Aufgabe F18T1A2 (12 Punkte)

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 $\alpha \in R$ mit $\alpha^2 = \alpha$).

Lösung:

zu (a) Sei $g = x^3 + \bar{1}$. Wir zeigen, dass $S = \{ax^2 + bx + c \mid a, b, c \in \mathbb{F}_2\}$ ein Repräsentantensystem der Nebenklassen in R ist. Weil es für a, b und c jeweils zwei Möglichkeiten gibt, folgt daraus dann $|R| = |S| = 2^3 = 8$ und außerdem

$$R \quad = \quad \{f + (g) \mid f \in S\} \quad = \quad \{ax^2 + bx + c + (g) \mid a, b, c \in \mathbb{F}_2\}.$$

Nach Definition der Repräsentantensysteme müssen wir dazu überprüfen, dass jede Nebenklasse in R genau ein Element aus S enthält. Sei also $f + (g)$ eine solche Nebenklasse, mit $f \in \mathbb{F}_2[x]$. Division mit Rest liefert Polynome $q, r \in \mathbb{F}_2[x]$ mit $f = qg + r$ und $r = \bar{0}$ oder $\operatorname{grad}(r) < \operatorname{grad}(g) = 3$. Es gibt also $a, b, c \in \mathbb{F}_2$ mit $r = ax^2 + bx + c \in S$ und $f - r = qg \in (g)$, woraus $f + (g) = r + (g)$ und insbesondere $r \in f + (g)$ folgt. Die Nebenklasse $f + (g)$ enthält also mindestens ein Element aus S.

Nehmen wir nun an, dass $r' \in S$ ein weiteres Element in $f + (g)$ ist. Aus $r' \in f + (g)$ folgt $r' + (g) = f + (g) = r + (g)$ und somit $r' - r \in (g)$, was mit $g | (r' - r)$ gleichbedeutend ist. Wegen $r' \in S$ gilt $r' = \bar{0}$ oder $\operatorname{grad}(r') < 3$, und dasselbe gilt auch für $r' - r$. Wegen $g | (r' - r)$ und $\operatorname{grad}(g) = 3$ ist nur $r' - r = \bar{0}$ möglich, woraus $r = r'$ folgt. Damit ist die Eindeutigkeit nachgewiesen.

zu (b) Ist $f + (g)$ eine Einheit in R mit $f \in S$, dann gibt es ein $h \in \mathbb{F}_2[x]$ mit der Eigenschaft $fh + (g) = (f + (g))(h + (g)) = 1 + (g) = 1_R$, was zu $fh - 1 \in (g)$ und zu $g \mid (fh - 1)$ äquivalent ist. Es gibt also ein $u \in \mathbb{F}_2[x]$ mit $fh - \bar{1} = ug \Leftrightarrow fh + ug = \bar{1}$. Daraus folgt, dass f und g in $\mathbb{F}_2[x]$ teilerfremd sind, denn jeder gemeinsamen Teiler $d \in \mathbb{F}_2[x]$ von f und g ist auch ein Teiler von $fh + ug = \bar{1}$ und somit eine Einheit in $\mathbb{F}_2[x]$.

Aus der Teilerfremdheit folgt insbesondere $(x - \bar{1}) \nmid f$, denn wegen $g(\bar{1}) = \bar{0}$ ist $x - \bar{1}$ ein Teiler von $\bar{g}$. Also ist $f + (g)$ im Fall $f(\bar{1}) = \bar{0}$ als Einheit ausgeschlossen, und für f bleiben nur noch die Möglichkeiten $\bar{1}, x, x^2, x^2 + x + \bar{1}$. Wegen $g = (x^2 + x + \bar{1})(x - \bar{1})$ ist $x^2 + x + 1$ nicht teilerfremd zu g und somit auch $x^2 + x + \bar{1} + (g)$ keine Einheit. Die Elemente

$$\bar{1} + (g) \quad , \quad x + (g) \quad , \quad x^2 + (g)$$

sind dagegen Einheiten in R. Für das erste Element ist dies wegen $1_R = \bar{1} + (g)$ offensichtlich, und für die beiden anderen Elemente folgt dies wegen $(x^3 - 1) + (g) = \bar{0} + (g) \Leftrightarrow x^3 + (g) = \bar{1} + (g)$ aus der Rechnung

$$(x + (g))(x^2 + (g)) \quad = \quad x^3 + (g) \quad = \quad \bar{1} + (g) \quad = \quad 1_R.$$

Insgesamt gibt es also genau drei Einheiten in R.

zu (c) Die einzige Einheit in R, die idempotent ist, ist das Einselement $1_R = 1 + (g)$. Ist nämlich $\alpha \in R^\times$ idempotent, dann können wir die Gleichung $\alpha^2 = \alpha$ mit α^{-1} multiplizieren und erhalten $\alpha = 1_R$; umgekehrt ist 1_R wegen $1_R^2 = 1_R$ idempotent. Jedes idempotente Element $\alpha \neq 1_R$ muss somit in

$$R \setminus R^\times \quad = \quad \{\bar{0} + (g), x + \bar{1} + (g), x^2 + \bar{1} + (g), x^2 + x + (g), x^2 + x + \bar{1} + (g)\}$$

liegen. Für diese fünf Elemente rechnen wir die Bedingung $\alpha^2 = \alpha$ einzeln nach. Es gilt

$$(\bar{0} + (g))^2 = \bar{0} + (g) \quad , \quad (x + \bar{1} + (g))^2 = (x + \bar{1})^2 + (g) = x^2 + \bar{1} + (g) \neq x + 1 + (g) \quad ,$$

$$(x^2 + \bar{1} + (g))^2 = (x^2 + \bar{1})^2 + (g) = x^4 + \bar{1} + (g) = (x + (g))(x^3 + (g)) + (1 + (g)) =$$
$$(x + (g))(1 + (g)) + (1 + (g)) = (x + (g)) + (1 + (g)) = x + 1 + (g) \neq x^2 + \bar{1} + (g) \quad ,$$

$$(x^2 + x + (g))^2 = (x^2 + x)^2 + (g) = x^4 + x^2 + (g) = x^2 + x + (g) \quad ,$$

$$(x^2 + x + \bar{1} + (g))^2 = (x^2 + x + \bar{1})^2 + (g) = x^4 + x^2 + \bar{1} + (g) = x + x^2 + \bar{1} + (g) = x^2 + x + \bar{1} + (g).$$

(Bei der Feststellung von „$\neq$“ haben wir jeweils verwendet, dass jedes Element nach (a) eine *eindeutige* Darstellung der Form $ax^2 + bx + c + (g)$ mit $a, b, c \in \mathbb{F}_2$ besitzt.) Die Menge der idempotenten Elemente ist also gegeben durch

$$\{0_R = \bar{0} + (g), 1_R = \bar{1} + (g), x^2 + x + (g), x^2 + x + \bar{1} + (g)\}.$$