4*. Es sei $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subset \mathbb{R}$. Bestimmen Sie alle Zwischenkörper der Erweiterung $\mathbb{Q} \subset K$.

Hinweis: Es gibt zumindest zwei Lösungswege. Einmal mit dem Fundamentalsatz der Galoistheorie und einmal (fast) ohne. In keinem Fall können Sie den Fundamentalsatz aber auf die Erweiterung $\mathbb{Q} \subset K$ anwenden.

Beweis (Variante A): Es ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ und $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Deshalb ist nach Blatt 9, Übung 1, $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 6$. Es gibt die offensichtlichen Zwischenkörper: $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$. Wir behaupten, dass das schon alle sind.

Beweis durch Widerspruch. Angenommen M ist ein weiterer Zwischenkörper. Dann ist $[M : \mathbb{Q}] \in \{2, 3\}$. Wir betrachten zuerst den Fall $[M : \mathbb{Q}] = 2$. Wir können annehmen $M = \mathbb{Q}(u)$ mit $u \in M$ (Satz vom primitiven Element, oder im Spezialfall hier Blatt 8, Übung 4). Nach Blatt 9, Übung 1 ist $2 \leq [\mathbb{Q}(u, \sqrt{2}) : \mathbb{Q}] \leq 4$. Wegen $M \neq \mathbb{Q}(\sqrt{2})$ muss aber $u \notin \mathbb{Q}(\sqrt{2})$ sein, und deshalb ist $2 < [\mathbb{Q}(u, \sqrt{2}) : \mathbb{Q}]$. Weiters ist $2 \mid [\mathbb{Q}(u, \sqrt{2}) : \mathbb{Q}]$. Das heißt $[M : \mathbb{Q}] = 4$. Aber dann ist $4 \mid [K : \mathbb{Q}] = 6$, ein Widerspruch.

Angenommen es ist $[M : \mathbb{Q}] = 3$. Dann ist $[K : M] = 2$. Man sieht leicht, dass jede quadratische Körpererweiterung normal ist. Wegen $\operatorname{char}(\mathbb{Q}) = 0$, ist die Erweiterung $K \supset M$ auch separabel. Also ist $K \supset M$ galoissch, und deshalb $|\operatorname{Gal}_M K| = 2$ und $M = K_{\operatorname{Gal}_M K}$. Es ist aber $\operatorname{Gal}_M K$ eine Untergruppe der Ordnung 2 von $\operatorname{Gal}_{\mathbb{Q}} K$. Wir bestimmen nun $\operatorname{Gal}_{\mathbb{Q}} K$: Weil $\sqrt[3]{2}$ die einzige Nullstelle von $X^3 - 2$ in K ist, ist für $\varphi \in \operatorname{Gal}_{\mathbb{Q}} K$ jedenfalls $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$ und $\varphi(\sqrt{2}) \in \{\pm\sqrt{2}\}$. Dass $\varphi(\sqrt{2}) = -\sqrt{2}$ tatsächlich möglich ist, folgt z.B. aus Korollar 9.9 angewandt auf $\mathrm{id}\colon \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$. Es folgt $|\operatorname{Gal}_{\mathbb{Q}} K| = 2$ und deshalb $\operatorname{Gal}_M K = \operatorname{Gal}_{\mathbb{Q}} K$. Der Fixkörper von $\operatorname{Gal}_{\mathbb{Q}} K$ ist aber $\mathbb{Q}(\sqrt[3]{2})$. Somit ist $M = \mathbb{Q}(\sqrt[3]{2})$, ein Widerspruch. $\square$

Einige Schlüsse in der ersten Variante funktionierten nur für quadratische Erweiterungen. Der folgende Ansatz, in dem wir die Körperweiterung $K \supset \mathbb{Q}$ als Teilerweiterung einen Galoiserweiterung auffassen, funktioniert immer.

Beweis (Variante B1): Es sei $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \omega)$, wobei $\omega = \frac{-1+i\sqrt{3}}{2} \in \mathbb{C}$ eine dritte Einheitswurzel sei. L ist Zerfällungskörper von $(X^2-2)(X^3-2)$ über $\mathbb{Q}$, und wegen $\operatorname{char}\mathbb{Q} = 0$ auch separabel über $\mathbb{Q}$. Damit ist $\mathbb{Q} \subset L$ eine Galoiserweiterung. Auf die Erweiterung $\mathbb{Q} \subset L$ ist also der Fundamentalsatz der Galoistheorie anwendbar: Die Zwischenkörper stehen in Bijektion zu den Untergruppen von $\operatorname{Gal}_{\mathbb{Q}} L$. Der Teilkörper K ist Fixkörper einer Untergruppe $H \subset \operatorname{Gal}_{\mathbb{Q}} L$. Um alle Zwischenkörper von $\mathbb{Q} \subset K$ zu finden, genügt es also alle Untergruppen von $\operatorname{Gal}_{\mathbb{Q}} L$ zu bestimmen, die H enthalten.

Es sei $M = \mathbb{Q}(\sqrt[3]{2}, \omega)$. Die Galoiserweiterung $M \supset \mathbb{Q}$ wurde bereits in Beispiel 14.8 im Vorlesungsskript betrachtet. Es gibt einen Automorphismus in $\operatorname{Gal}_{\mathbb{Q}} M$ mit $\omega \mapsto \omega$ und $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$. Dieser lässt sich mit Korollar 9.9 fortsetzen zu $\sigma \in \operatorname{Gal}_{\mathbb{Q}} L$ mit

$$\sigma(\omega) = \omega, \qquad \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \qquad \sigma(\sqrt{2}) = -\sqrt{2}.$$

Analog finden wir einen Automorphismus $\tau \in \operatorname{Gal}_{\mathbb{Q}} L$ mit

$$\tau(\omega) = \omega^2, \qquad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \qquad \tau(\sqrt{2}) = \sqrt{2}.$$

Damit gilt $\operatorname{ord}(\sigma) = 6$, $\operatorname{ord}(\tau) = 2$ und $\tau\sigma = \sigma^{-1}\tau$. Also ist $\langle \tau, \sigma \rangle \cong D_6$ und deshalb, wegen $|\operatorname{Gal}_{\mathbb{Q}} L| \leq 6$,

$$D_6 \cong \operatorname{Gal}_{\mathbb{Q}} L = \langle \tau, \sigma \rangle = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3, \tau\sigma^4, \tau\sigma^5\}.$$

K ist der Fixkörper von $H = \langle \tau \rangle$. Wir bestimmen nun alle Untergruppen, die τ enthalten. In einer solchen Untergruppe ist $\tau\sigma^k$ genau dann enthalten wenn es auch σ^k ist. Das heißt, es genügt Untergruppen zu betrachten die von τ und Potenzen von σ erzeugt werden. Das sind

$$\begin{aligned}
\langle \tau, \sigma \rangle &= \operatorname{Gal}_{\mathbb{Q}} L, \\
\langle \tau, \sigma^2 \rangle &= \{\mathrm{id}, \sigma^2, \sigma^4, \tau, \tau\sigma^2, \tau\sigma^4\}, \\
\langle \tau, \sigma^3 \rangle &= \{\mathrm{id}, \sigma^3, \tau, \tau\sigma^3\}, \\
\langle \tau \rangle &= \operatorname{Gal}_K L.
\end{aligned}$$

Die entsprechenden Fixkörper sind $\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{2})$, und K. □

In der letzten Variante verfolgen wir die gleiche Strategie wie in der vorigen Variante, verwenden aber einen anderen Ansatz um $\operatorname{Gal}_{\mathbb{Q}} L$ zu bestimmen.

Beweis (Variante B2): Es seien ω, L, und M wie in Variante B1. Aus Beispiel 14.8 im Vorlesungsskript wissen wir $\operatorname{Gal}_{\mathbb{Q}} M \cong S_3$. Weiters ist $\operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cong \mathbb{Z}_2$. Jedes $\sigma \in \operatorname{Gal}_{\mathbb{Q}} M$ lässt sich zu einem $\overline{\sigma} \in \operatorname{Gal}_{\mathbb{Q}} L$ mit $\overline{\sigma}(\sqrt{2}) = \sqrt{2}$ und $\overline{\sigma}|M = \sigma$ fortsetzen. Die Menge dieser Fortsetzungen bildet eine Untergruppe $A \subset \operatorname{Gal}_{\mathbb{Q}} L$, die zu $\operatorname{Gal}_{\mathbb{Q}} M$ isomorph ist. In gleicher Weise lässt sich jedes $\sigma \in \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ fortsetzen zu $\overline{\sigma} \in \operatorname{Gal}_{\mathbb{Q}} L$ mit $\overline{\sigma}(\sqrt[3]{2}) = \sqrt[3]{2}$, $\overline{\sigma}(\omega) = \omega$, und $\overline{\sigma}|\mathbb{Q}(\sqrt{2}) = \sigma$. Wir erhalten eine Untergruppe $B \subset \operatorname{Gal}_{\mathbb{Q}} L$ mit $B \cong \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$.

Wir beobachten weiters, dass M der Fixkörper von B ist, und $\mathbb{Q}(\sqrt{2})$ der Fixkörper von A ist. Weil diese beiden Körper galoissch über $\mathbb{Q}$ sind, folgt aus dem Fundamentalsatz der Galoistheorie, dass A und B Normalteiler von $\operatorname{Gal}_{\mathbb{Q}} L$

sind. Außerdem ist $A \cap B = \{\mathrm{id}\}$. Damit ist $\langle A, B\rangle = A \cdot B$ (dir), und aus Kardinalitätsgründen

$$\operatorname{Gal}_{\mathbb{Q}} L = A \cdot B \text{ (dir)} \cong \operatorname{Gal}_{\mathbb{Q}} M \times \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cong S_3 \times \mathbb{Z}_2.$$

(Es ist $D_6 \cong S_3 \times \mathbb{Z}_2$, das widerspricht also nicht der Variante B1.)

Mit etwas mehr Theorie lässt sich $\operatorname{Gal}_{\mathbb{Q}} L \cong \operatorname{Gal}_{\mathbb{Q}} M \times \operatorname{Gal}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$ auch auf einen Blick sehen: Die Aussage folgt sofort aus dem *Produktsatz der Galoistheorie*.

Der Körper K ist der Fixkörper von $\langle\tau\rangle \subset \operatorname{Gal}_{\mathbb{Q}} L$ mit $\tau(\omega) = \omega^2$, $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$, und $\tau(\sqrt{2}) = \sqrt{2}$. Wählt man den Isomorphismus $\operatorname{Gal}_{\mathbb{Q}}(\sqrt[3]{2}, \omega) \cong S_3$ wie in Beispiel 14.8 im Vorlesungsskript, so wird τ auf $t = \big((2\,3), 0 + 2\mathbb{Z}\big)$ abgebildet. Es gilt also alle Untergruppen von $S_3 \times \mathbb{Z}_2$ zu bestimmen, die t enthalten. Ist $H \subset S_3 \times \mathbb{Z}_2$ eine Untergruppe mit $t \in H$, und ist $p\colon S_3 \times \mathbb{Z}_2 \to S_3$ die Projektion auf die erste Komponente, so ist $\pi(H)$ eine Untergruppe von S_3, die die Permutation $(2\,3)$ enthält. Damit ist entweder $\pi(H) = \{(), (2\,3)\}$ oder $\pi(H) = S_3$. Die möglichen Urbilder dieser Untergruppen in $S_3 \times \mathbb{Z}_2$ sind damit $\langle t\rangle$, $\langle t, ((), 1 + 2\mathbb{Z})\rangle$, $S_3 \times \mathbf{0}$, und $S_3 \times \mathbb{Z}_2$. Die Fixkörper der entsprechenden Untergruppen von $\operatorname{Gal}_{\mathbb{Q}} L$ sind K, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}$. $\square$