2. Es sei K ein Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$.

(i) Bestimmen Sie alle Elemente von $\operatorname{Gal}_{\mathbb{Q}} K$ und zeigen Sie $\operatorname{Gal}_{\mathbb{Q}} K \cong D_4$.

(ii) Bestimmen Sie alle Zwischenkörper von $K \supset \mathbb{Q}$. Stellen Sie die Zwischenkörper, sowie die Untergruppen von $\operatorname{Gal}_{\mathbb{Q}} K$, jeweils in einem Diagramm dar.

Beweis: (i) In $\mathbb{C}$ zerfällt $X^4 - 2$ in Linearfaktoren und hat dort die Nullstellen $\{\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}\}$. Wir können also annehmen $K = \mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{C}$.

Es ist $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ (Satz 9.7). Wegen $i \notin \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ ist $X^2 + 1$ irreduzibel über $\mathbb{Q}(\sqrt[4]{2})$ und somit $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = 8$. Weil $\mathbb{Q}(\sqrt[4]{2}, i) \supset \mathbb{Q}$ galoissch ist [1], ist $|\operatorname{Gal}_{\mathbb{Q}} K| = [K : \mathbb{Q}] = 8$. Wir wollen nun 8 paarweise verschiedene $\mathbb{Q}$-Automorphismen von K konstruieren. Dazu wenden wir wiederholt Korollar 9.9 an.

Weil $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}$ ist, gibt es nach Korollar 9.9 ein $\varphi \in \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(i)$ mit $\varphi(i) = -i$ und $\varphi \mid \mathbb{Q} = \mathrm{id}_{\mathbb{Q}}$. Damit erhalten wir

$$\operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(i) = \{\mathrm{id}_{\mathbb{Q}(i)}, \varphi\}.$$

Wegen $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$ hat das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i)$ Grad 4, und es ist ein Teiler von $X^4 - 2$. Somit muss es also $X^4 - 2$ sein. Insbesondere ist $X^4 - 2$ auch irreduzibel über $\mathbb{Q}(i)$. Für die Fortsetzung $\overline{\varphi}\colon \mathbb{Q}(i)[X] \to \mathbb{Q}(i)[X]$ gilt $\overline{\varphi}(X^4 - 2) = X^4 - 2$. Aus Korollar 9.9 erhalten wir also jeweils 4 Fortsetzungen von $\mathrm{id}_{\mathbb{Q}(i)}$ bzw. φ auf K, indem wir $\sqrt[4]{2}$ auf eine beliebige andere Nullstelle von $X^4 - 2$ abbilden. Damit ergeben sich folgende acht $\mathbb{Q}$-Automorphismen von K:

$$\mathrm{id}\colon \begin{cases} i & \mapsto i \\ \sqrt[4]{2} & \mapsto \sqrt[4]{2} \end{cases} \quad \tau^2\colon \begin{cases} i & \mapsto i \\ \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \end{cases} \quad \tau\colon \begin{cases} i & \mapsto i \\ \sqrt[4]{2} & \mapsto i\sqrt[4]{2} \end{cases} \quad \tau^3\colon \begin{cases} i & \mapsto i \\ \sqrt[4]{2} & \mapsto -i\sqrt[4]{2} \end{cases}$$

$$\sigma\colon \begin{cases} i & \mapsto -i \\ \sqrt[4]{2} & \mapsto \sqrt[4]{2} \end{cases} \quad \tau^2\sigma \begin{cases} i & \mapsto -i \\ \sqrt[4]{2} & \mapsto -\sqrt[4]{2} \end{cases} \quad \tau\sigma\colon \begin{cases} i & \mapsto -i \\ \sqrt[4]{2} & \mapsto i\sqrt[4]{2} \end{cases} \quad \tau^3\sigma\colon \begin{cases} i & \mapsto -i \\ \sqrt[4]{2} & \mapsto -i\sqrt[4]{2} \end{cases}$$

Diese sind offensichtlich paarweise verschieden, also ist

$$\operatorname{Gal}_{\mathbb{Q}} K = \{\mathrm{id}, \tau, \tau^2, \tau^3, \sigma, \tau\sigma, \tau^2\sigma, \tau^3\sigma\}.$$

Es gilt $\operatorname{ord}(\tau) = 4$, $\operatorname{ord}(\sigma) = 2$, und weiters $\sigma\tau = \tau^{-1}\sigma$, denn

$$\begin{aligned} \sigma\tau(i) &= \sigma(i) = -i = \tau^3\sigma(i) = \tau^{-1}\sigma(i), \\ \sigma\tau(\sqrt[4]{2}) &= \sigma(i\sqrt[4]{2}) = -i\sqrt[4]{2} = \tau^3\sigma(\sqrt[4]{2}) = \tau^{-1}\sigma(\sqrt[4]{2}). \end{aligned}$$

[1] Die Erweiterung ist endlich-dimensional. Wegen $\operatorname{char}(\mathbb{Q}) = 0$ ist sie separabel, und weil K Zerfällungskörper von $X^4 - 2$ ist, ist die Erweiterung auch normal nach Satz 11.4.

Somit ist $\mathrm{Gal}_{\mathbb{Q}} K \cong D_4$. [2]

(ii) Wir haben bereits festgestellt, das $K \supset \mathbb{Q}$ galoissch ist. Nach dem Fundamentalsatz der Galoistheorie stehen also die Zwischenkörper von $K \supset \mathbb{Q}$ in Bijektion mit den Untergruppen von $G := \mathrm{Gal}_{\mathbb{Q}} K \cong D_4$. Wir bestimmen zuerst alle Untergruppen von G.

Natürlich sind die triviale Gruppe $\{\mathrm{id}\}$ und G selbst Untergruppen. Es ist $\mathrm{ord}(\tau) = \mathrm{ord}(\tau^3) = 4$. Die Elemente τ^2, σ, $\tau\sigma$, $\tau^2\sigma$ und $\tau^3\sigma$ haben jeweils Ordnung 2. [3] Damit erhalten wir alle zyklischen Untergruppen, wobei $\langle\tau\rangle = \langle\tau^3\rangle$ gilt. Nachdem jede Untergruppe der Ordnung 2 jedenfalls zyklisch ist, können also nur noch nicht-zyklische Untergruppen der Ordnung 4 fehlen. Diese müssen isomorph sein zu $\mathbb{Z}_2 \times \mathbb{Z}_2$ und werden demnach von zwei Elementen der Ordnung 2 erzeugt. Wir betrachten also für jedes Paar (α, β) von Elementen α, β der Ordnung 2, mit $\alpha \neq \beta$, die Untergruppe $\langle\alpha, \beta\rangle$. Wir erhalten entweder eine Untergruppe der Ordnung 4 oder $\langle\alpha, \beta\rangle = G$. Damit erhalten wir den in Abbildung 1 dargestellte Untergruppenverband.

Nun müssen wir zu jeder Untergruppe von G jeweils den Fixkörper finden, d.h., wir suchen Elemente die den Fixkörper als Erweiterung von $\mathbb{Q}$ erzeugen. (Siehe Abbildung 2.) Für viele Untergruppen ist das einfach. So ist zum Beispiel $\tau(i) = i$, also $i \in K_{\langle\tau\rangle} \setminus \mathbb{Q}$, und wegen $[K_{\langle\tau\rangle} : \mathbb{Q}] = (G : \langle\tau\rangle) = 2$ folgt $K_{\langle\tau\rangle} = \mathbb{Q}(i)$. Analog folgt $K_{\langle\tau^2,\sigma\rangle} = \mathbb{Q}(\sqrt{2})$. Weiters ist $\sigma(\sqrt[4]{2}) = \sqrt[4]{2}$, aber $\tau^2(\sqrt[4]{2}) = -\sqrt[4]{2} \neq \sqrt[4]{2}$. Also ist $\sqrt[4]{2} \in K_{\langle\sigma\rangle} \setminus K_{\langle\tau^2,\sigma\rangle}$ und deshalb $K_{\langle\sigma\rangle} = \mathbb{Q}(\sqrt[4]{2})$. Ähnlich schließt man $K_{\langle\tau^2\sigma\rangle} = \mathbb{Q}(i\sqrt[4]{2})$ und $K_{\langle\tau^2\rangle} = \mathbb{Q}(\sqrt{2}, i)$. Damit ist die linke Hälfte des Diagramms in Abbildung 2 gefunden.

Für die anderen Zwischenkörper sind die Erzeugenden vielleicht weniger offensichtlich. Wir gehen also systematisch vor. Betrachten wir zuerst $K_{\langle\tau^2,\tau\sigma\rangle}$. Wir wissen bereits $K_{\langle\tau^2\rangle} = \mathbb{Q}(\sqrt{2}, i)$. Durch zweimaliges Anwenden von Satz 9.7 sehen wir, dass

$$(1, \sqrt{2}, i, i\sqrt{2})$$

ein Erzeugendensystem des Vektorraums $\mathbb{Q}(\sqrt{2}, i)$ über $\mathbb{Q}$ ist. Wegen $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$ ist es auch eine Basis. Sei $a \in \mathbb{Q}(\sqrt{2}, i)$. Dann ist

$$a = a_1 + a_2\sqrt{2} + a_3 i + a_4 i\sqrt{2}$$

mit $a_1, \dots, a_4 \in \mathbb{Q}$. Es ist dann

$$\tau\sigma(a) = a_1 - a_2\sqrt{2} - a_3 i + a_4 i\sqrt{2}.$$

[2] Beispielsweise so: Aus $\mathrm{ord}(\tau) = 4$, $\mathrm{ord}(\sigma) = 2$ und $\sigma\tau = \tau^{-1}\sigma$ lässt sich die ganze Verknüpfungstafel von $\mathrm{Gal}_{\mathbb{Q}} K$ herleiten. Diese stimmt (bis auf mögliches Umbenennen der beiden Erzeuger, $\sigma \mapsto r$ und $\tau \mapsto d$) mit jener von D_4 überein, die wir aus Lemma 3.6 erhalten.

[3] Für τ^2 ist das klar wegen $\mathrm{ord}(\tau) = 4$. Für $k \in \mathbb{N}_0$ ist $(\tau^k\sigma)^2 = \tau^k\sigma\tau^k\sigma = \sigma\tau^{-k}\tau^k\sigma = \mathrm{id}$, und wegen $\tau^k\sigma \neq \mathrm{id}$, damit $\mathrm{ord}(\tau^k\sigma) = 2$.

Also gilt genau dann $a = \sigma(a)$, wenn $a_2 = a_3 = 0$ gilt. Daher ist $K_{\langle \tau^2, \tau\sigma \rangle} = \mathbb{Q}(i\sqrt{2})$.

Betrachten wir nun $K_{\langle \tau\sigma \rangle}$. Wir können dazu in der Erweiterung $K \supset \mathbb{Q}(i\sqrt{2})$ arbeiten. Es ist $K = \mathbb{Q}(i\sqrt{2}, \sqrt[4]{2})$ und wegen $[K : \mathbb{Q}(i\sqrt{2})] = 4$ muss $X^4 - 2$ das Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(i\sqrt{2})$ sein. Nach Satz 9.7 ist $(1, \sqrt[4]{2}, \sqrt{2}, (\sqrt[4]{2})^3)$ eine $\mathbb{Q}(i\sqrt{2})$-Basis von K. Sei $a \in K$. Dann ist

$$a = a_1 + a_2 \sqrt[4]{2} + a_3 \sqrt{2} + a_4 (\sqrt[4]{2})^3$$

mit $a_1, \ldots, a_4 \in \mathbb{Q}(i\sqrt{2})$. Wir erhalten

$$\tau\sigma(a) = a_1 + a_2 i \sqrt[4]{2} - a_3 \sqrt{2} - i a_4 (\sqrt[4]{2})^3 = a_1 - (i\sqrt{2} a_4) \sqrt[4]{2} - a_3 \sqrt{2} + \left(a_2 \frac{i}{\sqrt{2}} \right) (\sqrt[4]{2})^3.$$

Somit ist $a = \tau\sigma(a)$ genau dann, wenn $a_3 = 0$ und $a_2 = -i\sqrt{2} a_4$ gilt. Damit ist zum Beispiel $-i\sqrt{2}\sqrt[4]{2} + (\sqrt[4]{2})^3 = (1-i)(\sqrt[4]{2})^3$ in $K_{\langle \tau\sigma \rangle}$. Wegen $\tau^2((1-i)(\sqrt[4]{2})^3) = -(1-i)(\sqrt[4]{2})^3$ ist $(1-i)(\sqrt[4]{2})^3 \notin \mathbb{Q}(i\sqrt{2})$ und deshalb ist $K_{\langle \tau\sigma \rangle} = \mathbb{Q}((1-i)(\sqrt[4]{2})^3)$. Analog folgt $K_{\langle \tau^3\sigma \rangle} = \mathbb{Q}((1+i)(\sqrt[4]{2})^3)$.

(Man kann alternativ natürlich auch stets mit einer $\mathbb{Q}$-Basis des 8-dimensionalen Vektorraums K arbeiten.) $\square$

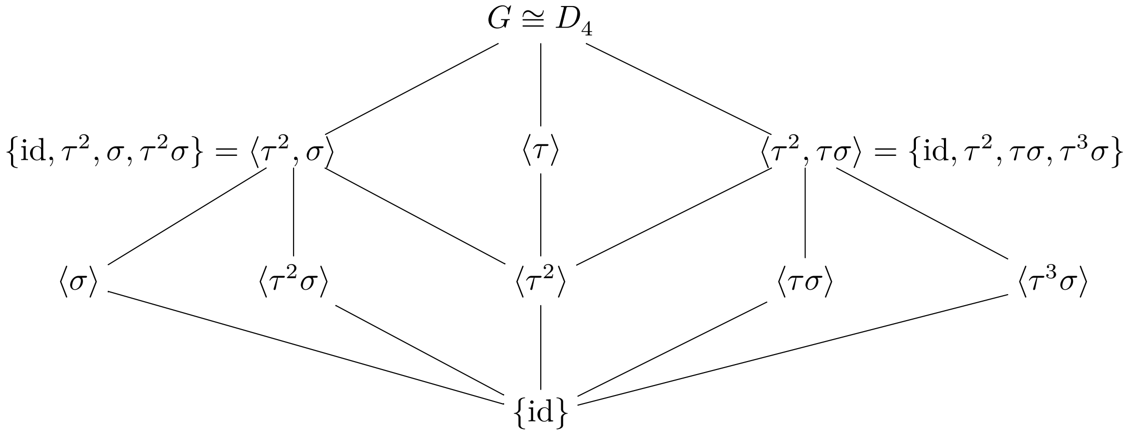

Abbildung 1: Untergruppenverband von $G \cong D_4$.

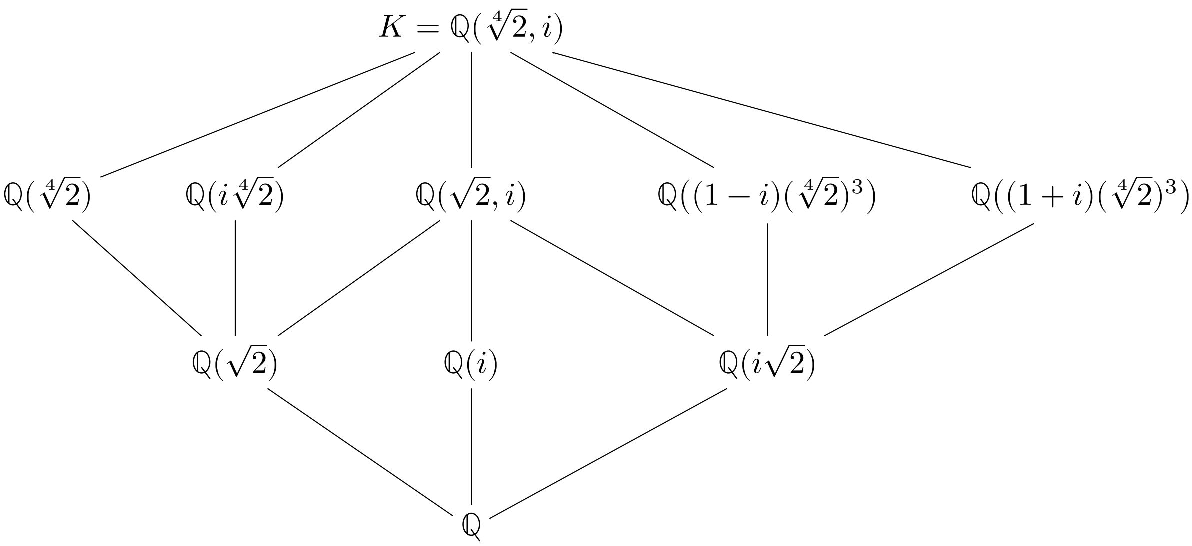

Abbildung 2: Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}, i)$.