Aufgabe H19T3A4 (12 Punkte)

Es bezeichne p eine Primzahl und $\mathbb{F}_p$ einen Körper mit p Elementen. Zeigen Sie:

(a) Ist $g \in \mathbb{F}_p[x]$ irreduzibel über $\mathbb{F}_p$ vom Grad $\mathrm{grad}(g) = m$, so ist die Teilbarkeitsrelation $g \mid (x^{p^m} - x)$ erfüllt.

(b) Genau dann ist $f \in \mathbb{F}_p[x]$ irreduzibel über $\mathbb{F}_p$, wenn für jedes $m \in \mathbb{N}$ mit $1 \leq m \leq \frac{1}{2}\mathrm{grad}(f)$ gilt, dass $\mathrm{ggT}(f, x^{p^m} - x) = 1$ ist.

Lösung:

zu (a) Sei $\mathbb{F}_p^{\mathrm{alg}}$ ein algebraischer Abschluss von $\mathbb{F}_p$ und $\alpha \in \mathbb{F}_p^{\mathrm{alg}}$ eine Nullstelle von g. Dann ist die Normierung $\tilde{g}$ von g ebenfalls irreduzibel und wegen $\tilde{g}(\alpha) = 0$ das Minimalpolynom von α über $\mathbb{F}_p$. Es folgt $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \mathrm{grad}(\tilde{g}) = \mathrm{grad}(g) = m$. Dies zeigt, dass $\mathbb{F}_p(\alpha)$ ein m-dimensionaler $\mathbb{F}_p$-Vektorraum ist und als solcher aus $|\mathbb{F}_p|^m = p^m$ Elementen besteht. Folglich ist $\mathbb{F}_p(\alpha)$ der eindeutig bestimmte Zwischenkörper von $\mathbb{F}_p^{\mathrm{alg}}|\mathbb{F}_p$ mit p^m Elementen, also $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^m}$. Nun sind laut Vorlesung die Elemente von $\mathbb{F}_{p^m}$ genau die Nullstellen des Polynoms $f_m = x^{p^m} - x$ in $\mathbb{F}_p^{\mathrm{alg}}$. Aus $f_m(\alpha) = 0$ folgt, dass das Minimalpolynom $\tilde{g} = \mu_{\mathbb{F}_p,\alpha}$ ein Teiler von f_m ist. Weil sich g und $\tilde{g}$ nur um eine Konstante aus $\mathbb{F}_p^\times$ unterscheiden, ist auch g ein Teiler von f_m.

zu (b) „$\Leftarrow$“ (durch Kontraposition) Ist f reduzibel, dann gibt es nicht-konstante Polynome $g, h \in \mathbb{F}_p[x]$ mit $f = gh$. Nach eventueller Vertauschung von g und h können wir $\mathrm{grad}(g) \leq \frac{1}{2}\mathrm{grad}(f)$ annehmen, denn im Fall $\mathrm{grad}(g), \mathrm{grad}(h) > \frac{1}{2}\mathrm{grad}(f)$ würde sich der Widerspruch $\mathrm{grad}(f) = \mathrm{grad}(g) + \mathrm{grad}(h) > \frac{1}{2}\mathrm{grad}(f) + \frac{1}{2}\mathrm{grad}(f) = \mathrm{grad}(f)$ ergeben. Außerdem dürfen wir annehmen, dass g irreduzibel ist; ansonsten ersetzen wir das Polynom g durch einen seiner irreduziblen Faktoren. Setzen wir nun $m = \mathrm{grad}(g)$, dann gilt $1 \leq m \leq \frac{1}{2}\mathrm{grad}(f)$. Aus Teil (a) ergibt sich, dass g ein Teiler von $x^{p^m} - x$ ist. Zusammen mit $g \mid f$ folgt $g \mid \mathrm{ggT}(f, x^{p^m} - x)$ und somit $\mathrm{ggT}(f, x^{p^m} - x) \neq 1$. Die Bedingung $\mathrm{ggT}(f, x^{p^m} - x)$ für $1 \leq m \leq \frac{1}{2}\mathrm{grad}(f)$ ist also verletzt.

„$\Rightarrow$“ Ist f irreduzibel, dann stimmt jeder Teiler von f in $\mathbb{F}_p[x]$ bis auf eine Konstante ungleich null mit $\bar{1}$ oder f überein. Sei $n = \mathrm{grad}(f)$ und nehmen wir an, es gibt ein $m \in \{1, ..., \frac{1}{2}n\}$ mit $\mathrm{ggT}(f, x^{p^m} - x) \neq 1$. Dann muss dieser größte gemeinsame Teiler also gleich f und das Polynom f somit ein Teiler von $x^{p^m} - x$ sein. Sei $\alpha \in \mathbb{F}_p^{\mathrm{alg}}$ eine Nullstelle von f. Wie in Teil (a) ausgeführt, gilt dann $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n$. Wegen $f \mid (x^{p^m} - x)$ ist α auch eine Nullstelle von $x^{p^m} - x$, woraus $\alpha \in \mathbb{F}_{p^m}$ und $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_{p^m}$ folgt. Es ist $\mathbb{F}_p(\alpha)$ also ein Zwischenkörper von $\mathbb{F}_{p^m}|\mathbb{F}_p$, und mit der Gradformel erhalten wir

$$m = [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_p(\alpha)] \cdot [\mathbb{F}_p(\alpha) : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_p(\alpha)] \cdot n \geq n > \tfrac{1}{2}n \geq m ,$$

ein Widerspruch. Also gilt $\mathrm{ggT}(f, x^{p^m} - x) = 1$ für $1 \leq m \leq \frac{1}{2}n$.