$ die Galoisgruppe von L über K. Dann ist $|G|$ ein Teiler von $[L : K]$ nach 15.6, und L heißt *Galoiserweiterung von K* oder *galoissch über K*, falls $|G| = [L : K]$ gilt.

Beispiel. $\mathbb{C}$ ist galoissch über $\mathbb{R}$, denn $|G(\mathbb{C}/\mathbb{R})| = 2$ nach 15.5, und es ist $[\mathbb{C} : \mathbb{R}] = 2$, da $\{1, i\}$ eine Basis von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum ist.

15.8 Charakterisierung von Galoiserweiterungen

Definition. Eine Körpererweiterung L von K heißt *separabel*, wenn jedes Element aus L separabel über K ist (vgl. 13.5).
Ein Polynom $f \in K[X]$ heißt *separabel*, wenn jeder irreduzible Faktor von f keine mehrfachen Nullstellen im Zerfällungskörper von f besitzt.

Satz.
Für eine endliche Körpererweiterung L eines Körpers K sind äquivalent:

(1) *L ist galoissch über K.*

(2) $L^{G(L/K)} = K$.

(3) *L ist normal und separabel.*

(4) *L ist Zerfällungskörper eines separablen Polynoms aus $K[X]$.*

Beweis. (1) $\Leftrightarrow$ (2) wurde in 15.6 gezeigt.

(2) $\Rightarrow$ (3) Nach 15.2 ist jedes $x \in L$ separabel über $L^{G(L/K)} = K$. Also ist L separabel über K. Sei $p \in K[X]$ irreduzibel, und sei $x \in L$ eine Nullstelle von p. Dann ist $p = cm_x$ mit einem $c \in K^*$ nach 11.9. Aus 15.2 folgt nun, dass p in Linearfaktoren in $L[X]$ zerfällt. Also ist L normal nach 13.3.

(3) $\Rightarrow$ (4) Da L über K normal ist, ist L Zerfällungskörper eines Polynoms $f \in K[X]$ nach 13.3. Da L separabel über K ist, ist f separabel (denn jeder normierte irreduzible Faktor von f ist Minimalpolynom aller seiner Nullstellen).

(4) $\Rightarrow$ (2) Sei $G := G(L/K)$, und sei L Zerfällungskörper eines separablen Polynoms $f \in K[X]$. Es gilt $K \subset L^G \subset L$.
Zeige: $L^G \subset K$ durch Induktion nach der Anzahl n der nicht in K liegenden Nullstellen von f. Ist $n = 0$, so ist $K = L^G = L$.

Sei nun $x \in L \setminus K$ eine Nullstelle von f. Das Minimalpolynom m_x ist ein irreduzibler Faktor von f, hat also lauter verschiedene Nullstellen $x, x_2, \ldots, x_r \in L$. Es folgt $r = \operatorname{grad}(m_x) = [K(x) : K] > 1$ nach 11.10. Nach Korollar 13.1 gibt es zu jedem $i = 2, \ldots, r$ einen K-Isomorphismus $\psi_i \colon K(x) \to K(x_i)$ mit $\psi_i(x) = x_i$, und nach 13.2 gibt es dazu jeweils ein $\sigma_i \in G$ mit $\sigma_i(x) = x_i$. Es ist $G(L/K(x)) \subset G$, also $L^G \subset L^{G(L/K(x))} \subset K(x)$ nach Induktionsvoraussetzung (denn betrachtet man f als Polynom in $K(x)[X]$, so bleibt f separabel und L ist Zerfällungskörper von f).
Sei nun $y \in L^G$. Zu zeigen: $y \in K$. Es ist $y = \lambda_0 + \lambda_1 x + \cdots + \lambda_{r-1} x^{r-1}$ mit $\lambda_0, \ldots, \lambda_{r-1} \in K$ nach 11.10, da $y \in L^G \subset K(x)$ ist. Es folgt
$y = \sigma_2(y) = \lambda_0 + \lambda_1 x_2 + \cdots + \lambda_{r-1} x_2^{r-1}$, $\ldots$,
$y = \sigma_r(y) = \lambda_0 + \lambda_1 x_r + \cdots + \lambda_{r-1} x_r^{r-1}$.
Also hat $h := y - (\lambda_0 + \lambda_1 X + \cdots + \lambda_{r-1} X^{r-1}) \in L^G[X]$ die r verschiedenen Nullstellen $x, x_2, \ldots, x_r$ und ist vom Grad $< r$. Es folgt $h = 0$, also $y - \lambda_0 = 0$ und $\lambda_i = 0$ für $i = 1, \ldots, r-1$. Dies ergibt $y = \lambda_0 \in K$.

□

15.9 Einbettung in eine Galoiserweiterung

Satz. *Jede endliche separable Körpererweiterung von K lässt sich in eine Galoiserweiterung von K einbetten.*

Beweis. Sei L endlich-separabel über K. Dann ist $L = K(u)$ mit einem separablen $u \in L$ (vgl. Korollar 13.5), und nach 15.8 ist der Zerfällungskörper des Minimalpolynoms m_u galoissch über K. □

Lernerfolgstest.
- Sei $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Bestimmen Sie das Minimalpolynom m_x in $Q[X]$ von $x := \sqrt{2} + \sqrt{3}$ mit der in 15.3 benutzten Methode.
- Verifizieren Sie, dass im Beweis in 15.5 tatsächlich $\sigma = \mathrm{id}$ folgt.
- Jedes $x \in K$ ist Nullstelle eines irreduziblen Polynoms $p \in K[X]$. Wie sieht p aus?

15.10 Übungsaufgaben 70 – 71

Aufgabe 70. Man bestimme die Galoisgruppe $G(L/\mathbb{Q})$ für

$$L = \mathbb{Q}(\sqrt{2}\,, \sqrt{3}\,, \sqrt{5}) \text{ und } L = \mathbb{Q}(\sqrt[3]{2})\,.$$

Aufgabe 71. Für $a \in \mathbb{Q}$ sei L_a der Zerfällungskörper des Polynoms $X^3 - a$. Man bestimme die Galoisgruppe $G(L_a/\mathbb{Q})$ in Abhängigkeit von a.

16 Hauptsatz der Galoistheorie

Lernziel.
Fertigkeiten: In gewissen Fällen Schlüsse aus dem Hauptsatz ziehen
Kenntnisse: Hauptsatz mit Anwendungen für zyklische Erweiterungen und endliche Körper

16.1 Hauptsatz

Definition. Sei K ein Körper, und sei L eine endliche Körpererweiterung von K. Ein *Zwischenkörper* Z ist ein Teilkörper von L mit $K \subset Z \subset L$.

Wenn L galoissch über K ist, liefert der Hauptsatz eine Übersicht über alle Zwischenkörper: Diese entsprechen eineindeutig den Untergruppen der Galoisgruppe $G(L/K) := \mathrm{Aut}_K L$.

Hauptsatz.
Sei L eine Galoiserweiterung eines Körpers K, und sei $G := G(L/K)$ die Galoisgruppe von L über K. Dann ist L galoissch über jedem Zwischenkörper, und man hat eine Bijektion von Mengen

$$\{\textit{Zwischenkörper}\} \xrightarrow{\sim} \{\textit{Untergruppen von } G\},$$
$$Z \longmapsto G(L/Z) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(z) = z \ \textit{ für alle } \ z \in Z\}$$

mit Umkehrabbildung

$$\{\textit{Untergruppen von } G\} \xrightarrow{\sim} \{\textit{Zwischenkörper}\},$$
$$H \longmapsto L^H := \{z \in L \mid \sigma(z) = z \ \textit{ für alle } \ \sigma \in H\}$$

Dabei gelten

(1) $\quad [Z : K] = \dfrac{|G|}{|G(L/Z)|}$

(2) $\quad Z \subset Z' \Longrightarrow G(L/Z') \subset G(L/Z) \quad \textit{und} \quad H \subset H' \Longrightarrow L^{H'} \subset L^H\,.$

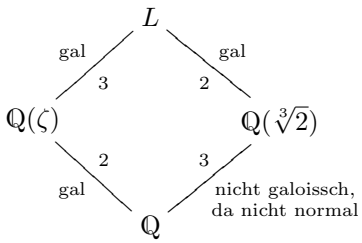
Beweis. Da L galoissch über K ist, ist L Zerfällungskörper eines separablen Polynoms aus $K[X] \subset Z[X]$. Also ist L Zerfällungskörper eines separablen Polynoms aus $Z[X]$, und daher ist L galoissch über Z (vgl.15.8). Zeige nun, dass die Abbildungen $Z \overset{\varphi}{\longmapsto} G(L/Z)$ und $H \overset{\psi}{\longmapsto} L^H$ invers zueinander sind. Es ist $\psi(\varphi(Z)) = L^{G(L/Z)} = Z$ nach 15.8.2, da L galoissch über Z. Weiter gilt $\varphi(\psi(H)) = G(L/L^H) = H$, denn es ist $H \subset G(L/L^H)$, und da L galoissch über L^H ist, gilt $|H| = [L : L^H] = |G(L/L^H)|$ nach 15.4 und 15.7. Es ist $|G| \underset{15.7}{=} [L : K] \underset{11.7}{=} [L : Z][Z : K] \underset{15.7}{=} |G(L/Z)| \cdot [Z : K]$. Hieraus folgt (1), und (2) ist klar nach Definition. □

16.2 Beispiel

Sei $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ mit $\zeta^2 + \zeta + 1 = 0$ und $\zeta^3 = 1$. Dann ist $[L : \mathbb{Q}] = 6$ nach 11.11, und L ist Zerfällungskörper von $f = X^3 - 2 \in \mathbb{Q}[X]$, denn

$$X^3 - 2 = (X - \sqrt[3]{2}) \cdot (X - \zeta\sqrt[3]{2}) \cdot (X - \zeta^2\sqrt[3]{2}) .$$

Also ist L galoissch über $\mathbb{Q}$ nach 15.8, und es folgt $|G(L/\mathbb{Q})| = 6$ nach Definition 15.7. Dies ergibt $G(L/\mathbb{Q}) \simeq S_3$ nach 15.5. Betrachte



Setze $\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$ und $\sigma(\zeta) = \zeta$. Dann ist $\sigma^2(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}$ und $\sigma^3 = \mathrm{id}$. Es folgt $G(L/\mathbb{Q}(\zeta)) = \{\mathrm{id}, \sigma, \sigma^2\}$.

16.3 Wann ist ein Zwischenkörper galoissch über K?

Seien $K \subset Z \subset L$ endliche Körpererweiterungen, wobei L galoissch über K sei. Dann ist L galoissch über Z nach 16.1, aber Z ist im Allgemeinen nicht galoissch über K. Sei $G := G(L/K)$ die Galoisgruppe von L über K.

Lemma. *Für jedes $\sigma \in G$ ist $\sigma(Z) := \{\sigma(z) \mid z \in Z\}$ ein Zwischenkörper, und es gilt $G(L/\sigma(Z)) = \sigma G(L/Z)\sigma^{-1}$ für alle $\sigma \in G$.*

Beweis. Für $\sigma, \tau \in G$ gilt

$$\begin{aligned} \tau \in G(L/\sigma(Z)) &\iff \tau(\sigma(z)) = \sigma(z)\ \forall z \in Z \\ &\iff \sigma^{-1} \circ \tau \circ \sigma \in G(L/Z) \\ &\iff \tau \in \sigma G(L/Z)\sigma^{-1} \end{aligned}$$

□

Satz. *Äquivalent sind*

(a) *Z ist galoissch über K.*

(b) *$\sigma(Z) = Z$ für alle $\sigma \in G$.*

(c) *$G(L/Z)$ ist Normalteiler in G.*