

§12. Der Hauptsatz der GALOIS–Theorie

$L : K$ sei eine beliebige Körpererweiterung und $G := \text{Gal}(L : K)$ die Galois–Gruppe von $L : K$. Es bezeichne $\mathcal{Z} = \mathcal{Z}(L : K)$ die Menge aller Zwischenkörper von $L : K$ und $\mathcal{U} = \mathcal{U}(G)$ die Menge aller Untergruppen von G . Nach (11.2) gilt:

$$U \in \mathcal{U} \implies L^U \in \mathcal{Z} \quad \text{und} \quad E \in \mathcal{Z} \implies \text{Gal}(L : E) \in \mathcal{U}$$

Wir können daher die beiden folgenden Abbildungen definieren

(12.1) DEF:

$\begin{aligned} \varepsilon : \mathcal{U} &\longrightarrow \mathcal{Z} \quad , \quad U \longmapsto L^U \\ \eta : \mathcal{Z} &\longrightarrow \mathcal{U} \quad , \quad E \longmapsto \text{Gal}(L : E) \end{aligned}$

(12.2) LEMMA: Für eine beliebige Körpererweiterung $L : K$ gilt:

a) $\eta(\varepsilon(U)) \supseteq U \quad \forall U \in \mathcal{U}$

b) $\varepsilon(\eta(E)) \supseteq E \quad \forall E \in \mathcal{Z}$

Bew: **a)** $\eta(\varepsilon(U)) = \eta(L^U) = \text{Gal}(L : L^U)$

Sei $\sigma \in U$ beliebig. Dann ist $\sigma : L \longrightarrow L$ ein K –Automorphismus von L , für den $\sigma(\alpha) = \alpha$ für alle $\alpha \in L^U$ gilt, d.h. σ ist ein L^U –Homomorphismus von L . Also gilt $\sigma \in \text{Gal}(L : L^U)$.

b) $\varepsilon(\eta(E)) = \varepsilon(\text{Gal}(L : E)) = L^{\text{Gal}(L:E)}.$

Sei $\alpha \in E$ beliebig. Für alle $\sigma \in \text{Gal}(L : E)$ gilt dann $\sigma(\alpha) = \alpha$, d.h. $\alpha \in L^{\text{Gal}(L:E)}$. •

Ziel: Im Falle einer Galois–Erweiterung $L : K$ gilt in (12.2) in beiden Fällen die Gleichheit, d.h. die beiden Abbildungen ε und η sind zueinander invers und damit bijektiv.

(12.3) Der Hauptsatz der GALOIS–Theorie

$L : K$ sei eine Galois–Erweiterung, und $G := \text{Gal}(L : K)$ sei die Galois–Gruppe von $L : K$.

Teil I) Es bezeichne $\mathcal{Z} = \{E \mid K \subseteq E \subseteq L, E \text{ Zwischenkörper}\}$ die Menge aller Zwischenkörper von $L : K$ und $\mathcal{U} = \{U \mid U \leq G\}$ die Menge aller Untergruppen von G . Die Abbildungen

$$\varepsilon : \mathcal{U} \longrightarrow \mathcal{Z} \quad \text{und} \quad \eta : \mathcal{Z} \longrightarrow \mathcal{U}$$

seien definiert durch

$$\forall U \in \mathcal{U} : \varepsilon(U) := L^U = \{\alpha \mid \alpha \in L, \forall \sigma \in U : \sigma(\alpha) = \alpha\} \subseteq L \quad (\text{Fixkörper von } U)$$

$$\forall E \in \mathcal{Z} : \eta(E) := \text{Gal}(L : E) = \{\sigma \mid \sigma : L \longrightarrow L \text{ ist ein } E\text{–Automorphismus}\} \leq G.$$

Dann gelten die folgenden Aussagen:

- a) ε und η sind bijektiv und zueinander invers.
- b) $\forall U, V \in \mathcal{U} : U \subseteq V \iff \varepsilon(U) \supseteq \varepsilon(V)$
- c) $\forall E, F \in \mathcal{Z} : E \subseteq F \iff \eta(E) \supseteq \eta(F)$.

Teil II) Ist E ein Zwischenkörper von $L : K$, so gilt:

- a) $L : E$ ist eine Galois–Erweiterung.
- b) Folgende Aussagen sind äquivalent:
 - 1) $E : K$ ist eine Galois–Erweiterung.
 - 2) Es gilt $\sigma(E) = E$ für alle $\sigma \in G$
 - 3) $\text{Gal}(L : E)$ ist ein Normalteiler von G .
- c) Ist $E : K$ eine Galois–Erweiterung, so gibt es einen Gruppenisomorphismus

$$\text{Gal}(L : K) / \text{Gal}(L : E) \cong \text{Gal}(E : K)$$

Bemerkung: Durch den Hauptsatz der Galois–Theorie wird eine bijektive Korrespondenz zwischen den Zwischenkörpern einer Galois–Erweiterung und den Untergruppen der zugehörigen Galois–Gruppe hergestellt. Dadurch kann das Problem, alle Zwischenkörper einer Galois–Erweiterung zu bestimmen, auf das Problem zurückgeführt werden, alle Untergruppen der Galois–Gruppe zu bestimmen. Da die Galois–Gruppe einer endlichen Körpererweiterung immer eine endliche Gruppe ist, ist dieses letzte Problem häufig viel einfacher zu lösen, zumal die Theorie der endlichen Gruppen sehr weit ausgebaut ist.