Aufgabe F18T3A5 (12 Punkte)

Es sei $K = \mathbb{Q}(i) \subseteq \mathbb{C}$ und $\alpha = \sqrt[4]{7} \in \mathbb{R}$. Sei $L \subseteq \mathbb{C}$ der Zerfällungskörper des Polynoms $f = x^4 - 7 \in K[x]$ über dem Grundkörper K.

(a) Zeigen Sie, dass $L = K(\alpha)$ gilt.

(b) Bestimmen Sie die Grade der Körpererweiterungen $L|\mathbb{Q}$ und $L|K$, und begründen Sie Ihre Antworten.

(c) Zeigen Sie, dass die Körpererweiterung $L|K$ galoissch ist.

(d) Es sei $\sigma \in \mathrm{Gal}(L|K)$ mit $\sigma(\alpha) = i\alpha$. Bestimmen Sie damit $\sigma^2(\alpha)$ und folgern Sie, dass $\mathrm{Gal}(L|K) = \langle\sigma\rangle$ gilt.

Lösung:

zu (a) Die Nullstellen von $f = x^4 - 7$ in $\mathbb{C}$ sind gegeben durch $\pm\alpha, \pm i\alpha$, wie man mit Hilfe der Gleichung $i^4 = 1$ unmittelbar nachrechnet. Setzen wir also $N = \{\alpha, -\alpha, i\alpha, -i\alpha\}$, dann ist der Zerfällungskörper L nach Definition durch $L = K(N)$ gegeben. Zu zeigen ist also

$$K(N) \quad = \quad K(\alpha).$$

Wegen $i \in K \subseteq K(\alpha)$ und $\alpha \in K(\alpha)$ gilt $\pm i\alpha \in K(\alpha)$ und somit $N \subseteq K(\alpha)$, denn $K(\alpha)$ ist als Körper unter Multiplikation abgeschlossen. Weil $K(\alpha)$ ein Zwischenkörper von $\mathbb{C}|K$ ist, folgt aus $N \subseteq K(\alpha)$ die Inklusion $K(N) \subseteq K(\alpha)$ (denn $K(N)$ ist nach Definition der *kleinste* Zwischenkörper von $\mathbb{C}|K$, der N als Teilmenge enthält). Die umgekehrte Inklusion $K(\alpha) \subseteq K(N)$ folgt unmittelbar aus $\alpha \in N \subseteq K(N)$ und der Tatsache, dass $K(N)$ ein Zwischenkörper von $\mathbb{C}|K$ ist.

zu (b) Zunächst bemerken wir, dass $L = K(\alpha) = \mathbb{Q}(i)(\alpha) = \mathbb{Q}(i, \alpha) = \mathbb{Q}(\alpha)(i)$ gilt. Dies verwenden wir, um in zwei Schritten und durch Anwendung der Gradformel den Erweiterungsgrad $[L : \mathbb{Q}]$ zu bestimmen. Nach dem Eisenstein-Kriterium, angwendet auf die Primzahl $p = 7$, ist das Polynom f in $\mathbb{Z}[x]$ irreduzibel, und nach dem Gaußschen Lemma auch in $\mathbb{Q}[x]$. Außerdem ist f normiert, und es gilt $f(\alpha) = 0$. Insgesamt ist f damit das Minimalpolynom von α über $\mathbb{Q}$, und wir erhalten

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad \mathrm{grad}(f) \quad = \quad 4.$$

Das Polynom $g = x^2 + 1$ ist normiert und erfüllt die Gleichung $g(i) = 0$. Wäre es in $\mathbb{Q}(\alpha)[x]$ reduzibel, dann würden wegen $\mathrm{grad}(g) = 2$ die beiden Nullstellen $\pm i$ von g in $\mathbb{Q}(\alpha)$ liegen. Aber dies ist nicht der Fall, denn wegen $\alpha \in \mathbb{R}$ gilt einerseits $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, andererseits aber $\pm i \notin \mathbb{R}$. Also ist g in $\mathbb{Q}(\alpha)[x]$ irreduzibel, insgesamt das Minimalpolynom von i über $\mathbb{Q}(\alpha)$. Daraus folgt $[L : \mathbb{Q}(\alpha)] = [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)] = \mathrm{grad}(g) = 2$, und mit der Gradformel erhalten wir

$$[L : \mathbb{Q}] \quad = \quad [L : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] \quad = \quad 2 \cdot 4 \quad = \quad 8.$$

Andererseits gilt auf Grund der Gradformel auch $[L:\mathbb{Q}] = [L:K] \cdot [K:\mathbb{Q}]$, also $[L:K] = \frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]}$. Da das Polynom $g \in \mathbb{Q}[x]$ irreduzibel über $\mathbb{Q}(\alpha)$ ist, ist es erst recht irreduzibel über $\mathbb{Q}$. Also ist g auch das Minimalpolynom von i über $\mathbb{Q}$, und es folgt $[K:\mathbb{Q}] = [\mathbb{Q}(i):\mathbb{Q}] = \mathrm{grad}(g) = 2$. Damit erhalten wir $[L:K] = \frac{[L:\mathbb{Q}]}{[K:\mathbb{Q}]} = \frac{8}{2} = 4$.

zu (c) Wie in Teil (a) gezeigt wurde, ist L Zerfällungskörper des Polynoms f über K. Daraus folgt, dass $L|K$ eine normale Erweiterung ist. Als normale Erweiterung ist $L|K$ insbesondere algebraisch, und wegen $\mathrm{char}(K) = 0$ ist jede algebraische Erweiterung von K eine separable Erweiterung. Als normale und separable Erweiterung ist $L|K$ nach Definition galoissch.

zu (d) Wegen $i \in K$, und weil σ ein K-Automorphismus von L ist, gilt $\sigma(i) = i$. Daraus folgt $\sigma(i\alpha) = \sigma(i)\sigma(\alpha) = i\sigma(\alpha)$ und

$$\sigma^2(\alpha) \quad = \quad \sigma(\sigma(\alpha)) \quad = \quad \sigma(i\alpha) \quad = \quad i\sigma(\alpha) \quad = \quad i(i\alpha) \quad = \quad -\alpha.$$

Damit wiederum erhalten wir $\sigma^4(\alpha) = \sigma^2(\sigma^2(\alpha)) = \sigma^2(-\alpha) = -\sigma^2(\alpha) = -(-\alpha) = \alpha$. Wegen $L = K(\alpha)$ ist jedes Element $\tau \in \mathrm{Gal}(L|K)$ durch das Bild $\tau(\alpha)$ bereits eindeutig festgelegt. Aus $\sigma^4(\alpha) = \alpha$ folgt deshalb $\sigma^4 = \mathrm{id}_L$; wegen $\sigma^2(\alpha) = -\alpha \neq \alpha$ ist andererseits $\sigma^2 \neq \mathrm{id}_L$.

Aus $\sigma^4 = \mathrm{id}_L$ und $\sigma^2 \neq \mathrm{id}_L$ folgt, dass σ in $\mathrm{Gal}(L|K)$ ein Element der Ordnung 4 ist, also $|\langle\sigma\rangle| = 4$ gilt. Da es sich bei $L|K$ um eine Galois-Erweiterung handelt, gilt $|\mathrm{Gal}(L|K)| = [L:K] = 4$. Aus $\langle\sigma\rangle \subseteq \mathrm{Gal}(L|K)$ und $|\mathrm{Gal}(L|K)| = 4 = |\langle\sigma\rangle|$ folgt $\mathrm{Gal}(L|K) = \langle\sigma\rangle$.