KAPITEL 6

# Galoiserweiterungen

## 1. Einführung

**Bemerkungen:** Sei $L|K$ eine endliche Körpererweiterung.

(1) Ist $L|K$ separabel, so gibt es nach dem Satz vom primitiven Element II ein $\alpha \in L$ mit $L = K(\alpha)$.
(2) Ist der Grundkörper $K$ vollkommen, also beispielsweise von Charakteristik 0 oder ein endlicher Körper, so ist $L|K$ separabel. Bei uns wird dies meist der Fall sein.
(3) Sei nun $L = K(\alpha)$ separabel vom Grad $n$ über $K$ und $f \in K[x]$ das Minimalpolynom von $\alpha$ über $K$. Dann gibt es paarweise verschiedene Elemente $\alpha_1, \ldots, \alpha_n \in \overline{K}$ mit

$$f = (x - \alpha_1) \ldots (x - \alpha_n).$$

(Natürlich kann man $\alpha_1 = \alpha$ annehmen.) Man erhält dann $n$ verschiedene $K$-Körperhomomorphismen

$$\sigma_i : K(\alpha) \to \overline{K} \text{ mit } \sigma_i(\alpha) = \alpha_i.$$

(4) Sei nun $L = K(\alpha)$ zusätzlich normal über $K$, d.h. $L$ ist der Zerfällungskörper eines Polynoms $g \in K[x]$. Dann zerfällt $f$ über $L$ in Linearfaktoren, d.h. $\alpha_1, \ldots, \alpha_n \in L$ und die $K$-Homomorphismen $\sigma_i : L \to \overline{K}$ sind wegen $\sigma_i(L) = L$ Automorphismen von $L$:

$$\mathrm{Aut}(L|K) = \{\sigma_1, \ldots, \sigma_n\}.$$

Insbesondere gilt also $|\mathrm{Aut}(L|K)| = [L : K]$. (Solche Erweiterungen werden wir im Folgenden studieren.)

DEFINITION. *Eine algebraische Körpererweiterung $L|K$ heißt* **Galoiserweiterung**, **Galois-Erweiterung** *oder* **galoissch**, *wenn $L|K$* **normal und separabel** *ist. Man schreibt*

$$\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K)$$

*und nennt die Automorphismengruppe auch die* **Galoisgruppe** *(oder* **Galois-Gruppe***) von $L|K$.*
*Die Erweiterung heißt* **abelsch**, *wenn $\mathrm{Gal}(L|K)$ abelsch ist; die Erweiterung heißt* **zyklisch**, *wenn $\mathrm{Gal}(L|K)$ eine zyklische Gruppe ist.*

Wir werden im Folgenden nur endliche Galoiserweiterungen anschauen. Der folgende Satz stellt zusammen, was wir bereits wissen.

SATZ. *Sei $L|K$ eine Galoiserweiterung vom Grad $n$.*

(1) *Es gibt ein $\alpha \in L$ mit $L = K(\alpha)$. Sei $f \in K[x]$ das Minimalpolynom von $\alpha$ über $K$. Es hat Grad $n$.*
(2) *Das Polynom $f$ zerfällt in $L[x]$ in paarweise verschiedene Linearfaktoren:*

$$f(x) = (x - \alpha)(x - \alpha_2) \ldots (x - \alpha_n).$$

(3) *Durch $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, n$, werden $K$-Automorphismen $\sigma_i : L \to L$ definiert, d.h.*

$$\mathrm{Gal}(L|K) = \mathrm{Aut}(L|K) = \{\sigma_1, \ldots, \sigma_n\}.$$

(4) *Es gilt*

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

---

Datei: kt_gal.tex. Version vom 1.7.2024

*Beweis:*

(1) Da $L|K$ galoissch ist, ist $L|K$ separabel. Nach dem Satz vom primitiven Element gibt es ein $\alpha \in L$ mit $L = K(\alpha)$. Das Minimalpolynom $f \in K[x]$ von $\alpha$ hat dann natürlich Grad $n = [L : K]$.

(2) Da $\alpha$ separabel über $K$ ist, hat das Minimalpolynom in einem algebraischen Abschluss $n$ verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n$, sodass
$$f = (x - \alpha_1) \ldots (x - \alpha_n) \in \overline{K}[x].$$
O.E. ist $\alpha_1 = \alpha$. Da das über $K$ irreduzible Polynom $f$ einen Nullstelle in $L$ hat, nämlich $\alpha$, liegen auch die anderen Nullstellen $\alpha_2, \ldots, \alpha_n$ in $L$, da $L|K$ normal ist.

(3) Die $K$-Homomorphismen $\sigma : K(\alpha) \to \overline{K}$ ergeben sich aus den Nullstellen von $f$ in $\overline{K}$, sodass sich die angegebene Form ergibt.

(4) Dies folgt aus (3). ■

**Beispiel:** Sei $K$ ein Körper der Charakteristik $\neq 2$ und $d \in K \setminus K^2$. Dann ist $f = x^2 - d \in K[x]$ irreduzibel und separabel. Ist $\alpha$ eine Nullstelle von $f$, so gilt wegen $\alpha^2 = d$
$$f = (x - \alpha)(x + \alpha),$$
neben der Identität gibt es also noch den Automorphismus $\sigma$ mit
$$\sigma(\alpha) = -\alpha, \quad \text{also} \quad \sigma(u + v\alpha) = u - v\alpha \text{ für } u, v \in K.$$
Es ist
$$\mathrm{Gal}(K(\alpha)|K) = \{\mathrm{id}_{K(\alpha)}, \sigma\}.$$
Insbesondere gilt also $\mathrm{Gal}(K(\alpha)|K) \simeq \mathbb{Z}_2$.

**Beispiel:** Sei $\alpha \in \mathbb{C}$ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms $f = x^3 - 3x + 1 \in \mathbb{Q}[x]$. In Aufgabe P23 haben wir die Zerlegung
$$f = (x - \alpha)(x - \frac{1}{1-\alpha})(x - \frac{\alpha - 1}{\alpha})$$
gezeigt. Als ist $\mathbb{Q}(\alpha)|\mathbb{Q}$ auch normal. Wir erhalten durch
$$\sigma(\alpha) = \frac{1}{1-\alpha}, \quad \tau(\alpha) = \frac{\alpha - 1}{\alpha}$$
zwei Automorphismen, und damit
$$\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\alpha)}, \sigma, \tau\}.$$
Es ist
$$\sigma^2(\alpha) = \sigma(\sigma(\alpha)) = \sigma(\frac{1}{1-\alpha}) = \frac{1}{1-\sigma(\alpha)} = \frac{1}{1 - \frac{1}{1-\alpha}} = \frac{1-\alpha}{-\alpha} = \frac{\alpha - 1}{\alpha} = \tau(\alpha),$$
also $\sigma^2 = \tau$. Da es 3 Automorphismen gibt, gilt $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) \simeq \mathbb{Z}_3$.

**Beispiel:** $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ist Zerfällungskörper der Polynome $x^2 - 2$ und $x^2 - 3$ über $\mathbb{Q}$, also normal über $\mathbb{Q}$. Da $\mathbb{Q}$ Charakteristik 0 hat, ist die Erweiterung auch separabel, und daher galoissch. Daher folgt aus $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ sofort
$$|\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q})| = 4.$$
Wie sehen die Automorphismen aus? Ist $f \in \mathbb{Q}[x]$ und $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ mit $f(\alpha) = 0$, so gilt auch $f(\sigma(\alpha)) = 0$ für jeden Automorphismus $\sigma$. Wendet man dies auf $x^2 - 2$ und $x^2 - 3$ an, so ergibt sich
$$\sigma(\sqrt{2}) \in \{\pm\sqrt{2}\} \quad \text{und} \quad \sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}.$$
Da es vier Automorphismen gibt und diese durch ihre Wirkung auf $\sqrt{2}$ und $\sqrt{3}$ bestimmt sind, können wir die Automorphismen direkt angeben:
$$\begin{aligned}
\sigma_1(\sqrt{2}) &= \sqrt{2}, & \sigma_1(\sqrt{3}) &= \sqrt{3}, \\
\sigma_2(\sqrt{2}) &= \sqrt{2}, & \sigma_2(\sqrt{3}) &= -\sqrt{3}, \\
\sigma_3(\sqrt{2}) &= -\sqrt{2}, & \sigma_3(\sqrt{3}) &= \sqrt{3}, \\
\sigma_4(\sqrt{2}) &= -\sqrt{2}, & \sigma_4(\sqrt{3}) &= -\sqrt{3}.
\end{aligned}$$

Es folgt sofort $\sigma_i^2 = \mathrm{id}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}$, und damit $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})|\mathbb{Q}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

**Beispiel:** $\mathbb{Q}(\sqrt[3]{2})$ ist keine Galoiserweiterung von $\mathbb{Q}$, da die Erweiterung nicht normal ist. Das Minimalpolynom von $\alpha = \sqrt[3]{2}$ ist $f = x^3 - 2$. Mit der 3-ten Einheitswurzel $\zeta = \frac{-1+i\sqrt{3}}{2}$ gilt

$$f = (x - \alpha)(x - \zeta\alpha)(x - \zeta^2\alpha).$$

Zerfällungskörper von $f$ ist

$$\mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha) = \mathbb{Q}(\alpha, \zeta).$$

Daher ist $\mathbb{Q}(\alpha, \zeta)$ eine Galoiserweiterung von $\mathbb{Q}$.

## 2. Der Hauptsatz der Galoistheorie

Die Galoistheorie liefert eine Beziehung zwischen den Untergruppen der Galoisgruppe und den Zwischenkörpern einer Galoiserweiterung.

Satz. *Sei $L|K$ eine endliche Galoiserweiterung mit Galoisgruppe* $\mathrm{Gal}(L|K)$.

(1) *Ist $H \subseteq \mathrm{Gal}(L|K)$ eine Untergruppe der Galoisgruppe, dann ist*

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ für alle } \sigma \in H\}$$

*ein Unterkörper von $L$, der $K$ enthält, also ein Zwischenkörper der Erweiterung $L|K$. Man nennt $L^H$ auch den* **Fixkörper** *der Untergruppe $H$.*

$$\{\mathrm{id}\} \subseteq H \subseteq \mathrm{Gal}(L|K) \quad \Longrightarrow \quad L \supseteq L^H \supseteq K.$$

(2) *Ist $E$ ein Zwischenkörper der Erweiterung $L|K$, d.h. $E$ ist ein Körper mit $K \subseteq E \subseteq L$, so ist $L|E$ eine Galoiserweiterung und* $\mathrm{Gal}(L|E)$ *eine Untergruppe von* $\mathrm{Gal}(L|K)$.

$$K \subseteq E \subseteq L \quad \Longrightarrow \quad \mathrm{Gal}(L|K) \supseteq \mathrm{Gal}(L|E) \supseteq \{\mathrm{id}\}.$$

*Beweis:*

(1) Da die Elemente von $\mathrm{Gal}(L|K)$, also auch die von $H$, den Körper $K$ festlassen, gilt $K \subseteq L^H$. Sind nun $\alpha, \beta \in L^H$, d.h. für alle $\sigma \in H$ gilt $\sigma(\alpha) = \alpha$ und $\sigma(\beta) = \beta$, so gilt natürlich auch

$$\sigma(\alpha + \beta) = \alpha + \beta \quad \text{und} \quad \sigma(\alpha\beta) = \alpha\beta$$

für alle $\sigma \in H$. Außerdem gilt im Fall $\alpha \neq 0$

$$\sigma(\frac{1}{\alpha}) = \frac{1}{\alpha}.$$

Dies zeigt, dass $L^H$ ein Körper ist, der $K$ enthält.

(2) Sei $E$ ein Körper mit $K \subseteq E \subseteq L$. Da $L$ Zerfällungskörper von Polynomen aus $K[x]$ ist, ist natürlich $L$ auch Zerfällungskörper von Polynomen aus $E[x]$ - man nehme die gleichen Polynome. Dies zeigt, dass $L|E$ normal ist. Da $L|K$ separabel ist, ist auch $L|E$ separabel. Daher ist $L|E$ eine Galoiserweiterung. Die Körperhomomorphismen aus $\mathrm{Gal}(L|E)$ sind Automorphismen von $L$, die $E$ festlassen, lassen auch $K$ festlassen. Daher können wir sie als Teilmenge von $\mathrm{Gal}(L|K)$ auffassen, d.h. $\mathrm{Gal}(L|E)$ ist eine Untergruppe von $\mathrm{Gal}(L|K)$. ■

**Achtung:** Ist $K \subseteq E \subseteq L$ und $L|K$ galoissch, so ist auch $L|E$ galoissch. Die Erweiterung $E|K$ muss nicht galoissch sein, wie man aus dem vorangegangenen Beispiel

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta)$$

sehen kann.

Was passiert, wenn wir die im Satz angegebenen Abbildungen hintereinander ausführen? Sei $L|K$ eine endliche Galoiserweiterung.

- Ist $H$ eine Untergruppe von $\mathrm{Gal}(L|K)$, so ist $L^H$ ein Zwischenkörper und damit $L|L^H$ eine Galoiserweiterung, also $\mathrm{Gal}(L|L^H)$ eine Untergruppe von $\mathrm{Gal}(L|L^H)$. Daher ist es naheliegend zu fragen, in welcher Beziehung
$$H \quad \text{und} \quad \mathrm{Gal}(L|L^H)$$
stehen.
- Ist $E$ ein Zwischenkörper der Erweiterung $L|K$, so ist $\mathrm{Gal}(L|E)$ eine Untergruppe von $\mathrm{Gal}(L|K)$, wir können also den Fixkörper $L^{\mathrm{Gal}(L|E)}$ betrachten und fragen, in welcher Beziehung
$$E \quad \text{und} \quad L^{\mathrm{Gal}(L|E)}$$
stehen.

Tatsächlich gilt in beiden Fällen die Gleichheit.

Satz. *Sei $L|K$ eine endliche Galoiserweiterung.*

(1) *Ist $H$ eine Untergruppe von* $\mathrm{Gal}(L|K)$*, so gilt*
$$H = \mathrm{Gal}(L|L^H).$$
(2) *Ist $E$ ein Zwischenkörper der Erweiterung $L|K$, so gilt*
$$E = L^{\mathrm{Gal}(L|E)}.$$

*Beweis:*

(1)
- $\mathrm{Gal}(L|L^H)$ enthält die Körperhomomorphismen von $L$, die $L^H$ festlassen. Da $L^H$ unter $H$ festbleibt, gilt natürlich
$$H \subseteq \mathrm{Gal}(L|L^H).$$
- Nach dem Satz vom primitiven Element gibt es ein $\alpha \in L$ mit $L = K(\alpha)$. Dann gilt natürlich auch
$$L = L^H(\alpha).$$
Sei $m_{\alpha,L^H} \in K^H[x]$ das Minimalpolynom von $\alpha$ über $L^H$. Wir betrachten nun
$$f = \prod_{\sigma \in H} (x - \sigma(\alpha)).$$
Für $\tau \in H$ gilt
$$\tau(f) = \prod_{\sigma \in H} (x - \tau(\sigma(\alpha))) = \prod_{\sigma \in H} (x - \sigma(\alpha)) = f.$$
Die Koeffizienten von $f$ bleiben fest unter den Elementen von $H$, sie liegen also in $L^H$, d.h.
$$f \in L^H[x].$$
Wegen $f(\alpha) = 0$ und der Eigenschaft des Minimalpolynoms folgt $m_{\alpha,L^H} \mid f$, also $\mathrm{grad}(m_{\alpha,L^H}) \leq \mathrm{grad}(f)$. Es folgt
$$|\mathrm{Gal}(L|L^H)| = [L : L^H] = [L^H(\alpha) : L^H] = \mathrm{grad}(m_{\alpha,L^H}) \leq \mathrm{grad}(f) = |H|.$$
Nun haben wir eben $H \subseteq \mathrm{Gal}(L|L^H)$ gezeigt, was
$$|H| \leq |\mathrm{Gal}(L|L^H)|$$
impliziert. Setzen wir beide Abschätzungen zusammen, so ergibt sich
$$|H| = |\mathrm{Gal}(L|L^H)|,$$
also wegen $H \subseteq \mathrm{Gal}(L|L^H)$ dann
$$H = \mathrm{Gal}(L|L^H),$$
was zu zeigen war.

(2)
- $E$ bleibt unter $\mathrm{Gal}(L|E)$ fest, was sofort
$$E \subseteq L^{\mathrm{Gal}(L|E)}$$
liefert.

- Wenden wir (1) auf $H = \mathrm{Gal}(L|E)$ an, so ergibt sich
$$\mathrm{Gal}(L|E) = \mathrm{Gal}(L|L^{\mathrm{Gal}(L|E)}).$$
Es folgt
$$[L : E] = |\mathrm{Gal}(L|E)| = |\mathrm{Gal}(L|L^{\mathrm{Gal}(L|E)})| = [L : L^{\mathrm{Gal}(L|E)}].$$
Mit $E \subseteq L^{\mathrm{Gal}(L|E)}$ ergibt sich dann
$$[L : L^{\mathrm{Gal}(L|E)}] \cdot [L^{\mathrm{Gal}(L|E)} : E] = [L : E] = [L : L^{\mathrm{Gal}(L|E)}],$$
also $[L^{\mathrm{Gal}(L|E)} : E] = 1$, und damit
$$E = L^{\mathrm{Gal}(L|E)},$$
was wir zeigen wollten. ■

Zur Vorbereitung des Hauptsatzes stellen wir noch einen Satz vor:

Satz. *Sei $L|K$ eine endliche Galoiserweiterung.*

(1) *Ist $H$ eine Untergruppe von $\mathrm{Gal}(L|K)$, so gilt für alle $\sigma \in \mathrm{Gal}(L|K)$*
$$\sigma(L^H) = L^{\sigma H \sigma^{-1}}.$$
(2) *Für Zwischenkörper $E, E'$ und $\sigma \in \mathrm{Gal}(L|K)$ gilt*
$$\sigma(E) = E' \quad \Longleftrightarrow \quad \sigma\,\mathrm{Gal}(L|E)\,\sigma^{-1} = \mathrm{Gal}(L|E').$$
(3) *Für einen Zwischenkörper $E$ gilt:*
$$E|K \text{ galoissch} \quad \Longleftrightarrow \quad \mathrm{Gal}(L|E) \text{ ist Normalteiler in } \mathrm{Gal}(L|K).$$
(4) *Ist $E$ ein Zwischenkörper, sodass $E|K$ galoissch ist, so ist die natürliche Abbildung $\mathrm{Gal}(L|K) \to \mathrm{Gal}(E|K)$ surjektiv mit Kern $\mathrm{Gal}(L|E)$. Insbesondere gilt*
$$\mathrm{Gal}(L|K)/\mathrm{Gal}(L|E) \xrightarrow{\simeq} \mathrm{Gal}(E|K).$$

*Beweis:*

(1) Für $\alpha \in L$ gilt:
$$\begin{aligned}
\alpha \in \sigma(L^H) &\iff \sigma^{-1}(\alpha) \in L^H \iff \tau(\sigma^{-1}(\alpha)) = \sigma^{-1}(\alpha) \text{ für alle } \tau \in H \iff \\
&\iff \sigma(\tau(\sigma^{-1}(\alpha))) = \alpha \text{ für alle } \tau \in H \iff \\
&\iff (\sigma\tau\sigma^{-1})(\alpha) = \alpha \text{ für alle } \tau \in H \iff \\
&\iff \tau'(\alpha) = \alpha \text{ für alle } \tau' \in \sigma H \sigma^{-1} \iff \\
&\iff \alpha \in L^{\sigma H \sigma^{-1}}.
\end{aligned}$$
Es folgt die Behauptung.

(2) Sei $E = L^H$ und $E' = L^{H'}$. Mit (1) ergibt sich:
$$\begin{aligned}
\sigma(E) = E' &\iff \sigma(L^H) = L^{H'} \iff L^{\sigma H \sigma^{-1}} = L^{H'} \iff \\
&\iff \sigma H \sigma^{-1} = H' \iff \sigma\,\mathrm{Gal}(L|E)\,\sigma^{-1} = \mathrm{Gal}(L|E').
\end{aligned}$$

(3) $E$ ist genau dann normal, also galoissch über $K$, wenn $\sigma(E) = E$ für alle $\sigma \in \mathrm{Gal}(L|K)$ gilt. Die Behauptung folgt dann mit (2).

(4) Die Aussage folgt daraus, dass sich jeder $K$-Automorphismus $E \to E$ zu einem $K$-Automorphismus $L \to L$ fortsetzen lässt. ■

Wir fassen die vorangegangenen Sätze im **Hauptsatz der Galoistheorie** zusammen:

Satz (Hauptsatz der Galoistheorie). *Sei $L|K$ eine endliche Galoiserweiterung.*

(1) *Es gibt eine Bijektion zwischen folgenden Mengen:*

$$\begin{array}{rcl} \{E \text{ Zwischenkörper von } L|K\} & \leftrightarrow & \{H \text{ Untergruppe von } \mathrm{Gal}(L|K)\} \\ E & \mapsto & \mathrm{Gal}(L|E) \\ L^H & \leftarrow & H \end{array}$$

*Dabei gilt*

$$E = L^{\mathrm{Gal}(L|E)} \quad \text{und} \quad H = \mathrm{Gal}(L|L^H).$$

(2) *Die Abbildungen in (1) sind inklusionsumkehrend, d.h.*
- $E_1 \subseteq E_2 \Longrightarrow \mathrm{Gal}(L|E_2) \subseteq \mathrm{Gal}(L|E_1)$
- $H_1 \subseteq H_2 \Longrightarrow L^{H_2} \subseteq L^{H_1}$

(3) *Für einen Zwischenkörper $E$ von $L|K$ gilt:*

$$E|K \text{ ist galoissch} \quad \Longleftrightarrow \quad \mathrm{Gal}(L|E) \text{ ist Normalteiler von } \mathrm{Gal}(L|K).$$

(4) *Ist $E$ ein Zwischenkörper von $L|K$ und $E|K$ galoissch, so gilt $\sigma(E) = E$ für alle $\sigma \in \mathrm{Gal}(L|K)$ und die Abbildung $\mathrm{Gal}(L|K) \xrightarrow{\sigma \mapsto \sigma|_L} \mathrm{Gal}(E|K)$ induziert einen Isomorphismus*

$$\mathrm{Gal}(L|K)/\mathrm{Gal}(L|E) \xrightarrow{\simeq} \mathrm{Gal}(E|K).$$

**Beispiel:** Sei $\alpha = \sqrt[3]{2} \in R$. Das Minimalpolynom von $\alpha$ ist $f = x^3 - 2$. Mit $\zeta = \frac{-1+i\sqrt{3}}{2}$ gilt

$$f = (x - \alpha)(x - \zeta\alpha)(x - \zeta^2\alpha).$$

Der Zerfällungskörper von $f$ ist also

$$L = \mathbb{Q}(\alpha, \zeta\alpha, \zeta^2\alpha) = \mathbb{Q}(\alpha, \zeta).$$

Wegen $\alpha \in \mathbb{R}$ und $\zeta \notin \mathbb{R}$, $\zeta^2 + \zeta + 1 = 0$ gilt $[\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] = 2$. Es folgt

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, \zeta) : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Da die Elemente von $\mathrm{Gal}(L|\mathbb{Q})$ die Zahlen $\alpha, \zeta\alpha, \zeta^2\alpha$ permutieren und es genau 6 Permutationen gibt, liefert jede Permutation auch einen Automorphismus:

| $x$ | $\alpha$ | $\zeta\alpha$ | $\zeta^2\alpha$ | $\zeta$ |
|---|---|---|---|---|
| $\mathrm{id}(x)$ | $\alpha$ | $\zeta\alpha$ | $\zeta^2\alpha$ | $\zeta$ |
| $\sigma_{(12)}(x)$ | $\zeta\alpha$ | $\alpha$ | $\zeta^2\alpha$ | $\zeta^2$ |
| $\sigma_{(13)}(x)$ | $\zeta^2\alpha$ | $\zeta\alpha$ | $\alpha$ | $\zeta^2$ |
| $\sigma_{(23)}(x)$ | $\alpha$ | $\zeta^2\alpha$ | $\zeta\alpha$ | $\zeta^2$ |
| $\sigma_{(123)}(x)$ | $\zeta\alpha$ | $\zeta^2\alpha$ | $\alpha$ | $\zeta$ |
| $\sigma_{(132)}(x)$ | $\zeta^2\alpha$ | $\alpha$ | $\zeta\alpha$ | $\zeta$ |

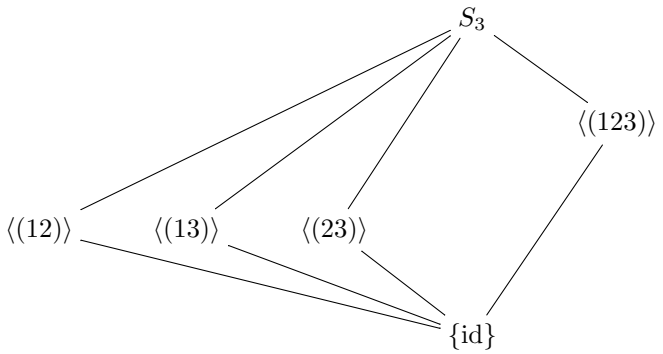
Die Gruppe $S_3$ besitzt drei Untergruppen der Ordnung 2, nämlich

$$\langle(12)\rangle, \quad \langle(13)\rangle, \quad \langle(23)\rangle,$$

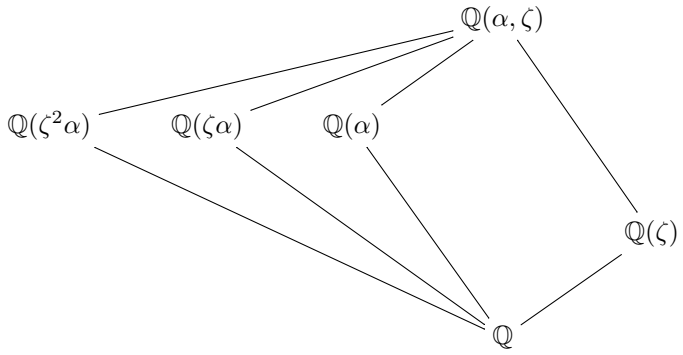
und eine Untergruppe der Ordnung 3, nämlich

$$\langle(123)\rangle = \{\mathrm{id}, (123), (132)\}.$$

Als Untergruppendiagramm erhält man



Damit erhält man das zugehörige Unterkörperdiagramm:




## 3. Ein galoistheoretischer Beweis zum Satz vom primitiven Element II

Beim Satz vom primitiven Element II haben wir zunächst in einem Lemma gezeigt, dass $K(\alpha + c\beta) = K(\alpha, \beta)$ gilt, wenn man einige Werte für $c$ ausschließt. Der nachfolgende Beweis mit Galoistheorie zeigt, warum die Charakterisierung der auszuschließenden Werte für $c$ natürlich ist.

LEMMA. *Sei $K$ ein Körper und $f, g \in K[x]$ separable irreduzible Polynome. Sei $L$ ein Zerfällungskörper von $f$ und $g$ über $K$. Dann ist $L|K$ separabel und normal, also galoissch. Sei*

$$f(x) = (x-\alpha)(x-\alpha_2)\dots(x-\alpha_m) \quad \textit{und} \quad g(x) = (x-\beta)(x-\beta_2)\dots(x-\beta_n)$$

*mit $\alpha, \alpha_2, \dots, \alpha_m, \beta, \beta_2, \dots, \beta_n \in L$. Dann gilt*

$$K(\alpha,\beta) = K(\alpha + c\beta) \textit{ für alle } c \in K \setminus \{0\} \textit{ mit } c \notin \{\frac{\alpha - \alpha_i}{\beta_j - \beta} : 2 \le i \le m, 2 \le j \le n\}.$$

*Beweis:* Sei $c \in K\setminus\{0\}$. Natürlich gilt $K(\alpha+c\beta) \subseteq K(\alpha,\beta)$. Wir betrachten den Fall $K(\alpha+c\beta) \subsetneq K(\alpha,\beta)$. Dann gilt

$$\mathrm{Gal}(L|K(\alpha+c\beta)) \supsetneq \mathrm{Gal}(L|K(\alpha,\beta)).$$

Es gibt also einen Automorphismus $\sigma \in \mathrm{Gal}(L|K)$ mit

$$\sigma(\alpha+c\beta) = \alpha + c\beta, \quad \text{aber} \quad \sigma(\alpha) \neq \alpha \text{ oder } \sigma(\beta) \neq \beta.$$

Wegen $c \neq 0$ gilt dann

$$\sigma(\alpha) \neq \alpha \quad \text{und} \quad \sigma(\beta) \neq \beta.$$

$\sigma$ permutiert die Nullstellen von $f$, also $\{\alpha, \alpha_2, \dots, \alpha_m\}$, und die Nullstellen von $g$, also $\{\beta, \beta_2, \dots, \beta_n\}$. Es gibt dann ein $i \in \{2, \dots, m\}$ und ein $j \in \{2, \dots, n\}$ mit

$$\sigma(\alpha) = \alpha_i \quad \text{und} \quad \sigma(\beta) = \beta_j.$$

Es folgt

$$\alpha + c\beta = \sigma(\alpha + c\beta) = \sigma(\alpha) + c\sigma(\beta) = \alpha_i + c\beta_j, \quad \text{also} \quad \alpha - \alpha_i = c(\beta_j - \beta),$$

und damit

$$c = \frac{\alpha - \alpha_i}{\beta_j - \beta}.$$

Schließt man also $c$ von obiger Form aus, so gilt $K(\alpha + c\beta) = K(\alpha, \beta)$. ■

## 4. Beispiele für Galoisgruppen

In der folgenden Tabelle sind ein paar Beispiele für Galoisgruppen (ohne Beweis) angegeben.

| Körpererweiterung über $\mathbb{Q}$ | Galoisgruppe |
|---|---|
| $\mathbb{Q}$ | $Z_1$ |
| $\mathbb{Q}(\sqrt{d})$ mit $d \in \mathbb{Q}^* \setminus \mathbb{Q}^{*2}$ | $Z_2$ |
| $\mathbb{Q}(\alpha)$ mit $\alpha^3 - 3\alpha + 1 = 0$ | $Z_3$ |
| $\mathbb{Q}(\sqrt{10 + \sqrt{10}})$ | $Z_4$ |
| $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ | $Z_2 \times Z_2$ |
| $\mathbb{Q}(\sqrt[3]{2}, \frac{-1+i\sqrt{3}}{2})$ | $S_3$ |
| $\mathbb{Q}(\sqrt{(2+\sqrt{2})(5+\sqrt{5})})$ | $Z_2 \times Z_4$ |
| $\mathbb{Q}(\sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ | $Q_8$ |
| $\mathbb{Q}(\sqrt{3+\sqrt{3}}, \sqrt{2})$ | $D_4$ (bzw. $D_8$) |