
18.04.2026


18.04.2026

Definition der Galois-Erweiterungen und Galoisgruppen

Definition (21.1)

Eine Körpererweiterung $L|K$ wird Galois-Erweiterung oder auch galois'sche Erweiterung genannt, wenn sie normal und separabel ist. Die Gruppe $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$ heißt dann die Galoisgruppe der Erweiterung $L|K$.

Ordnung der Galoisgruppe und Erweiterungsgrad

Satz (21.2)

Eine endliche Körpererweiterung $L|K$ ist genau dann galois'sch, wenn $[L : K] = |\mathrm{Aut}_K(L)|$ gilt. Insbesondere ist für jede Galois-Erweiterung $L|K$ also die Gleichung $|\mathrm{Gal}(L|K)| = [L : K]$ erfüllt.

Beweis von Satz 21.2

geg.: endl. Körpererweiterung $L|K$

z.zg.: $L|K$ ist galoissch $\Leftrightarrow |\mathrm{Aut}_K(L)| = [L:K]$

Erinnerung:
- $\mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L, \tilde{L})$, wobei $\tilde{L} \supseteq L$ alg. abg. Erw., mit Gleichheit genau dann, wenn $L|K$ normal
- Separabilitätsgrad $[L:K]_{sep} = |\mathrm{Hom}_K(L, \tilde{L})|$
  Es gilt $[L:K]_{sep} \leq [L:K]$ mit Gleichheit genau dann, wenn $L|K$ separabel ist

zu

da

zu (

„⇒" $L|K$ gal. $\Rightarrow L|K$ normal und sep. $\Rightarrow$

$|\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,\widetilde{L})| = [L:K]_{sep} = [L:K]$

$\uparrow L|K$ normal $\qquad \uparrow L|K$ sep.

„⇐" $|\mathrm{Aut}_K(L)| \leq |\mathrm{Hom}_K(L,\widetilde{L})| = [L:K]_{sep} \leq [L:K]$

immer erfüllt Vor. $\Rightarrow [L:K]_{sep} = [L:K] \Rightarrow$

$L|K$ sep. ebenso $\therefore |\mathrm{Aut}_K(L)| = |\mathrm{Hom}_K(L,\widetilde{L})|$

$\Rightarrow \mathrm{Aut}_K(L) = \mathrm{Hom}_K(L,\widetilde{L}) \Rightarrow L|K$ normal

$\uparrow \mathrm{Aut}_K(L) \subseteq \mathrm{Hom}_K(L,\widetilde{L})$

beide Mengen endl.

□

Der Fortsetzungssatz für Galois-Erweiterungen

Folgerung (21.3)

Sei $L|K$ eine Galois-Erweiterung, $f \in K[x]$ ein irreduzibles Polynom, und seien α, β zwei Nullstellen von f in L. Dann existiert ein Element $\sigma \in \mathrm{Gal}(L|K)$ mit $\sigma(\alpha) = \beta$.

Beweis von Folgerung 21.3

gfg.: Galois-Erw. $L|K$, $\alpha, \beta \in L$, $f \in K[x]$ irreduzibel mit $f(\alpha) = f(\beta) = 0$

Beh.: $\exists \sigma \in G$ mit $\sigma(\alpha) = \beta$, wobei $G = Gal(L|K) = Aut_K(L)$

Sei $\tilde{L}$ eine alg. abg. Erweiterung von L.

Fortsetzungssatz $\Rightarrow$ $\exists$ Fortsetzung von id_K (also ein K-Hom.) zu einem Hom. $\sigma_0 : K(\alpha) \to \tilde{L}$ mit $\sigma_0(\alpha) = \beta$ (beachte: $\beta \in L \Rightarrow \beta \in \tilde{L}$)

$\tilde{L}$ alg. abgeschlossen $\Rightarrow$ $\exists$ Fortsetzung von σ_0

Zu einem K-Hom. $\sigma : L \to \tilde{L}$.

$L|K$ ist normal $\Rightarrow \mathrm{Hom}_K(L, \tilde{L}) = \mathrm{Aut}_K(L)$

$\Rightarrow \sigma \in \mathrm{Aut}_K(L)$ (und $\sigma(\alpha) = \beta$) $\square$

Der Fixkörper einer Untergruppe der Galoisgruppe

Ist $L|K$ eine Galois-Erweiterung und M ein Zwischenkörper von $L|K$, dann $U = \mathrm{Gal}(L|M)$ eine Untergruppe von $G = \mathrm{Gal}(L|K)$.

Umgekehrt liefert auch jede Untergruppe von G einen Zwischenkörper von $L|K$. Allgemeiner liefert eine Untergruppe der Automorphismengruppe $\mathrm{Aut}(L)$ einen Teilkörper von L.

Definition (21.4)

Sei L ein Körper und G eine Untergruppe von $\mathrm{Aut}(L)$. Dann nennt man $L^G = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \ \forall\, \sigma \in G\}$ den Fixkörper von G.

$= [L:K]$

$(L, \tilde{L})$,

gleich-

al

$\mathrm{Hom}_K(L, \tilde{L})$

Gleich-

zusatzel ist

Nachweis der Teilkörpereigenschaft von

$L^G = \{\alpha \in L \mid \forall \sigma \in G : \sigma(\alpha) = \alpha\}$, wobei

G Untergruppe von $\mathrm{Aut}(L)$

zu überprüfen: (1) $1_L \in L^G$

(2) $\forall \alpha, \beta \in L^G : \alpha - \beta, \alpha\beta \in L^G$,

im Fall $\alpha \neq 0_K$ auch $\alpha^{-1} \in L^G$.

zu (1) Da jedes $\sigma \in G$ ein Körperaut. und

damit erst recht ein Ringhom. ist, gilt

jeweils $\sigma(1_L) = 1_L$. also: $1_L \in L^G$

zu (2) seien $\alpha, \beta \in L^G$. Dann gilt für alle

$\sigma \in G$ jeweils $\sigma(\alpha-\beta) = \sigma(\alpha) - \sigma(\beta)$

$= \alpha - \beta$ und $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$

$\uparrow \alpha, \beta \in L^G$

$\Rightarrow \alpha-\beta, \alpha\beta \in L^G$ Ist $\alpha \neq 0_K$, dann ex. α^{-1}

für jedes $\sigma \in G$ ebenso $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1}$

$= \alpha^{-1}$, also $\alpha^{-1} \in L^G$.

□

Eine alternative Beschreibung der Galoisgruppe

Proposition (21.5)

Sei L ein Körper, $G \leq \mathrm{Aut}(L)$ eine endliche Untergruppe und $K = L^G$ der zugehörige Fixkörper.

(i) Sei $\alpha \in L$ und $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\}$. Sind $\alpha_1, ..., \alpha_r$ die verschiedenen Elemente der Menge $G(\alpha)$, dann ist das Polynom $f = \prod_{i=1}^{r}(x - \alpha_i)$ das Minimalpolynom von α über dem Grundkörper K.

(ii) Die Erweiterung $L|K$ ist galoissch.

(iii) Die Erweiterung $L|K$ ist endlich.

(iv) Es gilt $G = \mathrm{Gal}(L|K)$ und $|G| = [L : K]$.

Folgerung (21.6)

Sei $L|K$ eine endliche Körpererweiterung und $G = \mathrm{Aut}_K(L)$. Genau dann ist $L|K$ galois'sch, wenn $L^G = K$ erfüllt ist.

Beweis von Prop 21.5:

geg: Körper L, $G \leq \mathrm{Aut}(L)$ endl. Untergr., $K = L^G$

zu (i) Sei $\alpha \in L$ und $G(\alpha) = \{\sigma(\alpha) \mid \sigma \in G\} = \{\alpha_1, \dots, \alpha_r\}$

Sei $f = \prod_{i=1}^{r} (x - \alpha_i)$ Beh.: $f \in K[x]$

Sei $\sigma \in G$ beliebig. Dann gilt $\sigma(G(\alpha)) \subseteq G(\alpha)$, denn:

$\beta \in G(\alpha) \Rightarrow \exists \tau \in G$ mit $\beta = \tau(\alpha) \Rightarrow \sigma(\beta) =$

$\sigma(\tau(\alpha)) = \underbrace{(\sigma \circ \tau)}_{\in G}(\alpha) \in G(\alpha)$. Also werden die

Elemente von $G(\alpha)$ durch σ nur permutiert

$\sigma(f) = \sigma\left(\prod_{i=1}^{r} (x - \alpha_i)\right) = \sigma\left(\prod_{\beta \in G(\alpha)} (x - \beta)\right) =$

$$\prod_{\beta \in G(\alpha)} (x - \sigma(\beta)) = \prod_{\beta \in G(\alpha)} (x - \beta) = f.$$

Also bleiben auch alle Koeff. von f unter allen $\sigma \in G$ fest. $\Rightarrow$ Alle Koeff. von f liegen in L^G. $\Rightarrow f \in K[x]$

Sei nun $g = \mu_{\alpha, K}$ $f \in K[x]$, $f(\alpha) = 0 \Rightarrow g \mid f$

$g(\alpha) = 0$ Sei $\sigma \in G$. „Nullstellen auf Nullstellen" $g(\sigma(\alpha)) = 0$

$\Rightarrow$ Alle Elemente aus $G(\alpha)$ sind Nullstellen von g. $\overset{g \mid f}{\Rightarrow} g = f$

$\Rightarrow f = \mu_{\alpha, K}$

zu (ii) z.zg.: (1) $L|K$ ist normal (2) $L|K$ ist separabel

zu (1) Sei $f \in K[x]$ ein irred. Polynom, dass in L eine Nullstelle α besitzt. z.zg.: f zerfällt über L in Linearfaktoren

β)

K]

) =

ich

= [L : K]

⊃

: K].

□

O.B.d.A. sei f normiert. $\Rightarrow f = \mu_{\alpha,K}$

i) $\Rightarrow f = \prod_{\beta \in G(\alpha)} (x - \beta)$ Da alle $\beta \in G(\alpha)$ in L liegen, zerfällt f über L in Linearfaktoren.

zu (2) Sei $\alpha \in L$ z.zg.: α ist separabel über K

gleichbed.: $f = \mu_{\alpha,K}$ ist ein separables Polynom. Teil (i) $\Rightarrow f = \prod_{\beta \in G(\alpha)} (x - \beta)$

Da f keine mehrfachen Nullstellen in L hat, ist es ein separables irred. Polynom.

zu (iii) z.zg.: $L|K$ ist endl. Erweiterung

Für jedes $\alpha \in L$ gilt $M_{\alpha,K} = \prod_{\beta \in G(\alpha)} (x - \beta)$.

$|G(\alpha)| \leq d$, wobei $d = |G|$

$\Rightarrow [K(\alpha) : K] = \operatorname{grad} M_{\alpha,K} \leq d \quad \forall \alpha \in L$.

Sei nun $\alpha \in L$ so gewählt, dass $[K(\alpha) : K]$ maximal ist. Beh.: $K(\alpha) = L$ (Ist dies gezeigt, dann sind wir fertig.)

„$\subseteq$" klar „$\supseteq$" Sei $\beta \in L$. Dann ist $K(\alpha, \beta)|K$ eine endliche separable Erweiterung. Satz vom Primitiven Elt. $\Rightarrow \exists \gamma \in L$ mit $K(\gamma) = K(\alpha, \beta)$

Maximalitätsvorg. von $\alpha \Rightarrow [K(\gamma) : K] \leq [K(\alpha) : K]$

$K(\alpha) \subseteq K(\gamma) = K(\alpha, \beta)$ $K(\alpha) = K(\gamma) = K(\alpha, \beta)$

$\Rightarrow$ $\Rightarrow \beta \in K(\alpha)$ ($\Rightarrow$ Beh.)

zu (iv) zzg: $G = \mathrm{Gal}(L|K)$ und $|G| = [L:K]$

Nach Def. ist G Teilmenge von $\mathrm{Gal}(L|K) = \mathrm{Gal}(L|L^G)$ Wie in Teil (iii) gezeigt, gilt

$[L:K] = [K(\alpha):K] \leq d = |G|$

$L|K$ ist endl. Galoissch. $\overset{\text{Satz 21.2}}{\Rightarrow} |\mathrm{Gal}(L|K)| = [L:K]$

$\Rightarrow |\mathrm{Gal}(L|K)| \leq |G|$, $G \subseteq \mathrm{Gal}(L|K)$ $\Rightarrow$

$G = \mathrm{Gal}(L|K)$ und $|G| = |\mathrm{Gal}(L|K)| = [L:K]$. $\square$

Beweis von Folgerung 21.6:

geg.: endl. Erw. $L|K$, $G = \mathrm{Aut}_K(L)$

z.zg.: $L|K$ ist galoissch $\iff$ $L^G = K$

„$\Leftarrow$" Satz 21.5 $\Rightarrow$ $L|L^G$ ist galoissch

$\overset{\text{Vor.}}{\Rightarrow}$ $L|K$ ist galoissch

„$\Rightarrow$" Vor.: $L|K$ ist gal. z.zg.: $K = L^G$

Auf jeden Fall gilt $K \subseteq L^G$ $\Rightarrow$ L^G ist ein Zwischenkörper von $L|K$ $\overset{\text{Gradformel}}{\Rightarrow}$

$$[L:K] = [L:L^G] \cdot [L^G:K]$$

Satz 21.5 $\Rightarrow$ $[L:L^G] = |G| \overset{L|K \text{ gal}}{=} [L:K]$

einsetzen $\rightarrow [L:K] = [L:k]\,[L^G:K] \Rightarrow$

$[L^G:K] = 1 \Rightarrow K = L^G.$ $\square$

Der Hauptsatz der Galoistheorie

Satz (21.7)

Sei $L|K$ eine endliche Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(L|K)$, $\mathcal{U}$ die Menge der Untergruppen von G und $\mathcal{Z}$ die Menge der Zwischenkörper von $L|K$. Dann sind durch die Zuordnungen

$$\phi : \mathcal{U} \to \mathcal{Z}, U \mapsto L^U \quad \text{und} \quad \psi : \mathcal{Z} \to \mathcal{U}, M \mapsto \mathrm{Gal}(L|M)$$

zueinander inverse Bijektionen zwischen $\mathcal{U}$ und $\mathcal{Z}$ gegeben.

Beweis von Satz 21.7:

geg: endl. Galois-Erw. $L|K$, $G = Gal(L|K)$

$\mathcal{U}$ = Untergr. von G, $\mathcal{Z}$ = Zwischenkörper von $L|K$

$\Phi : \mathcal{U} \to \mathcal{Z}$, $U \mapsto L^U$, $\Psi : \mathcal{Z} \to \mathcal{U}$, $M \mapsto Gal(L|M)$

zzg: $\Psi \circ \Phi = id_{\mathcal{U}}$, $\Phi \circ \Psi = id_{\mathcal{Z}}$, gleichbed. mit

(1) $\forall U \in \mathcal{U} : (\Psi \circ \Phi)(U) = U$ (2) $\forall M \in \mathcal{Z} : (\Phi \circ \Psi)(M) = M$

zu (1) Sei $U \in \mathcal{U}$, zzg: $Gal(L|L^U) = U$ Dies folgt direkt aus Teil (ix) von Satz 21.5

zu (2) Sei $M \in \mathcal{Z}$, $L^{Gal(L|M)} = M$ Mit $L|K$ ist auch $L|M$ eine Galoiserw., also normal und separabel (siehe WiSe 25-26)

Damit folgt die Beh. auf Folgerung 21.6 □