## H25-T1-A5

Es sei $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ der endliche Körper mit drei Elementen.

a) Bestimmen Sie alle normierten, irreduziblen Polynome vom Grad 2 in $\mathbb{F}_3[X]$.

b) Begründen Sie, warum der Faktorring $K := \mathbb{F}_3[X]/(X^2+1)$ ein Körper ist. Geben Sie die Anzahl dieses Körpers an.

c) Zerlegen Sie das Polynom $f := X^8 - 1$ im Polynomring $\mathbb{F}_3[X]$ in irreduzible Faktoren.

d) Geben Sie ein Polynom $g$ in $\mathbb{F}_3[X]$ an, dessen Restklasse in $K$ eine primitive 8-te Einheitswurzel ist.

**Lösung**

a) Sei $f \in \mathbb{F}_3[X]$ ein normiertes Polynom vom Grad 2, demnach hat $f$ folgende Form

$$f = X^2 + aX + b, \quad a, b \in \mathbb{F}_3.$$

Ist $b = 0$, dann kann $f$ nicht irreduzibel sein (hat dann 0 als Nullstelle), demnach bleiben genau 6 Polynome übrig. Diese kann man alle auf Nullstellen prüfen. Es bleiben $X^2 + 1, X^2 + X + 2, X^2 + 2x + 2$ als normierte, nullstellenfreie und demnach irreduzible Polynome übrig.

b) Nach a) ist $X^2 + 1$ irreduzibel in $\mathbb{F}_3[X]$. demnach ist $K$ ein Körper mit $3^{\deg(f)} = 9$ Elementen (für eine ausführlichere Begründung verweise ich auf das Skript).

c) $f = X^8 - 1$ kann man bereits in $\mathbb{Z}[X]$ zerlegen als $(X^4 - 1)(X^4 + 1) = (X^2 - 1)(X^2 + 1)(X^4 + 1)$. In $\mathbb{F}_3[X]$ kann man $X^4 + 1$ weiter zerlegen in $(X^2 + X + 2)(X^2 + 2X + 2)$. Demnach ist nach a) und den bisherigen Überlegungen in c) die iireduzible Zerlegung von $f$ in $\mathbb{F}_3[X]$ gegeben durch

$$(X^2 - 1)(X^2 + 1)(X^2 + X + 2)(X^2 + 2X + 2).$$

d) Aus c) folgt, dass $[X^8-1] = 0 \in K$, denn $X^2+1 \mid X^8-1$. Demnach ist $[X]$ eine 8-te Einheitswurzel, denn $[X]^8 = [1]$. Jedoch ist $[X]^4 = [1]$. Wir suchen also eine Wurzel von $[X]$. Aus Gradgründen kommen da nur Grad 1 Polynome in Frage. Wir probieren $[X + 2]$ und sehen $[X + 2]^2 = [X^2 + 4X + 4] = [X^2 + X + 1] = [X]$. Demnach ist z.B. $[X + 2]$ eine primitive 8-te Einheitswurzel.