§11 Galois–Erweiterungen

(11.1) DEF: Eine endliche Körpererweiterung $L : K$ heißt eine **Galois–Erweiterung (GE)**, wenn gilt:

$$|\operatorname{Gal}(L:K)| \;=\; [\,L:K\,]\,.$$

Beispiele: $\mathbb{C} : \mathbb{R}$ ist eine Galois–Erweiterung (10.13b)
$\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ ist **keine** Galois–Erweiterung (10.13a)
$\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}$ ist eine Galois–Erweiterung (s. Aufgabe 38b)) .

Ziel: Bei einer Galois–Erweiterung lassen sich alle Zwischenkörper mit Hilfe der Untergruppen der Galois–Gruppe bestimmen. Genauer: Es gibt eine bijektive Korrespondenz zwischen den Zwischenkörpern einer Galois–Erweiterung und den Untergruppen der Galois–Gruppe .

Sei $L : K$ eine Körpererweiterung mit der Galois–Gruppe $G := \operatorname{Gal}(L : K)$.
Für jedes $\sigma \in G$ ist dann $\operatorname{Fix}(\sigma) = \{\alpha \mid \alpha \in L\,,\, \sigma(\alpha) = \alpha\}$ ein Zwischenkörper von $L : K$ (10.5b) . Für eine Untergruppe $U \leq G$ ist daher

$$L^U := \bigcap_{\sigma\in U} \operatorname{Fix}(\sigma)\,.$$

ein Zwischenkörper von $L : K$. Es ist

$$K \subseteq L^U \;=\; \{\alpha \mid \alpha \in L\,,\, \forall\, \sigma \in U \,:\, \sigma(\alpha) = \alpha\,\} \subseteq L$$

d.h. jede Untergruppe $U \leq G$ liefert einen Zwischenkörper L^U von $L : K$.
Ist umgekehrt E ein Zwischenkörper von $L : K$, so ist

$$\operatorname{Gal}(L : E) \leq \operatorname{Gal}(L : K) = G$$

eine Untergruppe von $\operatorname{Gal}(L : K)$. Zusammenfassend gilt:

(11.2) SATZ: $L : K$ sei eine Körpererweiterung mit der Galois–Gruppe $G := \operatorname{Gal}(L : K)$. Dann gilt:

a) Für jede Untergruppe $U \leq G$ ist $L^U = \{\alpha \mid \alpha \in L\,,\, \forall\, \sigma \in U \,:\, \sigma(\alpha) = \alpha\,\}$ ein Zwischenkörper von $L : K$, der sog. **Fixkörper von** U .

b) Für jeden Zwischenkörper E von $L : K$ ist $\operatorname{Gal}(L : E)$ eine Untergruppe von G .

$$\begin{array}{ccc} K \subseteq E \subseteq L & \qquad & U \leq G \\ \downarrow & & \downarrow \\ \operatorname{Gal}(L:E) \leq G & & K \subseteq L^U \subseteq L \end{array}$$

(11.3) LEMMA: L sei ein Körper und U eine endliche Untergruppe der Gruppe $(\mathrm{Aut}(L), \circ)$ aller Körperautomorphismen von L. Die Abbildung $\mathrm{spur}_U : L \longrightarrow L$ sei definiert durch

$$\mathrm{spur}_U(\alpha) := \sum_{\sigma \in U} \sigma(\alpha) \quad (\forall\, \alpha \in L)$$

(spur_U heißt die **Spur–Abbildung von** L **bzgl.** U). Dann gilt:

a) $\forall\, \alpha, \beta \in L \,:\, \mathrm{spur}_U(\alpha + \beta) = \mathrm{spur}_U(\alpha) + \mathrm{spur}_U(\beta)$

b) $\forall\, \tau \in U : \tau \circ \mathrm{spur}_U = \mathrm{spur}_U$.

c) $\mathrm{spur}_U \neq 0$.

(11.4) SATZ: $L : K$ sei eine Körpererweiterung, und $U \leq \mathrm{Gal}(L : K)$ sei eine endliche Untergruppe. Dann gilt:

$$[L : L^U] \;=\; |\,U\,|$$

(11.5) KOROLLAR: $L : K$ sei eine endliche Körpererweiterung und $U \leq G := \mathrm{Gal}(L : K)$ eine beliebige Untergruppe. Dann gilt:

a) $L : L^U$ ist eine Galois–Erweiterung .

b) $\mathrm{Gal}(L : L^U) = U$.

(11.6) KOROLLAR: $L : K$ sei eine endliche Körpererweiterung und $G := \mathrm{Gal}(L : K)$ die Galois–Gruppe. Dann gilt:

a) $U \leq G \implies [L : K] = |U| \cdot [L^U : K]$

b) $[L : K] = |G| \cdot [L^G : K]$ (d.h. insbesondere, daß $|G|$ ein Teiler von $[L : K]$ ist).

(11.7) SATZ: $L : K$ sei eine Körpererweiterung und $G := \mathrm{Gal}(L : K)$ die Galois–Gruppe . Dann sind folgende Aussagen äquivalent:

a) $L : K$ ist eine Galois–Erweiterung

b) $L : K$ ist endlich, und es gilt $L^G = K$.

(11.8) SATZ: $L : K$ sei eine Körpererweiterung und E ein Zwischenkörper von $L : K$. Dann gilt:

a) Ist $L : K$ eine Galois–Erweiterung , so ist auch $L : E$ eine Galois–Erweiterung

b) Ist $L : K$ eine Galois–Erweiterung , so ist $E : K$ i.a. **keine** Galois–Erweiterung

c) Sind $L : E$ und $E : K$ Galois–Erweiterungen, so ist $L : K$ i.a. **keine** Galois–Erweiterung .

(11.9) KOROLLAR: $L : K$ sei eine Galois–Erweiterung mit der Galois–Gruppe G , E ein Zwischenkörper von $L : K$ und $H := \mathrm{Gal}(L : E)$. Dann gilt

$$|\,\mathrm{H}_K(E, L)| \;=\; [E : K] \;=\; (G : H)\,,$$

wobei $\mathrm{H}_K(E, L)$ die Menge aller K–Homomorphismen von E in L bezeichnet und $(G : H)$ den Index von H in G .