Galoistheorie

Def. • Eine Körpererweiterung $L|K$ heißt galois'sch (oder Galois-Erweiterung), wenn sie normal und separabel ist.

• In diesem Fall wird $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{id}_K\}$ die Galoisgruppe der Erweiterung genannt.

• Ist L Zerfällungskörper eines Polynoms $f \in K[x]$ über K, dann wird $\mathrm{Gal}(L|K)$ auch mit $\mathrm{Gal}(f|K)$

- In diesem Fall wird $\mathrm{Gal}(L|K) = \mathrm{Aut}_K(L)$ bezeichnet und die Galoisgruppe des Polynoms f genannt.

Möglichkeiten, Elemente von $\mathrm{Gal}(L|K)$ oder $\mathrm{Gal}(f|K)$ konkret anzugeben:

- Ist $L = K(\alpha_1, \dots, \alpha_m)$ (mit $m \in \mathbb{N}$ und $\alpha_1, \dots, \alpha_m \in L$), dann ist jedes $\sigma \in \mathrm{Gal}(L|K)$ durch $\sigma(\alpha_j)$ mit $1 \leq j \leq m$ eindeutig festgelegt.
- Sind $\alpha_1, \dots, \alpha_m$ die verschiedenen Nullstellen von f in L, dann entspricht jedes Element $\sigma \in \mathrm{Gal}(f|K)$ einem Element $\hat{\sigma} \in S_m$ der

symmetrischen Gruppe S_m. Dabei besteht zwischen σ und $\hat{\sigma}$ jeweils der Zusammenhang $\sigma(\alpha_i) = \alpha_j \iff \hat{\sigma}(i) = j$ für alle i, j mit $1 \le i, j \le m$.

Beispiel: Man überprüft leicht, dass $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ der Zerfällungskörper des Polynoms $f = (x^2-2)(x^2-3)$ über $k = \mathbb{Q}$ ist. Die Nullstellen von f sind $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$, $\alpha_3 = \sqrt{3}$, $\alpha_4 = -\sqrt{3}$.

Man kann zeigen: Die Elemente von $G = \mathrm{Gal}(L|k)$ sind gegeben durch $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ mit $\sigma_1(\sqrt{2}) = \sqrt{2}$, $\sigma_1(\sqrt{3}) = \sqrt{3}$ ($\Rightarrow \sigma_1 = \mathrm{id}_L$), $\sigma_2(\sqrt{2}) = -\sqrt{2}$, $\sigma_2(\sqrt{3}) = \sqrt{3}$,

Zerfällungskörper des Polynoms $f = (x^2-2)(x^2-3)$ über $K = \mathbb{Q}$ ist. Die Nullstellen von f sind $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$,

$\sigma_3(\sqrt{2}) = \sqrt{2}$, $\sigma_3(\sqrt{3}) = -\sqrt{3}$, $\sigma_4(\sqrt{2}) = -\sqrt{2}$, $\sigma_4(\sqrt{3}) = -\sqrt{3}$.

$\sigma_2(\alpha_1) = \sigma_2(\sqrt{2}) = -\sqrt{2} = \alpha_2$

$\sigma_2(\alpha_2) = \sigma_2(-\sqrt{2}) = -\sigma_2(\sqrt{2}) = -(-\sqrt{2}) = \sqrt{2} = \alpha_1$

$\sigma_2(\alpha_3) = \sigma_2(\sqrt{3}) = \sqrt{3} = \alpha_3$

$\sigma_2(\alpha_4) = \sigma_2(-\sqrt{3}) = -\sigma_2(\sqrt{3}) = -\sqrt{3} = \alpha_4$

$\Rightarrow$ Das Bild von σ_2 in S_4 ist gegeben durch $\hat{\sigma}_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ $= (12)$. Genauso überprüft man, dass $\hat{\sigma}_1 = \mathrm{id}$, $\hat{\sigma}_3 = (34)$ und $\hat{\sigma}_4 = (12)(34)$. Das Bild von G in S_4 ist also $\{\mathrm{id}, (12), (34), (12)(34)\}$.

Aussagen zur Bestimmung von Elementen der Galoisgruppe $G = Gal(L|K)$, für eine endliche Galois-Erw. $L|K$:

- Ist $\sigma \in G$ und $\alpha \in L$ Nullstelle eines Polynoms $g \in K[x]$, dann muss $\sigma(\alpha)$ ebenfalls eine Nullstelle von g sein.
- Ist $g \in K[x]$ irreduzibel und sind $\alpha, \beta \in L$ Nullstellen von g, dann existiert ein Element $\sigma \in G$ mit $\sigma(\alpha) = \beta$.

- Es gilt stets $|G| = [L:K]$. Also muss insb. $\mathrm{ord}(\sigma)$ für jedes $\sigma \in G$ ein Teiler von $[L:K]$ sein.

Informationen zum Isomorphietyp einer Galoisgruppe

- Sind $m, n \in \mathbb{Z} \setminus \{0, 1\}$ verschiedene quadratfreie Zahlen, dann gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt{m}, \sqrt{n})|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. (Das wurde nur für $m=2$, $n=3$ gezeigt, aber der Beweis läuft für alle anderen Zahlen genauso.)

- Ist $f \in K[x]$ ein Polynom mit separablen irred. Faktoren (immer erfüllt, falls $\operatorname{char} K = 0$ oder K endl.), und sind $\alpha_1, \dots, \alpha_n$ die verschiedenen Nullst. von f in L, dann ist $\mathrm{Gal}(f|K)$ isomorph zu einer Untergr. von S_n.
- Ist f irreduzibel vom Grad n, dann ist diese Untergruppe transitiv und die Ordnung durch n teilbar ($U \leq S_n$ transitiv $\Leftrightarrow \forall i, j \in \{1, \dots, n\}\ \exists \sigma \in U : \sigma(i) = j$)
- Ist q eine Primzahlpotenz > 1 und $n \in \mathbb{N}$, dann gilt $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$. Dabei ist ein Isom. $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$ gegeben durch $a + n\mathbb{Z} \mapsto \varphi_q^a$, wobei φ_q den

Frobenius-Automorphismus $\varphi_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$, $\alpha \mapsto \alpha^q$ bezeichnet.

- Ist $n \in \mathbb{N}$, $n \geq 2$ und $\zeta_n = e^{2\pi i/n}$, dann gilt $\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. Dabei existiert ein Isom. $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$, der jedem Element $a+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ (mit $a \in \mathbb{Z}$, $\mathrm{ggT}(a,n)=1$) den Automorphismus σ_a mit $\sigma_a(\zeta_n) = \zeta_n^a$ zuordnet.

Beispiel: $\mathrm{Gal}(\mathbb{Q}(\zeta_8)|\mathbb{Q}) = \{\sigma_1, \sigma_3, \sigma_5, \sigma_7\}$ mit $\sigma_1 = \mathrm{id}_{\mathbb{Q}(\zeta_8)}$, $\sigma_3(\zeta_8) = \zeta_8^3$, $\sigma_5(\zeta_8) = \zeta_8^5$ und $\sigma_7(\zeta_8) = \zeta_8^7$

F25T3A4

Für jedes $a \in \mathbb{Z}$ sei $f_a = x^4 + ax^2 + 1 \in \mathbb{Q}[x]$ und $G_a = \mathrm{Gal}(f_a) = \mathrm{Gal}(L_a|\mathbb{Q})$, wobei $L_a \subseteq \mathbb{C}$ den Zerfällungskörper von f_a über $\mathbb{Q}$ bezeichnet.

(a) Bestimmen Sie ein $a \in \mathbb{Z}$ mit $G_a = \{\mathrm{id}_{L_a}\}$.

Es ist $|G_a| = |\{\mathrm{id}_{L_a}\}| = 1$ genau dann, wenn $[L_a : \mathbb{Q}] = 1$ ist (denn die Ordnung der Galoisgr. stimmt überein mit dem Erweiterungsgrads des Zerfällungskörpers). Dies ist äquivalent zu $L_a = \mathbb{Q}$.

$[L_a : \mathbb{Q}] = 1$ ist (denn die Ordnung der Galoisgr.

Also muss a so gewählt werden, dass alle komplexen Nullstellen von f_a in $\mathbb{Q}$ liegen. Die einzige Nullstelle von $x^2 - 2x + 1 = (x-1)^2$ ist 1, und die Nullstellen von $x^4 - 2x^2 + 1$ sind folglich genau die Zahlen, deren Quadrat 1 ist, also ± 1. $\Rightarrow$

wähle $a = -2$, überprüfe (durch Nachrechnen):
$f_{-2} = (x-1)^2(x+1)^2$ Dieses Polynom zerfällt über $\mathbb{Q}$ in Linearfaktoren. Folglich ist $L_{-2} = \mathbb{Q}$ und $G_{-2} = \mathrm{Gal}(\mathbb{Q}|\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\} = \{\mathrm{id}_{L_{-2}}\}$

(b) Bestimmen Sie ein $a \in \mathbb{Z}$, so dass die einzigen Elemente von G_a die Identität und die komplexe Konjugation sind.

(Suche ein Polynom der angeg. Form mit Zerfällungskörper $\mathbb{Q}(i)$, denn dieser Körper hat die beiden angeg. Automorphismen.)

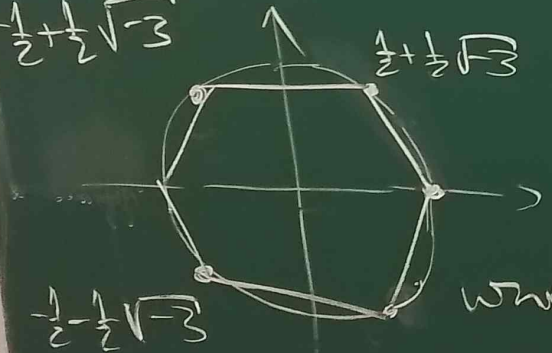
Betrachte das Pol. $(x^2+1)^2 = x^4 + 2x^2 + 1 = f_2$.

Es gilt $f_2 = (x+i)^2(x-i)^2$, somit zerfällt f_2 über $\mathbb{Q}(i)$ in Linearfaktoren. Außerdem bilden die Nullstellen $\pm i$ ein Erz.-system von $\mathbb{Q}(i)|\mathbb{Q}$. $\Rightarrow L_2 = \mathbb{Q}(i)$

Weil -1 in $\mathbb{Z}\setminus\{0,1\}$ eine quadratfreie Zahl ist, gilt lt. Vl. $[\mathbb{Q}(i):\mathbb{Q}] = [\mathbb{Q}(\sqrt{-1}):\mathbb{Q}] = 2$ und somit $|G_2| = [L_2:\mathbb{Q}] = 2$. Eines der beiden Elemente von G_2 ist id_{L_2}. Sei $\iota: \mathbb{C} \to \mathbb{C}, z \mapsto \bar{z}$ die komplexe Konjugation. Weil $\mathbb{Q}(i)|\mathbb{Q}$ als Erweiterung vom Grad 2 normal ist, ist $\tau = \iota|_{\mathbb{Q}(i)}$ ein Element von $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(i)) = G_2$. Wegen $\tau(i) = \bar{i} = -i \neq i$ ist dies ein nichttriviales Element. Also ist das zweite Element von G_2 die komplexe Konjugation.

(c) Bestimmen Sie den Isomorphietyp von G_{-1}.

Gesucht ist der Isomorphietyp der Galoisgruppe des Polynoms $f_{-1} = x^4 - x^2 + 1$. Es gilt $f_{-1}(x) = g_{-1}(x^2)$ mit $g_{-1} = x^2 - x + 1$. Laut p-q-Formel sind die Nullstellen von g_{-1} gegeben durch $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$.



Das sind primitive sechste Einheitswurzeln. Jedes Quadrat einer primitiven 12-ten Einheitswurzel ist eine primitive sechste Einheitswurzel (denn aus $\mathrm{ord}(\zeta) = 12$ mit $\zeta \in \mathbb{C}^\times$ folgt $\mathrm{ord}(\zeta^2) = \frac{12}{2} = 6$). Da beide Nullstellen

von g_{-1} primitive 6-te Einheitswurzeln sind, ist also jede primitive 12-te Einheitswurzel eine Nullstelle von f_{-1}, denn die Nullstellen von f_{-1} sind genau die Zahlen $\alpha \in \mathbb{C}$ mit $g_{-1}(\alpha^2) = 0$.

Da es genau $\varphi(12) = \varphi(3)\,\varphi(4) = 2 \cdot 2 = 4$ primitive 12-te Einheitswurzeln gibt, sind die Nullstellen von f_{-1} wegen $\operatorname{grad} f_{-1} = 4$ genau die 12-ten Einheitswurzeln.

Also ist $f_{-1} = \Phi_{12}$, das 12-te Kreisteilungspolynom.

Laut Vorlesung gilt $\mathrm{Gal}(\Phi_{12} | \mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_{12}) | \mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^\times \cong (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, mit $\zeta_{12} = e^{2\pi i/12}$.
Also gilt auch $G_{-1} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. □