

## Kap. III    Galois–Theorie

### §10 Die Galois-Gruppe einer Körpererweiterung

**(10.1) LEMMA:**  $L : K$  und  $L' : K$  seien Körpererweiterungen. Für einen Körperhomomorphismus  $\sigma : L \longrightarrow L'$  sind folgende Aussagen äquivalent:

- a)  $\sigma$  ist  $K$ –linear                      b)  $\sigma(a) = a \quad \forall a \in K$ .

**(10.2) DEF:**  $L : K$  und  $L' : K$  seien Körpererweiterungen.

a) Ein Körperhomomorphismus  $\sigma : L \longrightarrow L'$  heißt ein  $K$ –**Homomorphismus**, wenn  $\sigma(a) = a$  für alle  $a \in K$  gilt. Es bezeichne  $H_K(L, L')$  die Menge aller  $K$ –Homomorphismen von  $L$  nach  $L'$ .

b) Ein bijektiver  $K$ –Homomorphismus  $\sigma : L \longrightarrow L$  heißt ein  $K$ –**Automorphismus von  $L$** .

**(10.3) SATZ:**  $L : K$  sei eine Körpererweiterung. Dann bildet die Menge

$$\text{Gal}(L : K) := \{\sigma \mid \sigma : L \longrightarrow L \text{ } K\text{–Automorphismus}\}$$

aller  $K$ –Automorphismen von  $L$  eine Gruppe bzgl. der Hintereinanderausführung.

$(\text{Gal}(L : K), \circ)$  heißt die **Galois–Gruppe von  $L : K$** .

**(10.4) BEISPIELE:** a)  $\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \{\text{id}\}$ .

b)  $\text{Gal}(\mathbb{C} : \mathbb{R}) = \{\text{id}, k\} \quad (k : z \longmapsto \bar{z})$ .

**(10.5) LEMMA:**  $L : K$  sei eine Körpererweiterung und  $\sigma \in \text{Gal}(L : K)$ . Dann gilt:

a) Ist  $\alpha \in L$  Nullstelle eines Polynoms  $f \in K[T]$ , so ist auch  $\sigma(\alpha) \in L$  eine Nullstelle von  $f$ .

b)  $\text{Fix}(\sigma) := \{\beta \mid \beta \in L, \sigma(\beta) = \beta\}$  ist ein Zwischenkörper von  $L : K$ , der sog. **Fixkörper von  $\sigma$** .

**(10.6) SATZ:**  $L : K$  sei eine endliche einfache Körpererweiterung mit  $\alpha$  als primitivem Element.  $m_\alpha \in K[T]$  sei das Minimalpolynom von  $\alpha$  über  $K$ , und  $N$  sei die Menge aller Nullstellen von  $m_\alpha$ , die in  $L$  liegen. Dann ist die Abbildung

$$\omega : \text{Gal}(L : K) \longrightarrow N, \quad \sigma \longmapsto \sigma(\alpha)$$

bijektiv.

**(10.7) KOROLLAR:**  $L : K$  sei eine endliche einfache Körpererweiterung. Dann gilt:

$$|\text{Gal}(L : K)| \leq [L : K].$$

**Ziel:** Dieses Ergebnis gilt für alle endlichen Körpererweiterungen.

**(10.8) KOROLLAR:**  $L : K$  sei eine endliche einfache Körpererweiterung,  $L = K(\alpha)$ . Dann gilt:

- a)  $\sigma, \tau \in \text{Gal}(L : K) : \sigma = \tau \iff \sigma(\alpha) = \tau(\alpha)$   
 b) Zu je zwei Nullstellen  $\beta, \gamma \in L$  des Minimalpolynoms von  $\alpha$  über  $K$  existiert genau ein  $K$ -Automorphismus  $\sigma \in \text{Gal}(L : K)$  mit  $\sigma(\beta) = \gamma$ .

**(10.9) BEM:** Satz (10.6) liefert eine Methode zur Bestimmung der Galois-Gruppe einer endlichen einfachen Körpererweiterung  $L : K$ :

- a) Bestimme ein primitives Element  $\alpha$  von  $L : K$  ( $L = K(\alpha)$ )  
 b) Bestimme das Minimalpolynom  $m_\alpha$  von  $\alpha$  über  $K$  ( $r := \text{grad}(m_\alpha)$ )  
 c) Bestimme alle Nullstellen  $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_r$  von  $m_\alpha$  in  $L$   
 d) Durch die Zuordnung  $\alpha \mapsto \alpha_i$  ( $i = 1, 2, \dots, r$ ) sind alle  $K$ -Automorphismen von  $L$  eindeutig festgelegt

- e) Für  $\sigma \in \text{Gal}(L : K)$  mit  $\sigma(\alpha) = \beta \in \{\alpha_1, \alpha_2, \dots, \alpha_r\}$  und  $x = \sum_{l=0}^{r-1} a_l \alpha^l \in L$  ( $a_l \in K$ ) gilt

$$\sigma(x) = \sigma\left(\sum_{l=0}^{r-1} a_l \alpha^l\right) = \sum_{l=0}^{r-1} \sigma(a_l) \sigma(\alpha)^l = \sum_{l=0}^{r-1} a_l \beta^l$$

### **(10.10) UNABHÄNGIGKEITSSATZ**

$L$  und  $L'$  seien Körper. Sind  $\sigma_1, \dots, \sigma_n$  paarweise verschiedene Körperhomomorphismen von  $L$  in  $L'$ , so ist  $\{\sigma_1, \dots, \sigma_n\}$  eine linear unabhängige Teilmenge des  $L'$ -Vektorraumes  $\text{Abb}(L, L')$ .

**(10.11) SATZ:**  $L$  und  $L'$  seien Körper und  $\sigma_1, \dots, \sigma_n$  paarweise verschiedene Körperhomomorphismen von  $L$  in  $L'$ . Ferner sei

$$F := \{\alpha \mid \alpha \in L, \sigma_1(\alpha) = \sigma_2(\alpha) = \dots = \sigma_n(\alpha)\} \subseteq L$$

Dann gilt: a)  $F$  ist ein Unterkörper von  $L$  b)  $[L : F] \geq n$ .

**(10.12) SATZ:** Ist  $L : K$  eine endliche Körpererweiterung, so gilt  $|\text{Gal}(L : K)| \leq [L : K]$ .

**(10.13) BEISPIELE:** a)  $|\text{Gal}(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q})| = 1 < 3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ .

b)  $|\text{Gal}(\mathbb{C} : \mathbb{R})| = 2 = [\mathbb{C} : \mathbb{R}]$ .

Wir werden im folgenden gerade solche Körpererweiterungen  $L : K$  genauer untersuchen, für die  $|\text{Gal}(L : K)| = [L : K]$  gilt. Dies sind die sog. Galois-Erweiterungen.