Hinweis: *Die Vorbereitungsaufgaben werden in der Zentralübung unterstützt.*

Vorbereitung 1

Wir betrachten den Ring $R = \mathbb{Z}_3[x]$. Beachten und nutzen Sie im Folgenden die Isomorphie zwischen $(\mathbb{Z}_3[x]/(g), +, \cdot)$ und $(\mathbb{Z}_3[x]_{\text{grad}(g)}, +_g, \cdot_g)$, die für alle $g \in R$ durch die Abbildung $[f]_g \to Rem_g(f)$ gegeben ist. Wir schreiben gelegentlich $p \in \mathbb{Z}_3[x]/(g)$ für $p \in \mathbb{Z}_3[x]_{\text{grad}(g)}$.

Sei $g(x) = x^2 + 2x + 1$.

1. Bestimmen Sie alle Elemente des Rings $\mathbb{Z}_3[x]/(g)$.
2. Bestimmen Sie die Spalten der Additions- und Multiplikations-Verknüpfungstafeln zum Element $[x + 2]_g \in \mathbb{Z}_3[x]/(g)$.
3. Berechnen Sie Polynome $p(x) \in \mathbb{Z}_3[x]$ und $r(x) \in \mathbb{Z}_3[x]_2$ mit der Eigenschaft
$$x^4 + x + 1 = p(x) \cdot (x^2 + 2x + 1) + r(x)\,.$$
4. Ist der Restklassenring $\mathbb{Z}_3[x]/(g)$ ein Körper? Begründung!

Lösung

1. Wir stellen die Elemente des Rings $\mathbb{Z}_3[x]/(x^2 + 2x + 1)$ durch die Reste in $\mathbb{Z}_3[x]_2$ dar. Es gilt
$$Z_3[x]_2 = \{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}\,.$$
2.

$+$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1

$\cdot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
$x+2$	0	$x+2$	$2x+1$	2	$x+1$	$2x$	1	x	$2x+2$

3. Es gilt $p(x) = x^2 + x$ und $r(x) = 1$.
4. Der Restklassenring $\mathbb{Z}_3[x]/(x^2 + 2x + 1)$ ist kein Körper, weil er nicht nullteilerfrei ist. Es gilt
$$(x + 1) \cdot (x + 1) = x^2 + 2x + 1 \equiv_g 0\,.$$

Vorbereitung 2

Ist $x^4 + x^3 + 1$ irreduzibel in GF(2)[x]? Begründung!

Lösung

Antwort: $p(x) = x^4 + x^3 + 1$ ist irreduzibel in $GF(2)$.
Bemerkung: $GF(2)$ ist isomorph zu $\langle \mathbb{Z}_2, +_2, \cdot_2 \rangle$.

Widerspruchsbeweis:

Wir nehmen an, dass p reduzibel ist. Dann gibt es Polynome $p_1, p_2 \in \mathbb{Z}_2[x]$ mit $\text{grad}(p_i) \geq 1$, $(i = 1, 2)$ und $p = p_1 \cdot p_2$.
p besitzt keine Nullstelle, denn $p(0) = p(1) = 1$. Daraus folgt, dass weder p_1 noch p_2 linear, d.h., vom Grad 1 sein kann. Also gilt $\text{grad}(p_1) = \text{grad}(p_2) = 2$.
Wir machen dan Ansatz $p_1 = x^2 + ax + b$ und $p_2 = x^2 + cx + d$.
Dann gilt

$$\begin{aligned} x^4 + x^3 + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd\,. \end{aligned}$$

Koeffizientenvergleich ergibt die 4 Gleichungen

$$(1)\ a + c = 1, \quad (2)\ b + d + ac = 0, \quad (3)\ ad + bc = 0, \quad (4)\ bd = 1\,.$$

Aus (4) folgt $b = d = 1$. Eingesetzt in (3) folgt $a + c = 0$ im Widerspruch zu (1).