Aufgabe F17T3A5 (12 Punkte)

Sei K ein endlicher Körper mit q Elementen. Man zeige, dass das Polynom $x^2 + x + 1$ genau dann irreduzibel über K ist, wenn $q \equiv -1 \bmod 3$.

Lösung:

„$\Rightarrow$" Ist $q \equiv -1 \bmod 3$ nicht erfüllt, dann gilt entweder $q \equiv 0 \bmod 3$ oder $q \equiv 1 \bmod 3$. Als Elementezahl eines endlichen Körpers ist q eine Primzahlpotenz. Aus $q \equiv 0 \bmod 3$ folgt also, dass q eine 3-Potenz ist. Es gilt dann $\mathrm{char}(K) = 3$, und daraus folgt $\bar{1}^2 + \bar{1} + \bar{1} = \bar{1} + \bar{1} + \bar{1} = \bar{0}$. Das Polyom $f = x^2 + x + \bar{1}$ besitzt also die Nullstelle $\bar{1} \in K$, und folglich ist f wegen $\mathrm{grad}(f) > 1$ nicht irreduzibel.

Betrachten wir nun den Fall $q \equiv 1 \bmod 3$. Dann ist 3 ein Teiler der Gruppenordnung $q - 1$ von $K^\times$. Laut Vorlesung ist $K^\times$ außerdem zyklisch, es gibt also ein $\alpha \in K^\times$ mit $K^\times = \langle \alpha \rangle$. Setzen wir $\gamma = \alpha^{(q-1)/3}$, dann gilt $(\gamma - \bar{1})(\gamma^2 + \gamma + \bar{1}) = \gamma^3 - \bar{1} = \alpha^{q-1} - \bar{1} = \bar{1} - \bar{1} = \bar{0}$. Wegen $\mathrm{ord}(\alpha) = q - 1$ ist $\gamma \neq \bar{1}$, also $\gamma - \bar{1} \neq \bar{0}$. Es folgt $\gamma^2 + \gamma + \bar{1} = \bar{0}$. Also ist γ eine Nullstelle von f, und das Polynom f ist auch in diesem Fall nicht irreduzibel in $K[x]$.

„$\Leftarrow$" Ist $f = x^2 + x + \bar{1}$ in $K[x]$ reduzibel, dann besitzt f wegen $\mathrm{grad}(f) = 2$ in K eine Nullstelle γ. Ist $\gamma = \bar{1}$, dann gilt $\bar{1} + \bar{1} + \bar{1} = \bar{1}^2 + \bar{1} + \bar{1} = f(\bar{1}) = f(\gamma) = \bar{0}$. Es folgt $\mathrm{char}(K) = 3$. Damit muss $q = |K|$ dann eine 3-Potenz sein und insbesondere $q \equiv 0 \bmod 3$, also $q \not\equiv -1 \bmod 3$ gelten. Im Fall $\gamma \neq \bar{1}$ ist γ wegen $\gamma^3 - \bar{1} = (\gamma - \bar{1})(\gamma^2 + \gamma + \bar{1}) = (\gamma - \bar{1})f(\gamma) = \bar{0}$ ein Element der Ordnung 3 in $K^\times$ ist. Nach dem Satz von Lagrange ist 3 damit ein Teiler der Gruppenordnung $|K^\times| = q - 1$. Es folgt $q \equiv 1 \bmod 3$, also $q \not\equiv -1 \bmod 3$ auch in diesem Fall.