

Beweis des Hauptsatzes der GALOIS–Theorie

Beweis von Teil I):

a) Gezeigt wird: $\eta \circ \varepsilon = \text{id}_{\mathcal{U}}$ und $\varepsilon \circ \eta = \text{id}_{\mathcal{Z}}$

Für alle $U \in \mathcal{U}$ gilt: $(\eta \circ \varepsilon)(U) = \text{Gal}(L : L^U) \stackrel{(11.5)}{=} U = \text{id}_{\mathcal{U}}(U) \implies \eta \circ \varepsilon = \text{id}_{\mathcal{U}}$.

Für alle $E \in \mathcal{Z}$ gilt: $(\varepsilon \circ \eta)(E) = L^{\text{Gal}(L:E)} \stackrel{(11.7)}{=} E = \text{id}_{\mathcal{Z}}(E) \implies \varepsilon \circ \eta = \text{id}_{\mathcal{Z}}$.

b) “ $\implies$ “

$U \subseteq V \implies \varepsilon(V) = L^V \subseteq L^U = \varepsilon(U)$; denn

$\alpha \in L^V \implies \sigma(\alpha) = \alpha \ \forall \sigma \in V \implies \sigma(\alpha) = \alpha \ \forall \sigma \in U \ (U \subseteq V) \implies \alpha \in L^U$

c) “ $\implies$ “

$E \subseteq F \implies \eta(F) = \text{Gal}(L : F) \subseteq \text{Gal}(L : E) = \eta(E)$; denn

$\sigma \in \text{Gal}(L : F) \implies \sigma$ ist ein F –Automorphismus von L . Wegen $E \subseteq F$ ist dann aber σ auch ein E –Automorphismus von L , d.h. $\sigma \in \text{Gal}(L : E)$

b) “ $\impliedby$ “

Gele $\varepsilon(V) \subseteq \varepsilon(U)$. Nach dem bereits geführten Teilbeweis von c) folgt $\eta(\varepsilon(U)) \subseteq \eta(\varepsilon(V))$. Mit a) ergibt sich $U \subseteq V$.

c) “ $\impliedby$ “

Gele $\eta(F) \subseteq \eta(E)$. Nach dem bereits geführten Teilbeweis von b) folgt $\varepsilon(\eta(E)) \subseteq \varepsilon(\eta(F))$. Mit a) ergibt sich $E \subseteq F$. •

Beweis von Teil II):

a) Gilt nach (11.8a).

b) Sei $H := \text{Gal}(L : E)$. Da $L : K$ (nach Vor.) und $L : E$ (nach a)) Galois–Erweiterungen sind, gilt

$$|G| = [L : K] \text{ und } |H| = [L : E]$$

1) $\implies$ 2) Da $E : K$ ein Galois–Erweiterung ist, gilt $|\text{Gal}(E : K)| = [E : K]$, woraus mit (11.9) folgt

$$(\star) \quad |\text{Gal}(E : K)| = |\text{H}_K(E, L)|$$

Es sei $i := \text{id}_L|E : E \longrightarrow L$ die Einbettung. Für jedes $\sigma \in \text{Gal}(E : K)$ ist dann $i \circ \sigma \in \text{H}_K(E, L)$, d.h. durch die Zuordnung $\sigma \longmapsto i \circ \sigma$ wird eine Abbildung

$$h : \text{Gal}(E : K) \longrightarrow \text{H}_K(E, L)$$

definiert. h ist injektiv; denn aus $i \circ \sigma = h(\sigma) = h(\tau) = i \circ \tau$ folgt $\sigma = \tau$. Wegen $(\star)$ ist dann h sogar bijektiv.

Sei nun $\sigma \in G$ beliebig. Dann besitzt $\sigma|E \in \text{H}_K(E, L)$ ein Urbild $\tau \in \text{Gal}(E : K)$ unter h , d.h. es gilt $\sigma|E = i \circ \tau$. Folglich:

$$\underline{\sigma(E)} = i \circ \tau(E) = i(\tau(E)) = i(E) = \underline{E}$$

2) $\implies$ 1) Es genügt, $E^{\text{Gal}(E:K)} \subseteq K$ zu zeigen. Da die umgekehrte Inklusion klar ist, folgt dann die Gleichheit, so daß $E : K$ nach (11.7) eine Galois-Erweiterung ist.

Sei $\alpha \in E^{\text{Gal}(E:K)}$ ein beliebiges Element. Es soll $\alpha \in L^G$ gezeigt werden, woraus $\alpha \in K$ folgt, da $L : K$ nach Voraussetzung eine Galois-Erweiterung ist und somit $L^G = K$ gilt.

Sei $\sigma \in G$ beliebig. Dann gilt $\sigma(E) = E$ nach Voraussetzung, so daß σ einen K -Automorphismus $\sigma' \in \text{Gal}(E : K)$ mit $\sigma'(\beta) = \sigma(\beta) \quad (\forall \beta \in E)$ definiert. Es folgt $\alpha = \sigma'(\alpha) = \sigma(\alpha)$, Also $\alpha \in L^G$. •

Für den nächsten Beweis benötigen wir den folgenden Hilfssatz:

(12.4) HILFSSATZ: $L : K$ sei eine Galois-Erweiterung und E ein Zwischenkörper von $L : K$. Dann gilt für jedes $\sigma \in G$:

a) $\sigma(E)$ ist ein Zwischenkörper von $L : K$ b) $\text{Gal}(L : \sigma(E)) = \sigma \circ \text{Gal}(L : E) \circ \sigma^{-1}$.

Bew: a) ist klar b) Für einen Automorphismus $\tau : L \longrightarrow L$ gilt:

$\tau \in \text{Gal}(L : \sigma(E)) \iff \tau$ ist ein $\sigma(E)$ -Automorphismus von $L \iff \tau(\sigma(\alpha)) = \sigma(\alpha) \quad (\forall \alpha \in E) \iff (\sigma^{-1} \circ \tau \circ \sigma)(\alpha) = \alpha \quad (\forall \alpha \in E) \iff \sigma^{-1} \circ \tau \circ \sigma \in \text{Gal}(L : E) \iff \tau \in \sigma \circ \text{Gal}(L : E) \circ \sigma^{-1}$. •

2) $\implies$ 3) Klar ist $\text{Gal}(L : E) \leq G$. Noch z.z. $\forall \sigma \in G : \sigma \circ \text{Gal}(L : E) \circ \sigma^{-1} = \text{Gal}(L : E)$. Sei $\sigma \in G$ beliebig. Nach Voraussetzung gilt dann $\sigma(E) = E$. Mit (12.4b) ergibt sich dann

$$\text{Gal}(L : E) = \text{Gal}(L : \sigma(E)) \stackrel{(12.4b)}{=} \sigma \circ \text{Gal}(L : E) \circ \sigma^{-1}$$

3) $\implies$ 2) Z.z. $\text{Gal}(L : E)$ Normalteiler in $G \implies \sigma(E) = E \quad (\forall \sigma \in G)$.

$\sigma \in G \implies \text{Gal}(L : E) \stackrel{NT}{=} \sigma \circ \text{Gal}(L : E) \circ \sigma^{-1} \stackrel{(12.4b)}{=} \text{Gal}(L : \sigma(E))$. Mit Teil a) ergibt sich: $\eta(E) = \text{Gal}(L : E) = \text{Gal}(L : \sigma(E)) = \eta(\sigma(E)) \implies E = \sigma(E)$ (da η injektiv ist). •

Wir kommen nun zum Beweis von c):

c) Nach Voraussetzung ist $E : K$ eine Galois-Erweiterung, so daß nach b) $\overline{\sigma(E)} = E \quad \forall \sigma \in G$ gilt. Damit definiert jedes $\sigma \in G$ einen K -Automorphismus $\sigma' : E \longrightarrow E \quad (\alpha \mapsto \sigma(\alpha))$. Definiere eine Abbildung

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

ω ist ein Gruppenhomomorphismus: $\omega(\sigma \circ \tau) = (\sigma \circ \tau)' = \sigma' \circ \tau' = \omega(\sigma) \circ \omega(\tau) \quad (\forall \sigma, \tau \in G)$

$\text{Kern}(\omega) = \text{Gal}(L : E)$ $\sigma \in G : \sigma \in \text{Kern}(\omega) \iff \sigma' = \omega(\sigma) = id_E \iff \sigma(\alpha) = \alpha \quad \forall \alpha \in E \iff \sigma \in \text{Gal}(L : E)$

ω ist surjektiv Sei $U := \text{Bild}(\omega) \leq \text{Gal}(E : K)$ Z.z. $U = \text{Gal}(E : K)$

Es genügt zu zeigen: $E^U \stackrel{!}{=} E^{\text{Gal}(E:K)} = K$ ($E : K$ ist eine Galois-Erweiterung!). Dann folgt aus Teil I,a) die Behauptung $U = \text{Gal}(E : K)$, da die Abbildung ε injektiv ist.

$K \subseteq E^U$ ist klar. Sei umgekehrt $\alpha \in E^U$ beliebig. Dann gilt $\alpha \in E$ und $\tau(\alpha) = \alpha \quad \forall \tau \in U = \text{Bild}(\omega)$. Z.z. $\alpha \in K$. Da nach Voraussetzung $L : K$ eine Galois-Erweiterung ist, gilt $K = L^G$. Wir wollen deshalb $\alpha \in L^G$ zeigen. Sei $\sigma \in G$ beliebig. Dann folgt $\omega(\sigma) = \sigma' \in \text{Bild}(\omega) = U$ und daraus $\sigma(\alpha) = \sigma'(\alpha) = \alpha$, also $\alpha \in L^G = K$. Insgesamt gilt daher $E^U = K$.

Nach dem Homomorphiesatz für Gruppen ist

$$\begin{array}{ccc} \omega^* & : & \text{Gal}(L : K) / \text{Kern}(\omega) \longrightarrow \text{Gal}(E : K) \\ & & \parallel \\ & & \text{Gal}(L : K) / \text{Gal}(L : E) \end{array}$$

ein Gruppenisomorphismus.

Damit ist der Hauptsatz der Galois-Theorie vollständig bewiesen. ••

Wir wollen noch einige Folgerungen aus dem Hauptsatz ziehen. Zunächst halten wir fest, was die Bijektivität von ε und η im einzelnen bedeutet:

(12.5) KOROLLAR: $L : K$ sei eine Galois-Erweiterung, $G := \text{Gal}(L : K)$. Dann gilt:

- a) Zu jedem Zwischenkörper E von $L : K$ gibt es eine Untergruppe $U \leq G$ mit $E = L^U$.
- b) Sind $U, V \leq G$ Untergruppen von G mit $L^U = L^V$, so folgt $U = V$.
- c) Zu jeder Untergruppe $U \leq G$ gibt es einen Zwischenkörper E von $L : K$ mit $U = \text{Gal}(L : E)$.
- d) Sind E und F Zwischenkörper von $L : K$ mit $\text{Gal}(L : E) = \text{Gal}(L : F)$, so folgt $E = F$.

(12.6) KOROLLAR: Jede Galois-Erweiterung besitzt nur endlich viele Zwischenkörper.

Bew: $|\mathcal{Z}| = |\mathcal{U}| \leq 2^{|G|} < \infty$ (G ist endlich und $\mathcal{U} \subseteq \mathcal{P}(G)$, Potenzmenge von G). •

(12.7) KOROLLAR: $L : K$ sei eine Galois-Erweiterung, $G := \text{Gal}(L : K)$. Ist dann jede Untergruppe von G auch Normalteiler von G , so ist die Körpererweiterung $E : K$ für jeden Zwischenkörper E von $L : K$ eine Galois-Erweiterung. Die Voraussetzung über die Untergruppen von G ist insbesondere dann erfüllt, wenn G eine abelsche Gruppe ist. Es gibt aber auch nichtabelsche Gruppen (z.B. die Quaternionengruppe Q), in denen jede Untergruppe Normalteiler ist.

Bew: Folgt sofort aus (12.3) Teil II), b). •