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 $L|K$.

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.

Ergänzungen zum Hauptsatz der Galoistheorie

Satz (21.8)

(i) Sind $U_1, U_2 \in \mathcal{U}$ mit $U_1 \subseteq U_2$, dann folgt $L^{U_1} \supseteq L^{U_2}$.

(ii) Sind umgekehrt $M_1, M_2 \in \mathcal{Z}$ mit $M_1 \subseteq M_2$, dann ist $\mathrm{Gal}(L|M_1) \supseteq \mathrm{Gal}(L|M_2)$.

(iii) Es gilt $L^{\{\mathrm{id}_L\}} = L$, $L^G = K$ und $\mathrm{Gal}(L|L) = \{\mathrm{id}_L\}$, $\mathrm{Gal}(L|K) = G$.

(iv) Ist M ein Zwischenkörper und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe, dann gilt $[L : M] = |U|$ und $[M : K] = (G : U)$.

Satz 21.8, nur Teil (iv)

gegeben: Zwischenkörper M von $L|K$, $U = \mathrm{Gal}(L|M)$ zugeh. Untergr.

zu zeigen: $|U| = |\mathrm{Gal}(L|M)|$ und $(G:U) = [M:K]$

Mit $L|K$ ist auch $L|M$ galoissch. $\Rightarrow |U| = |\mathrm{Gal}(L|M)| = [L:M]$ Gradformel $\Rightarrow |G| = [L:K] = [L:M] \cdot [M:K] = |U| \cdot [M:K] \Rightarrow [M:K] = \frac{|G|}{|U|} = (G:U)$. □

Anwendung 1: Bestimmung aller Zwischenkörper von $L|K$ für $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{2},\sqrt{3})$

(1) Nachweis, dass $L|K$ endlich galoissch ist

Überprüfe, dass L Zerf.körp. von $f=(x^2-2)(x^2-3)$ über $\mathbb{Q}$ ist (siehe Skript). $\Rightarrow L|K$ ist eine endl. normale Erw.

$\Rightarrow L|K$ ist algebraisch $\overset{\text{char}(K)=0}{\Rightarrow}$ $L|K$ ist auch separabel

(2) Zeige: $[L:K]=4$

Gradformel $\Rightarrow [L:k]=[L:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$

$2\in\mathbb{Z}\setminus\{0,1\}$, quadratfrei $\Rightarrow [\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=4$

Sei $g=x^2-3\in\mathbb{Q}(\sqrt{2})[x]$. g ist normiert, $g(\sqrt{3})=0$. $\Rightarrow$ g ist über $\mathbb{Q}(\sqrt{2})$ reduzibel. $\overset{\text{grad}(g)=2}{\underset{g(\sqrt{3})=0}{\Rightarrow}}$ $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$ $\lightning$ da $2,3\in\mathbb{Z}\setminus\{0,1\}$ verschiedene quadratfr. Zahlen

also: $g = \mu_{\sqrt{3}, \mathbb{Q}(\sqrt{2})} \Rightarrow [L : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]$

$= \operatorname{grad}(g) = 2 \Rightarrow [L : K] = 2 \cdot 2 = 4$

(3) Bestimme $G = \mathrm{Gal}(L|K)$ bzs auf Isomorphie

$L|K$ galoissch, $[L : K] = 4 \Rightarrow |G| = 4$

4 Primzahlquadrat $\rightarrow$ G ist abelsch $\rightarrow$

$G \cong \mathbb{Z}/4\mathbb{Z}$ oder $G \cong (\mathbb{Z}/2\mathbb{Z})^2$

Ang. $G \cong \mathbb{Z}/4\mathbb{Z} \Rightarrow G$ ist zykl. von Ordn. 4

$\Rightarrow G$ hat genau eine Untergp. U von Ordn. 2

$\xrightarrow{\text{Satz 21.8 (iv)}}$ $L|K$ hat genau einen Zwischenkrp.

M von $L|K$ mit $[M : K] = (G : U) = \frac{|G|}{|U|}$

$= \frac{4}{2} = 2$ Es gibt aber (mind.) zwei verschiedene solche Zwischenkörper, nämlich $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$. ↯

$\Rightarrow G \cong (\mathbb{Z}/2\mathbb{Z})^2$

(4) Bestimmung aller Zwischenkörper

Bestimme die Anzahl der Untergr. von G.

Lagrange $\Rightarrow$ Jede Untergr. von G hat Ordnung 1, 2 oder 4. Die einzigen Untergr. der Ordn. 1 bzw. 4 sind $\{id_L\}$ bzw. G. (Die korrespondierenden Zwischenkrp. sind L bzw. K.) Da 2 Primzahl ist, ist jede Untergr. von G der Ordn. 2 zyklisch. Jede solche Untergr. enthält genau ein Element der Ordn. 2. Sonst ist die Anzahl der Untergr. von Ordn. 2 gleich

$\sqrt{2}$)] da Anzahl der Elt. der Ordn. 2. In $(\mathbb{Z}/2\mathbb{Z})^2$ gibt es davon drei Stück ($(\bar{1},\bar{0})$, $(\bar{0},\bar{1})$, $(\bar{1},\bar{1})$), also gilt dasselbe für U. $\Rightarrow$ G hat genau drei Untergr. der Ordn. 2. $\overset{s.o.}{\Rightarrow}$ $L|K$ hat genau drei Zwischenkörp. M_1, M_2, M_3 mit $[M_j : K] = 2$ für $j = 1,2,3$, und abgesehen von L und K gibt es keine weiteren Zw.körp.

Zwei dieser Zwischenkörp. sind schon bekannt, nämlich $M_1 = \mathbb{Q}(\sqrt{2})$ und $M_2 = \mathbb{Q}(\sqrt{3})$. $\sqrt{6} = \sqrt{2}\cdot\sqrt{3} \in L$

$\Rightarrow M_3 = \mathbb{Q}(\sqrt{6})$ ist weiterer Zw.-körp.:

$6 \in \mathbb{Z}\setminus\{0,1\}$ quadratfrei, $6 \neq 2,3$ $\Rightarrow$ $[M_3 : K] = 2$ und $M_3 \neq M_1, M_2$. also: $L|K$ hat genau 5 Zwischenkörp, nämlich $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{6})$, $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

olche

↓

1,
bzw. 4
den
zahl ist,
Jede
der Ordn. 2
2 gleich

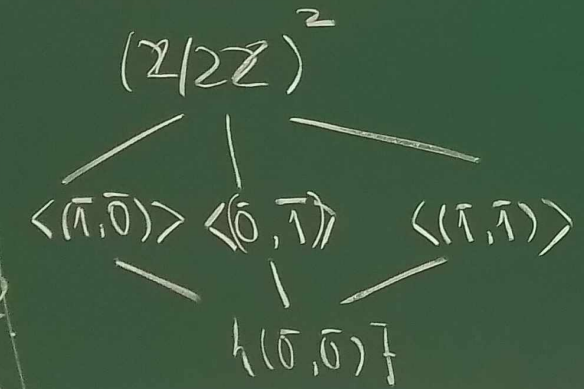
bereits bekannt: $G = \{id, \sigma, \tau, \sigma\tau\}$, wobei

$\sigma(\sqrt{2}) = -\sqrt{2}$, $\sigma(\sqrt{3}) = \sqrt{3}$

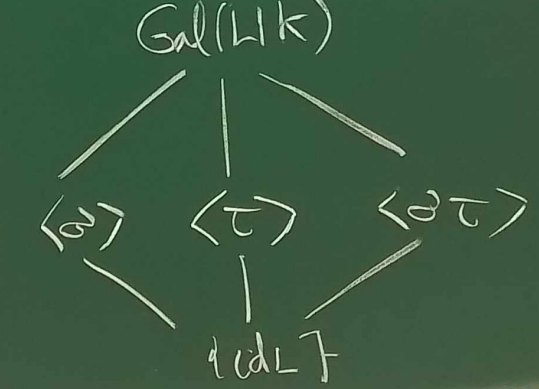
$\tau(\sqrt{2}) = \sqrt{2}$, $\tau(\sqrt{3}) = -\sqrt{3}$

Leicht zu überprüfen: Durch $(\bar{0},\bar{0}) \mapsto id_L$, $(\bar{1},\bar{0}) \mapsto \sigma$, $(\bar{0},\bar{1}) \mapsto \tau$, $(\bar{1},\bar{1}) \mapsto \sigma\circ\tau$ ist ein Isom. $(\mathbb{Z}/2\mathbb{Z})^2 \to Gal(L|K)$ definiert.

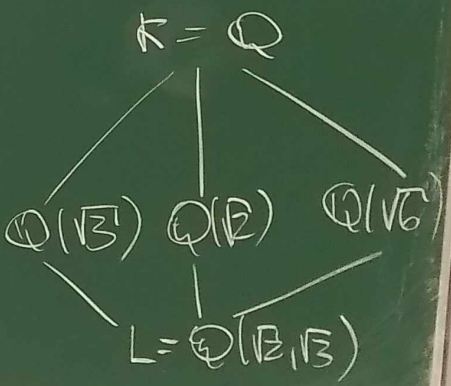
Untergruppen von $(\mathbb{Z}/2\mathbb{Z})^2$



Untergr. von $Gal(L|K)$



Zwischenkörper von $\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}$



$$(\sigma\circ\tau)(\sqrt{6}) = (\sigma\circ\tau)(\sqrt{2})\cdot(\sigma\circ\tau)(\sqrt{3}) = \sigma(\sqrt{2})\cdot\sigma(-\sqrt{3})$$

$$= -\sigma(\sqrt{2})\cdot\sigma(\sqrt{3}) = -(-\sqrt{2})\cdot\sqrt{3} = \sqrt{2}\cdot\sqrt{3} = \sqrt{6}$$

$$\Rightarrow \sqrt{6} \in L^{\langle\sigma\tau\rangle}$$

Normalteiler und normale Teilerweiterungen

Proposition (21.9)

Sei M ein Zwischenkörper von $L|K$ und $U = \mathrm{Gal}(L|M)$ die zugehörige Untergruppe von $G = \mathrm{Gal}(L|K)$. Dann sind folgende Aussagen äquivalent:

(i) Die Erweiterung $M|K$ ist normal.

(ii) Die Untergruppe U ist Normalteiler von G.

In diesem Fall erhalten wir durch $\sigma \mapsto \sigma|_M$ eine Abbildung $G \to \mathrm{Gal}(M|K)$, und diese induziert einen natürlichen Isomorphismus $G/U \cong \mathrm{Gal}(M|K)$.

Beweis von Prop. 21.9:

geg: endl. Galois-Erw. $L|K$, M Zwischenkörper von $L|K$,
$U = \mathrm{Gal}(L|M)$ zugeh. Untergr. von $G = \mathrm{Gal}(L|K)$

Sei $\sigma \in G$. zeige zunächst: $\sigma U \sigma^{-1} = \mathrm{Gal}(L|\sigma(M))$ (*)

Sei $\tau' \in U$. Dann gilt die Äquivalenz

$\tau' \in \sigma U \sigma^{-1} \Leftrightarrow \exists \tau \in U : \sigma \tau \sigma^{-1} = \tau' \Leftrightarrow$

$\exists \tau \in U : \tau = \sigma^{-1} \tau' \sigma \Leftrightarrow \sigma^{-1} \tau' \sigma \in U \Leftrightarrow$

$\sigma^{-1} \tau' \sigma \in \mathrm{Gal}(L|M) \Leftrightarrow \forall \alpha \in M : (\sigma^{-1} \tau' \sigma)(\alpha) = \alpha$

$\Leftrightarrow \forall \alpha \in M : \tau'(\sigma(\alpha)) = \sigma(\alpha)$

$\Leftrightarrow \tau' \in \mathrm{Gal}(L|\sigma(M))$

Beweise nun die Äquivalenz der Aussagen

(i) $U \trianglelefteq G$ (ii) $M|K$ ist normale Erw.

„(i) $\Rightarrow$ (ii)" Sei $\tilde{L}$ ein alg. abg. Erweiterungskörper von L

Es genügt zu zeigen: $\mathrm{Hom}_K(M, \tilde{L}) = \mathrm{Aut}_K(M)$

„$\supseteq$" ist offensichtlich (wegen $M \subseteq L \subseteq \tilde{L}$)

„$\subseteq$" Sei $\sigma \in \mathrm{Hom}_K(M, \tilde{L})$ Da $\tilde{L}$ alg. abg. und $L|M$ ein alg. Erw. ist, existiert eine Fortsetzung τ von σ zu einem Element von $\mathrm{Hom}_K(L, \tilde{L})$ $L|K$ ist normal $\Rightarrow \tau \in \mathrm{Aut}_K(L) \Rightarrow \tau \in G$

(i) $\Rightarrow \tau U \tau^{-1} = U \overset{\text{s.o.}}{\Rightarrow} \mathrm{Gal}(L|\tau(M)) \overset{(*)}{=} \tau U \tau^{-1} = U = \mathrm{Gal}(L|M) \overset{\text{Hauptsatz der Galoisth.}}{\Longrightarrow} \tau(M) = M \overset{\tau|_M = \sigma}{\Longrightarrow} \sigma(M) = M \overset{\sigma \in \mathrm{Hom}_K(M, \tilde{L})}{\Longrightarrow} \sigma \in \mathrm{Aut}_K(M)$

„(ii) ⇒ (i)" Vor: $M|K$ ist normal

z.zg: $U \trianglelefteq G$ Sei $\sigma \in G$. z.zg: $\sigma U \sigma^{-1} = U$

Wegen (*) reicht es z.zg: $\sigma(M) = M$

Als Element von G liegt σ in $\mathrm{Aut}_K(L)$.

damit auch in $\mathrm{Hom}_K(L, \tilde{L}) \to \sigma|_M$

$\in \mathrm{Hom}_K(M, \tilde{L}) \overset{\text{Vor.}}{\Longrightarrow} \sigma \in \mathrm{Aut}_K(M)$

$\to \sigma(M) = M$.

Zeigen nun noch $G/U \cong \mathrm{Gal}(M|K)$.

Definiere $\phi: G = \mathrm{Gal}(L|K) \to \mathrm{Gal}(M|K)$

durch $\sigma \mapsto \sigma|_M$. (beachte dabei:

$\sigma \in G \to \sigma \in \mathrm{Hom}_K(L, \tilde{L}) \Rightarrow \sigma|_M \in$
$\mathrm{Hom}_K(M, \tilde{L}) \overset{M/K \text{ ist normal}}{\Longrightarrow} \sigma|_M \in \mathrm{Aut}_K(M)$)

Die ~~Abbildung~~ ϕ ist ein Hom., denn für alle $\sigma, \sigma' \in G$ und alle $\alpha \in M$ gilt

$(\sigma|_M) \circ (\sigma'|_M)(\alpha) = (\sigma \circ \sigma')(\alpha) =$

$(\sigma \circ \sigma')|_M \Rightarrow \phi(\sigma) \circ \phi(\sigma') =$

$(\sigma|_M) \circ (\sigma'|_M) = (\sigma \circ \sigma')|_M = \phi(\sigma \circ \sigma')$.

Noch zu überprüfen (1) Surjektivität von ϕ

(2) $\ker(\phi) = U = \mathrm{Gal}(L|M)$

zu (1) Sei $\tau \in \mathrm{Gal}(M|K) \to \tau \in \mathrm{Hom}_K(M, \tilde{L})$

L/K alg. $\overset{\tilde{L} \text{ alg. abg.}}{\Longrightarrow}$ $\exists \sigma \in \mathrm{Hom}_K(L, \tilde{L})$ mit $\sigma|_M = \tau$

$L|K$ normal $\Rightarrow$ $\sigma \in \mathrm{Aut}_K(L) \to \sigma \in G$

und $\phi(\sigma) = \sigma_{|M} = \tau$

zu (3) Für jedes $\sigma \in G$ gilt die Äquivalenz

$\sigma \in \ker(\phi) \iff \phi(\sigma) = \mathrm{id}_M \iff \forall \alpha \in M : \sigma(\alpha) = \alpha$

$\iff \sigma \in \mathrm{Gal}(L|M) \iff \sigma \in U$. □

Bem. Sei $f \in K[x]$ irred., L der Zerf.-kp. von f über K, $\alpha_1, \dots, \alpha_n \in L$ die verschl. Nullst. von f in L.

Sei $G = \mathrm{Gal}(L|K)$. Da jedes σ die Nullstellen von f wieder auf Nullst. abbildet, gilt $\sigma|_S \in \mathrm{Per}(S)$ für $S = \{1, \dots, n\}$. Die Elemente von $\mathrm{Per}(S)$ können vg. $|S| = n$ mit den Elementen von S_n identifiziert werden

Bsp: $G = \mathrm{Gal}(L|K)$, $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$.

L ist Zerf.körp von $f = (x^2-2)(x^2-3)$ über $\mathbb{Q}$, mit den Nullst. $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$

$G = \{\mathrm{id}_L, \sigma, \tau, \sigma\tau\}$

i	1	2	3	4
α_i	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
$\sigma(\alpha_i)$	$-\sqrt{2}$	$\sqrt{2}$	$\sqrt{3}$	$-\sqrt{3}$
	α_2	α_1	α_3	α_4

$\Rightarrow \sigma$ entspricht in S_4 der Permutation $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\,2)$

Genauso sieht man: τ entspricht $(3\,4)$, $\sigma\tau$ dem Element $(1\,2)(3\,4)$

Man kann G also mit der Untergr. $\{\mathrm{id}, (1\,2), (3\,4), (1\,2)(3\,4)\} = \langle (1\,2), (3\,4) \rangle$ von S_4 identifizieren.