universität wien

# BACHELORARBEIT

Titel der Bachelorarbeit

## Galoisgruppe von $X^n - a$ über $\mathbb{Q}$


Verfasser

Felix Hinterreiter


angestrebter akademischer Grad

Bachelor of Science (BSc)

Wien, September 2023

| | |
|---|---|
| Studienkennzahl lt. Studienblatt: | A 033 621 |
| Studienrichtung lt. Studienblatt: | Bachelorstudium Mathematik |
| Betreuer: | Assoz. Prof. Dr. Dietrich Burde |

## Abstract

Ziel dieser Arbeit ist es, die Galoisgruppe von $X^n - a$ über $\mathbb{Q}$ zu bestimmen, wobei $X^n - a \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$ ist. Dazu wird im ersten Abschnitt eine Bedingung für die Irreduzibilität von $X^n - a$ über $\mathbb{Q}$ formuliert und bewiesen. Anschließend werden einige Lemmata angeführt, die dann im zweiten Abschnitt der Arbeit verwendet werden. Im zweiten Abschnitt wird zuerst der Grad vom Zerfällungskörper von $X^n - a$ nach $\mathbb{Q}$ bestimmt, womit sich dann zeigen lässt, dass die Galoisgruppe von $X^n - a$ über $\mathbb{Q}$ isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ ist. Im Weiteren wird dann der Fall, dass $n$ eine 2-er Potenz ist, behandelt womit sich dann die Galoisgruppe für beliebiges $n$ bestimmen lässt. Im dritten Abschnitt werden die Zwischenkörper der Erweiterung $\mathbb{Q}(\sqrt[6]{2}, \zeta_6)/\mathbb{Q}$ bestimmt. Im Appendix befinden sich Abbildungen, bei denen man die Zwischenkörper der Erweiterungen $\mathbb{Q}(\sqrt[2]{2}, \zeta_2)/\mathbb{Q}, ..., \mathbb{Q}(\sqrt[8]{2}, \zeta_8)/\mathbb{Q}$ ablesen kann.

# Inhaltsverzeichnis

# 1 Vorbereitungen

## 1.1 Semidirektes Produkt

Im Lemma 2.7 werden wir zeigen, dass $\mathrm{Gal}(X^n - a, \mathbb{Q})$ eine Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ ist. Deswegen beginnen wir damit, das semidirekte Produkt von Gruppen zu definieren.

**Definition 1.1.** [1, Seite 39, Definition 2.28.] Eine Gruppe $G$ ist das semidirekte Produkt seiner Untergruppen $N$ und $Q$, falls $N$ ein Normalteiler ist und $G \to G/N$ einen Isomorphismus $Q \to G/N$ induziert. Wir schreiben dann $G = N \rtimes Q$ oder auch $G = N \rtimes_\theta Q$, wobei $\theta : Q \to \mathrm{Aut}(N)$.

Nach [1, Seite 39, Satz 2.9.6.] kann das semidirekte Produkt $N \rtimes_\theta Q$ aus zwei Gruppen $N$ und $Q$ und einem Homomorphismus $\theta : Q \to \mathrm{Aut}(N)$ konstruiert werden, indem $G = N \times Q$ als Menge aufgefasst wird und mit dem Produkt

$$(n, q)(n', q') = (n \cdot \theta(q)(n'), qq')$$

ausgestattet wird.

*Beispiel* 1.2. Wir betrachten das semidirekte Produkt $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. Es gilt $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, denn für $\varphi \in \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ gilt $\varphi(k) = k\varphi(1)$. Also muss gelten $\langle \varphi(1) \rangle = \mathbb{Z}/n\mathbb{Z}$. Somit haben die Elemente $\varphi$ aus $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ die Form $\varphi(a) = la$ für ein $l$ mit $\mathrm{ggT}(l, n) = 1$. Da die Elemente $\theta(l)(a)$ von $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ die Form $a \mapsto la$ haben, hat das Produkt in $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ die Form $(a, b)(a', b') = (a + ba', bb')$.

## 1.2 Irreduzibilität von $X^n - a$ über $\mathbb{Q}$

Wir werden nur den Fall betrachten, dass $X^n - a$ irreduzibel über $\mathbb{Q}$ ist. Deswegen beginnen wir damit, eine Bedingung für die Irreduzibilität von $X^n - a$ über $\mathbb{Q}$ zu finden. Folgendes Lemma wird das Problem auf den Fall zurückführen, dass $n$ eine Primzahlpotenz ist.

**Lemma 1.3.** *[8, Seite 422, Lemma 1.2.] Sei $K$ ein Körper und $n = kl$ mit $\mathrm{ggT}(k, l) = 1$, dann ist $X^n - a$ genau dann irreduzibel über $K$, wenn $X^k - a$ und $X^l - a$ irreduzibel über $K$ sind.*

*Beweis.* ($\Rightarrow$) Es ist $X^{kl} - a = (X^k)^l - a = (X^l)^k - a$ und somit sind $X^k - a$ und $X^l - a$ irreduzibel über $K$ falls $X^n - a$ irreduzibel über $K$ ist.

($\Leftarrow$) Sei $\alpha$ eine Nullstelle von $X^n - a$, dann ist $\alpha^k$ eine Nullstelle von $X^l - a$. Da $X^l - a$ irreduzibel über $K$ ist, ist $[K(\alpha^k) : K] = l$. Analog ist $[K(\alpha^l) : K] = k$. Also wird $[K(\alpha) : K]$ von $k$ und von $l$ geteilt und da $\mathrm{ggT}(k, l) = 1$ ist, ist somit $kl \leq [K(\alpha) : K]$. Es ist aber $\alpha$ eine Nullstelle von $X^n - a$ und somit ist $kl \geq [K(\alpha) : K]$, da das Minimalpolynom von $\alpha$ über $K$ das Polynom $X^n - a$ teilt. Folglich ist $kl = [K(\alpha) : K]$ und somit ist $X^n - a$ das Minimalpolynom von $\alpha$ über $K$. Also ist $X^n - a$ irreduzibel über $K$.

□

Sei $p_1^{\nu_1} \cdot ... \cdot p_m^{\nu_m}$ die Primfaktorzerlegung von $n$, dann ist nach Lemma 1.3 $X^n - a$ genau dann irreduzibel über $\mathbb{Q}$, wenn $X^{p_i^{\nu_i}} - a$ irreduzibel über $\mathbb{Q}$ ist für alle $i = 1, ..., m$. Als nächstes werden wir eine Bedingung für die Irreduzibilität von $X^p - a$ über $K$ finden, wobei $p$ eine Primzahl ist.

**Definition 1.4.** Sei $K$ ein Körper und $n \in \mathbb{N}$, dann schreibe $a \in K^n$, falls ein $b \in K$ existiert mit $a = b^n$.

**Lemma 1.5.** *[8, Seite 423, Lemma 1.3.] Sei $K$ ein Körper und $p \in \mathbb{N}$ eine Primzahl, dann ist $X^p - a$ genau dann irreduzibel über $K$, wenn $a \notin K^p$ ist.*

*Beweis.* ($\Rightarrow$) Sei $X^p - a$ irreduzibel über $K$ und $\alpha \in K$ mit $a = \alpha^p$, dann ist $\alpha$ eine Nullstelle von $X^p - a$ und somit ist $X^p - a$ nicht irreduzibel über $K$, was ein Widerspruch ist.

($\Leftarrow$) Sei $a \notin K^p$ und $X^p - a$ nicht irreduzibel über $K$, dann hat $X^p - a$ einen Teiler $f$ mit Grad $k$, wobei $1 \leq k < p$ ist. Sei $c$ der konstante Term von $f$, dann ist $c \in K$. Die Nullstellen von $X^p - a$ haben die Form $\zeta_p^i \sqrt[p]{a}$ für $i = 0, ..., p-1$ und somit ist

$$c = \prod_{j=1}^{k} \zeta_p^{i_j} \sqrt[p]{a} = \zeta_p^e \sqrt[p]{a}^k \text{ mit } e = \sum_{j=1}^{k} i_j.$$

Da $\mathrm{ggT}(p, k) = 1$ ist, existieren $s, t \in \mathbb{Z}$ mit $ps + kt = 1$. Es ist

$$\sqrt[p]{a} = \sqrt[p]{a}^{ps} \sqrt[p]{a}^{kt} = a^s (\frac{c}{\zeta_p^e})^t$$

und somit ist $\sqrt[p]{a}\zeta_p^{et} = a^s c^t \in K$. Es ist aber $\sqrt[p]{a}\zeta_p^{et}$ eine Nullstelle von $X^p - a$ und somit ist $a = (\sqrt[p]{a}\zeta_p^{et})^p = (a^s c^t)^p \in K^p$, was ein Widerspruch ist.

□

Das nächste Lemma wird den Fall $X^{p^\nu} - a$, wobei $\nu \geq 2$ ist, vorbereiten.

**Lemma 1.6.** *[8, Seite 423, Lemma 1.4.] Es sei $K$ ein Körper, $p \in \mathbb{N}$ eine Primzahl und $X^p - a$ irreduzibel über $K$. Falls $\alpha$ eine Nullstelle von $X^p - a$ ist und*

*(i) falls $p$ ungerade ist, ist $\alpha \notin K(\alpha)^p$.*

*(ii) falls $p = 2$ ist, dann ist $\alpha \in K(\alpha)^2$ genau dann, wenn $a \in -4K^4$ ist.*

*Beweis.* (i) Es sei $X^p - a$ irreduzibel über $K$ und $\alpha$ eine Nullstelle von $X^p - a$, wobei $\alpha = \omega^p$ mit $\omega \in K(\alpha)$ ist. Sei $\sigma_i \in \mathrm{Gal}(K(\sqrt[p]{a}, \zeta_p)/K)$, dann ist $\sigma_i(\alpha) = \zeta_p^i \alpha$ für $i = 0, ..., p-1$. Sei weiter $\omega_i = \sigma_i(\omega)$, dann ist $\zeta_p^i \alpha = \omega_i^p$. Da $\omega \in K(\alpha)$ ist, aber $\omega \notin K$ ist, hat das Minimalpolynom $f$ von $\omega$ über $K$ Grad $p$. Somit hat $f$, da $K(\sqrt[p]{a}, \zeta_p)/K$ eine normale Erweiterung ist, $p$ verschiedene Nullstellen. Sei $\omega'$ eine

dieser Nullstellen, dann existiert ein $\sigma' \in \mathrm{Gal}(K(\sqrt[p]{a}, \zeta_p)/K)$ mit $\sigma'(\omega) = \omega'$. Ist $\sigma'(\alpha) = \zeta_p^j \alpha$, dann ist $\sigma'(\omega) = \omega_j$. Also sind $\omega_0, ..., \omega_{p-1}$ die Nullstellen von $f$ und somit ist $z := \omega_0 \cdot ... \cdot \omega_{p-1} \in K$. Da $\zeta_p^i \alpha = \omega_i^p$ ist, ist

$$\prod_{k=0}^{p-1} \zeta_p^k \alpha = \prod_{k=0}^{p-1} \omega_k^p = z^p.$$

Da $p$ ungerade ist, ist $1 \cdot \zeta_p^1 \cdot \zeta_p^2 \cdot ... \cdot \zeta_p^{p-1} = 1$ und somit ist $a = z^p \in K^p$. Also ist nach Lemma 1.5 $X^p - a$ nicht irreduzibel, was ein Widerspruch ist.

(ii) ($\Rightarrow$) Es sei $\alpha = \omega^2$ mit $\omega = q + r\alpha$, wobei $q, r \in K$ sind. Da

$$\alpha = (q + r\alpha)^2 = q^2 + 2qr\alpha + r^2\alpha^2 = q^2 + 2qr\alpha + r^2 a$$

ist, ist $2qr = 1$ und $q^2 + r^2 a = 0$. Somit ist $a = -4q^4 \in -4K^4$.

($\Leftarrow$) Es sei $a = -4r^4$, wobei $r \in K$. Sei $q = \frac{1}{2r}$, dann ist

$$(r + q\alpha)^2 = (r + \frac{1}{2r}\alpha)^2 = r^2 + \alpha + \frac{1}{4r^2}\alpha^2 = r^2 + \alpha + \frac{1}{4r^2}(-4r^4) = \alpha.$$

Und somit ist $\alpha \in K(\alpha)$.

□

Mit diesem Lemma können wir jetzt eine Bedingung für die Irreduzibilität von $X^{p^\nu} - a$ über $K$ formulieren, wobei $\nu \geq 2$ ist.

**Lemma 1.7.** *[8, Seite 424, Lemma 1.5.] Sei $K$ ein Körper, $p \in \mathbb{N}$ eine Primzahl und $\nu \in \mathbb{N}$ mit $\nu \geq 2$, dann ist,*

*(i) falls $p$ ungerade ist, $X^{p^\nu} - a$ genau dann irreduzibel über $K$, wenn $a \notin K^p$ ist.*

*(ii) falls $p = 2$ ist, $X^{2^\nu} - a$ genau dann irreduzibel über $K$, wenn $a \notin K^2$ und $a \notin -4K^4$ ist.*

*Beweis.* (i) ($\Rightarrow$) Sei $X^{p^\nu} - a$ irreduzibel über $K$ und $a = b^p$ für ein $b \in K$, dann ist

$$X^{p^\nu} - a = (X^{p^{\nu-1}})^p - b^p = (X^{p^{\nu-1}} - b) \sum_{j=0}^{p-1} (X^{p^{\nu-1}})^j b^{p-1-j}$$

und somit ist $X^{p^\nu} - a$ nicht irreduzibel über $K$, was ein Widerspruch ist.

($\Leftarrow$) Sei $a \notin K^p$ und $\alpha$ eine Nullstelle von $X^{p^\nu} - a$, dann ist $\alpha_1 = \alpha^{p^{\nu-1}}$ eine Nullstelle von $X^p - a$. Lemma 1.5 liefert, dass $[K(\alpha_1) : K] = p$ ist und Lemma 1.6 liefert, dass $\alpha_1 \notin K(\alpha_1)^p$ ist. Sei $\alpha_2$ so, dass $\alpha_2^p = \alpha_1$ ist, dann ist $\alpha_2$ eine Nullstelle von $X^p - \alpha_1 \in K(\alpha_1)[X]$. Wegen Lemma 1.5 ist dann $X^p - \alpha_1$

irreduzibel über $K(\alpha_1)$ und somit ist $[K(\alpha_2) : K(\alpha_1)] = p$. Weiter ist wegen Lemma 1.6 $\alpha_2 \notin K(\alpha_2)^p$. Induktiv folgt dann, dass

$$[K(\alpha_{\nu-1}) : K] = [K(\alpha_{\nu-1}) : K(\alpha_{\nu-2})] \cdot ... \cdot [K(\alpha_1) : K] = p^\nu$$

ist. Es ist aber $\alpha_{\nu-1} = \alpha$ und somit $[K(\alpha) : K] = p^\nu$. Also ist $X^{p^\nu} - a$ das Minimalpolynom von $\alpha$ über $K$ und somit ist $X^{p^\nu} - a$ irreduzibel über $K$.

(ii) ($\Rightarrow$) Ist $X^{2^\nu} - a$ irreduzibel über $K$ und $a = b^2$ für ein $b \in K$, dann ist

$$X^{2^\nu} - b^2 = (X^{2^{\nu-1}} - b)(X^{2^{\nu-1}} + b)$$

und somit nicht irreduzibel, was ein Widerspruch ist. Ist $a = -4b^4$ für ein $b \in K$, dann ist

$$X^{2^\nu} - a = X^{4 \cdot 2^{\nu-2}} + 4b^4 = (X^{2 \cdot 2^{\nu-2}} + 2bX^{2^{\nu-2}} + 2b^2)(X^{2 \cdot 2^{\nu-2}} - 2bX^{2^{\nu-2}} + 2b^2)$$

und somit nicht irreduzibel, was ein Widerspruch ist.

($\Leftarrow$) Sei analog zu (i) $a \notin K^2$, $a \notin -4K^4$ und $\alpha$ eine Nullstelle von $X^{2^\nu} - a$, dann ist $\alpha_1 = \alpha^{2^{\nu-1}}$ eine Nullstelle von $X^2 - a$. Da $a \notin K^2$ ist und $\alpha_1$ eine Nullstelle von $X^2 - a$ ist, ist $[K(\alpha_1) : K] = 2$ und nach Lemma 1.6 ist $\alpha_1 \notin K(\alpha_1)^2$, da $a \notin -4K^4$ ist. Sei $\alpha_2$ so, dass $\alpha_2^2 = \alpha_1$ ist, dann ist $\alpha_2$ eine Nullstelle von $X^2 - \alpha_1 \in K(\alpha_1)[X]$. Da $\alpha_1 \notin K(\alpha_1)^2$, ist $X^2 - \alpha_1$ irreduzibel über $K(\alpha_1)$. Nun ist nach Lemma 1.6 $\alpha_2 \notin K(\alpha_2)^2$, falls $\alpha_1 \notin -4K(\alpha_1)^4$ ist. Wäre $\alpha_1 \in -4K(\alpha_1)^4$, dann wäre $-\alpha_1$ ein Quadrat in $K(\alpha_1)^2$. Es existiert ein $\sigma \in \mathrm{Gal}(K(\alpha_1)/K)$ mit $\sigma(\alpha_1) = -\alpha_1$. Wäre also $-\alpha_1 = (r + q\alpha_1)^2$ für $r, q \in K$, dann wäre $\alpha_1 = (r - q\alpha_1)^2$ durch Anwendung von $\sigma$. Aber es ist $\alpha_1 \notin K(\alpha_1)^2$ und somit ist $\alpha_1 \notin -4K(\alpha_1)^4$. Induktiv folgt nun, dass

$$[K(\alpha_{\nu-1}) : K] = [K(\alpha_{\nu-1}) : K(\alpha_{\nu-2})] \cdot ... \cdot [K(\alpha_1) : K] = 2^\nu$$

ist. Es ist aber $\alpha_{\nu-1} = \alpha$ und somit $[K(\alpha) : K] = 2^\nu$. Also ist $X^{2^\nu} - a$ das Minimalpolynom von $\alpha$ über $K$ und somit ist $X^{2^\nu} - a$ irreduzibel über $K$.

□

Mit den Lemmata 1.3 bis 1.7 können wir nun leicht den allgemeinen Fall zeigen.

**Korollar 1.8.** *[8, Seite 425, Lemma 1.6.] Das Polynom $X^n - a \in \mathbb{Q}[X]$ ist genau dann irreduzibel über $\mathbb{Q}$, wenn*

*(i) $a \notin \mathbb{Q}^p$ für alle Primzahlen $p$ mit $p|n$ ist und*

*(ii) $a \notin -4\mathbb{Q}^4$, falls $4|n$, ist.*

*Beweis.* Sei $p_1^{\nu_1} \cdot ... \cdot p_m^{\nu_m}$ die Primfaktorzerlegung von $n$, dann ist nach Lemma 1.3 $X^n - a$ genau dann irreduzibel über $\mathbb{Q}$, wenn $X^{p_i^{\nu_i}} - a$ irreduzibel über $\mathbb{Q}$ ist für alle $i = 1, ..., m$. Die Polynome $X^{p_i^{\nu_i}} - a$ sind aber wegen Lemma 1.5 und Lemma 1.7 genau dann irreduzibel über $\mathbb{Q}$, wenn $a \notin \mathbb{Q}^p$ für alle Primzahlen $p$ mit $p|n$ ist und $a \notin -4\mathbb{Q}^4$, falls $4|n$, ist. □

## 1.3 Galoisgruppe von $X^n - 1$ über $\mathbb{Q}$

Als nächstes werden wir die Galoisgruppe von $X^n-1$ über $\mathbb{Q}$ bestimmen, da wir $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ in Satz 2.4 und $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ in Abschnitt 2.3 und Abschnitt 2.4 benötigen werden. Das Polynom $X^n - 1$ ist aber nicht irreduzibel über $\mathbb{Q}$, also werden wir zuerst das Minimalpolynom von $\zeta_n$ über $\mathbb{Q}$ bestimmen.

**Definition 1.9.** [1, Seite 110, Definition 4.23.]

(i) Die Menge der $n$-ten Einheitswurzeln ist eine zyklische Untergruppe von $\mathbb{C}^\times$ der Ordnung $n$.

(ii) Für die Menge der primitiven $n$-ten Einheitswurzeln $U_n = \{\zeta_n^k : 1 \leq k \leq n, \mathrm{ggT}(k, n) = 1\}$ gilt $|U_n| = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

**Lemma 1.10.** *[1, Seite 110, Satz 4.9.1.] Sei $f(X) = \prod_{k\in(\mathbb{Z}/n\mathbb{Z})^\times}(X - \zeta_n^k)$, dann ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ eine Galoiserweiterung und $f = \Phi_n$, wobei $\Phi_n$ das $n$-te Kreisteilungspolynom und somit das Minimalpolynom von $\zeta_n$ über $\mathbb{Q}$ ist.*

*Beweis.* Das Polynom $X^n - 1$ ist separabel und hat Nullstellen in $\mathbb{Q}(\zeta_n)$. Somit ist $\mathbb{Q}(\zeta_n)$ der Zerfällungskörper von $X^n - 1$ und somit ist $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ eine Galoiserweiterung. Das Minimalpolynom von $\zeta_n$ über $\mathbb{Q}$ ist irreduzibel über $\mathbb{Q}$ und somit separabel. Um zu zeigen, dass $f = \Phi_n$ ist, reicht es also zu zeigen, dass die Nullstellen der beiden Polynome übereinstimmen. Sei $\alpha$ eine Nullstelle von $\Phi_n$ und $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\sigma(\zeta_n) = \alpha$, dann ist

$$\mathrm{ord}(\alpha) = \mathrm{ord}(\sigma(\zeta_n)) = \mathrm{ord}(\zeta_n) = n.$$

Also ist jede Nullstelle von $\Phi_n$ eine primitive $n$-te Einheitswurzel und somit eine Nullstelle von $f$. Sei umgekehrt $\zeta$ eine Nullstelle von $f$, dann existiert ein $1 \leq k \leq n-1$ mit $\zeta = \zeta_n^k$ und $\mathrm{ggT}(n, k) = 1$. Dann entsteht $\zeta$ aus $\zeta_n$ durch wiederholtes Potenzieren mit den Primteilern von $k$. Also können wir induktiv annehmen, dass $k = p$ prim ist und $p \nmid n$. Da $\zeta_n$ eine Nullstelle von $X^n - 1$ ist, gilt $\Phi_n|(X^n - 1)$ und somit gibt es ein $g \in \mathbb{Q}[X]$ mit $X^n - 1 = g\Phi_n$. Da $X^n - 1 \in \mathbb{Z}[X]$ ist und $g, \Phi_n$ normiert sind, gilt nach dem Lemma von Gauß, dass $g, \Phi_n \in \mathbb{Z}[X]$ sind. Sei $\Phi_n(\zeta_n^p) \neq 0$, dann ist

$$0 = (\zeta_n^p)^n - 1 = (g\Phi_n)(\zeta_n^p) = g(\zeta_n^p)\Phi_n(\zeta_n^p)$$

und somit ist $g(\zeta_n^p) = 0$. Also ist $\zeta_n$ eine Nullstelle von $g(X^p) \in \mathbb{Z}[X]$ und deshalb $\Phi_n|g(X^p)$ in $\mathbb{Q}[X]$. Somit existiert ein $h \in \mathbb{Q}[X]$ mit $g(X^p) = h\Phi_n$ und nach dem Lemma von Gauß folgt wieder, dass $h \in \mathbb{Z}[X]$ ist. Sei $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ der Reduktionshomomorphismus modulo $p$. Dann ist

$$\pi(g)^p = \pi(g^p) = \pi(g(X^p)) = \pi(h)\pi(\Phi_n).$$

Also haben $\pi(\Phi_n)$ und $\pi(g)$ in $\mathbb{F}_p[X]$ einen gemeinsamen Primteiler und somit ist das Polynom

$$X^n - [1] = \pi(X^n - 1) = \pi(g)\pi(\phi_n) \in \mathbb{F}_p[X]$$

nicht separabel. Das steht aber wegen $p \nmid n$ im Widerspruch zum Ableitungskriterium. Und somit ist also $\Phi(\zeta_n^p) = 0$. □

**Korollar 1.11.** *[1, Seite 111, Satz 4.9.2.] Sei $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, wobei $\sigma_k(\zeta_n) = \zeta_n^k$ für ein $k \in \mathbb{Z}$ ist, dann ist die Abbildung*

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma_k &\mapsto [k] \end{aligned}$$

*ein Gruppenisomorphismus.*

*Beweis.* Die Abbildung ist ein injektiver Homomorphismus. Da wegen Lemma 1.10 gilt, dass $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ ist, ist die Abbildung auch surjektiv. □

In Lemma 2.11 werden wir die Untergruppen von $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^e})/\mathbb{Q}) \cong (\mathbb{Z}/2^e\mathbb{Z})^\times$ benötigen. Folgendes Lemma wird uns ermöglichen, diese zu bestimmen.

**Lemma 1.12.** *[11] Sei $e \geq 3$, dann wird $(\mathbb{Z}/2^e\mathbb{Z})^\times$ von -1 und 5 erzeugt wobei 5 Ordnung $2^{e-2}$ hat.*

*Beweis.* Die Ordnung von -1 ist 2. Wir zeigen, dass $\mathrm{ord}(5) = 2^{e-2}$ ist mit Induktion nach $e$.
*Induktionsanfang (e=3):* Ist $e = 3$, dann ist die $\mathrm{ord}(5) = 2 = 2^{e-2}$.
*Induktonsvoraussetzung:* Die Ordnung von 5 in $(\mathbb{Z}/2^m\mathbb{Z})^\times$ ist $2^{m-2}$ für alle $3 \leq m \leq e$ für ein $e \in \mathbb{N}$ mit $e \geq 3$.
*Induktionsschritt ($e \to e+1$):* Die Ordnung von 5 in $(\mathbb{Z}/2^{e+1}\mathbb{Z})^\times$ ist ein Vielfaches von $2^{e-2}$, da $2^{e-2}$ die Ordnung von 5 in $(\mathbb{Z}/2^e\mathbb{Z})^\times$ ist. Die Ordnung von 5 in $(\mathbb{Z}/2^{e-1}\mathbb{Z})^\times$ ist $2^{e-3}$ und somit ist $5^{2^{e-3}} \equiv 1 \pmod{2^{e-1}}$. Also ist $5^{2^{e-3}} \equiv 1 + k2^{e-1} \pmod{2^e}$ mit $k \in \{0, 1\}$. Jedoch ist $k \neq 0$, denn sonst würde $2^{e-3}$ von der Ordnung von 5 in $(\mathbb{Z}/2^e\mathbb{Z})^\times$ geteilt werden, was aber der Induktionsvoraussetzung widersprechen würde. Also ist $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{2^e}$ und somit ist $5^{2^{e-3}} \equiv 1 + 2^{e-1} + k2^e \pmod{2^{e+1}}$ mit $k \in \{0, 1\}$. Quadrieren beider Seiten liefert

$$\begin{aligned} 5^{2^{e-2}} &\equiv (1 + 2^{e-1} + k2^e)^2 && \pmod{2^{e+1}} \\ &\equiv 1 + 2^{2e-2} + k^2 2^{2e} + 2^e + k2^{e+1} + k2^{2e} && \pmod{2^{e+1}} \\ &\equiv 1 + 2^e && \pmod{2^{e+1}}. \end{aligned}$$

Erneutes Quadrieren liefert $5^{2^{e-1}} \equiv 1 \pmod{2^{e+1}}$ und somit ist $2^{e-1}$ die Ordnung von 5 in $(\mathbb{Z}/2^{e+1}\mathbb{Z})^\times$. Es ist $5^k \equiv 1 \pmod 4$ für alle $k \in \mathbb{N}$ und es ist $-1 \equiv 3 \pmod 4$. Also erhalten wir insgesamt, dass $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle -1, 5 \rangle$ ist und 5 die Ordnung $2^{e-2}$ hat. □

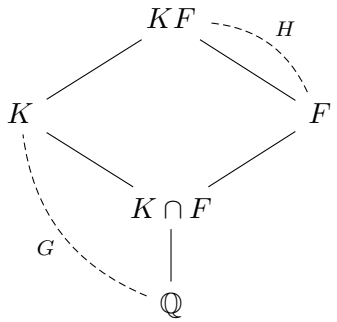
## 1.4 Galoisgruppe eines Kompositums

Im Lemma 1.23 und Abschnitt 2.4 werden wir jeweils die Galoisgruppe eines Kompositums benötigen. Deswegen werden wir diese im Folgenden bestimmen.

**Lemma 1.13.** *[9, Seite 266, Theorem 1.12] Es sei $K/\mathbb{Q}$ eine endliche Galoiserweiterung und $F/\mathbb{Q}$ eine endliche Körpererweiterung. Seien $K, F$ Teilkörper eines Körpers, dann sind $KF/F$ und $K/K \cap F$ Galoiserweiterungen. Sei $H$ die Galoisgruppe von $KF/F$ und $G$ die Galoisgruppe von $K/\mathbb{Q}$ und sei $\sigma \in H$, dann ist die Einschränkung von $\sigma$ auf $K$ in $G$ und die Abbildung*

$$\begin{aligned} \tau : H &\to \mathrm{Gal}(K/K \cap F) \\ \sigma &\mapsto \sigma|_K \end{aligned}$$

*ein Isomorphismus.*

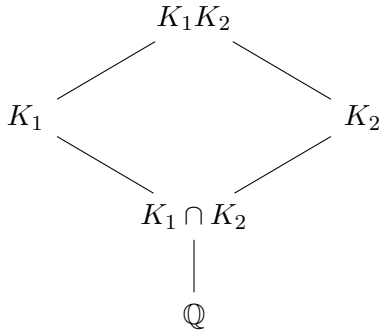



*Beweis.* Sei $\sigma \in H$, dann ist $\sigma|_K \in \mathrm{Aut}(K)$ und hält $\mathbb{Q}$ fest und somit ist $\sigma|_K \in G$. Ist $\sigma|_K$ die Identität auf $K$, dann ist $\sigma$ die Identität auf $KF$, da $F$ von $\sigma$ festgehalten wird. Also ist $\tau$ injektiv. Sei $H'$ das Bild von $\tau$, dann wird $K \cap F$ von allen Elementen aus $H'$ festgehalten. Wird umgekehrt $\alpha \in K$ von allen Elementen aus $H'$ festgehalten, dann wird $\alpha$ auch von allen Elementen aus $H$ festgehalten. Also ist $\alpha \in F$ und somit ist $\alpha \in K \cap F$. Folglich ist $K \cap F$ der Fixkörper von $H'$ und somit ist $H' = \mathrm{Gal}(K/K \cap F)$. □

**Lemma 1.14.** *[9, Seite 267, Theorem 1.14] Seien $K_1/\mathbb{Q}$ und $K_2/\mathbb{Q}$ endliche Galoiserweiterungen mit Galoisgruppen $G_1$ und $G_2$ und seien $K_1, K_2$ Teilkörper eines Körpers, dann ist $K_1K_2/\mathbb{Q}$ eine Galoiserweiterung. Sei $G$ die Galoisgruppe von $K_1K_2/\mathbb{Q}$, dann ist die Abbildung*

$$\begin{aligned} \tau : G &\to G_1 \times G_2 \\ \sigma &\mapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

*ein injektiver Gruppenhomomorphismus. Ist weiter $K_1 \cap K_2 = \mathbb{Q}$, dann ist $\tau$ ein Gruppenisomorphismus.*




*Beweis.* Separabilität und Normalität werden unter Kompositum beibehalten und somit ist $K_1K_2/\mathbb{Q}$ eine Galoiserweiterung. Weiter ist $\tau$ offensichtlich ein Homomorphismus. Sei $\sigma \in G$ und ist $\sigma$ auf $K_1$ eingeschränkt die Identität auf $K_1$ und auf $K_2$ eingeschränkt die Identität auf $K_2$, dann ist $\sigma$ auch auf $K_1K_2$ die Identität. Also ist $\tau$ injektiv.

Es sei nun $K_1 \cap K_2 = \mathbb{Q}$. Sei $\sigma_1 \in G_1$, dann liefert Lemma 1.13 ein $\sigma \in \mathrm{Gal}(K_1K_2/K_2)$ mit $\sigma|_{K_1} = \sigma_1$. Es ist $\sigma \in G$ und $K_2$ wird von $\sigma$ fest gehalten, also liegt $G_1 \times \{\mathrm{id}_{K_2}\}$ im Bild von $\tau$. Analog liegt auch $\{\mathrm{id}_{K_1}\} \times G_2$ im Bild von $\tau$. Also liegt $G_1 \times G_2$ im Bild von $\tau$ und somit ist $\tau$ eine Isomorphismus. □

## 1.5 Abelsche Galoisgruppe

**Definition 1.15.** Eine Körpererweiterung $L/K$ heißt abelsch, falls $\mathrm{Gal}(L/K)$ eine abelsche Gruppe ist.

In Definition 2.5 werden wir bemerken, dass $(\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n))/\mathbb{Q}$ eine abelsche Erweiterung ist. Deswegen werden wir im Folgenden alle Polynome der Form $X^n - a$ bestimmen, die eine abelsche Galoisgruppe über $\mathbb{Q}$ haben.

**Lemma 1.16.** *Hat $X^n - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann ist $\zeta_n \in \mathbb{Q}(\sqrt[n]{a})$.*

*Beweis.* Sei $\zeta_n \notin \mathbb{Q}(\sqrt[n]{a})$, dann existiert ein $\sigma_{0,k} \in \mathrm{Gal}(X^n - a, \mathbb{Q})$ mit $\sigma_{0,k}(\sqrt[n]{a}) = \sqrt[n]{a}$ und $\sigma_{0,k}(\zeta_n) = \zeta_n^k$ für ein $k$ mit $k \not\equiv 1 \,(\mathrm{mod}\, n)$. Es existiert auch ein $\sigma_{1,1} \in \mathrm{Gal}(X^n - a, \mathbb{Q})$ mit $\sigma_{1,1}(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n$ und $\sigma_{1,1}(\zeta_n) = \zeta_n$. Es gilt

$$\sigma_{1,1}\sigma_{0,k}(\sqrt[n]{a}) = \sigma_{1,1}(\sqrt[n]{a}) = \sqrt[n]{a}\zeta_n$$

und

$$\sigma_{0,k}\sigma_{1,1}(\sqrt[n]{a}) = \sigma_{0,k}(\sqrt[n]{a}\zeta_k) = \sqrt[n]{a}\zeta_n^k.$$

Da aber $k \not\equiv 1 \,(\mathrm{mod}\, n)$ ist, ist $\sqrt[n]{a}\zeta_n \neq \sqrt[n]{a}\zeta_n^k$ und somit ist $\mathrm{Gal}(X^n - a, \mathbb{Q})$ nicht abelsch. □

**Definition 1.17.** Sei $K$ ein Körper und $\alpha$ algebraisch über $K$, dann bezeichnen wir mit $O_K(\alpha)$ die Ordnung von $\alpha$ in der Quotientengruppe $K(\alpha)^\times/K^\times$.

*Bemerkung* 1.18. Sei $\alpha \in \mathbb{Q}$ und $K$ ein Körper mit Charakteristik 0, dann ist $O_K(\sqrt[2^e]{a})$ eine 2-er Potenz.

**Lemma 1.19.** *[6, Seite 320, Lemma 1.5.] Sei $K$ ein Körper mit Charakteristik 0, $e \geq 3$ und $\zeta_4 \notin K(\sqrt[2^e]{a}) \setminus K$, dann ist $[K(\sqrt[2^e]{a}) : K] = O_K(\sqrt[2^e]{a})$.*

*Beweis.* Es reicht den Fall $O_K(\sqrt[2^e]{a}) = 2^e$ zu zeigen, da wenn $O_K(\sqrt[2^e]{a}) = 2^k$ mit $1 \leq k < e$ ist, dann ist $\sqrt[2^e]{a}^{2^k} \in K$. Somit existiert ein $b \in K$ mit $a = b^{2^{e-k}}$. Also reduziert sich das Problem auf $O_K(\sqrt[2^k]{b}) = 2^k$. Nach Korollar 1.8 ist $X^{2^e} - a$ genau dann nicht irreduzibel über $K$ wenn $a = b^2$ oder $a = -4b^4$ für ein $b \in K$. Ist $a = b^2$, dann gilt $O_K(\sqrt[2^e]{a}) \leq 2^{e-1}$ und somit reduziert sich das Problem in diesem Fall. Ist $a = -4b^4$, dann ist $\sqrt[4]{a} = \pm(1 \pm \zeta_4)b$. Klarerweise ist somit $\zeta_4 \in K(\sqrt[2^e]{a})$. Ist $\zeta_4 \in K$, so ist $\sqrt[4]{a} \in K$, was $O_K(\sqrt[2^e]{a}) = 2^e$ widerspricht. Ist $\zeta_4 \notin K$, dann ist $\zeta_4 \in K(\sqrt[2^e]{a}) \setminus K$, was auch ein Widerspruch ist. Also ist $X^{2^e} - a$ irreduzibel über $K$ und somit ist $[K(\sqrt[2^e]{a}) : K] = O_K(\sqrt[2^e]{a})$. □

**Lemma 1.20.** *[4, Seite 390, Lemma 2.1.] Es sei $K$ ein Körper mit Charakteristik 0 und $e \geq 3$. Ist $\zeta_4 \notin K(\sqrt[2^e]{a}) \setminus K$, dann hat die Erweiterung $K(\sqrt[2^e]{a})/K$ zu jedem Teiler von $[K(\sqrt[2^e]{a}) : K]$ einen eindeutigen Zwischenkörper.*

*Beweis.* Sei $L$ ein Körper mit $L \subseteq K(\sqrt[2^e]{a})$ und sei $l = \min\{k : k|2^e \text{ und } \sqrt[2^e]{a}^k \in L\}$, dann ist $O_L(\sqrt[2^e]{a}) = l$ und $K(\sqrt[2^e]{a}^l) \subseteq L \subseteq K(\sqrt[2^e]{a})$. Nach Lemma 1.19 ist $[K(\sqrt[2^e]{a}) : L] = l$, da $\zeta_4 \notin K(\sqrt[2^e]{a}) \setminus L$ ist. Es ist aber $[K(\sqrt[2^e]{a}) : K(\sqrt[2^e]{a}^l)] \leq l$ und somit ist $[L : K(\sqrt[2^e]{a}^l)] = 1$ und folglich ist $L = K(\sqrt[2^e]{a}^l)$. Also ist $L$ eindeutig. □

**Lemma 1.21.** *[13, Seite 114, Lemma 2.1.] Es sei $K$ ein Körper und $m, n \in \mathbb{N}$ mit $\mathrm{ggT}(m, n) = 1$. Ist $a = b_1^m = b_2^n$ mit $b_1, b_2 \in K$, dann existiert ein $b \in K$ mit $a = b^{mn}$.*

*Beweis.* Sei $k = m + n$, dann ist $\mathrm{ggT}(mn, k) = 1$ und somit existieren $q, r \in \mathbb{Z}$ mit $qk - rmn = 1$. Sei nun $b = \frac{(b_1 b_2)^q}{a^r}$, dann ist

$$b^{mn} = (\frac{(b_1 b_2)^q}{a^r})^{mn} = \frac{(a^n a^m)^q}{a^{rmn}} = a^{(n+m)q - rmn} = a.$$

□

**Lemma 1.22.** *[13, Seite 115, Lemma 2.4.] Sei $p \in \mathbb{N}$ eine Primzahl und hat $X^{p^\nu} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann ist $a^{\omega_{p^\nu}} = b^{p^\nu}$ für ein $b \in \mathbb{Q}$, wobei $\omega_n$ die Anzahl an $n$-ten Einheitswurzeln ist, die in $\mathbb{Q}$ liegen.*

*Beweis.* Es sei zuerst $p = 2$.
*Induktionsanfang ($\nu = 1$):* Ist $\nu = 1$, dann ist die klarerweise $a^2 = b^2$ für ein $b \in \mathbb{Q}$.
*Induktonsvoraussetzung:* Hat $X^{2^m} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann ist $a^2 = b^{2^m}$ für alle $1 \leq m \leq \nu - 1$ für ein $\nu \in \mathbb{N}$ mit $\nu \geq 2$.

*Induktionsschritt ($\nu - 1 \to \nu$):* Die Substitutuion $Y = X^2$ liefert, dass $Y^{2^{\nu-1}} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$ hat, falls $X^{2^\nu} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$ hat. Also existiert nach Induktionsvoraussetzung ein $b_1 \in \mathbb{Q}$ mit $a^2 = b_1^{2^{\nu-1}}$. Ist $b_1 = b^2$ für ein $b \in \mathbb{Q}$, so folgt die Behauptung. Es sei nun also $b_1 \notin \mathbb{Q}^2$. Sei $\alpha$ eine Nullstelle von $X^{2^\nu} - a$, dann ist $\alpha = \zeta_{2^{\nu+1}}^i \sqrt[4]{b_1}$ für ein $i \in \mathbb{N}$. Da $\mathbb{Q}(\alpha, \zeta_{2^\nu})/\mathbb{Q}$ eine abelsche Erweiterung ist und $\mathbb{Q}(\alpha, \zeta_{2^\nu}) \subseteq \mathbb{Q}(\alpha, \zeta_{2^{\nu+1}})$ ist, ist $\mathbb{Q}(\sqrt[4]{b_1})/\mathbb{Q}$ eine abelsche Erweiterung. Ist $b_1 \in -4\mathbb{Q}^4$ dann ist $b_1 = -(2b^2)^2$ für ein $b \in \mathbb{Q}$ und somit ist $a^2 = b_1^{2^{\nu-1}} = (2b^2)^{2^\nu}$ und somit folgt die Behauptung. Sei also $b_1 \notin \mathbb{Q}^2$ und $b_1 \notin -4\mathbb{Q}^4$, dann ist nach Korollar 1.8 $X^4 - b_1$ irreduzibel über $\mathbb{Q}$. Somit ist nach Lemma 1.16 $\zeta_4 \in \mathbb{Q}(\sqrt[4]{b_1})$, woraus folgt, dass $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{b_1})$ ist. Somit ist $b_1 = -b^2$ für ein $b \in \mathbb{Q}$. Also ist $a^2 = (-b^2)^{2^{\nu-1}} = b^{2^\nu}$.
Es sei nun $p$ ungerade.
*Induktionsanfang ($\nu = 1$):* Sei $a \notin \mathbb{Q}^p$, dann ist nach Korollar 1.8 $X^p - a$ irreduzibel über $\mathbb{Q}$. Somit ist $[\mathbb{Q}(\sqrt[p]{a}) : \mathbb{Q}] = p$. Hat $X^p - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann ist nach Lemma 1.16 $\zeta_p \in \mathbb{Q}(\sqrt[p]{a})$. Also ist $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\sqrt[p]{a})$. Aber nach Lemma 1.11 ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ und $(p-1) \nmid p$, was ein Widerspruch ist.
*Induktonsvoraussetzung:* Hat $X^{p^m} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann ist $a = b^{p^m}$ für alle $1 \leq m \leq \nu - 1$ für ein $\nu \in \mathbb{N}$ mit $\nu \geq 2$.
*Induktionsschritt ($\nu - 1 \to \nu$):* Hat $X^{p^\nu} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann hat auch $X^{p^{\nu-1}} - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$. Also existiert nach Induktionsvoraussetzung ein $b_1 \in \mathbb{Q}$ mit $a = b_1^{p^{\nu-1}}$. Ist $b_1 = b^p$ für ein $b \in \mathbb{Q}$, so folgt die Behauptung. Es sei nun also $b_1 \notin \mathbb{Q}^p$. Sei $\alpha$ eine Nullstelle von $X^{p^\nu} - a$, dann ist $\alpha = \zeta_{p^\nu}^i \sqrt[p]{b_1}$ für ein $i \in \mathbb{N}$. Da $\mathbb{Q}(\alpha, \zeta_{p^\nu})/\mathbb{Q}$ eine abelsche Erweiterung ist, ist $\mathbb{Q}(\sqrt[p]{b_1})/\mathbb{Q}$ eine abelsche Erweiterung und die Behauptung folgt analog zum Induktionsanfang. □

**Lemma 1.23.** *[13, Seite 116, Theorem 2.1.] Sei $\omega_n$ die Anzahl an $n$-ten Einheitswurzeln, die in $\mathbb{Q}$ liegen, dann hat $X^n - a$ genau dann eine abelsche Galoisgruppe über $\mathbb{Q}$, wenn $a^{\omega_n} = b^n$ für ein $b \in K$ ist.*

*Beweis.* ($\Leftarrow$) Sei $a^{\omega_n} = b^n$, dann ist $a = \zeta_{\omega_n}^i \sqrt[\omega_n]{b}^n$ für ein $i$ mit $\mathrm{ggT}(i, n) = 1$. Es ist $\mathbb{Q}(\sqrt[\omega_n]{b}, \zeta_{n\omega_n})$ der Zerfällungskörper von $X^n - a$. Da $\omega_n \in \{1, 2\}$ ist, ist $\mathbb{Q}(\sqrt[\omega_n]{b})/\mathbb{Q}$ eine abelsche Galoiserweiterung. Da $\mathbb{Q}(\zeta_{n\omega_n})$ auch eine abelsche Galoiserweiterung ist, ist nach Lemma 1.14 $\mathrm{Gal}(\mathbb{Q}(\sqrt[\omega_n]{b}, \zeta_{n\omega_n})/\mathbb{Q})$ eine Untergruppe der abelschen Gruppe $\mathrm{Gal}(\mathbb{Q}(\sqrt[\omega_n]{b})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{n\omega_n})/\mathbb{Q})$ und somit hat $X^n - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$.

($\Rightarrow$) Ist $p_1^{\nu_1} \cdot ... \cdot p_m^{\nu_m}$ die Primfakrorzerlegung von $n$ und hat $X^n - a$ eine abelsche Galoisgruppe über $\mathbb{Q}$, dann hat auch $X^{p_i^{\nu_i}} - a$ für $i = 1, ..., m$ eine abelsche Galoisgruppe über $\mathbb{Q}$. Also ist nach Lemma 1.22 $a^{\omega_{p_i^{\nu_i}}} = b_i^{p_i^{\nu_i}}$ mit $b_i \in \mathbb{Q}$ für $i = 1, ..., m$ und somit existiert nach Lemma 1.21 ein $b \in \mathbb{Q}$ mit $a^{\omega_n} = b^n$.

□

**Korollar 1.24.** *[5, Seite 119, Proposition 2 (A)] Die Polynome der Form $X^n - a \in \mathbb{Q}[X]$, die irreduzibel über $\mathbb{Q}$ sind, wobei $\mathrm{Gal}(X^n - a, \mathbb{Q})$ abelsch ist, sind genau*

*(i)* $X - c$

*(ii)* $X^2 - c$, *wobei* $\sqrt{c} \notin \mathbb{Q}$ *ist*

*(iii)* $X^4 + c^2$, *wobei* $c^2 \notin 4\mathbb{Q}^4$ *ist*

*(iv)* $X^{2^h} + c^{2^{h-1}}$, *wobei* $h \geq 3$ *und* $c \neq 0$ *ist.*

*Beweis.* Es sei $X^n - a$ irreduzibel über $\mathbb{Q}$, wobei $\mathrm{Gal}(X^n - a, \mathbb{Q})$ abelsch ist und es sei $p \in \mathbb{N}$ eine ungerade Primzahl mit $p|n$. Nach Lemma 1.23 ist $a^{\omega_n} = b^n$ für ein $b \in \mathbb{Q}$. Da $\omega_n \in \{1, 2\}$ ist und $p$ ungerade ist, existiert ein $d \in \mathbb{Q}$ mit $a = d^p$. Also ist $X^n - a$ nicht irreduzibel über $\mathbb{Q}$ und somit muss $n$ eine 2-er Potenz sein. Sei nun also $n = 2^q$ mit $q \in \mathbb{N}$, dann ist nach Lemma 1.23 $a^2 = c^{2^q}$ für ein $c \in \mathbb{Q}$. Ist $q \geq 1$, dann ist $a = \pm c^{2^{q-1}}$. Mit Korollar 1.8 folgt dann die Behauptung. Umgekehrt sind die Polynome (i)-(iv) alle irreduzibel über $\mathbb{Q}$ wegen Korollar 1.8 und sie haben alle eine abelsche Galoisgruppe wegen Lemma 1.23. □

# 2 Galoisgruppe von $X^n - a$ über $\mathbb{Q}$

## 2.1 Grad von $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ nach $\mathbb{Q}$

Da $|\mathrm{Gal}(X^n - a, \mathbb{Q})| = [\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}]$ ist, ist es sinnvoll $[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}]$ zu bestimmen. Folgende Formel wird uns dies ermöglichen.

**Lemma 2.1.** *Sei* $K$ *ein Körper, dann gilt* $[K(\alpha, \beta) : K] = \frac{[K(\alpha):K][K(\beta):K]}{[K(\alpha)\cap K(\beta):K]}$.

*Beweis.* Sei $L = K(\alpha) \cap K(\beta)$, dann gilt

$$\begin{aligned}[K(\alpha) : K][K(\beta) : K] =& [K(\alpha) : L][L : K][K(\beta) : L][L : K] \\ =& [K(\alpha) : L][K(\beta) : L][L : K][L : K] \\ =& [K(\alpha, \beta) : K][L : K].\end{aligned}$$

□

Um die Formel aus Lemma 2.1 tatsächlich verwenden zu können, müssen wir zuerst $[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]$ bestimmen. Folgendes Lemma soll das vorbereiten. Der dort konstruierte Körper $K$ wird, wie wir im darauffolgenden Lemma zeigen werden, der Durchschnitt von $\mathbb{Q}(\sqrt[n]{a})$ und $\mathbb{Q}(\zeta_n)$ sein.

**Lemma 2.2.** *[5, Seite 118, Lemma] Sei* $X^n - a$ *irreduzbel über* $\mathbb{Q}$ *und sei* $m = \max\{q : q|n$ *und* $\zeta_q \in \mathbb{Q}(\sqrt[n]{a})\}$ *und sei* $K$ *ein Körper mit* $\mathbb{Q}(\zeta_m) \subseteq K \subseteq \mathbb{Q}(\sqrt[n]{a})$, *dann ist* $K = \mathbb{Q}(\sqrt[n]{a^l})$, *falls* $l = [\mathbb{Q}(\sqrt[n]{a}) : K]$.

*Beweis.* Sei $p(X)$ das Minimalpolynom von $\sqrt[n]{a}$ über $K$, dann gilt $p(X)|(X^n - a)$ und die Nullstellen von $p$ haben die Form $\sqrt[n]{a}\zeta_n^i$ für gewisse $i$. Somit ist $p(X) = \prod_{j=1}^{l}(X - \sqrt[n]{a}\zeta_n^{i_j})$

und der konstante Term von $p$ ist

$$\prod_{j=1}^{l} \sqrt[n]{a}\zeta_n^{i_j} = \sqrt[n]{a}^l \zeta_n^e \in K \subseteq \mathbb{Q}(\sqrt[n]{a}) \text{ mit } e = \sum_{j=1}^{l} i_j.$$

Somit ist $\zeta_n^e \in \mathbb{Q}(\sqrt[n]{a})$. Nach Definition von $m$ gilt $\zeta_n^e \in \mathbb{Q}(\zeta_m) \subseteq K$ und somit ist $\sqrt[n]{a}^l \in K$. Es gilt $[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}(\sqrt[n]{a}^l)] \leq l$, da $\sqrt[n]{a}$ das Polynom $X^l - \sqrt[n]{a}^l \in \mathbb{Q}(\sqrt[n]{a}^l)[X]$ annulliert. Da aber $\mathbb{Q}(\sqrt[n]{a}^l) \subseteq K$ gilt, ist

$$l \geq [\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}(\sqrt[n]{a}^l)] = [\mathbb{Q}(\sqrt[n]{a}) : K][K : \mathbb{Q}(\sqrt[n]{a}^l)] = l[K : \mathbb{Q}(\sqrt[n]{a}^l)]$$

und somit ist $[K : \mathbb{Q}(\sqrt[n]{a}^l)] = 1$. Also ist $K = \mathbb{Q}(\sqrt[n]{a}^l)$. □

**Lemma 2.3.** *Sei $k = \max\{q : q|n$ und $\sqrt[q]{a} \in \mathbb{Q}(\zeta_n)\}$, dann ist $\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}(\sqrt[k]{a})$ und $[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = k$.*

*Beweis.* Sei $m$ wie in Lemma 2.2, dann ist $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\sqrt[n]{a})$. Sei nun $K = \mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n)$, dann gilt nach Lemma 2.2, dass $K = \mathbb{Q}(\sqrt[n]{a}^l)$ ist, wobei $l = [\mathbb{Q}(\sqrt[n]{a}) : K]$ und somit ist $[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = \frac{n}{l} = k$. □

Nun können wir die Formel aus Lemma 2.1 verwenden, um $[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}]$ zu bestimmen.

**Satz 2.4.** *[5, Seite 117] Sei $X^n - a$ irreduzibel über $\mathbb{Q}$ und $k = \max\{l : l|n$ und $\sqrt[l]{a} \in \mathbb{Q}(\zeta_n)\}$, dann ist*

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \frac{n\varphi(n)}{k}.$$

*Beweis.* Nach Lemma 2.1 ist

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \frac{[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}.$$

Da $\sqrt[n]{a}$ eine Nullstelle von $X^n - a$ ist und $X^n - a$ irreduzibel über $\mathbb{Q}$ ist, ist $X^n - a$ das Minimalpolynom von $\sqrt[n]{a}$ über $\mathbb{Q}$ und somit ist $[\mathbb{Q}(\sqrt[n]{a}) : \mathbb{Q}] = n$. Nach Lemma 1.11 ist $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ und nach Lemma 2.3 ist $[\mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}] = k$. Also ist insgesamt $[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \frac{n\varphi(n)}{k}$. □

Als nächstes werden wir feststellen, dass $k$ eine 2-er Potenz ist. Dazu definieren wir $h, t_1$ und $t_2$.

**Definition 2.5.** [5, Seite 118] Sei $h = \max\{l : l|n$ und $X^l - a$ hat eine abelsche Galoisgruppe über $\mathbb{Q}\}$, dann ist wegen Korollar 1.24 $h$ eine 2-er Potenz. Somit existiert ein $t_1 \in \mathbb{N}$ mit $h = \varphi(h)t_1$. Ist $k$ wie in Satz 2.4, dann ist die Erweiterung $\mathbb{Q}(\sqrt[k]{a})/\mathbb{Q}$ eine abelsche Erweiterung und somit existiert ein $t_2 \in \mathbb{N}$ mit $h = kt_2$. Insgesamt ist also $h = \varphi(h)t_1 = kt_2$ mit $t_2|t_1$.

**Lemma 2.6.** *[5, Seite 119, Proposition 2 (B)] Sei $X^n - a$ irreduzibel über $\mathbb{Q}$, dann ist $h = \max\{2^q : 2^q | n \text{ und } a = -c^{2^{q-1}},\ c \in \mathbb{Q}\}$ und*

$$k = 2^s = \begin{cases} h, \text{ falls } h = 1 \text{ oder } h = 2^q, a = -c^{2^{q-1}} \text{ und } \zeta_{2^{q+1}}\sqrt{c} \in \mathbb{Q}(\zeta_n) \\ \frac{h}{2} \text{ sonst.} \end{cases}$$

*Beweis.* Dass $h = \max\{2^q : 2^q | n \text{ und } a = -c^{2^{q-1}},\ c \in \mathbb{Q}\}$ ist, folgt aus Korollar 1.24. Da $h = \varphi(h)t_1$ ist und $h$ eine 2-er Potenz ist, ist $t_1 = 1$, falls $h = 1$ ist und $t_1 = 2$, falls $h > 1$ ist. Da $t_2 | t_1$ gilt, ist $t_2 \in \{1, 2\}$. Sei $h = 2^q$ mit $q \geq 1$, dann ist $t_2 = 1$ genau dann, wenn der Zerfällungskörper von $X^{2^q} - c^{2^{q-1}}$ in $\mathbb{Q}(\zeta_n)$ liegt und das ist genau dann, wenn $\zeta_{2^{q+1}}\sqrt{c} \in \mathbb{Q}(\zeta_n)$ ist. □

## 2.2 Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$

**Satz 2.7.** *Sei $X^n - a$ irreduziblel über $\mathbb{Q}$, dann ist $\mathrm{Gal}(X^n - a, \mathbb{Q})$ isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ mit Index $2^s$.*

*Beweis.* Es sei $\sigma_{i,k} \in \mathrm{Gal}(X^n - a, \mathbb{Q})$ mit

$$\begin{aligned} \sigma_{i,k}(\sqrt[n]{a}) &= \sqrt[n]{a}\zeta_n^i \\ \sigma_{i,k}(\zeta_n) &= \zeta_n^k \end{aligned}$$

für ganze Zahlen $i$, $k$, wobei $\mathrm{ggT}(k, n) = 1$. Die Verknüpfen zweier Elemente $\sigma_{i,k}, \sigma_{i',k'}$ liefert

$$\begin{aligned} \sigma_{i,k} \circ \sigma_{i',k'}(\sqrt[n]{a}) &= \sigma_{i,k}(\sqrt[n]{a}\zeta_n^{i'}) = \sigma_{i,k}(\sqrt[n]{a})\sigma_{i,k}(\zeta_n^{i'}) \\ &= \sqrt[n]{a}\zeta_n^i\zeta_n^{i'k} = \sqrt[n]{a}\zeta_n^{i+i'k} \\ &= \sigma_{i+i'k,l}(\sqrt[n]{a}) \end{aligned}$$

und

$$\sigma_{i,k} \circ \sigma_{i',k'}(\zeta_n) = \sigma_{i,k}(\zeta_n^{k'}) = \zeta_n^{kk'} = \sigma_{l,kk'}(\zeta_n).$$

Also insgesamt ist

$$\sigma_{i,k} \circ \sigma_{i',k'} = \sigma_{i+i'k,kk'}.$$

Sei $\psi : \mathrm{Gal}(X^n - a, \mathbb{Q}) \to \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ definiert durch $\sigma_{i,k} \mapsto (i, k)$ eine nach Konstruktion injektive Abbildung, dann ist

$$\psi(\sigma_{i,k}) \circ \psi(\sigma_{i',k'}) = (i, k) \circ (i', k') = (i + i'k, kk') = \psi(\sigma_{i+i'k,kk'})$$

und somit ist $\psi$ ein Homomorphismus. Also ist $\mathrm{Gal}(X^n - a, \mathbb{Q})$ isomorph zu einer Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. Da $|\mathrm{Gal}(X^n - a, \mathbb{Q})| = \frac{n\varphi(n)}{2^s}$ und $|\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times| = n\varphi(n)$ ist, ist der Index $2^s$. □

**Korollar 2.8.** *Sei $X^n - a$ irreduzibel über $\mathbb{Q}$, dann ist* $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ *genau dann, wenn $n$ ungerade ist oder $n$ gerade und $\sqrt{a} \notin \mathbb{Q}(\zeta_n)$ ist.*

*Beweis.* Nach Lemma 2.3 und Lemma 2.6 ist $s = 0$ genau dann, wenn $n$ ungerade ist oder $n$ gerade und $\sqrt{a} \notin \mathbb{Q}(\zeta_n)$ ist. Nach Satz 2.7 ist $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ genau dann, wenn $s = 0$ ist. □

Somit haben wir den Fall, wenn $n$ ungerade ist und den Fall, dass $n$ gerade ist und $s = 0$ ist, abgeschlossen. Deswegen ist im Folgenden nun $n$ gerade und $s \geq 1$. Sei $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt[2^s]{a}))$, dann ist $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$. In folgendem Lemma werden wir den Fall, dass $n$ gerade ist und $s = 1$ ist, behandeln.

**Lemma 2.9.** *[7, Seite 275, Theorem B] Sei $n$ gerade und $s = 1$, dann ist*

$$\mathrm{Gal}(X^n - a, \mathbb{Q}) = \{(i,k) : i \equiv \begin{cases} 0 \,(\mathrm{mod}\, 2), & \textit{falls } k \in H \\ 1 \,(\mathrm{mod}\, 2), & \textit{falls } k \notin H \end{cases}\}.$$

*Beweis.* Die Menge ist eine Untergruppe von $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ mit Index 2. Da $\sqrt{a} \in \mathbb{Q}(\zeta_n)$ ist, ist $\sqrt{a} = \sum_{j=1}^n a_j \zeta_n^j$ mit $a_j \in \mathbb{Q}$. Sei $\sigma_k \in H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{a}))$, dann wird $\sqrt{a}$ von $\sigma_k$ festgehalten. Sei $\sigma_{i,k} \in \mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_n)/\mathbb{Q})$, dann ist

$$\sqrt{a} = \sigma_k(\sqrt{a}) = \sum_{j=1}^n a_j \zeta_n^{jk} = \sigma_{i,k}(\sum_{j=1}^n a_j \zeta_n^j) = \sigma_{i,k}(\sqrt{a}) = \sigma_{i,k}(\sqrt[n]{a})^{n/2} = \sqrt{a} \cdot (-1)^i.$$

Also ist $i \equiv 0 \,(\mathrm{mod}\, 2)$, falls $\sigma_k \in H$ ist. Da $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{a})) = \{\sigma_u \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) : \sigma_u(\sqrt{a}) = \sqrt{a}\}$ ist, gilt umgekehrt, falls $i \equiv 1 \,(\mathrm{mod}\, 2)$ ist, dass $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ nicht in $H$ sein kann, da $\sqrt{a}$ nicht von $\sigma_k$ festgehalten wird. □

## 2.3 Fall $n = 2^e$

In Kapitel 2.4 werden wir $\mathrm{Gal}(X^n - a, \mathbb{Q}) = \mathrm{Gal}(X^{2^e m} - a, \mathbb{Q})$, wobei $e \geq 1$ und $m$ ungerade ist, mit Lemma 1.14 auf $\mathrm{Gal}(X^{2^e} - a, \mathbb{Q})$ und $\mathrm{Gal}(X^m - a, \mathbb{Q})$ aufteilen. Wir wissen schon, dass $\mathrm{Gal}(X^m - a, \mathbb{Q}) \cong \mathbb{Z}/m\mathbb{Z} \rtimes (\mathbb{Z}/m\mathbb{Z})^\times$ ist. Also müssen wir noch $\mathrm{Gal}(X^{2^e} - a, \mathbb{Q})$ bestimmen. Da das nächste Lemma $e \geq 3$ voraussetzt, werden wir die Fälle $e = 1$ und $e = 2$ gesondert behandeln.

Ist $e = 1$, so ist $s = 0$, da $n$ gerade ist und $\sqrt{a} \notin \mathbb{Q}(\zeta_2) = \mathbb{Q}(-1) = \mathbb{Q}$ ist, da $X^2 - a$ nach Voraussetzung irreduzibel über $\mathbb{Q}$ ist.

Ist $e = 2$ und ist $\sqrt{a} \in \mathbb{Q}(\zeta_4)$, dann ist $\sqrt{a} = d + \zeta_4 c$ mit $d, c \in \mathbb{Q}$. Also ist dann $a = d^2 + 2dc\zeta_4 - c^2$ und somit muss $d = 0$ oder $c = 0$ sein. Folglich ist $\sqrt{a} = \zeta_4 c$ und somit ist $a = -c^2$. Wählt man $b = 2c^2$, dann ist $a = -4b^4$ mit $b \in \mathbb{Q}$ und somit ist $X^4 - a$ nach Korollar 1.8 nicht irreduzibel und somit ist $\sqrt{a} \notin \mathbb{Q}(\zeta_4)$, wenn $X^4 - a$ irreduzibel ist. Also ist auch hier $s = 0$. Somit ist in beiden Fällen $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$. Es sei somit im Weiteren $e \geq 3$. Im folgenden Lemma werden wir $\mathbb{Q}(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e}) = \mathbb{Q}(\sqrt[2^s]{a})$ genauer bestimmen.

**Definition 2.10.** Sei $E$ ein Körper mit Charakteristik 0, dann heißt $E$

(i) quadratischer Teilkörper des Körpers $L$, falls $E$ Teilkörper von $L$ ist und $[E : \mathbb{Q}] = 2$.

(ii) quadratischer Teilkörper der Erweiterung $L/K$, falls $E$ Teilkörper von $L$ ist und $[E : K] = 2$.

**Lemma 2.11.** *[7, Seite 278, Proposition 6] Sei $X^{2^e} - a$ irreduzibel über $\mathbb{Q}$ und $e \geq 3$, dann ist,*

*(a) falls $s = 1$ ist, und*

*(i) falls $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\zeta_4)$ ist, $H = \langle 5 \rangle = \{k \in (\mathbb{Z}/2^e\mathbb{Z})^\times : k \equiv 1 \,(\mathrm{mod}\, 4)\}$.*

*(ii) falls $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{2})$ ist, $H = \langle -1, 5^2 \rangle = \{k \in (\mathbb{Z}/2^e\mathbb{Z})^\times : k \equiv 1, 7 \,(\mathrm{mod}\, 8)\}$.*

*(iii) falls $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{-2})$ ist, $H = \langle -5 \rangle = \{k \in (\mathbb{Z}/2^e\mathbb{Z})^\times : k \equiv 1, 3 \,(\mathrm{mod}\, 8)\}$.*

*(b) falls $s \geq 2$ ist, $\mathbb{Q}(\sqrt[2^s]{a}) = \mathbb{Q}(\zeta_{2^{s+1}})$ und $H = \langle 5^{2^{s-1}} \rangle = \{k \in (\mathbb{Z}/2^e\mathbb{Z})^\times : k \equiv 1 \,(\mathrm{mod}\, 2^{s+1})\}$.*

*Beweis.* (a) Da $\mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\zeta_{2^e})$ und $[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$ kommen für $\mathbb{Q}(\sqrt{a})$ genau die quadratischen Teilkörper von $\mathbb{Q}(\zeta_{2^e})$ in Frage. Diese korrespondieren nach dem Hauptsatz der Galoistheorie mit den Untergruppen von $\mathbb{Z}/2^e\mathbb{Z}$ mit Index $2^{e-2}$. Diese Untergruppen sind $\langle 5 \rangle$, $\langle -1, 5^2 \rangle$ und $\langle -5 \rangle$.

(i) Die Elemente von $\langle 5 \rangle$ sind genau die Elemente $u$ von $(\mathbb{Z}/2^e\mathbb{Z})^\times$ mit $u \equiv 1 \,(\mathrm{mod}\, 4)$. Sei $\sigma_u \in \mathrm{Gal}(\mathbb{Q}(\zeta_{2^e})/\mathbb{Q}(\sqrt{a}))$ mit $\sigma_u(\zeta_{2^e}) = \zeta_{2^e}^u$, dann wird $\zeta_4$ von $\sigma_u$ festgehalten, denn

$$\sigma_u(\zeta_4) = \sigma_u(\zeta_{2^e}^{2^{e-2}}) = \zeta_{2^e}^{u2^{e-2}} = \zeta_{2^e}^{4l2^{e-2}+2^{e-2}} = \zeta_{2^e}^{4l2^{e-2}} \cdot \zeta_{2^e}^{2^{e-2}} = 1 \cdot \zeta_4.$$

Da $[\mathbb{Q}(\zeta_4) : \mathbb{Q}] = 2$ ist, ist $\mathbb{Q}(\zeta_4)$ der Fixkörper von $\langle 5 \rangle$ und somit ist $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\zeta_4)$.

(ii) Die Elemente von $\langle -1, 5^2 \rangle$ sind genau die Elemente $u$ von $(\mathbb{Z}/2^e\mathbb{Z})^\times$ mit $u \equiv 1, 7 \,(\mathrm{mod}\, 8)$. Sei $\sigma_u$ wie in (i), dann wird $\zeta_8 + \zeta_8^{-1}$ von $\sigma_u$ festgehalten, denn

$$\begin{aligned}
&u \equiv 1 \,(\mathrm{mod}\, 8) \Rightarrow \\
&\quad \sigma_u(\zeta_8 + \zeta_8^{-1}) = \sigma_u(\zeta_{2^e}^{2^{e-3}} + \zeta_{2^e}^{-2^{e-3}}) = \sigma_u(\zeta_{2^e}^{2^{e-3}}) + \sigma_u(\zeta_{2^e}^{-2^{e-3}}) \\
&\quad = \zeta_{2^e}^{u2^{e-3}} + \zeta_{2^e}^{-u2^{e-3}} = \zeta_{2^e}^{8l2^{e-3}+2^{e-3}} + \zeta_{2^e}^{-8l2^{e-3}-2^{e-3}} \\
&\quad = 1 \cdot \zeta_8 + 1 \cdot \zeta_8^{-1} \\
&u \equiv 7 \,(\mathrm{mod}\, 8) \Rightarrow \\
&\quad \sigma_u(\zeta_8 + \zeta_8^{-1}) = \ldots = \zeta_{2^e}^{8l2^{e-3}-2^{e-3}} + \zeta_{2^e}^{-8l2^{e-3}+2^{e-3}} \\
&\quad = 1 \cdot \zeta_8^{-1} + 1 \cdot \zeta_8.
\end{aligned}$$

Da $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ist, ist $\mathbb{Q}(\sqrt{2})$ der Fixkörper von $\langle -1, 5^2 \rangle$ und somit ist $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{2})$.

(iii) Die Elemente von $\langle -5 \rangle$ sind genau die Elemente $u$ von $(\mathbb{Z}/2^e\mathbb{Z})^\times$ mit $u \equiv 1, 3 \pmod 8$. Sei $\sigma_u$ wie in (i), dann wird $\zeta_8 - \zeta_8^{-1}$ von $\sigma_u$ festgehalten, denn

$$\begin{aligned} u \equiv 1 \pmod 8 \Rightarrow \\ \sigma_u(\zeta_8 - \zeta_8^{-1}) = ... = \zeta_{2^e}^{8l2^{e-3}+2^{e-3}} - \zeta_{2^e}^{-8l2^{e-3}-2^{e-3}} \\ = 1 \cdot \zeta_8 - 1 \cdot \zeta_8^{-1} \\ u \equiv 3 \pmod 8 \Rightarrow \\ \sigma_u(\zeta_8 - \zeta_8^{-1}) = ... = \zeta_{2^e}^{8l2^{e-3}+3\cdot 2^{e-3}} - \zeta_{2^e}^{-8l2^{e-3}-3\cdot 2^{e-3}} \\ = 1 \cdot \zeta_8^3 - 1 \cdot \zeta_8^{-3} = -\zeta_8^{-1} + \zeta_8. \end{aligned}$$

Da $\zeta_8 - \zeta_8^{-1} = \sqrt{-2}$ und $[\mathbb{Q}(\sqrt{-2}) : \mathbb{Q}] = 2$ ist, ist $\mathbb{Q}(\sqrt{-2})$ der Fixkörper von $\langle -5 \rangle$ und somit ist $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{-2})$.

(b) Die Gruppe $(\mathbb{Z}/2^e\mathbb{Z})^\times$ hat nur eine Untergruppe mit Index $2^s$ für $s \geq 2$. Diese Untergruppe ist $\langle 5^{2^{s-1}} \rangle = \{u \in (\mathbb{Z}/2^e\mathbb{Z})^\times : u \equiv 1 \pmod{2^{s+1}}\}$. Sei $\sigma_u$ wie in (a)(i), dann wird $\zeta_{2^{s+1}}$ von $\sigma_u$ festgehalten, denn

$$\sigma_u(\zeta_{2^{s+1}}) = \sigma_u(\zeta_{2^e}^{2^{e-s-1}}) = \zeta_{2^e}^{2^{s+1}l2^{e-s-1}+2^{e-s-1}} = \zeta_{2^e}^{l2^e} \cdot \zeta_{2^{s+1}} = \zeta_{2^{s+1}}.$$

Da $[\mathbb{Q}(\zeta_{2^{s+1}}) : \mathbb{Q}] = \varphi(2^{s+1}) = 2^s$ ist, ist $\mathbb{Q}(\zeta_{2^{s+1}})$ der Fixkörper von $\langle 5^{2^{s-1}} \rangle$ und somit ist $\mathbb{Q}(\sqrt[2^s]{a}) = \mathbb{Q}(\zeta_{2^{s+1}})$.

□

Hiermit können wir jetzt einen Satz formulieren, der den Fall $n = 2^e$ abschließen wird.

**Satz 2.12.** *[7, Seite 279, Proposition 7] Sei $X^n - a$ irreduzibel über $\mathbb{Q}$ und $s \geq 2$, sodass $\mathbb{Q}(\sqrt[2^s]{a}) = \mathbb{Q}(\zeta_{2^{s+1}})$ ist, dann ist,*

*(a) falls $a = -c^{2^s}$ für ein $c \in \mathbb{Q}$ ist,*

$$\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong \{(i, k) : i \equiv \frac{k-1}{2} \pmod{2^s}\}.$$

*(b) falls $a = -2^{2^{s-1}} c^{2^s}$ für ein $c \in \mathbb{Q}$ ist,*

$$\mathrm{Gal}(X^n - a, \mathbb{Q}) = \{(i, k) : i \equiv \begin{cases} \frac{k-1}{2} \pmod{2^s}, \text{ falls } k \equiv 1, 7 \pmod 8 \\ 2^{s-1} + \frac{k-1}{2} \pmod{2^s}, \text{ falls } k \equiv 3, 5 \pmod 8 \end{cases}\}.$$

*Beweis.* (a) Sei $a = -c^{2^s}$ für ein $c \in \mathbb{Q}$ , dann annulliert $c$ das Polynom $X^{2^s} + a$. Also ist $c = \sqrt[2^s]{a}\zeta_{2^{s+1}}^z$ für ungerades $z$, denn $\sqrt[2^s]{a}^{2^s} \zeta_{2^{s+1}}^{2^s z} + a = a \cdot (-1)^z + a = 0$. Es gilt

nun

$$\sqrt[2^s]{a}\zeta_{2^{s+1}}^z = c = \sigma_{i,k}(c) = \sigma_{i,k}(\sqrt[2^s]{a}\zeta_{2^{s+1}}^z) = \sigma_{i,k}(\sqrt[2^e]{a}^{2^{e-s}}\zeta_{2^e}^{z2^{e-s-1}})$$
$$= (\sqrt[2^e]{a}\zeta_{2^e}^i)^{2^{e-s}}(\zeta_{2^e}^k)^{z2^{e-s-1}} = \sqrt[2^s]{a}\zeta_{2^s}^i\zeta_{2^{s+1}}^{zk} = \sqrt[2^s]{a}\zeta_{2^{s+1}}^{zk+2i}.$$

Daraus folgt, dass $\zeta_{2^{s+1}}^z = \zeta_{2^{s+1}}^{zk+2i}$ ist und somit ist $i \equiv z \cdot \frac{1-k}{2} \pmod{2^s}$ und

$$G := \{(i,k) : i \equiv z \cdot \frac{1-k}{2} \pmod{2^s}\}.$$

Sei $t \in \mathbb{Z}$ so, dass $tz \equiv -1 \pmod{2^s}$, dann bildet der Automorphismus $\tau : \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ mit $\tau(i,k) = (ti,k)$ die Gruppe $G$ auf die gewünschte Gruppe ab.

(b) Sei $a = -2^{2^{s-1}}c^{2^s}$ mit $c \in \mathbb{Q}$, dann annulliert $2c$ das Polynom $X^{2^s} + 2^{2^{s-1}}a$. Also ist $2c = \sqrt[2^s]{a}\sqrt{2}\zeta_{2^{s+1}}^z$ für ungerades $z$. Aus dem Beweis von Lemma 2.11(a)(ii) folgt, dass $\sigma_{i,k}(\sqrt{2}) = \sqrt{2}$ für $k \equiv 1, 7 \pmod 8$ ist und mit $\zeta_8^3 = -\zeta_8^{-1}$ und $\zeta_8^5 = -\zeta_8$ folgt, dass $\sigma_{i,k}(\sqrt{2}) = -\sqrt{2}$ für $k \equiv 3, 5 \pmod 8$ ist.

Mit der gleichen Rechnung wie in (a) erhält man für den Fall $k \equiv 1, 7 \pmod 8$, dass $i \equiv z \cdot \frac{1-k}{2} \pmod{2^s}$ ist und für den Fall $k \equiv 3, 5 \pmod 8$, dass $i \equiv 2^{s-1} + z \cdot \frac{1-k}{2} \pmod{2^s}$ ist. Da $t$ ungerade ist, ist

$$t2^{s-1} \equiv (2t'+1)2^{s-1} \equiv 2^s t' + 2^{s-1} \equiv 2^{s-1} \pmod{2^s}$$

und somit folgt der Rest analog zu (a).

□

## 2.4 Allgemeines $n$

Wir haben bisher $\mathrm{Gal}(X^n - a, \mathbb{Q})$ für ungerades $n$ und für 2er-Potenzen bestimmt. In diesem Kapitel werden wir diese beiden Fälle kombinieren, um $\mathrm{Gal}(X^n - a, \mathbb{Q})$ für beliebiges $n$ zu bestimmen. Sei dazu $n = 2^e m$, wobei $m > 1$ und ungerade ist und $e \geq 1$ ist und sei weiter $L = \mathbb{Q}(\sqrt[2^e]{a}, \zeta_{2^e})$ und $M = \mathbb{Q}(\sqrt[m]{a}, \zeta_m)$. Nach Lemma 1.14 ist $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong \mathrm{Gal}(L/\mathbb{Q}) \times \mathrm{Gal}(M/\mathbb{Q})$, falls $L \cap M = \mathbb{Q}$ ist. Im Folgenden betrachten wir den Fall $L \cap M \supsetneq \mathbb{Q}$.

**Lemma 2.13.** *[7, Seite 281 Proposition 8] Sei $X^n - a$ irreduzibel über $\mathbb{Q}$ und $n, L, M$ wie oben, dann ist $[L \cap M : \mathbb{Q}] \leq 2$.*

*Beweis.* Es ist $\mathbb{Q}(\sqrt[2^s]{a}) = \mathbb{Q}(\sqrt[n]{a}) \cap \mathbb{Q}(\zeta_n)$ und nach Lemma 1.16 ist $\zeta_{2^s} \in \mathbb{Q}(\sqrt[2^s]{a})$, da $\mathbb{Q}(\sqrt[2^s]{a})/\mathbb{Q}$ eine abelsche Erweiterung ist. Also ist $\mathbb{Q}(\zeta_{2^s}) \subseteq \mathbb{Q}(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e})$ und somit ist

$$[L : \mathbb{Q}] = \frac{2^e\varphi(2^e)}{[\mathbb{Q}(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e}) : \mathbb{Q}]} = \frac{2^e\varphi(2^e)}{[\mathbb{Q}(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e}) : \mathbb{Q}(\zeta_{2^s})][\mathbb{Q}(\zeta_{2^s}) : \mathbb{Q}]} \leq \frac{2^e\varphi(2^e)}{1 \cdot 2^{s-1}}.$$

Weiter ist somit

$$\frac{n\varphi(n)}{2^s} = [LM : \mathbb{Q}] = \frac{[L : \mathbb{Q}][M : \mathbb{Q}]}{[L \cap M : \mathbb{Q}]} \leq \frac{2^e\varphi(2^e)m\varphi(m)}{2^{s-1}[L \cap M : \mathbb{Q}]} = \frac{n\varphi(n)}{2^{s-1}[L \cap M : \mathbb{Q}]}.$$

Daraus folgt dann wiederum $[L \cap M : \mathbb{Q}] \leq 2$. □

Als nächstes formulieren wir ein Lemma, das angibt, wann $[L \cap M : \mathbb{Q}] = 2$ ist.

**Lemma 2.14.** *[7, Seite 281, Proposition 9] Sei $X^n - a$ irreduzibel über $\mathbb{Q}$ und $n, L, M$ wie oben und sei $s \geq 2$, dann ist $[L \cap M : \mathbb{Q}] = 2$ genau dann, wenn ein $b \in \mathbb{Q}$ existiert, sodass $\mathbb{Q}(\sqrt{b})$ ein quadratischer Teilkörper von $\mathbb{Q}(\zeta_m)$ ist und entweder*

*(i) $e = s = 2$ und $a = -(2b)^2c^4$ für ein $c \in \mathbb{Q}$, oder*

*(ii) $e > s \geq 2$, und $a = -b^{2^{s-1}}c^{2^s}$ oder $a = -(2b)^{2^{s-1}}c^{2^s}$ für ein $c \in \mathbb{Q}$.*

*Beweis.* (i) ($\Leftarrow$) Sei $e = s = 2$ und seien $b, c \in \mathbb{Q}$ mit $a = -(2b)^2c^4$ und $\sqrt{b} \in \mathbb{Q}(\zeta_m)$, dann ist $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{-(2b)^2c^4}) = \mathbb{Q}(\sqrt{-1}2bc^2) = \mathbb{Q}(\zeta_4)$, da $2bc^2 \in \mathbb{Q}$. Weiter ist $\mathbb{Q}(\sqrt[4]{a}) = \mathbb{Q}(\sqrt[4]{-(2b)^2c^4}) = \mathbb{Q}(\sqrt[4]{-1}\sqrt{2}\sqrt{b}c) = \mathbb{Q}(\zeta_8(\zeta_8 + \zeta_8^{-1})\sqrt{b}) = \mathbb{Q}((1 + \zeta_4)\sqrt{b})$ und somit $\sqrt{b} \in \mathbb{Q}(\sqrt[4]{a})$, da $1 + \zeta_4 \in \mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{a}) \subseteq \mathbb{Q}(\sqrt[4]{a})$. Es ist auch $\mathbb{Q}(\sqrt[4]{a}) = L$, da $e = 2$. Genauso ist $\sqrt{b} \in M$. Also ist insgesamt $\mathbb{Q}(\sqrt{b}) \subseteq L \cap M$ und somit ist $[L \cap M : \mathbb{Q}] \geq 2$. Also ist wegen Lemma 2.13 $[L \cap M : \mathbb{Q}] = 2$.

($\Rightarrow$) Sei $e = s = 2$ und $[L \cap M : \mathbb{Q}] = 2$, dann ist $\zeta_4 \in \mathbb{Q}(\sqrt[4]{a})$, da $Q(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e}) = \mathbb{Q}(\sqrt[2^s]{a})$ und $e = s = 2$. Es sei nun $L \cap M = \mathbb{Q}(\sqrt{b})$ für ein $b \in \mathbb{Q}$. Also ist $\sqrt{b} \in M$, aber $[M : \mathbb{Q}(\zeta_m)] = m$ ist ungerade und somit muss gelten $\sqrt{b} \in \mathbb{Q}(\zeta_m)$.

Da $\zeta_4 \in \mathbb{Q}(\sqrt[4]{a})$ ist, muss gelten $\mathbb{Q}(\sqrt[4]{a}) = \mathbb{Q}(\zeta_4, \sqrt{b_1})$ für ein $b_1 \in \mathbb{Q}$. Es ist $\mathbb{Q}(\sqrt{b}) \subseteq \mathbb{Q}(\zeta_4, \sqrt{b_1})$ und da $b \neq -1$ ist, ist $\mathbb{Q}(\sqrt{b}) = \mathbb{Q}(\sqrt{\pm b_1})$. In beiden Fällen ist $\mathbb{Q}(\sqrt[4]{a}) = \mathbb{Q}(\zeta_4, \sqrt{b})$. Es ist $\mathbb{Q}(\zeta_4, \sqrt{b}) = \mathbb{Q}(\sqrt[4]{-(2b)^2})$, da $\sqrt[4]{-(2b)^2} = (1 + \zeta_4)\sqrt{b}$. Also ist $\mathbb{Q}(\sqrt[4]{a}) = \mathbb{Q}(\sqrt[4]{-(2b)^2})$. Somit ist $a = -(2b)^2c^4$.

(ii) ($\Leftarrow$) Es sei $e > s \geq 2$, und $b, c \in \mathbb{Q}$ mit $\sqrt{b} \in \mathbb{Q}(\zeta_m)$. Sei weiter $a = -b^{2^{s-1}}c^{2^s}$, dann ist $Q(\sqrt[2^s]{a}) = \mathbb{Q}(\sqrt[2^s]{-b^{2^{s-1}}c^{2^s}}) = \mathbb{Q}(\zeta_{2^{s+1}}\sqrt{b})$. Es ist $\zeta_{2^{s+1}} \in L$, da $e > s$ und somit ist $\sqrt{b} \in L$. Es ist aber $\sqrt{b} \in M$ und somit $\mathbb{Q}(\sqrt{b}) \subseteq L \cap M$ und wegen Lemma 2.13 ist schließlich $[L \cap M : \mathbb{Q}] = 2$.

Sei $a = -(2b)^{2^{s-1}}c^{2^s}$, dann ist $Q(\sqrt[2^s]{a}) = \mathbb{Q}(\sqrt[2^s]{-(2b)^{2^{s-1}}c^{2^s}}) = \mathbb{Q}(\zeta_{2^{s+1}}\sqrt{2}\sqrt{b})$. Es ist wieder $\zeta_{2^{s+1}} \in L$ und es ist $\sqrt{2} = \zeta_8 + \zeta_8^{-1} \in L$, da $e \geq 3$. Somit folgt auch hier, dass $[L \cap M : \mathbb{Q}] = 2$ ist.

($\Rightarrow$) Es seien $e > s \geq 2$ und $[L \cap M : \mathbb{Q}] = 2$. Da $\mathbb{Q}(\sqrt[2^s]{a})/\mathbb{Q}$ eine abelsche Erweiterung ist, ist nach Lemma 1.23 $a^2 = b_1^{2^s}$ für ein $b_1 \in \mathbb{Q}$. Da $a$ kein

Quadrat in $\mathbb{Q}$ ist, ist $a = -b_1^{2^{s-1}}$ und somit ist $\sqrt[2^s]{a} = \zeta_{2^{s+1}}\sqrt{b_1}$. Ist $\sqrt{b_1} \in \mathbb{Q}(\zeta_{2^e})$, dann ist $\mathbb{Q}(\sqrt[2^e]{a}) \cap \mathbb{Q}(\zeta_{2^e}) = \mathbb{Q}(\sqrt[2^s]{a})$, da $e > s$ ist. Dann ist

$$[L \cap M : \mathbb{Q}] = \frac{[L : \mathbb{Q}][M : \mathbb{Q}]}{[LM : \mathbb{Q}]} = \frac{\frac{2^e\varphi(2^e)}{2^s} m\varphi(m)}{\frac{n\varphi(n)}{2^s}} = 1$$

und somit $L \cap M = \mathbb{Q}$. Also ist $\sqrt{b_1} \notin \mathbb{Q}(\zeta_{2^e})$ und $\mathbb{Q}(\zeta_{2^e}, \sqrt{b_1})$ ein quadratischer Teilkörper der Erweiterung $\mathbb{Q}(\zeta_{2^e}, \sqrt[2^e]{a})/\mathbb{Q}(\zeta_{2^e})$.

Sei nun $L \cap M = \mathbb{Q}(\sqrt{b})$ mit $\sqrt{b} \in \mathbb{Q}(\zeta_m)$, dann ist $\sqrt{b} \in L$ aber $\sqrt{b} \notin \mathbb{Q}(\zeta_{2^e})$, da kein quadratischer Teilkörper von $\mathbb{Q}(\zeta_{2^e})$ in $M$ liegt. Also ist auch $\mathbb{Q}(\zeta_{2^e}, \sqrt{b})$ ein quadratischer Teilkörper der Erweiterung $\mathbb{Q}(\zeta_{2^e}, \sqrt[2^e]{a})/\mathbb{Q}(\zeta_{2^e})$. Lemma 1.20 liefert aber, dass die Erweiterung $\mathbb{Q}(\zeta_{2^e}, \sqrt[2^e]{a})/\mathbb{Q}(\zeta_{2^e})$ zu jedem Teiler von $[\mathbb{Q}(\zeta_{2^e}, \sqrt[2^e]{a}) : \mathbb{Q}(\zeta_{2^e})]$ einen eindeutigen Teilkörper besitzt. Folglich ist $\mathbb{Q}(\zeta_{2^e}, \sqrt{b}) = \mathbb{Q}(\zeta_{2^e}, \sqrt{b_1})$ und somit $b_1 = b\gamma^2$ für ein $\gamma \in \mathbb{Q}(\zeta_{2^e})$. Da aber $\gamma^2 \in \mathbb{Q}$ ist, ist $\gamma^2 = \pm c$ oder $\gamma^2 = \pm 2c$ für ein $c$ in $\mathbb{Q}$. Also ist $b_1 = \pm bc^2$ oder $b_1 = \pm 2bc^2$ und somit ist $a = -b^{2^{s-1}}c^{2^s}$ oder $a = -(2b)^{2^{s-1}}c^{2^s}$.

Abschließend ist noch zu zeigen, dass, falls $e = s \geq 3$ ist, $L \cap M = \mathbb{Q}$ ist. Da $e = s$ ist, ist $\mathbb{Q}(\sqrt[2^e]{a}) = \mathbb{Q}(\zeta_{2^{e+1}})$ wegen Lemma 2.11(b) und somit ist $\zeta_8 \in \mathbb{Q}(\sqrt[2^e]{a}) = L$. Folglich sind $\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{-2})$ 3 verschiedene quadratische Teilkörper von $L$. Das sind auch alle quadratischen Teilkörper von $L$, da wir im Beweis von Lemma 2.11 gesehen haben, dass $\mathbb{Q}(\zeta_{2^{e+1}}) = L$ nur 3 quadratische Teilkörper hat. Keiner dieser Körper ist aber ein Teilkörper von $M$ und somit ist $L \cap M = \mathbb{Q}$. □

**Satz 2.15.** *[7, Seite 283, Theorem D] Es sei $X^n - a$ irreduzibel über $\mathbb{Q}$ mit $n = 2^e m$, wobei $m > 1$ ungerade und $e \geq 1$ ist. Sei weiter $\mathbb{Q}(\sqrt[2^e]{a}, \zeta_{2^e}) \cap \mathbb{Q}(\sqrt[m]{a}, \zeta_m) = \mathbb{Q}(\sqrt{b})$ ein quadratischer Teilkörper von $\mathbb{Q}(\zeta_m)$ und $H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\sqrt{b}))$, dann ist,*

*(a) falls $a = -b^{2^{s-1}}c^{2^s}$ ist,* $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong$

$$\{(i,k) : i \equiv \begin{cases} \frac{k-1}{2} \pmod{2^s}, \text{ falls } k \in H \\ \frac{k-1}{2} + 2^{s-1} \pmod{2^s}, \text{ falls } k \notin H \end{cases} \}.$$

*(b) falls $a = -(2b)^{2^{s-1}}c^{2^s}$ ist,* $\mathrm{Gal}(X^n - a, \mathbb{Q}) \cong$

$$\{(i,k) : i \equiv \begin{cases} \frac{k-1}{2} \pmod{2^s}, \text{ falls } \begin{cases} k \in H \text{ und } k \equiv 1, 7 \pmod 8, \text{ oder} \\ k \notin H, \text{ und } k \equiv 3, 5 \pmod 8 \end{cases} \\ \frac{k-1}{2} + 2^{s-1} \pmod{2^s}, \text{ falls } \begin{cases} k \in H \text{ und } k \equiv 3, 5 \pmod 8, \text{ oder} \\ k \notin H \text{ und } k \equiv 1, 7 \pmod 8 \end{cases} \end{cases} \}.$$

*Beweis.* (a) Sei $\sigma_k \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ mit $\sigma_k(\zeta_n) = \zeta_n^k$, dann ist wie im Beweis von Lemma 2.9 $\sigma_{i,k}(\sqrt{b}) = \sqrt{b}$, falls $\sigma_k \in H$ ist und $\sigma_{i,k}(\sqrt{b}) = -\sqrt{b}$, falls $\sigma_k \notin H$ ist. Der Rest des Beweises ist analog zum Beweis von Lemma 2.12. Sei $a = -b^{2^{s-1}}c^{2^s}$

mit $b, c \in \mathbb{Q}$, dann anulliert $bc$ das Polynom $X^{2^s} - b^{2^{s-1}}a$. Also ist $bc = \sqrt[2^s]{a}\sqrt{b}\zeta_{2^{s+1}}^z$ für ungerades $z$. Es gilt nun

$$\sqrt[2^s]{a}\sqrt{b}\zeta_{2^{s+1}}^z = bc = \sigma_{i,k}(bc) = \sigma_{i,k}(\sqrt[2^s]{a}\sqrt{b}\zeta_{2^{s+1}}^z) = \begin{cases} \sqrt{b}\sqrt[2^s]{a}\zeta_{2^{s+1}}^{zk+2i}, \text{ falls } k \in H \\ -\sqrt{b}\sqrt[2^s]{a}\zeta_{2^{s+1}}^{zk+2i}, \text{ falls } k \notin H. \end{cases}$$

Seien $t$ und $\tau$ wie im Beweis von Lemma 2.12, so folgt die Behauptung.

(b) Der Beweis funktioniert ganz analog zu (a), nur anuulliert hier $2bc$ das Polynom $X^{2^s} - (2b)^{2^{s-1}}a$ und somit ist

$$\sqrt[2^s]{a}\sqrt{2b}\zeta_{2^{s+1}}^z = \begin{cases} \sqrt{b}\sqrt[2^s]{a}\zeta_{2^{s+1}}^{zk+2i}, \text{ falls } \begin{cases} k \in H \text{ und } k \equiv 1, 7 \,(\mathrm{mod}\, 8), \text{ oder} \\ k \notin H, \text{ und } k \equiv 3, 5 \,(\mathrm{mod}\, 8) \end{cases} \\ -\sqrt{b}\sqrt[2^s]{a}\zeta_{2^{s+1}}^{zk+2i}, \text{ falls } \begin{cases} k \in H \text{ und } k \equiv 3, 5 \,(\mathrm{mod}\, 8), \text{ oder} \\ k \notin H \text{ und } k \equiv 1, 7 \,(\mathrm{mod}\, 8) \end{cases} \end{cases},$$

da $\sigma_{i,k}(\sqrt{2}) = \sqrt{2}$ für $k \equiv 1, 7 \,(\mathrm{mod}\, 8)$ und $\sigma_{i,k}(\sqrt{2}) = -\sqrt{2}$ für $k \equiv 3, 5 \,(\mathrm{mod}\, 8)$ ist.

□

*Bemerkung* 2.16. Es sei $X^n - a$ irreduzibel über $\mathbb{Q}$.

- Ist $n$ ungerade oder $n$ gerade und $s = 0$, dann beschreibt Korollar 2.8 die Galoisgruppe.
- Ist $n$ gerade und $s = 1$, dann beschreibt Lemma 2.9 die Galoisgruppe.
- Ist $n = 2^e$ mit $e \geq 3$ und $s \geq 2$, dann beschreibt Satz 2.12 die Galoisgruppe.
- Ist $n = 2^e m$ mit $e \geq 1$ und $m > 1$ ungerade, $s \geq 2$ und ist $\mathbb{Q}(\sqrt[2^e]{a}, \zeta_{2^e}) \cap \mathbb{Q}(\sqrt[m]{a}, \zeta_m) = \mathbb{Q}$, dann beschreiben Korollar 2.8, Lemma 2.9 und Satz 2.12 gemeinsam mit Lemma 1.14 die Galoisgruppe.
- Ist $n = 2^e m$ mit $e \geq 1$ und $m > 1$ ungerade, $s \geq 2$ und ist $[\mathbb{Q}(\sqrt[2^e]{a}, \zeta_{2^e}) \cap \mathbb{Q}(\sqrt[m]{a}, \zeta_m) : \mathbb{Q}] = 2$, dann beschreibt Satz 2.15 die Galoisgruppe.

Somit haben wir für beliebiges $n$ die Galoisgruppe von $X^n - a$ über $\mathbb{Q}$ bestimmt.

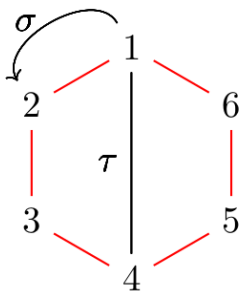
# 3 Beispiele

## 3.1 $X^6 - 2$

Im Folgenden werden wir die Zwischenkörper der Erweiterung $K/\mathbb{Q}$ bestimmen, wobei $K$ der Zerfällungskörper von $f(X) = X^6 - 2 \in \mathbb{Q}[X]$ ist. Da $f$ wegen Korollar 1.8 irreduzibel über $\mathbb{Q}$ ist und $s = 0$ ist, ist wegen Korollar 2.8

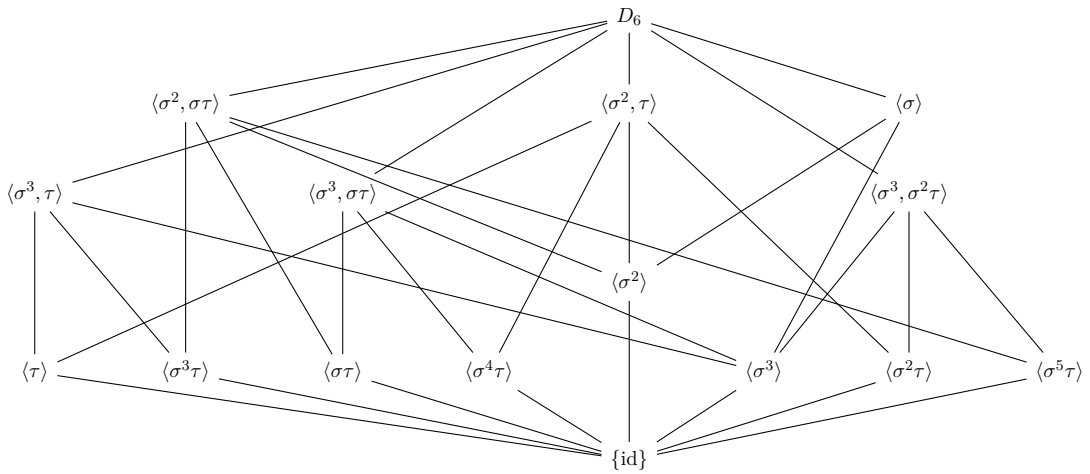
$$\mathrm{Gal}(f, \mathbb{Q}) \cong \mathbb{Z}/6\mathbb{Z} \rtimes (\mathbb{Z}/6\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \cong D_6.$$

Nach dem Hauptsatz der Galoistheorie korrespondieren die Untergruppen der Galoisgruppe mit den Zwischenkörpern. Um die Zwischenkörper zu finden, müssen wir also die Untergruppen von $D_6$ finden und dann die zugehörigen Körper.
Da $|D_6| = 12$ ist, können die Untergruppen wegen dem Satz von Lagrange die Ordnungen 1,2,3,4,6,12 haben. Wir betrachten ein Regelmäßiges 6-Eck und bezeichnen wie in nachstehender Abbildung die Drehung um $\frac{\pi}{3}$ mit $\sigma$ und eine Spiegelung mit $\tau$.




- Die einzige Untergruppe der Ordnung 1 ist $\{\mathrm{id}\}$.
- Untergruppen der Ordnung 2 werden von einem Element der Ordnung 2 erzeugt. Die Elemente der Ordnung 2 sind die 6 Spiegelungen und die Drehung um $\pi$. Also sind $\langle\sigma^3\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle, \langle\sigma^2\tau\rangle, \langle\sigma^3\tau\rangle, \langle\sigma^4\tau\rangle, \langle\sigma^5\tau\rangle$ die Untergruppen der Ordnung 2.
- Untergruppen der Ordnung 3 werden von einem Element der Ordnung 3 erzeugt. Die Elemente der Ordnung 3 sind die Drehung um $\frac{2\pi}{3}$ und die Drehung um $\frac{4\pi}{3}$. Diese erzeugen aber die gleiche Untergruppe. Somit ist $\langle\sigma^2\rangle$ die einzige Untergruppe der Ordnung 3.
- Untergruppen der Ordnung 4 werden von einem Element der Ordnung 4 oder 2 Elementen der Ordnung 2 erzeugt. Die Gruppe $D_6$ hat aber kein Element der Ordnung 4. Es ergeben 2 Spiegelungen eine Drehung und somit muss die Drehung um $\pi$ in der Untergruppe liegen. Also sind $\langle\sigma^3, \tau\rangle, \langle\sigma^3, \sigma\tau\rangle, \langle\sigma^3, \sigma^2\tau\rangle$ die Untergruppen der Ordnung 4.
- Untergruppen der Ordnung 6 werden von einem Element der Ordnung 6 oder einem Element der Ordnung 2 und einem Element der Ordnung 3 erzeugt. Die Elemente der Ordnung 6 sind die Drehung um $\frac{\pi}{3}$ und die Drehung um $\frac{5\pi}{3}$. Diese erzeugen aber die gleiche Untergruppe. Somit sind $\langle\sigma\rangle, \langle\sigma^2, \tau\rangle, \langle\sigma^2, \sigma\tau\rangle$ die Untergruppen der Ordnung 6.
- Die einzige Untergruppe der Ordnung 12 ist $D_6$ selbst.

Wir erhalten folgendes Diagramm, wobei eine Verbindung bedeutet, dass die untere Gruppe Untergruppe der oberen Gruppe ist.




Wir bemerken, dass $\sigma$ und $\tau$ mit den Elementen $\sigma_{1,1}$ und $\sigma_{0,5}$ aus $\mathrm{Gal}(f,\mathbb{Q})$ übereinstimmen, wobei $\sigma_{i,j}(\sqrt[6]{2}) = \sqrt[6]{2}\zeta_6^i$ und $\sigma_{i,j}(\zeta_6) = \zeta_6^j$ ist. Nun müssen wir die zugehörigen Zwischenkörper finden. Wir zeigen, dass $K^{\langle\sigma\tau\rangle} = \mathbb{Q}(\sqrt[6]{2}(1+\zeta_6))$ ist. Wie in [12, Seite 90] betrachten wir die $\mathbb{Q}$-lineare Abbildung $\sigma\tau\text{-id}_K : K \to K$. Es gilt $K^{\langle\sigma\tau\rangle} = \ker(\sigma\tau - \mathrm{id}_K)$. Als nächstes bestimmen wir die Darstellungsmatrix von $\sigma\tau$ bezüglich der $\mathbb{Q}$-Basis $\{1, \sqrt[6]{2}, \sqrt[6]{2}^2, \sqrt[6]{2}^3, \sqrt[6]{2}^4, \sqrt[6]{2}^5, \zeta_6, \sqrt[6]{2}\zeta_6, \sqrt[6]{2}^2\zeta_6, \sqrt[6]{2}^3\zeta_6, \sqrt[6]{2}^4\zeta_6, \sqrt[6]{2}^5\zeta_6\}$ von $K$. Wenden wir nun $\sigma\tau$ an alle Basiselemente an, dann erhalten wir

$$
\begin{aligned}
1 &\mapsto 1 & \zeta_6 &\mapsto \zeta_6^5 = 1-\zeta_6\\
\sqrt[6]{2} &\mapsto \sqrt[6]{2}\zeta_6 & \sqrt[6]{2}\zeta_6 &\mapsto \sqrt[6]{2}\zeta_6\\
\sqrt[6]{2}^2 &\mapsto \sqrt[6]{2}^2\zeta_6^2 = \sqrt[6]{2}^2(\zeta_6-1) & \sqrt[6]{2}^2\zeta_6 &\mapsto \sqrt[6]{2}^2\zeta_6\\
\sqrt[6]{2}^3 &\mapsto \sqrt[6]{2}^3\zeta_6^3 = -\sqrt[6]{2}^3 & \sqrt[6]{2}^3\zeta_6 &\mapsto \sqrt[6]{2}^3\zeta_6^2 = \sqrt[6]{2}^3(\zeta_6-1)\\
\sqrt[6]{2}^4 &\mapsto \sqrt[6]{2}^4\zeta_6^4 = -\sqrt[6]{2}^4\zeta_6 & \sqrt[6]{2}^4\zeta_6 &\mapsto \sqrt[6]{2}^4\zeta_6^3 = -\sqrt[6]{2}^4\\
\sqrt[6]{2}^5 &\mapsto \sqrt[6]{2}^5\zeta_6^5 = \sqrt[6]{2}^5(1-\zeta_6) & \sqrt[6]{2}^5\zeta_6 &\mapsto \sqrt[6]{2}^5\zeta_6^4 = -\sqrt[6]{2}^5\zeta_6.
\end{aligned}
$$

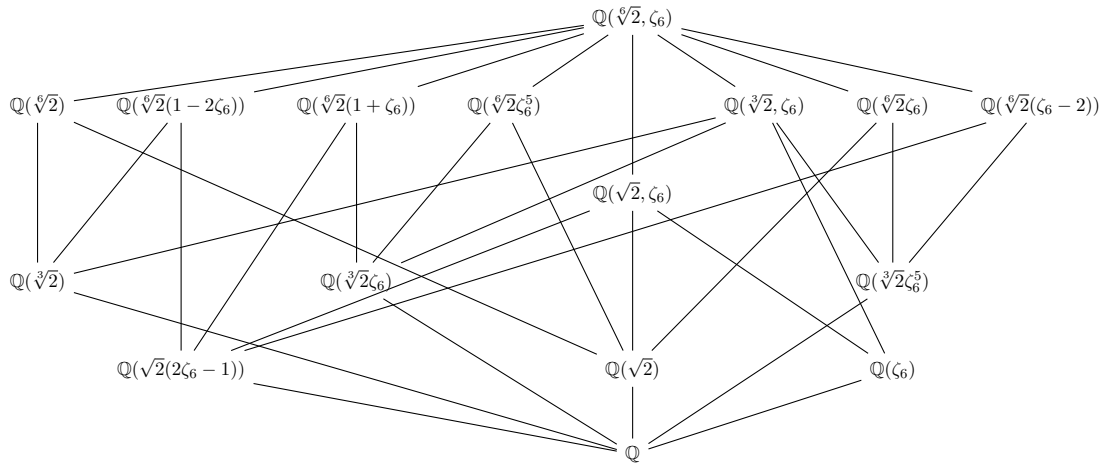
Folglich haben wir die Darstellungsmatrix

$$D(\sigma\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

und erhalten

$$\begin{aligned} \ker(\sigma\tau - \mathrm{id}_K) =& \{(a,b,0,-d,-e,-2f,0,b,c,2d,e,f) : a,b,c,d,e,f \in \mathbb{Q}\} \\ =& \{a + b(\sqrt[6]{2}(1+\zeta_6) + c\sqrt[6]{2}^2\zeta + d(\sqrt[6]{2}^3(2\zeta_6 - 1) \\ & + e\sqrt[6]{2}^4(\zeta_6 - 1) + f\sqrt[6]{2}^5(\zeta_6 - 2) : a,b,c,d,e,f \in \mathbb{Q}\} \\ =& \mathbb{Q}(\sqrt[6]{2}(1+\zeta_6)). \end{aligned}$$

Ganz analog können wir auch die anderen Zwischenkörper finden und erhalten schließlich folgendes Diagramm.

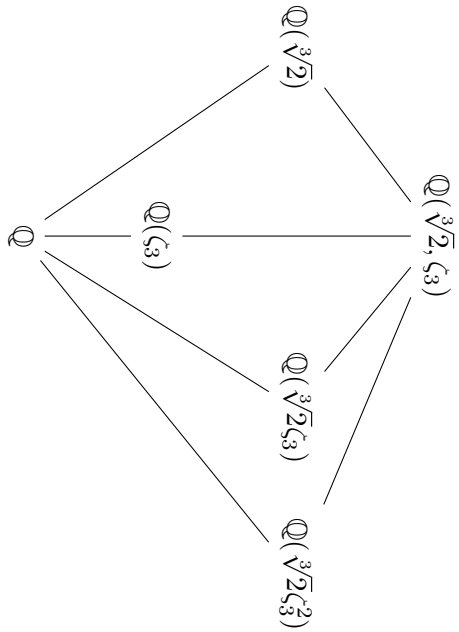


# 4 Appendix

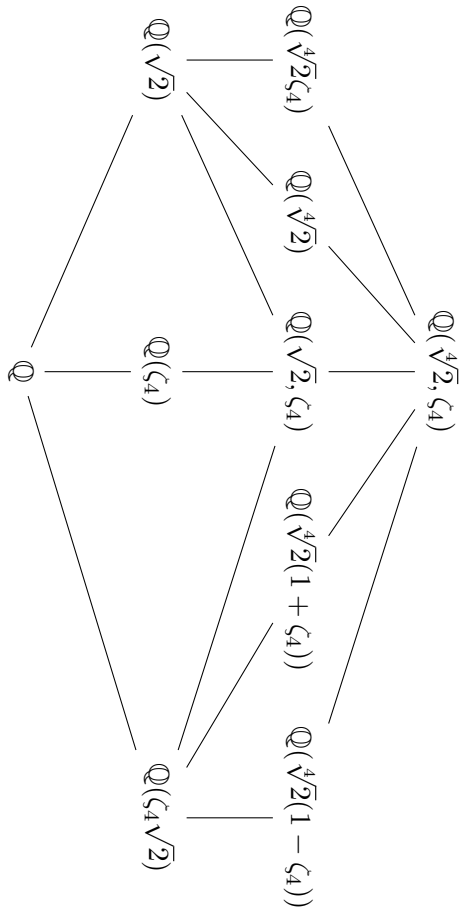
Analog zu Abschnitt 3 wurden für $X^2-2, X^3-2, ..., X^8-2$ die Galoisgruppen über $\mathbb{Q}$ und deren Untergruppen bestimmt. Anschließend wurden die zu diesen Untergruppen korrespondierenden Zwischenkörper bestimmt. Die Resultate können in folgenden Abbildungen abgelesen werden. Für $X^2-2, X^3-2$ und $X^4-2$ können die Zwischenkörper auch in [3, Seite 22, Seite 24] gefunden werden. Die Fälle $X^5-2$ und $X^8-2$ werden in [2, Seite 2] beziehungsweise in [10, Folie 38] vorbereitet.

$\mathrm{Gal}(X^2-2,\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$

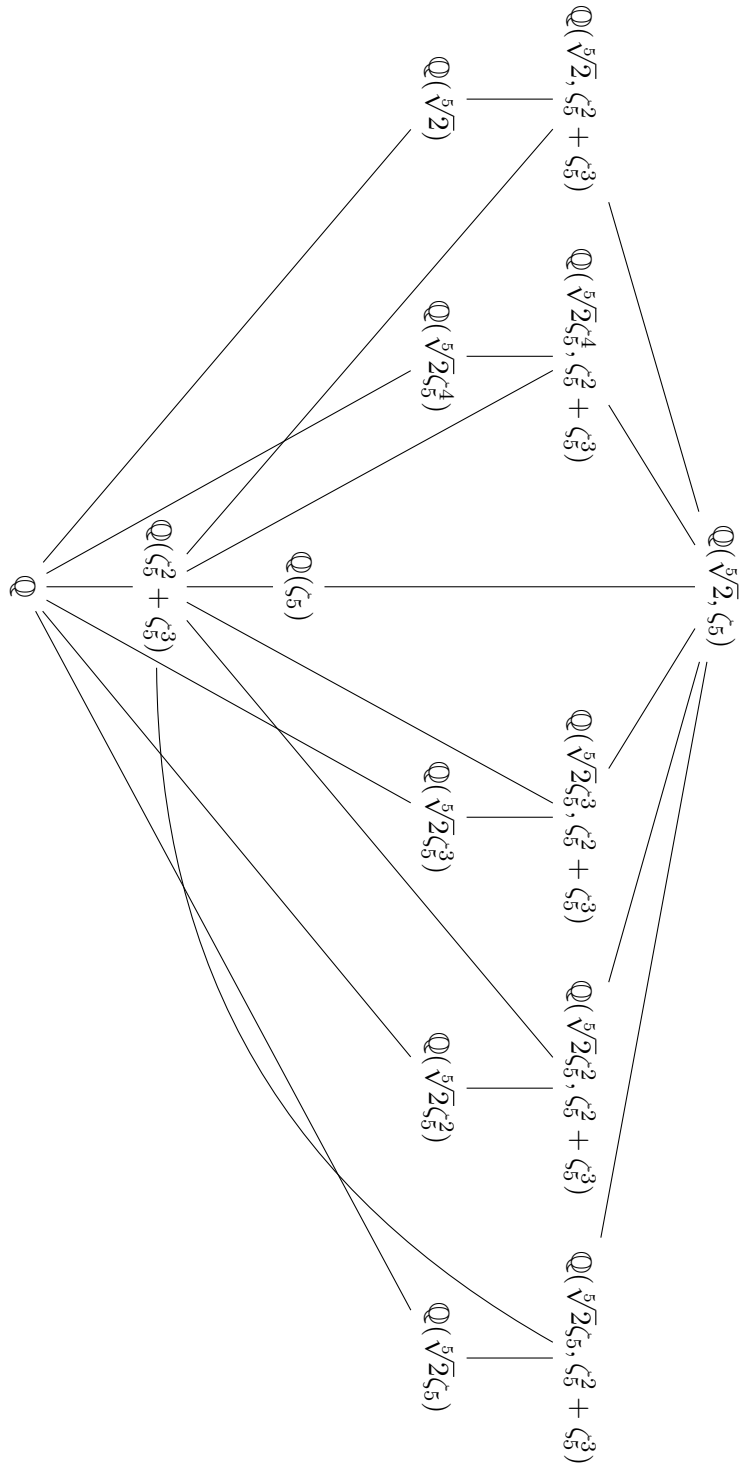

$\mathrm{Gal}(X^3-2,\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$



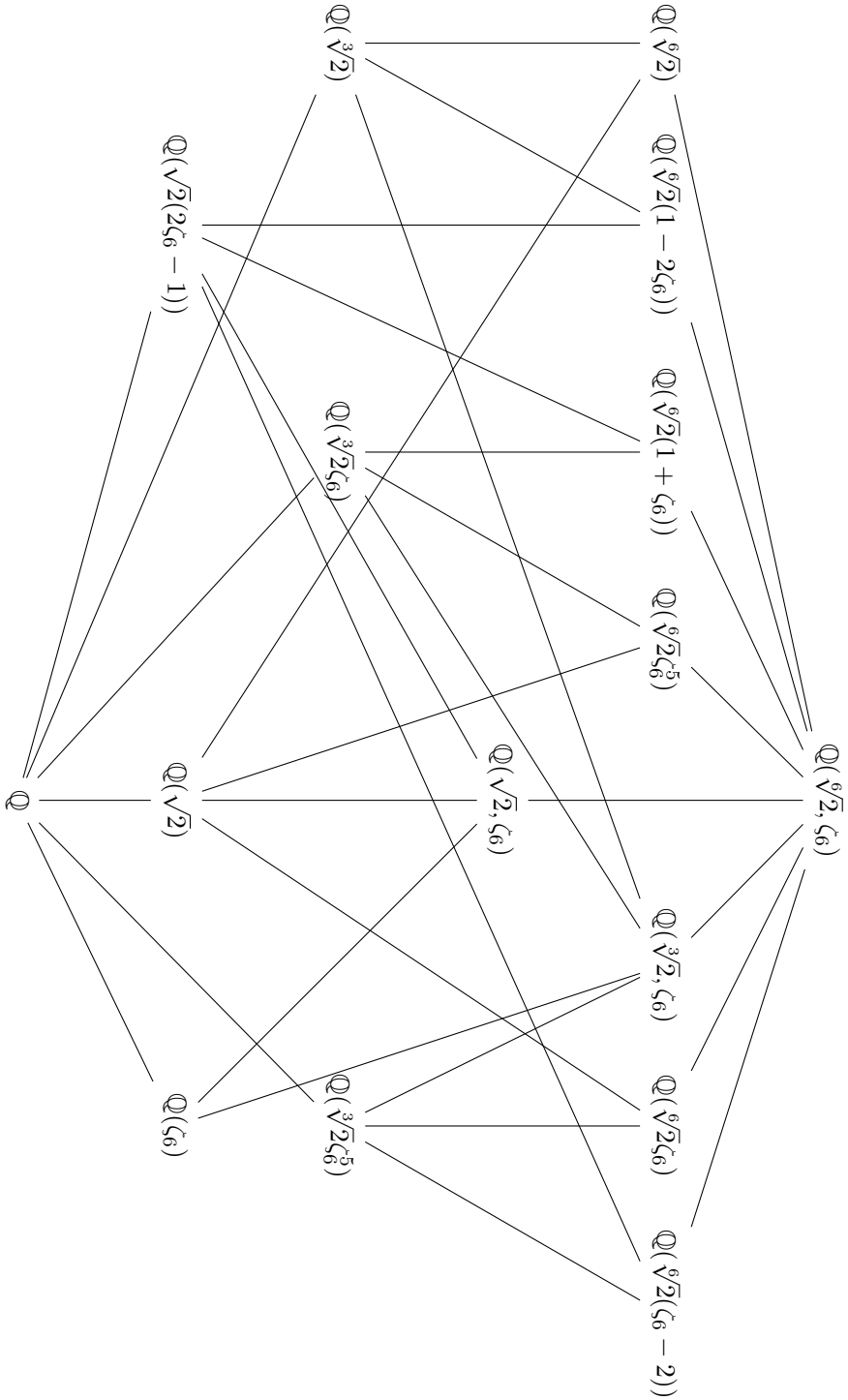
$\mathrm{Gal}(X^4 - 2, \mathbb{Q}) \cong D_4$



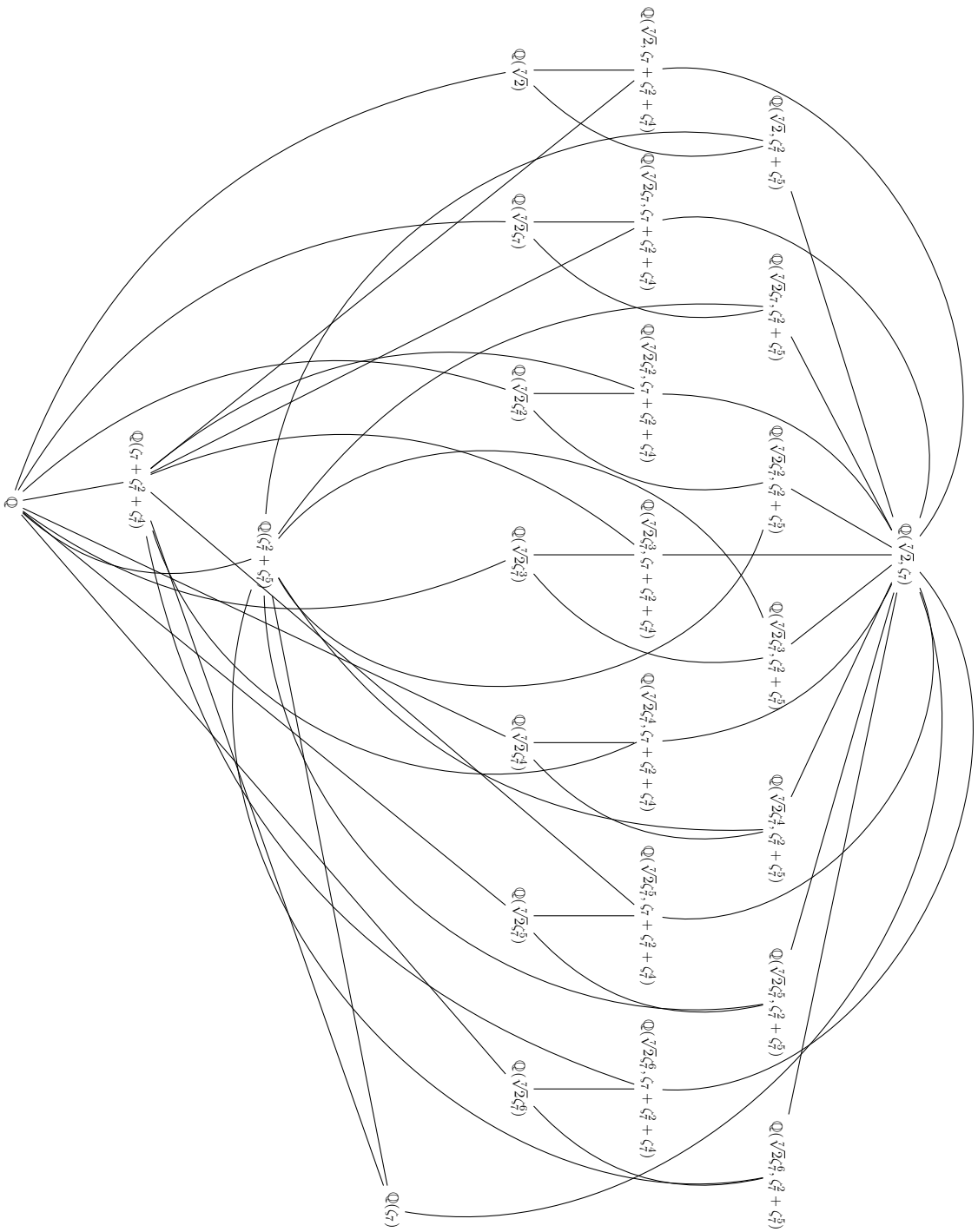
$\mathrm{Gal}(X^5 - 2, \mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$



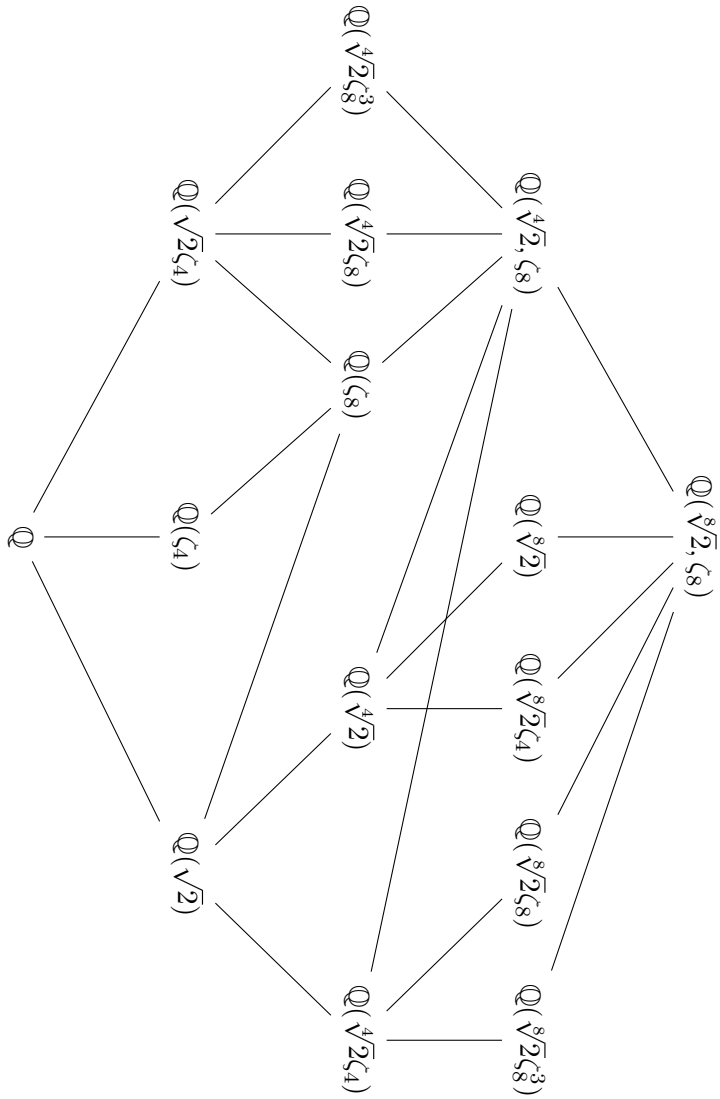
$\mathrm{Gal}(X^6 - 2, \mathbb{Q}) \cong D_6$



$\mathrm{Gal}(X^7 - 2, \mathbb{Q}) \cong \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z}$



$\mathrm{Gal}(X^8 - 2, \mathbb{Q}) \cong QD_8$



# Literatur


[1] Dietrich Burde. Algebra. Vorlesungsskriptum, 2020.

[2] Bryden Cais. Solutions to homework 11. URL:https://www.math.arizona.edu/~cais/594Page/soln/soln11.pdf. Zugegriffen: 01.09.2023.

[3] Keith Conrad. The galois correapondence. URL:https://kconrad.math.uconn.edu/blurbs/galoistheory/galoiscorr.pdf. Zugegriffen: 01.09.2023.

[4] MariáAcosta de Orozco and William Yslas Vélez. The lattice of subfields of a radical extension. *Journal of Number Theory*, 15(3):388–405, 1982.

[5] David Gay and William Vélez. On the degree of the splitting field of an irreducible binomial. *Pacific Journal of Mathematics*, 78(1):117–120, 1978.

[6] David Gay and William Vélez. The torsion group of a radical extension. *Pacific Journal of Mathematics*, 92(2):317–327, 1981.

[7] Eliot T Jacobson and William Y Vélez. The galois group of a radical extension of the rationals. *manuscripta mathematica*, 67:271–284, 1990.

[8] Gregory Karpilovsky. *Topics in field theory*. Elsevier, 1989.

[9] S LANG. Algebra (revised third edition). *Graduate Text in Mathematics*, 2002.

[10] Matthew Macauley. Chapter 8: Fields and galois theory. URL:http://www.math.clemson.edu/~macaule/classes/s22_math4120/slides/new/math4120_slides_chapter8_h.pdf. Zugegriffen: 01.09.2023.

[11] Arturo Magidin. Mathematics stack exchange question 74086. URL:https://math.stackexchange.com/q/74086(version:2011-10-19). Zugegriffen: 02.08.2023.

[12] Joachim Mahnkopf. Algebra 2. Vorlesungsskriptum, 2023.

[13] William Vélez. On normal binomials. *Acta Arithmetica*, 36(2):113–124, 1980.