Aufgabe F17T1A2 (12 Punkte)

Betrachten Sie die Körpererweiterung $L = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{3}}) \subseteq \mathbb{C}$ über $\mathbb{Q}$. Sei $x = \sqrt{2+\sqrt{3}} \in L$.

(a) Zeigen Sie, dass $x - \sqrt{2-\sqrt{3}} = \sqrt{2}$ gilt.

(b) Bestimmen Sie das Minimalpolynom von x über $\mathbb{Q}$.

(c) Bestimmen Sie das Minimalpolynom von x über $\mathbb{Q}(\sqrt{2})$.

(d) Bestimmen Sie die Galoisgruppe von $\mathrm{Gal}(L|\mathbb{Q})$.

Lösung:

zu (a) Es gilt

$$\begin{aligned}(x - \sqrt{2-\sqrt{3}})^2 &= x^2 - 2\sqrt{2-\sqrt{3}}x + (\sqrt{2-\sqrt{3}})^2 = \left(2+\sqrt{3}\right) - 2\sqrt{2^2-3} + \left(2-\sqrt{3}\right) \\ &= 4 - 2\sqrt{1} = 2.\end{aligned}$$

Da $x - \sqrt{2-\sqrt{3}}$ außerdem positiv ist, erhalten wir $x - \sqrt{2-\sqrt{3}} = \sqrt{2}$.

zu (b) Zunächst bestimmen wir ein Polynom mit x als Nullstelle. Die Rechnung

$$x = \sqrt{2+\sqrt{3}} \quad \Rightarrow \quad x^2 = 2+\sqrt{3} \quad \Rightarrow \quad x^2 - 2 = \sqrt{3} \quad \Rightarrow \quad (x^2-2)^2 = 3 \quad \Rightarrow$$
$$x^4 - 4x^2 + 4 = 3 \quad \Rightarrow \quad x^4 - 4x^2 + 1 = 0$$

zeigt, dass x eine Nullstelle des Polynoms $f = X^4 - 4X^2 + 1$ ist. Es bleibt zu zeigen, dass f irreduzibel ist. Es gilt

$$\begin{aligned}f(X+1) &= (X+1)^4 - 4(X+1)^2 + 1 = (X^4 + 4X^3 + 6X^2 + 4X + 1) - (4X^2 + 8X + 4) + 1 \\ &= X^4 + 4X^3 + 2X^2 - 4X - 2\end{aligned}$$

Auf Grund des Eisenstein-Kriteriums (angwendet auf die Primzahl $p = 2$) ist $f(X+1)$ in $\mathbb{Z}[X]$ und auch in $\mathbb{Q}[X]$ irreduzibel. Wäre nun f in $\mathbb{Q}[X]$ reduzibel, dann gäbe es nicht-konstante Polynome $g, h \in \mathbb{Q}[X]$ mit $f = gh$, und $f(X+1) = g(X+1)h(X+1)$ wäre eine Zerlegung von $f(X+1)$ in nicht-konstante Polynome, im Widerspruch zur Irreduzibilität von $f(X+1)$. Insgesamt ist f also irreduzibel in $\mathbb{Q}[x]$, normiert, und es gilt $f(x) = 0$. Damit ist f das Minimalpolynom von x über $\mathbb{Q}$.

(Es gibt mindestens zwei weitere Möglichkeiten, die Irreduzibilität von f zu beweisen: Man zeigt, dass f in $\mathbb{Q}$ keine Nullstellen hat, indem man $f(1), f(-1) \neq 0$ überprüft und anschließend noch nachrechnet, dass es keine Zerlegung der Form $f = (X^2+aX+b)(X^2+cX+d)$ mit $a, b, c, d \in \mathbb{Z}$ gibt. Oder man zeigt, dass $[\mathbb{Q}(x) : \mathbb{Q}] \geq 4$ gilt, indem man nachweist, dass $\sqrt{2}$ und $\sqrt{3}$ in $\mathbb{Q}(x)$ enthalten sind. Damit kann das Minimalpolynom $\mu_{x,\mathbb{Q}}$ von x kein echter Teiler von f sein, denn daraus würde $[\mathbb{Q}(x) : \mathbb{Q}] = \mathrm{grad}(\mu_{x,\mathbb{Q}}) < 4$ folgen.)

zu (c) *Vorüberlegung:* Wie man leicht überprüft, sind die vier Nullstellen von f durch $\pm\sqrt{2 \pm \sqrt{3}}$ gegeben. Somit ist f das Produkt der vier Linearfaktoren $X \pm \sqrt{2 \pm \sqrt{3}}$. Das Minimalpolynom von x über $\mathbb{Q}(\sqrt{2})$ ist wegen $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{2})] = 2$ ein Produkt von zwei dieser Linearfaktoren. Bei der Auswahl der richtigen zwei Faktoren kommt uns das Ergebnis aus Teil (a) zur Hilfe.

Wir betrachten das Polynom $g = (X - \sqrt{2+\sqrt{3}})(X + \sqrt{2-\sqrt{3}}) = (X-x)(X+\sqrt{2-\sqrt{3}})$. Dieses ist wegen

$$\begin{aligned}(X-x)(X+\sqrt{2-\sqrt{3}}) &= X^2 + (\sqrt{2-\sqrt{3}} - x)X - x\sqrt{2-\sqrt{3}} \\ &= X^2 - \sqrt{2}X - \sqrt{2^2-3} = X^2 - \sqrt{2}X - 1\end{aligned}$$

in $\mathbb{Q}(\sqrt{2})[X]$ enthalten, und es gilt $g(x) = 0$. Dies zeigt, dass das Minimalpolynom von x über $\mathbb{Q}(\sqrt{2})$ ein Teiler von g in $\mathbb{Q}(\sqrt{2})[X]$ sein muss. Weil $\sqrt{2}$ eine Nullstelle des nach dem Eisenstein-Kriterium irreduziblen Polynoms $h = X^2 - 2 \in \mathbb{Q}[X]$ ist, gilt $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \operatorname{grad}(h) = 2$. Weil f nach (b) das Minimalpolynom von x über $\mathbb{Q}$ ist, gilt $[\mathbb{Q}(x) : \mathbb{Q}] = \operatorname{grad}(g) = 4$. Es folgt

$$\begin{aligned}[\mathbb{Q}(\sqrt{2},x) : \mathbb{Q}(\sqrt{2})] \cdot 2 &= [\mathbb{Q}(\sqrt{2},x) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \\ [\mathbb{Q}(\sqrt{2},x) : \mathbb{Q}] &\geq [\mathbb{Q}(x) : \mathbb{Q}] = 4\end{aligned}$$

und somit $[\mathbb{Q}(\sqrt{2},x) : \mathbb{Q}(\sqrt{2})] \geq 2$. Das Minimalpolynom von x über $\mathbb{Q}(\sqrt{2})$ ist also mindestens vom Grad 2. Es kann somit kein echter Teiler von g sein. Weil g außerdem normiert ist, muss es sich bei g um das gesuchte Minimalpolynom handeln.

zu (d) Wegen Teil (c) gilt $[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},x) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \operatorname{grad}(g) \cdot 2 = 2 \cdot 2 = 4$. Als algebraische Erweiterung von $\mathbb{Q}$ ist $L|\mathbb{Q}$ separabel. Um zu zeigen, dass $L|\mathbb{Q}$ auch normal ist, weisen wir nach, dass L der Zerfällungskörper von f über $\mathbb{Q}$ ist. Für jedes $\alpha \in \mathbb{R}$ gilt die Äquivalenz

$$\begin{aligned}f(\alpha) = 0 \quad &\Leftrightarrow \quad \alpha^4 - 4\alpha^2 + 1 = 0 \quad \Leftrightarrow \quad \alpha^4 - 4\alpha^2 + 4 = 3 \quad \Leftrightarrow \quad (\alpha^2-2)^2 = 3 \\ &\Leftrightarrow \quad (\alpha^2-2)^2 - \sqrt{3}^2 = 0 \quad \Leftrightarrow \quad (\alpha^2 - 2 - \sqrt{3})(\alpha^2 - 2 + \sqrt{3}) = 0 \\ &\Leftrightarrow \quad \alpha^2 \in \{2 \pm \sqrt{3}\} \quad \Leftrightarrow \quad \alpha \in \left\{\pm\sqrt{2\pm\sqrt{3}}\right\}.\end{aligned}$$

Nach Definition des Zerfällungskörpers müssen wir also $L = \mathbb{Q}(N)$ mit $N = \{\pm\sqrt{2\pm\sqrt{3}}\}$ nachweisen. Es gilt $x = \sqrt{2+\sqrt{3}} \in \mathbb{Q}(N)$ und $\sqrt{2} = x - \sqrt{2-\sqrt{3}} \in \mathbb{Q}(N)$, daraus folgt $L \subseteq \mathbb{Q}(N)$. Umgekehrt ist $x = \sqrt{2+\sqrt{3}} \in L$ und $\sqrt{2-\sqrt{3}} = x - \sqrt{2} \in L$, daraus folgt $N \subseteq L$ und $\mathbb{Q}(N) \subseteq L$. Insgesamt ist $L|Q$ also eine Galois-Erweiterung, und es gilt $|\operatorname{Gal}(L|\mathbb{Q})| = [L : \mathbb{Q}] = 4$.

Als Gruppe der Ordnung 4 ist $\operatorname{Gal}(L|\mathbb{Q})$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$ oder zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Im Fall $\operatorname{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ wäre die Galoisgruppe zyklisch von Ordnung 4, es gäbe dann genau eine Untergruppe von Ordnung 2 und (gleichbedeutend) genau eine Untergruppe vom Index 2 in $\operatorname{Gal}(L|\mathbb{Q})$. Nach dem Hauptsatz der Galoistheorie würde daraus folgen, dass es in $L|\mathbb{Q}$ genau einen Zwischenkörper vom Grad 2 über $\mathbb{Q}$ gibt. Einer dieser Zwischenkörper ist $\mathbb{Q}(\sqrt{2})$. Aber wegen $x^2 - 2 = \sqrt{3} \in L$ ist $\mathbb{Q}(\sqrt{3})$ ebenfalls ein Zwischenkörper vom Grad 2 über $\mathbb{Q}$, und aus der Vorlesung ist $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$ bekannt. Also kann $\operatorname{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$ nicht zutreffen, und als einzige Möglichkeit bleibt $\operatorname{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.