Aufgabe F19T3A3 (12 Punkte)

Sei $\zeta = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$ (mit $i^2 = -1$) und seien $K = \mathbb{Q}(\zeta)$, $L = \mathbb{Q}(\zeta, \sqrt[4]{2})$. Zeigen Sie:

(a) Es gilt $\zeta^4 = -1$, und K ist der Zerfällungskörper von $x^4 + 1$ über $\mathbb{Q}$.

(b) Das Polynom $f = x^4 + 2$ ist irreduzibel über $\mathbb{Q}$.

(c) Der Körper L ist Zerfällungskörper von f über $\mathbb{Q}$.

Lösung:

zu (a) Es ist $(1+i)^2 = 1^2+2i+i^2 = 1+2i+(-1) = 2i$ und $(1+i)^4 = ((1+i)^2)^2 = (2i)^2 = 2^2(-i)^2 = -4$. Daraus folgt

$$\zeta^4 \quad = \quad \left(\frac{1+i}{\sqrt{2}}\right)^4 \quad = \quad \frac{(1+i)^4}{(\sqrt{2})^4} \quad = \quad \frac{(-4)}{4} \quad = \quad -1.$$

Die Gleichungen $\zeta^4 = -1 \neq 1$ und $\zeta^8 = (\zeta^4)^2 = (-1)^2 = 1$ zeigen, dass ζ in der multiplikativen Gruppe $\mathbb{C}^\times$ ein Element der Ordnung 8 ist. Die Elemente ζ^k mit $k \in \mathbb{Z}$, $0 \leq k < 8$ sind somit alle verschieden. Aus $\zeta^4 = -1$, $(\zeta^3)^4 = (\zeta^4)^3 = (-1)^3 = -1$, $(\zeta^5)^4 = (-1)^5 = -1$ und $(\zeta^7)^4 = (-1)^7 = -1$ folgt nun, dass $\zeta, \zeta^3, \zeta^5, \zeta^7$ vier verschiedene Nullstellen von $x^4 + 1$ sind. Als Polynom vom Grad 4 über einem Körper besitzt x^4+1 höchstens vier Nullstellen; dies zeigt, dass $N = \{\zeta, \zeta^3, \zeta^5, \zeta^7\}$ die gesamte Nullstellenmenge von $x^4 + 1$ in $\mathbb{C}$ ist. Um nachzuweisen, dass K der Zerfällungskörper dieses Polynoms in $\mathbb{C}$ über $\mathbb{Q}$ ist, müssen wir nun die Gleichung

$$\mathbb{Q}(\zeta) \quad = \quad \mathbb{Q}(N)$$

überprüfen. Die Inklusion „$\subseteq$“ ist erfüllt, denn aus $\zeta \in N$ folgt $\zeta \in \mathbb{Q}(N)$, und dies wiederum impliziert $\mathbb{Q}(\zeta) \subseteq \mathbb{Q}(N)$. Auch die umgekehrte Inklusion „$\supseteq$“ ist gültig, denn weil $\mathbb{Q}(\zeta)$ als Teilkörper von $\mathbb{C}$ bezüglich Multiplikation abgeschlossen ist, sind mit $\zeta \in \mathbb{Q}(\zeta)$ auch die Elemente $\zeta^3, \zeta^5, \zeta^7$ in $\mathbb{Q}(\zeta)$ enthalten. Insgesamt gilt also $N \subseteq \mathbb{Q}(\zeta)$, und daraus folgt $\mathbb{Q}(N) \subseteq \mathbb{Q}(\zeta)$.

zu (b) Auf Grund des Eisenstein-Kriteriums, angewendet auf die Primzahl 2, ist f über $\mathbb{Z}$ irreduzibel. Nach dem Gaußschen Lemma folgt daraus die Irreduzibilität des Polynoms über $\mathbb{Q}$.

zu (c) Sei $\alpha = \sqrt[4]{2}$. Dann ist die Nullstellenmenge von f in $\mathbb{C}$ gegeben durch $M = \{\zeta^k\alpha \mid k \in \{1,3,5,7\}\}$. Denn einerseits gilt für jedes $k \in \{1,3,5,7\}$ nach Teil (a) jeweils

$$f(\zeta^k\alpha) \quad = \quad (\zeta^k\alpha)^4 + 2 \quad = \quad (\zeta^k)^4\alpha^4 + 2 \quad = \quad (-1)\cdot 2 + 2 \quad = \quad 0.$$

Andererseits sind mit $\zeta, \zeta^3, \zeta^5, \zeta^7$ wegen $\alpha \neq 0$ auch die Elemente $\zeta^k\alpha$ mit $k \in \{1,3,5,7\}$ alle verschieden. Weil f als Polynom vom Grad 4 über dem Körper $\mathbb{C}$ höchstens vier Nullstellen besitzt, muss M also die gesamte Nullstellenmenge von f sein. Für den Nachweis, dass L Zerfällungskörper von f über $\mathbb{Q}$ ist, müssen wir nun

$$\mathbb{Q}(\zeta, \alpha) \quad = \quad \mathbb{Q}(M) \qquad \text{überprüfen.}$$

Die Inklusion „$\supseteq$“ ist erfüllt, denn $\mathbb{Q}(\zeta, \alpha)$ enthält die Elemente ζ und α und damit (da $\mathbb{Q}(\zeta, \alpha)$ als Teilkörper von $\mathbb{C}$ unter der Multiplikation abgeschlossen ist) auch alle Elemente aus M. Aus $M \subseteq \mathbb{Q}(\zeta, \alpha)$ folgt nun $\mathbb{Q}(M) \subseteq \mathbb{Q}(\zeta, \alpha)$. Für den Nachweis von „$\subseteq$“ bemerken wir zunächst, dass mit $\zeta\alpha$ auch das Elemente $(\zeta\alpha)^2 = \zeta^2\alpha^2 = i\sqrt{2}$ in $\mathbb{Q}(M)$ enthalten ist. Mit $\zeta\alpha, \zeta^3\alpha$ liegt auch $i = \zeta^2 = \frac{\zeta^3\alpha}{\zeta\alpha}$ und $\sqrt{2} = i^{-1}(i\sqrt{2})$ in $\mathbb{Q}(M)$. Es folgt $\zeta = \frac{1+i}{\sqrt{2}} \in \mathbb{Q}(M)$ und schließlich $\alpha = \zeta^{-1}(\zeta\alpha) \in \mathbb{Q}(M)$. Aus $\{\zeta, \alpha\} \subseteq \mathbb{Q}(M)$ folgt dann $\mathbb{Q}(\zeta, \alpha) \subseteq \mathbb{Q}(M)$.