

Galois-Erweiterungen

Im Folgenden sei wieder $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$ ein Körper.

- Erinnerung:
- Sei $\tilde{f} = (f_i)_{i \in I}$ eine Familie von Polynomen in $K[X]$. Der kleinste Körper L , der sowohl K als auch die Nullstellen der f_i enthält heißt **Zerfällungskörper** von \tilde{f} .
 - Sei $K \subseteq L$ eine Körpererweiterung. Dann sind $\text{Hom}_K(L, K') = \{ f: L \rightarrow K' \text{ Körperhomomorphismus} \mid f|_K = \text{id} \}$ die **K -Homomorphismen** $L \rightarrow K'$.
 - Ist $K \subseteq L$ eine (endliche) Körpererweiterung, so dass L ein Zerfällungskörper ist, dann gilt:
$$\begin{aligned} \text{Hom}_K(L, \bar{L}) &= \text{K-Homomorphismen } L \rightarrow \bar{L} \\ &= \text{Hom}_K(L, L). \end{aligned}$$

Definition 81

Sei $L \supseteq K$ eine endliche Körpererweiterung, so dass L ein Zerfällungskörper einer Familie von Polynomen in $K[X]$ ist, dann nennen wir $L \supseteq K$ eine **Galois-Erweiterung**.

Lemma 82

Sei $L \supseteq K$ eine Galois-Erweiterung und $f \in \text{Hom}_K(L, L)$. Dann ist f bijektiv.

Beweis

Sei $f \in \text{Hom}_K(L, L)$. Angenommen f ist nicht injektiv. Dann gibt es $a, b \in L$, $a \neq b$, mit $f(a) = f(b)$. $\Rightarrow f(a-b) = 0$.

Da $a \neq b$, ist $c := a-b \neq 0$. $\Rightarrow c^{-1} \in L$

$$\Rightarrow \begin{cases} f(c^{-1}(a-b)) = f(c^{-1}) \cdot f(a-b) = f(c^{-1}) \cdot 0 = 0 \\ f(c^{-1}(a-b)) = f(c^{-1} \cdot c) = f(1) = 1 \end{cases} \quad \begin{matrix} \hookrightarrow & \Rightarrow f \text{ ist} \\ & \text{injektiv.} \end{matrix}$$

(Bemerkung: Dieses Argument funktioniert allgemein für Körperhomomorphismen nicht nur K -Homomorphismen).

Noch 2.2: f ist surjektiv: Da $f \in \text{Hom}_K(L, L)$, ist f ein Vektorraum-Homomorphismus vom K -Vektorraum L nach L . Da L ein endlich-dimensionaler K -Vektorraum ist, impliziert f injektiv automatisch dass f auch injektiv ist. \square

Korollar 83

Sei L/K eine Galois-Erweiterung. Dann ist $\text{Hom}_K(L, L)$ eine Gruppe.

Definition 84

Sei L/K eine Galois-Erweiterung. Dann ist

$$\text{Gal}(L/K) := \text{Hom}_K(L, L)$$

die Galoisgruppe von L über K .

Korollar 85

Sei L/K eine Galois-Erweiterung, dann gilt $\#\text{Gal}(L/K) = [L : K]$.

Beweis

Anwendung von Satz 80 auf Galois-Erweiterungen.

Satz 86 (Galois-Gruppe einer einzelnen Gleichung)

Sei $f \in K[X]$ mit $d = \deg(f)$. Seien $z_1, \dots, z_d \in \mathbb{C}$ die Nullstellen von f , so dass $z_i \neq z_j$ für $i \neq j$. Sei $L := \mathbb{Z}FK(f)$ (d.h. $z_i \in L$ für $1 \leq i \leq d$).

Dann definiert

$$\begin{aligned}\varphi: \text{Gal}(L/K) &\rightarrow S(\{z_1, \dots, z_d\}) \quad (= \text{Gruppe der bijektiven} \\ &\quad \text{Abbildungen} \\ &\quad \{z_1, \dots, z_d\} \rightarrow \{z_1, \dots, z_d\}) \\ \sigma &\mapsto \sigma|_{\{z_1, \dots, z_d\}} \\ &\stackrel{?}{=} S_d\end{aligned}$$

einen injektiven Gruppenhomomorphismus. Insbesondere gilt, dass $\#\text{Gal}(L/K) = [L : K]$ die Zahl $d! = \#S_d$ teilt.

Beweis

Wohldefiniertheit: Sei $f = \sum_{i=0}^d a_i x^i$. Dann gilt:
 $f(\sigma(z_j)) = \sum_{i=0}^d a_i \sigma(z_j)^i = \sigma \left(\sum_{i=0}^d a_i z_j^i \right) = \sigma(f) = 0$
 $\Rightarrow \sigma(\{z_1, \dots, z_d\}) = \{z_1, \dots, z_d\}$

Da σ bijektiv ist, $\sigma|_{\{z_1, \dots, z_d\}} \in S(\{z_1, \dots, z_d\})$

Gruppenhomomorphismus: Seien $\sigma, \sigma' \in \text{Gal}(L/K)$. Dann gilt:

$$\begin{aligned}\varphi(\sigma \circ \sigma') &= (\sigma \circ \sigma')|_{\{z_1, \dots, z_d\}} \\ &= \sigma|_{\{z_1, \dots, z_d\}} \circ \sigma'|_{\{z_1, \dots, z_d\}} = \varphi(\sigma) \circ \varphi(\sigma')\end{aligned}$$

Injektivität: $\ker(\varphi) = \{ \sigma \in \text{Gal}(L/K) \mid \varphi(\sigma) = \sigma|_{\{z_1, \dots, z_d\}} = \text{id}_{\{z_1, \dots, z_d\}} \}$

$$\stackrel{\downarrow}{=} \{ \text{id}_L \}$$

weil $L = \mathbb{Z}[\text{FK}(f)] = K(z_1, \dots, z_d)$

$\Rightarrow \varphi$ ist injektiv. \square

Lemma 87

(so dass f keine doppelten Nullstellen hat)

Sei $L \supseteq K$ eine Galois-Erweiterung mit $L = \mathbb{Z}[\text{FK}(f)]$ für $f \in K[X]$.
 Dann ist f irreduzibel, genau dann, wenn $\text{Gal}(L/K)$ transitiv auf den Nullstellen von f operiert (d.h. für alle Nullstellen y, z von f finden wir $\sigma \in \text{Gal}(L/K)$ mit $\sigma(y) = z$).

Beweis

Seien $y, z \in L$ Nullstellen von f . Angenommen f ist irreduzibel.

Mit Lemma 77 finden wir einen K -Homomorphismus $\sigma: K(y) \rightarrow K(z)$, so dass $\sigma(y) = z$. Mit Korollar 78 können wir σ zu einem K -Homomorphismus $L \rightarrow L$ fortsetzen.

Angenommen $f = g \cdot h$ mit $g, h \in K[X]$ und $\deg(g), \deg(h) \geq 1$. Da jeder $\sigma \in \text{Gal}(L/K)$ die Nullstellen von g auf die Nullstellen von g abbildet (und die Nullstellen von h auf die Nullstellen von h), operiert $\text{Gal}(L/K)$ nicht transitiv auf den Nullstellen von f .

Definition 88

Sei $L \supseteq K$ eine Galois-Erweiterung und $G \subseteq \text{Gal}(L/K)$ eine Untergruppe.
 Dann definieren wir $L^G := \{ a \in L \mid \sigma(a) = a \text{ für alle } \sigma \in G \}$.

Wir nennen L^G den Fixkörper von G in L .

Lemma 89

Sei $L \supseteq K$ eine Galois-Erweiterung und $G \subseteq \text{Gal}(L/K)$ eine Untergruppe.

Dann ist $L \supseteq L^G$ eine Galois-Erweiterung mit Galois-Gruppe $G = \text{Gal}(L/L^G)$.

Beweis

Zunächst zeigen wir, dass $L \supseteq L^G$ eine Galois-Erweiterung ist:

Sei $\sigma: L \rightarrow L$ ein L^G -Homomorphismus. Da $K \subseteq L^G$, ist σ ein K -Homomorphismus. Mit Satz 79 folgt, dass $\sigma: L \rightarrow L$, d.h. $\sigma \in \text{Hom}_K(L, L)$. $\Rightarrow \sigma \in \text{Hom}_{L^G}(L, L)$

$\stackrel{\text{Satz 79}}{\Rightarrow} L$ ist Zerfällungskörper einer Familie von Polynomen aus $L^G[X]$.

$\Rightarrow L \supseteq L^G$ ist eine Galois-Erweiterung.

Und es gilt: $\text{Gal}(L/L^G) = \text{Hom}_{L^G}(L, L)$

$$\begin{aligned} &= \{ \sigma: L \rightarrow L \text{ Körperhomomorphismus} \mid \sigma|_{L^G} = \text{id}_{L^G} \} \\ &= \{ \sigma \in \text{Gal}(L/K) \mid \sigma|_{L^G} = \text{id}_{L^G} \} \\ &= G. \end{aligned}$$

□

Satz 90 (Hauptsatz der Galois-Theorie)

Sei $L \supseteq K$ eine Galois-Erweiterung mit Galois-Gruppe $G := \text{Gal}(L/K)$.

Dann ist die Abbildung

$$\Psi: \{ \text{Untergruppen von } G \} \rightarrow \{ \text{Zwischenkörper } K \leq E \leq L \}$$
$$H \quad \mapsto \quad L^H$$

ist bijektiv und es gilt: $\Psi^{-1}(E) = \text{Gal}(L/E)$.

Beweis

Sei $K \subseteq E \subseteq L$. Wie im Lemma 87 beweisen wir, dass $L \supseteq E$ eine Galois-Erweiterung ist. Wir definieren die Abbildung

$$\begin{aligned} \phi: \{ \text{Zwischenkörper } K \subseteq E \subseteq L \} &\rightarrow \{ \text{Untergruppen von } \text{Gal}(L/K) \} \\ E &\mapsto \text{Gal}(L/E) \end{aligned}$$

(Es ist $\text{Gal}(L/E)$ ein Untergruppe von $\text{Gal}(L/K)$, weil $K \subseteq E$ impliziert:

$$\text{Gal}(L/E) = \text{Hom}_E(L, L) \subseteq \text{Hom}_K(L, L) = \text{Gal}(L/K).$$

Behauptung (1) $\psi \circ \phi = \text{id}_{\text{Zwischenkörper}}$ (2) $\phi \circ \psi = \text{id}_{\text{Untergruppen von } \text{Gal}(L/K)}$

Zu (1): Sei $K \subseteq E \subseteq L$. Dann ist $(\psi \circ \phi(E)) = \psi(\text{Gal}(L/E)) = L^{\text{Gal}(L/E)}$.

Da $\text{Gal}(L/E) = \text{Hom}_E(L, L)$, lässt $\text{Gal}(L/E)$ fixiert, so dass $E \subseteq L^{\text{Gal}(L/E)}$. Auch $E \subseteq L^{\text{Gal}(L/E)}$ ist eine Galois-Erweiterung (Beweis wie in Lemma 89). Mit Korollar 85:

$$\begin{aligned} [L^{\text{Gal}(L/E)} : E] &= \# \text{Gal}(L^{\text{Gal}(L/E)} / E) \\ &\stackrel{\text{per Definition}}{=} \# \text{Hom}_E(L^{\text{Gal}(L/E)}, L^{\text{Gal}(L/E)}) \\ &= 1, \quad \text{weil jedes Element } \sigma \in \text{Gal}(L^{\text{Gal}(L/E)}, E) \\ &\quad \text{sich durch Korollar 78 zu einem} \\ &\quad \text{Element in } \text{Gal}(L/E) \text{ fortsetzen lässt.} \\ &\Rightarrow \sigma = \text{id}|_{L^{\text{Gal}(L/E)}}. \end{aligned}$$

Zu (2): Sei $\{\text{id}\} \subseteq H \subseteq \text{Gal}(L/K)$ eine Untergruppe. Dann ist:

$$\begin{aligned} (\phi \circ \psi(H)) &= \phi(L^H) = \text{Gal}(L/L^H) \\ &= \text{Hom}_{L^H}(L, L) \\ &= \text{Körperhomomorphismen } L \rightarrow L, \text{ die } L^H \text{ fixiert lassen.} \\ &= H. \end{aligned}$$

Bemerkung Sei $L \supseteq K$ eine Galois-Erweiterung und sei $H \subseteq \text{Gal}(L/K)$ eine Untergruppe vom Index $[\text{Gal}(L/K) : H] = 2$.

Dann ist nach Satz 90: $L \supseteq L^H$ ist eine Galois-Erweiterung mit Galoisgruppe H .

$$\xrightarrow{\text{Korollar 85}} [L : L^H] = \#H$$

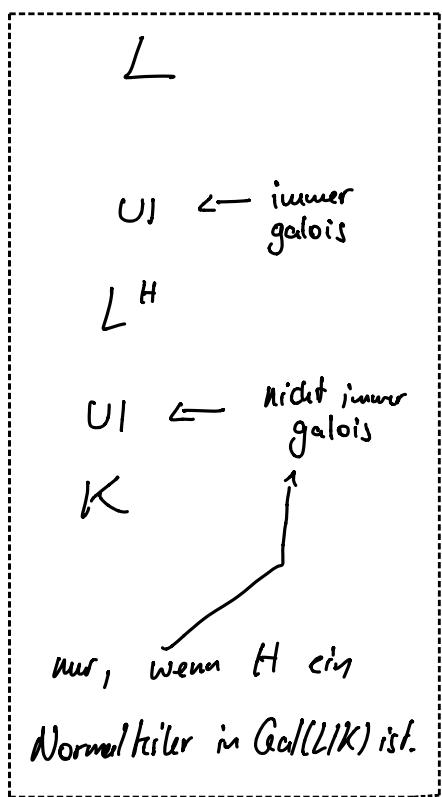
$$\Rightarrow [L^H : K] = \frac{[L : K]}{[L : L^H]} = \frac{\# \text{Gal}(L/K)}{\# H}$$

$$= [\text{Gal}(L/K) : H] = 2$$

$\Rightarrow L^H \supseteq K$ ist eine Körpererweiterung vom Grad 2. D.h.
wir können alle Elemente in L^H durch Elemente in K
und die p.q.-Formel ausdrücken!

Diese Beobachtung haben wir in der Einleitung zur Vorlesung
benutzt, um r und s durch eine p.q.-Formel zu beschreiben.

Bemerkung Sei $L \supseteq K$ eine Galois-Erweiterung mit
Galois Gruppe $\text{Gal}(L/K)$ und H eine
Untergruppe: Dann ist $L \supseteq L^H$ eine
Galois-Erweiterung, aber $L^H \supseteq K$
nicht unbedingt.



Satz 91

Sei $L \supseteq K$ eine Galois-Erweiterung und $H \subseteq \text{Gal}(L/K)$. Dann ist $L^H \supseteq K$ eine Galois-Erweiterung, genau dann wenn H ein Normalteiler in $\text{Gal}(L/K)$ ist. Dann ist $\text{Gal}(L^H/K) \cong \frac{\text{Gal}(L/K)}{H}$.

Beweis

Sei $L^H \supseteq K$ eine Galois-Erweiterung. Dann definieren wir den Gruppenhomomorphismus
 $\varphi: \text{Gal}(L/K) \rightarrow \text{Gal}(L^H/K)$

$$\sigma \mapsto \sigma|_{L^H}.$$

$$\begin{aligned} \text{Es gilt dann: } \ker(\varphi) &= \{ \sigma \in \text{Gal}(L/K) \mid \sigma|_{L^H} = \text{id}_{L^H} \} \\ &= H \end{aligned}$$

$\Rightarrow H$ ist ein Normalteiler in $\text{Gal}(L/K)$.

= alg. Abbildung von L

Sei jetzt $H \subseteq \text{Gal}(L/K)$ ein Normalteiler. Sei $\sigma \in \text{Hom}_K(L^H, \bar{L})$.

Nach Satz 79 genügt es zu zeigen, dass $\sigma(L^H) = L^H$. Mit Korollar 78 können wir σ zu einem $\sigma' \in \text{Hom}_K(L, \bar{L})$ fortsetzen.

$$\Rightarrow \sigma' \in \text{Hom}_K(L, \bar{L}). \Rightarrow \sigma \in \text{Hom}_K(L^H, \bar{L}).$$

Sei $a \in L^H$ und $b = \sigma(a)$. Wir müssen zeigen, dass $\bar{\tau}(b) = b$ für alle $\bar{\tau} \in H$ ist.

Da H ein Normalteiler ist, gilt $\sigma H = H\sigma$, d.h. es existiert $\bar{\tau}' \in H$ mit $\bar{\tau} \circ \sigma = \sigma \circ \bar{\tau}'$. Dann gilt:

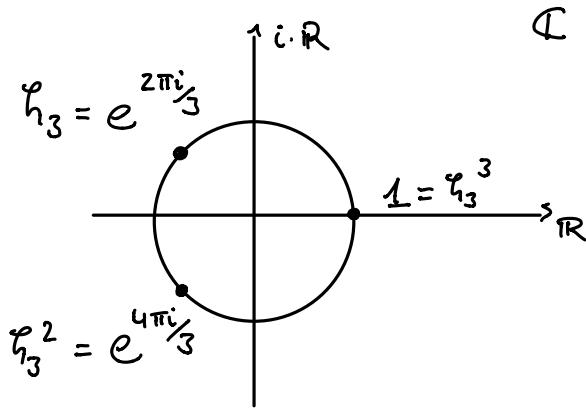
$$\bar{\tau}(b) = (\bar{\tau} \circ \sigma)(a) = (\sigma \circ \bar{\tau}')(a) = \sigma(\bar{\tau}'(a)) \stackrel{\bar{\tau}' \in H}{=} \sigma(a) = b$$

$\Rightarrow b \in L^H$. $\Rightarrow \sigma(L^H) \subseteq L^H$. Mit der gleichen Argumentation für σ^{-1} erhalten wir $\sigma^{-1}(L^H) \subseteq L^H \Rightarrow \sigma(L^H) = L^H$. \square

Einheitswurzeln

Sei $\zeta_n := e^{\frac{2\pi i}{n}}$.

ζ_n heißt n -te Einheitswurzel.



ζ_n hat die Eigenschaft, dass $\zeta_n^n = 1$, aber $\zeta_n^i \neq 1$ für $1 \leq i < n$.

Der Körper $\mathbb{Q}(\zeta_n)$ heißt der n -te Kreishilfungskörper.

Es gilt: $\mathbb{Q}(\zeta_n) = \text{ZFK}(X^n - 1)$.

Insbesondere ist $\mathbb{Q}(\zeta_n) \supset \mathbb{Q}$ eine Galois-Erweiterung.

Beweis: Sei $f = X^n - 1$. Dann gilt: $f(\zeta_n^i) = (\zeta_n^i)^n - 1 = (\zeta_n^n)^i - 1 = 0$.

D.h. die ζ_n^i sind alle Nullstellen von f . Andererseits ist für $i \neq j$:

mit $0 \leq j < i < n$: $(\zeta_n^i)^j = \zeta_n^j \Rightarrow \zeta_n^{i-j} = 1 \neq 1$. D.h. $\zeta_n^i \neq \zeta_n^j$.

$$\Rightarrow f = \prod_{i=0}^{n-1} (X - \zeta_n^i)$$

Es gilt auch: $\zeta_n^i \in \mathbb{Q}(\zeta_n)$. D.h. alle Nullstellen von f sind in $\mathbb{Q}(\zeta_n)$ enthalten $\stackrel{\text{Satz 79}}{\Rightarrow} \mathbb{Q}(\zeta_n) = \text{ZFK}(f)$.

Was ist $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$?

Per Definition: $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \text{Hom}_{\mathbb{Q}}(\mathbb{Q}(\zeta_n), \mathbb{Q}(\zeta_n))$.

Ausserdem: $\mathbb{Q}(\zeta_n) = \left\{ \sum_{i=0}^{n-1} a_i \zeta_n^i \mid a_i \in \mathbb{Q} \right\}$ (siehe Vorlesung 7).

\Rightarrow D.h. $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ ist eindeutig definiert durch Angabe von $\sigma(\zeta_n)$, denn dann gilt: $\sigma(\zeta_n^i) = \sigma(\zeta_n)^i$ und somit ist σ auf allen Elementen der \mathbb{Q} -Basis $\{1, \zeta_n, \dots, \zeta_n^{n-1}\}$ angegeben.

Da $\sigma(\zeta_n)$ eine Nullstelle von $X^n - 1$ sein muss, existiert i mit $\sigma(\zeta_n) = \zeta_n^i$.

Da σ auch invertierbar ist, existiert $\tau \in \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\tau(\zeta_n^i) = \tau(\zeta_n)^i = \zeta_n^j$. Es existiert ein j mit $\tau(\zeta_n) = \zeta_n^j$

Insgesamt:

$$\zeta_n^{i \cdot j} = \zeta_n \Rightarrow i \cdot j \equiv 1 \pmod{n} \quad (\text{da. } \zeta_n^{k+n} = \zeta_n^k)$$

D.h. $i \in \mathbb{Z}_{nZ}$ hat ein multiplikativ Inverses.

$$\begin{aligned} \Rightarrow \# \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &= \# \{i \in \mathbb{Z}_{nZ} \mid \exists j \in \mathbb{Z}_{nZ} : i \cdot j \equiv 1 \pmod{n}\} \\ &=: \varphi(n) \quad (\text{Euler's Phi-Funktion}). \end{aligned}$$

$$\Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n).$$

Bemerkung: Es gilt: $\varphi(n) := \#\{1 \leq i \leq n \mid \text{ggT}(i, n) = 1\}$.

Beweis, Übung.

Es gilt dann z.B.: $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \text{Fixkörper von } H = \langle \sigma \rangle$, wobei $\sigma(\zeta_n) = \zeta_n^{-1}$.

$$\Rightarrow \# H = 2$$

$$\Rightarrow [\text{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q}) : H] = \frac{\varphi(n)}{2}$$

$$\Rightarrow [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$$