Aufgabe H13T2A1 (2+4 Punkte)

(a) Zeigen Sie, dass das Polynom $f = x^4 + x + 1 \in \mathbb{F}_2[x]$ irreduzibel ist.

(b) Sei α eine Nullstelle des Polynoms f aus Teilaufgabe (a) in einem algebraischen Abschluss $\mathbb{F}_2^{\text{alg}}$ von $\mathbb{F}_2$. Zeigen Sie, dass $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$ gilt, dass $\alpha \in \mathbb{F}_{16}^\times$ gilt, und dass α ein Erzeuger der multiplikativen Gruppe $\mathbb{F}_{16}^\times$ von $\mathbb{F}_{16}$ ist.

Lösung:

zu (a) Wegen $f(\bar{0}) = \bar{0}^4 + \bar{0} + \bar{1} = \bar{1}$ und $f(\bar{1}) = \bar{1}^4 + \bar{1} + \bar{1} = \bar{3} = \bar{1}$ besitzt f jedenfalls keine Nullstelle in $\mathbb{F}_2[x]$. Wenn f dennoch reduzibel ist, muss es wegen $\text{grad}(f) = 4$ Produkt zweier irreduzibler Faktoren vom Grad 2 sein. Das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_2[x]$ ist $x^2 + x + \bar{1}$. Die einzige mögliche Zerlegung von f in zwei irreduzible Faktoren vom Grad 2 wäre also $(x^2 + x + \bar{1})(x^2 + x + \bar{1})$. Es gilt aber $(x^2 + x + \bar{1})(x^2 + x + \bar{1}) = x^4 + x^2 + \bar{1}$. Also existiert eine solche Zerlegung für das Polynom f nicht, und folglich ist f in $\mathbb{F}_2[x]$ irreduzibel.

zu (b) Auf Grund der Irreduzibilität von f und wegen $f(\alpha) = \bar{0}$ gilt $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = \text{grad}(f) = 4$. Also ist $\mathbb{F}_2(\alpha)$ als $\mathbb{F}_2$-Vektorraum isomorph zu $\mathbb{F}_2^4$. Es folgt $|\mathbb{F}_2(\alpha)| = |\mathbb{F}_2^4| = 2^4 = 16$. Weil $\mathbb{F}_{16}$ der einzige Teilkörper von $\mathbb{F}_2^{\text{alg}}$ mit 16 Elementen ist, folgt $\mathbb{F}_2(\alpha) = \mathbb{F}_{16}$.

Offenbar ist α ein Element von $\mathbb{F}_{16} = \mathbb{F}_2(\alpha)$. Somit ist $\alpha \notin \mathbb{F}_{16}^\times$ nur für möglich, wenn $\alpha = \bar{0}$ gilt. Aber dies ist ausgeschlossen, denn im Gegensatz zu α ist $\bar{0}$ keine Nullstelle von f. Nehmen wir nun an, dass α zwar in $\mathbb{F}_{16}^\times$ enthalten, aber kein Erzeuger dieser Gruppe ist. Wegen $|\mathbb{F}_{16}^\times| = 16 - 1 = 15$ muss die Elementordnung $\text{ord}(\alpha)$ dann ein echter Teiler von 15, also gleich 1, 3 oder 5 sein. Im Fall $\text{ord}(\alpha) = 1$ wäre $\alpha = \bar{1}$, aber dies ist unmöglich, weil $\bar{1}$ keine Nullstelle von f ist.

Wäre $\text{ord}(\alpha) = 3$, dann würde $\alpha^3 = \bar{1}$ folgen. Das Element α wäre damit eine Nullstelle des Polynoms $g = x^3 - \bar{1}$. Aber auch dies ist ausgeschlossen. Denn f ist als normiertes, irreduzibles Polynom mit $f(\alpha) = \bar{0}$ das Minimalpolynom von α über $\mathbb{F}_2$. Daraus folgt, dass kein Polynom ungleich Null mit einem Grad kleiner als $\text{grad}(f) = 4$ existiert, dass α als Nullstelle besitzt. Betrachten wir nun noch den Fall $\text{ord}(\alpha) = 5$. In diesem Fall würde $\alpha^5 = \bar{1}$ gelten. Daraus würde sich $\bar{0} = \alpha^5 - \bar{1} - \alpha \cdot \bar{0} = \alpha^5 - \bar{1} - \alpha f(\alpha) = \alpha^5 - \bar{1} - \alpha(\alpha^4 + \alpha + \bar{1}) = \alpha^5 - \bar{1} - \alpha^5 - \alpha^2 - \alpha = \alpha^2 + \alpha + \bar{1}$ ergeben. Dann wäre α Nullstelle des Polynoms $h = x^2 + x + \bar{1}$ vom Grad 2, was wiederum unmöglich ist, weil das Minimalpolynom von α vom Grad 4 ist.