**Aufgabe F13T2A4** (6 Punkte)

Sei $K = \mathbb{F}_5(\sqrt[4]{3})$. Zeigen Sie, dass $K$ eine galoissche Erweiterung von $\mathbb{F}_5$ ist und bestimmen Sie ihre galoissche Gruppe. Bestimmen Sie weiter den Verband der Zwischenkörper von $K$ über $\mathbb{F}_5$ (das heißt alle Zwischenkörper geordnet nach Inklusionen). Bestimmen Sie schließlich die Anzahl der primitiven Elemente der Erweiterung $K$ über $\mathbb{F}_5$.

*Hinweis:*

Die Verwendung der Bezeichnung $\sqrt[4]{3}$ ist unüblich und auch nicht besonders zweckmäßig, denn es gibt keine Möglichkeit, auf den algebraischen Erweiterungen $L$ von $\mathbb{F}_5$ auf „natürliche“ Weise Wurzelfunktionen $\sqrt[n]{\cdot} : L \to L$ zu definieren. Das Problem besteht darin, dass es für vorgegebenes $\alpha \in L$ im Allgemeinen mehrere $\beta \in L$ mit $\beta^n = \alpha$ gibt, und dass man keine einfache Regel angeben kann, die aus diesen Elementen jeweils eines auswählt. Anders sieht die Situation zum Beispiel für die positiven reellen Zahlen aus, da man sich hier zum Beispiel dafür entscheiden kann, immer die positive Quadratwurzel zu wählen. Für die Aufgabe fixieren wir einen algebraischen Abschluss $\mathbb{F}_5^{\text{alg}}$ von $\mathbb{F}_5$ und interpretieren $\alpha = \sqrt[4]{3}$ einfach als ein beliebiges Element in $\mathbb{F}_5^{\text{alg}}$ mit der Eigenschaft $\alpha^4 = \bar{3}$.

*Lösung:*

Das Element $\alpha = \sqrt[4]{3}$ ist Nullstelle des Polynoms $f = x^4 - \bar{3} \in \mathbb{F}_5[x]$, also algebraisch über $\mathbb{F}_5$, und $\mathbb{F}_5(\alpha)|\mathbb{F}_5$ somit eine endliche Erweiterung. Aus der Vorlesung ist bekannt, dass jede endliche Erweiterung eines endlichen Körpers automatisch eine Galois-Erweiterung ist, und dass diese Galoisgruppe zyklisch von Ordnung $n$ ist, wobei $n$ den Grad der Erweiterung bezeichnet. Für $G = \text{Gal}(\mathbb{F}_5(\alpha)|\mathbb{F}_5)$ gilt also $G \cong \mathbb{Z}/n\mathbb{Z}$ mit $n = [\mathbb{F}_5(\alpha) : \mathbb{F}_5]$. Wenn wir zeigen können, dass $f$ in $\mathbb{F}_5[x]$ irreduzibel ist, dann ist $f$ als irreduzibles normiertes Polynom mit $f(\alpha) = \bar{0}$ das Minimalpolynom von $\alpha$ über $\mathbb{F}_5$, und es folgt $n = \text{grad}(f) = 4$, also $G \cong \mathbb{Z}/4\mathbb{Z}$.

Nehmen wir an, dass $f$ reduzibel ist. Wegen $\text{grad}(f) = 4$ besitzt $f$ dann entweder eine Nullstelle in $\mathbb{F}_5$, oder $f$ ist als Produkt zweier normierter, irreduzibler Polynome vom Grad 2 darstellbar. (Die beiden Faktoren können normiert gewählt werden, weil auch $f$ normiert ist.) Wegen $f(\bar{0}) = -\bar{3} \neq \bar{0}$, $f(\bar{1}) = \bar{1} - \bar{3} = -\bar{2} = \bar{3} \neq \bar{0}$, $f(\bar{2}) = \overline{16} - \bar{3} = \overline{13} = \bar{3} \neq \bar{0}$, $f(\bar{3}) = \overline{81} - \bar{3} = \overline{78} = \bar{3} \neq \bar{0}$, $f(\bar{4}) = f(-\bar{1}) = (-\bar{1})^4 - \bar{3} = -\bar{2} - \bar{3} \neq \bar{0}$ besitzt $f$ keine Nullstelle in $\mathbb{F}_5$.

Um zu zeigen, dass $f$ keine Darstellung der Form $f = gh$ mit normierten irreduziblen Polynomen $g, h$ vom Grad 2 besizt, könnte man die Polynome in der Form $g = x^2 + ax + b$, $h = x^2 + cx + d$ mit $a, b, c, d \in \mathbb{F}_5$ ansetzen, anschließend mit Hilfe der Gleichung $f = gh$ ein Gleichungssystem für diese Elemente herleiten und nachrechnen, dass diese Gleichungssystem nicht lösbar ist.

In dieser Situation gibt es aber einen kürzeren Weg. Wegen $f = gh$ und $f(\alpha) = \bar{0}$ ist $g(\alpha) = \bar{0}$ oder $h(\alpha) = \bar{0}$. In jedem Fall ist $\alpha$ also Nullstelle eines normierten, irreduziblen Polynoms vom Grad 2, und dieses Polynom ist somit das Minimalpolynom von $\alpha$ über $\mathbb{F}_5$. Daraus folgt $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 2$, als zweidimensionaler $\mathbb{F}_5$-Vektorraum ist $\mathbb{F}_5(\alpha)$ also isomorph zu $\mathbb{F}_5^2$. Aus $|\mathbb{F}_5(\alpha)| = |\mathbb{F}_5^2| = 5^2 = 25$ folgt $\mathbb{F}_{25}$, denn $\mathbb{F}_{25}$ ist der eindeutig bestimmte Zwischenkörper von $\mathbb{F}_5^{\text{alg}}|\mathbb{F}_5$ mit 25 Elementen. Weil $\bar{0}$ keine Nullstelle von $f$ ist, ist $\alpha$ ein Element der multiplikativen Gruppe $\mathbb{F}_{25}^\times$ mit $25 - 1 = 24$ Elementen. Wegen $\alpha^4 = \bar{3}$, $\alpha^8 = \bar{3}^2 = \bar{9} = \bar{4} \neq \bar{1}$, $\alpha^{16} = \bar{4}^2 = \overline{16} = \bar{1}$ ist $\alpha$ in $\mathbb{F}_{25}^\times$ ein Element der Ordnung 16. Nach dem Satz von Lagrange müsste $|\langle\alpha\rangle| = 16$ ein Teiler von 24 sein. Weil das aber offensichtlich nicht der Fall ist, hat unsere Annahme, dass $f$ reduzibel ist, insgesamt zu einem Widerspruch geführt.

Damit ist $[\mathbb{F}_5(\alpha) : \mathbb{F}_5] = 4$ und $G \cong \mathbb{Z}/4\mathbb{Z}$ nachgewiesen. Als $\mathbb{F}_5$-Vektorraum ist $\mathbb{F}_5(\alpha)$ isomorph zu $\mathbb{F}_5^4$, es gilt also $|\mathbb{F}_5(\alpha)| = 5^4 = 625$. Daraus folgt $\mathbb{F}_5(\alpha) = \mathbb{F}_{625} = \mathbb{F}_{5^4}$. Laut Vorlesung sind für jedes $n \in \mathbb{N}$ die Zwischenkörper von $\mathbb{F}_{5^n}$ gegeben durch $\mathbb{F}_{5^d}$, wobei $d$ die Teiler von $n$ in $\mathbb{N}$ durchläuft, und es gilt $\mathbb{F}_{5^d} \subseteq \mathbb{F}_{5^{d'}}$ genau dann, wenn $d$ ein Teiler von $d'$ gilt. Für $n = 4$ sind $1, 2, 4$ die einzigen Teiler von 4 in $\mathbb{N}$. Also sind $\mathbb{F}_{5^1} = \mathbb{F}_5$, $\mathbb{F}_{5^2} = \mathbb{F}_{25}$ und $\mathbb{F}_{5^4} = \mathbb{F}_{625}$ die einzigen Zwischenkörper von $\mathbb{F}_5(\alpha)|\mathbb{F}_5$, und diese sind durch $\mathbb{F}_5 \subseteq \mathbb{F}_{25} \subseteq \mathbb{F}_{625}$ linear geordnet.

Bestimmen wir nun noch die Anzahl der primitiven Elemente von $\mathbb{F}_5(\alpha)|\mathbb{F}_5$, also die Anzahl der Elemente $\beta \in \mathbb{F}_5(\alpha)$ mit $\mathbb{F}_5(\beta) = \mathbb{F}_5(\alpha)$. Für jedes $\beta \in \mathbb{F}_5(\alpha)$ gilt $\mathbb{F}_5(\beta) = \mathbb{F}_5(\alpha)$ genau dann, wenn $\beta \notin \mathbb{F}_{25}$ gilt. Ist nämlich $\beta \in \mathbb{F}_{25}$, dann folgt $\mathbb{F}_5(\beta) \subseteq \mathbb{F}_{25}$ und somit $\mathbb{F}_5(\beta) \neq \mathbb{F}_5(\alpha)$, da $\mathbb{F}_5(\alpha) = \mathbb{F}_{625}$ kein Teilkörper von $\mathbb{F}_{25}$ ist. Setzen wir umgekehrt $\mathbb{F}_5(\beta) \subsetneq \mathbb{F}_5(\alpha)$ voraus, dann folgt $\mathbb{F}_5(\beta) = \mathbb{F}_5$ oder $\mathbb{F}_5(\beta) = \mathbb{F}_{25}$, denn andere Zwischenkörper von $\mathbb{F}_5(\alpha)|\mathbb{F}_5$ gibt es nicht. Wegen $\mathbb{F}_5 \subseteq \mathbb{F}_{25}$ folgt in beiden Fällen $\mathbb{F}_5(\beta) \subseteq \mathbb{F}_{25}$. Die gesuchte Elementezahl ist also $|\mathbb{F}_5(\alpha) \setminus \mathbb{F}_{25}| = |\mathbb{F}_{625}| - |\mathbb{F}_{25}| = 625 - 25 = 600$.