F18-T1-A2

Sei R der Ring $\mathbb{F}_2[X]/(X^3+1)$.

a) Bestimmen Sie die Anzahl der Elemente in R und geben Sie diese an.

b) Finden Sie alle Einheiten in R.

c) Finden Sie alle idempotenten Elemente in R (also alle $f \in R$ mit $f^2 = f$).

Lösungsvorschlag. Zu a). Es ist

$$\mathbb{F}_2[X]/(X^3+1) = \{[f(X)] | f(X) \in \mathbb{F}_2[X]\} = \{[0],[1],[X],[X+1],[X^2],[X^2+1],[X^2+X],[X^2+X+1]\},$$

denn $[X^3] = [1] \in \mathbb{F}_2[X]/(X^3-1)$, und die Annahme $[f(X)] = [g(X)] \in \mathbb{F}_2[X]/(X^3-1)$ für $f \neq g \in \mathbb{F}_2[X]$ mit $\deg(f), \deg(g) < 3$ würde zu dem Widerspruch $[f-g] = [0]$, also $(X^3-1)|(f-g)$, mit $f-g \neq 0$ und $\deg(f-g) < 3 = \deg(X^3-1)$ führen. Insbesondere können wir also ablesen

$$|\mathbb{F}_2[X]/(X^3-1)| = 8.$$

Alternative: Es ist $X^3+1 = (X+1)(X^2+X+1) \in \mathbb{F}_2[X]$. Da $P(X) := X^2+X+1 \in \mathbb{F}_2[X]$ keine Nullstellen in $\mathbb{F}_2$ besitzt ($P(0) = 1 = P(1) \in \mathbb{F}_2$) folgt wegen $\deg(P) = 2$ bereits, dass P irreduzibel über $\mathbb{F}_2$ ist. Insbesondere ist damit $\mathrm{ggT}(X+1, P(X)) = 1$ und wir erhalten mit Hilfe des chinesischen Restsatzes einen Isomorphismus

$$\begin{aligned} \pi\colon \mathbb{F}_2[X]/((X+1)P(X)) &\xrightarrow{\simeq} \mathbb{F}_2[X]/(X+1) \times \mathbb{F}_2[X]/(P(X)) \simeq \mathbb{F}_2 \times \mathbb{F}_2[X]/(P(X)), \\ [f] &\longmapsto (f(1), [f]) \end{aligned}$$

(der Isomorphismus $\mathbb{F}_2[X]/(X+1) \xrightarrow{\simeq} \mathbb{F}_2$ ist gegeben durch $[f] \mapsto f(1)$). Da P irreduzibel ist über $\mathbb{F}_2$ ist $\mathbb{F}_2[X]/(P(X))$ bekanntlich ein Körper mit $2^{\deg(P)} = 4$ Elementen und wir erhalten

$$|R| = |\mathbb{F}_2 \times \mathbb{F}_2[X]/(P(X))| = |\mathbb{F}_2| \cdot |\mathbb{F}_2[X]/(P(X))| = 2 \cdot 4 = 8.$$

Die Elemente von $R \simeq \mathbb{F}_2 \times \mathbb{F}_2[X]/(P)$ können wir damit aufzählen als (die Urbilder unter π von)

$$\{(0,[0]),(0,[1]),(0,[X]),(0,[X+1]),(1,[0]),(1,[1]),(1,[X]),(1,[X+1])\}.$$

Zu b). Da π aus a) (alternative Variante) ein Isomorphismus ist, ist $r \in R$ genau dann eine Einheit, wenn $\pi(r)$ eine Einheit in $\mathbb{F}_2 \times \mathbb{F}_2[X]/(P(X))$ ist. Im Folgenden nennen wir als Abkürzung $K := \mathbb{F}_2[X]/(P(X))$. Da $\mathbb{F}_2$ und K Körper sind gilt offenbar

$$(\mathbb{F}_2 \times K)^\times = \{(a,b) \in \mathbb{F}_2 \times K | a \in \mathbb{F}_2^\times,\ b \in K^\times\} = \mathbb{F}_2^\times \times K^\times.$$

Um die Umkehrabbildung $\pi^{-1}\colon \mathbb{F}_2 \times K \to R$ anzugeben, bestimmen wir zuerst $e_1, e_2 \in \mathbb{F}_2[X]$, so dass $\pi([e_1]) = (1,0)$ und $\pi([e_2]) = (0,1)$. Wir setzen $e_1 := X^2+X+1$ und

$e_2 := X(X+1) = X^2 + X$. Damit ist dann bekanntlich π^{-1} gegeben durch $\pi^{-1}(a, [b]) = [e_1 a + e_2 b]$, und wir erhalten

$$\begin{aligned} R^\times &= \{\pi^{-1}((a,[b])) \mid (a,[b]) \in \mathbb{F}_2^\times \times K^\times\} \\ &= \{\pi^{-1}((1,[b])) \mid [b] \in K^\times\} \\ &= \{\pi^{-1}((1,[1])), \pi^{-1}((1,[X])), \pi^{-1}((1,[X+1]))\} \\ &= \{[1], [X^2+X+1+X(X^2+X)], [X^2+X+1+(X+1)(X^2+X)]\} \\ &= \{[1], [X], [X^2]\} \end{aligned}$$

Zu c). Da π ein Isomorphismus ist, gilt für ein $f \in R$ offensichtlich $f^2 = f$ genau dann, wenn $\pi(f)^2 = \pi(f)$, es genügt also wieder, die idempotenten Elemente in $\mathbb{F}_2 \times K$ zu finden. Wir erhalten die Bedingung $(a,b) = (a,b)^2 = (a^2, b^2)$, ein Element $(a,b) \in \mathbb{F}_2 \times K$ ist also genau dann idempotent, wenn $a \in \mathbb{F}_2$ und $b \in K$ idempotent sind. Da das Polynom $X^2 - X = X(X-1)$ über einem Körper nur die Nullstellen 0 und 1 besitzt, sind die idempotenten Elemente in $\mathbb{F}_2 \times K$ damit gerade $\{(0,0), (1,0), (0,1), (1,1)\}$. Die Idempotenten Elemente in R sind also

$$\{\pi^{-1}((0,0)), \pi^{-1}((1,0)), \pi^{-1}((0,1)), \pi^{-1}((1,1))\} = \{[0], [e_1], [e_2], [1]\} \subset R.$$