Aufgabe H17T2A3 (14 Punkte)

Ist p eine Primzahl und $q = p^k$ für ein $k \in \mathbb{N}$, so bezeichne $\mathbb{F}_q$ den endlichen Körper mit q Elementen. Betrachten Sie die Polynome $f = x^7 + x + 1 \in \mathbb{F}_2[x]$ und $g = x^7 - x - 1 \in \mathbb{Q}[x]$.

(a) Zeigen Sie, dass f keine Nullstellen in den Körpern $\mathbb{F}_2$, $\mathbb{F}_4$ und $\mathbb{F}_8$ besitzt.

(b) Folgern Sie aus (a), dass f in $\mathbb{F}_2[x]$ irreduzibel ist.

(c) Zeigen Sie, dass g in $\mathbb{Q}[x]$ irreduzibel ist.

Lösung:

zu (a) Das Polynom f hat keine Nullstelle in $\mathbb{F}_2$, denn es gilt $f(\bar{0}) = \bar{0}^7 + \bar{0} + \bar{1} = \bar{1} \neq \bar{0}$ und $f(\bar{1}) = \bar{1}^7 + \bar{1} + \bar{1} = \bar{3} = \bar{1} \neq \bar{0}$. Nehmen wir nun an, dass α eine Nullstelle von f in $\mathbb{F}_4$ ist. Wegen $f(\bar{0}) \neq \bar{0}$ liegt α in $\mathbb{F}_4^\times$. Weil $\mathbb{F}_4^\times$ eine Gruppe der Ordnung 3 ist, gilt $\alpha^3 = \bar{1}$ und $\alpha^7 = (\alpha^3)^2 \cdot \alpha = \bar{1}^2 \cdot \alpha = \alpha$. Es folgt $f(\alpha) = \alpha^7 + \alpha + \bar{1} = \alpha + \alpha + \bar{1} = \bar{2}\alpha + \bar{1} = \bar{1} \neq \bar{0}$, im Widerspruch zur Annahme. Also hat f in $\mathbb{F}_4$ keine Nullstelle.

Nehmen wir nun an, dass α eine Nullstelle von f in $\mathbb{F}_8$ ist. Aus $f(\bar{0}) \neq \bar{0}$ folgt $\alpha \in \mathbb{F}_8^\times$. Weil dies eine Gruppe der Ordnung 7 ist, gilt $\alpha^7 = \bar{1}$. Auf Grund unserer Annahme erhalten wir $\bar{0} = f(\alpha) = \alpha^7 + \alpha + \bar{1} = \bar{1} + \alpha + \bar{1} = \alpha$, aber dies steht im Widerspruch zu $\alpha \in \mathbb{F}_8^\times$. Also besitzt f auch in $\mathbb{F}_8$ keine Nullstelle.

zu (b) Angenommen, das Polynom f ist in $\mathbb{F}_2[x]$ reduzibel. Sei $f = \prod_{i=1}^r f_i$ die Zerlegung von f in irreduzible, normierte Faktoren $f_i \in \mathbb{F}_2[x]$. (Diese existiert, weil $\mathbb{F}_2[x]$ als Polynomring über einem Körper ein faktorieller Ring ist.) Weil f reduzibel ist, muss $r \geq 2$ gelten, und somit existiert wegen $\mathrm{grad}(f) = 7$ mindestens ein irreduzibler Faktor f_i vom Grad ≤ 3.

Sei nun $\mathbb{F}_2^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_2$, der auch $\mathbb{F}_4$ und $\mathbb{F}_8$ als Teilkörper enthält, und sei $\alpha \in \mathbb{F}_2^{\mathrm{alg}}$ eine Nullstelle von f_i. Dann ist f_i das Minimalpolynom von α über $\mathbb{F}_2$. Für den Erweiterungsgrad $n = [\mathbb{F}_2(\alpha) : \mathbb{F}_2]$ folgt $n = \mathrm{grad}(f_i) \leq 3$. Also ist $\mathbb{F}_2(\alpha)$ als $\mathbb{F}_2$-Vektorraum isomorph zu $\mathbb{F}_2^n$. Es folgt $|\mathbb{F}_2(\alpha)| = |\mathbb{F}_2^n| = 2^n$ und somit $\mathbb{F}_2(\alpha) = \mathbb{F}_{2^n}$. Daraus folgt, dass α in einem der Körper $\mathbb{F}_2$, $\mathbb{F}_4$ oder $\mathbb{F}_8$. Wegen $f_i(\alpha) = \bar{0}$ gilt auch $f(\alpha) = \bar{0}$. Aber in Teil (a) wurde gezeigt, dass f in keinem der drei Körper $\mathbb{F}_2, \mathbb{F}_4, \mathbb{F}_8$ eine Nullstelle besitzt. Die Annahme, dass f reduzibel ist, hat also zu einem Widerspruch geführt.

zu (c) Das Polynom g liegt in $\mathbb{Z}[x]$ und ist primitiv, und f ist das Bild von g in $\mathbb{F}_2[x]$. Weil f irreduzibel ist, folgt die Irreduzibilität von g in $\mathbb{Z}[x]$ aus dem Reduktionskriterium. Nach dem Lemma von Gauß ist g damit auch in $\mathbb{Q}[x]$ irreduzibel.