C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 1

Aufgabe 1 Man zeige oder widerlege.
Sei R ein Ring. Sei $x \in R$. Wir schreiben $1 = 1_R$.

(1) Es ist $x \cdot 0 = 0$.

(2) Es ist $(-1) \cdot x = -x$.

(3) Ist $x^2 = 0$, dann ist $x = 0$.

(4) Ist $x^2 = 1$, dann ist $x \in \{1, -1\}$.

Lösung zu Aufgabe 1:

(1) Richtig. Beweis:

$$x \cdot 0 + x \cdot 0 = x \cdot (0 + 0) = x \cdot 0$$

Daraus folgt, dass

$$x \cdot 0 = x \cdot 0 + x \cdot 0 - x \cdot 0 = x \cdot 0 - x \cdot 0 = 0.$$

(2) Richtig. Beweis:

$$(-1) \cdot x + x = (-1) \cdot x + 1 \cdot x = (-1 + 1) \cdot x = 0 \cdot x = 0,$$

Hierbei begründet man die Umformung $0 \cdot x = 0$ genau wie in (1). Daraus folgt

$$(-1) \cdot x = (-1) \cdot x + x - x = 0 - x = -x.$$

(3) Falsch. Für $R = \mathbb{Z}/4\mathbb{Z}$ und $x = 2$ ist $x^2 = 4 = 0$, aber $2 \neq 0$.
Oder, alternativ: $R = \mathbb{Q}^{2\times 2}$, $x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

(4) Falsch. Für $R = \mathbb{Z}/12\mathbb{Z}$ und $x = 5$ ist $x^2 = 25 = 1$, aber $5 \notin \{1, -1\}$.
Oder, alternativ: $R = \mathbb{Q} \times \mathbb{Q}$ und $x = (1, -1)$.

Aufgabe 2 Sei R ein Ring.

(1) Sei R kommutativ. Man zeige die Eigenschaft (Ring 5) für den Polynomring $R[X]$.

(2) Sei $I \trianglelefteq R$. Man zeige die Eigenschaft (Ring 7) für den Faktorring R/I.

Lösung zu Aufgabe 2:

(1) Seien $f(X), g(X), h(X) \in R[X]$. Wir schreiben $f(X) = \sum_{i\geq 0} a_i X^i$, $g(X) = \sum_{j\geq 0} b_j X^j$, $h(X) = \sum_{k\geq 0} c_k X^k$.

Zunächst ist $f(X)\cdot g(X) = \sum_{l\geq 0} d_l X^l$, wobei $d_l = \sum_{0\leq i\leq l} a_i b_{l-i}$ ist. Damit ist $(f(X)\cdot g(X))\cdot h(X) = \sum_{n\geq 0} e_n X^n$, wobei

$$e_n = \sum_{0\leq l\leq n} d_l c_{n-l} = \sum_{0\leq l\leq n} \left(\sum_{0\leq i\leq l} a_i b_{l-i}\right)\cdot c_{n-l} = \sum_{0\leq l\leq n}\left(\sum_{0\leq i\leq l} a_i b_{l-i} c_{n-l}\right) = \sum_{0\leq i\leq l\leq n} a_i b_{l-i} c_{n-l}.$$

Andererseits ist $g(X)\cdot h(X) = \sum_{m\geq 0} d'_m X^l$, wobei $d'_m = \sum_{0\leq j\leq m} b_j c_{m-j}$ ist. Daraus ergibt sich $f(X)\cdot(g(X)\cdot h(X)) = \sum_{n\geq 0} e'_n X^n$ mit

$$e'_n = \sum_{0\leq i\leq n} a_i d'_{n-i} = \sum_{0\leq i\leq n} a_i \cdot \left(\sum_{0\leq j\leq n-i} b_j c_{n-i-j}\right) = \sum_{0\leq i\leq n}\left(\sum_{0\leq j\leq n-i} a_i b_j c_{n-i-j}\right).$$

Wir sind fertig, sobald wir $e_n = e'_n$ bewiesen haben. Wir substituieren hierfür im Ausdruck für e'_n in der inneren Summe $j = l - i$:

$$e'_n = \sum_{0\leq i\leq n}\left(\sum_{0\leq l-i\leq n-i} a_i b_j c_{n-i-(l-i)}\right) = \sum_{0\leq i\leq n}\left(\sum_{i\leq l\leq n} a_i b_{l-i} c_{n-l}\right) = \sum_{0\leq i\leq l\leq n} a_i b_{l-i} c_{n-l} = e_n.$$

(2) Seien $r, r', s, s' \in R$, dann gilt

$$\begin{aligned}((r+I)+(r'+I))\cdot((s+I)+(s'+I)) &= ((r+r')+I)\cdot((s+s')+I)\\ &= ((r+r')\cdot(s+s'))+I\\ &= (r\cdot s + r\cdot s' + r'\cdot s + r'\cdot s') + I\\ &= ((r\cdot s)+I)+((r\cdot s')+I)\\ &\quad +((r'\cdot s)+I)+((r'\cdot s')+I)\\ &= (r+I)\cdot(s+I)+(r+I)\cdot(s'+I)\\ &\quad +(r'+I)\cdot(s+I)+(r'+I)\cdot(s'+I).\end{aligned}$$

Aufgabe 3

(1) Seien R und S Ringe. Sei $f : R \to S$ ein Ringisomorphismus.

Man zeige: Es ist $f^{-1} : S \to R$ ein Ringisomorphismus.

(2) Sind $\mathbb{Z}/4\mathbb{Z}$ und $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ isomorph?

(3) Sind $\mathbb{Z}/6\mathbb{Z}$ und $(\mathbb{Z}/3\mathbb{Z})\times(\mathbb{Z}/2\mathbb{Z})$ isomorph?

Lösung zu Aufgabe 3:

(1) Wenn f bijektiv ist, ist selbstverständlich auch f^{-1} bijektiv. Es verbleibt also nur zu zeigen, dass f^{-1} ein Ringhomomorphismus ist:

Da $f(1_R) = 1_S$ ist, natürlich auch $f^{-1}(1_S) = 1_R$. Sind nun $s, s' \in S$, dann ist

$$\begin{aligned}f^{-1}(s+s') &= f^{-1}\left(\ f(f^{-1}(s)) \ + \ f(f^{-1}(s'))\ \right)\\ &= f^{-1}\left(\ f\left(f^{-1}(s)+f^{-1}(s')\right)\ \right)\\ &= f^{-1}(s)+f^{-1}(s').\end{aligned}$$

und

$$\begin{aligned} f^{-1}(s \cdot s') &= f^{-1}\left(\, f(f^{-1}(s)) \, \cdot \, f(f^{-1}(s')) \, \right) \\ &= f^{-1}\left(\, f\left(f^{-1}(s) \cdot f^{-1}(s')\right) \, \right) \\ &= f^{-1}(s) \cdot f^{-1}(s'). \end{aligned}$$

(2) Nein. Sei *angenommen*, es gibt einen Isomorphismus $f : \mathbb{Z}/4\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dann ist $f(1) = (1,1)$. Daraus folgt

$$(0,0) = f(0) \neq f(2) = f(1+1) = f(1) + f(1) = (1,1) + (1,1) = (0,0).$$

Widerspruch.

(3) Ja. Wir argumentieren mit dem eindeutigen Ringhomomorphismus $f : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, welcher gegeben ist durch $f(k) = (k + 2\mathbb{Z}, k + 3\mathbb{Z})$.

Dieser ist surjektiv: wir haben $f(4) = (4 + 2\mathbb{Z}, 4 + 3\mathbb{Z}) = (0 + 2\mathbb{Z}, 1 + 3\mathbb{Z})$ und $f(3) = (3 + 2\mathbb{Z}, 3 + 3\mathbb{Z}) = (1 + 2\mathbb{Z}, 0 + 3\mathbb{Z})$. Für beliebige $a, b \in \mathbb{Z}$ ist deshalb $(a + 2\mathbb{Z}, b + 3\mathbb{Z}) = a \cdot (1 + 2\mathbb{Z}, 0 + 3\mathbb{Z}) + b \cdot (0 + 2\mathbb{Z}, 1 + 3\mathbb{Z}) = a \cdot f(3) + b \cdot f(4) = f(a \cdot 3 + b \cdot 4)$.

Nun bestimmen wir den Kern von f:

$$k \in \mathrm{Kern}(f) \Leftrightarrow (k + 2\mathbb{Z} = 0 + 2\mathbb{Z}) \wedge (k + 3\mathbb{Z} = 0 + 3\mathbb{Z}) \Leftrightarrow 2|k \wedge 3|k \Leftrightarrow 6|k \Leftrightarrow k \in 6\mathbb{Z}.$$

Nach dem Homomorphiesatz (Satz 30), ist der Ringhomomorphismus

$$\begin{aligned} \overline{f} : \mathbb{Z}/6\mathbb{Z} &\to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \\ k + 6\mathbb{Z} &\mapsto (k + 2\mathbb{Z}, k + 3\mathbb{Z}) \end{aligned}$$

ein Isomorphismus.

Aufgabe 4

(1) Hat $X^4 + \frac{1}{2}X + 1 \in \mathbb{Q}[X]$ eine Nullstelle in $\mathbb{Q}$?
Zerfällt es in ein Produkt zweier normierter Faktoren von Grad 2?

(2) Gibt es ein $f(X) \in \mathbb{Q}[X]$ ohne Nullstelle in $\mathbb{Q}$, das in $\mathbb{Q}[X]$ in ein Produkt zweier Faktoren von Grad $\geqslant 1$ zerfällt?

(3) Gibt es ein $f(X) \in \mathbb{Q}[X]$ ohne Nullstelle in $\mathbb{Q}$, das in $\mathbb{Q}[X]$ in ein Produkt zweier Faktoren von Grad 3 zerfällt?

Lösung zu Aufgabe 4:

(1) Wir zeigen zunächst mithilfe des Satzes von Descartes (Satz 10), dass $f(X) = X^4 + \frac{1}{2}X + 1$ keine Nullstelle $a \in \mathbb{Q}$ besitzt. Ist a eine Nullstelle von $f(X)$, so auch von $2 \cdot f(X) = 2X^4 + X + 2$. Nun dürfen wir Satz 10 anwenden - eine Nullstelle $a \in \mathbb{Q}$ muss von der Form $\frac{u}{v}$ sein, wobei $u, v \in \mathbb{Z}$ Teiler von 2 sind, d.h. $u, v \in \{-2, -1, 1, 2\}$. Damit ist $\frac{u}{v} \in \{-2, -1, -\frac{1}{2}, \frac{1}{2}, 1, 2\}$. Setzt man diese potentiellen Nullstellen in $f(X)$ bzw. $2f(X)$ ein, so sieht man, dass keine tatsächlich eine Nullstelle ist. Es hat f also keine rationale Nullstelle.

Nehmen wir nun an, dass $f(X) = (X^2 + aX + b)(X^2 + cX + d)$ mit $a, b, c, d \in \mathbb{Q}$ ist. Ausmultiplizieren dieser Gleichung ergibt

$$X^4 + \frac{1}{2}X + 1 = X^4 + (a + c)X^3 + (ac + b + d)X^2 + (ad + bc)X + bd.$$

Daraus ergibt sich das folgende Gleichungssystem

$$\text{(I)} \qquad a + c = 0$$
$$\text{(II)} \qquad ac + b + d = 0$$
$$\text{(III)} \qquad ad + bc = \frac{1}{2}$$
$$\text{(IV)} \qquad bd = 1.$$

Aus (I) ergibt sich $c = -a$. Eingesetzt in (II) und (III) ergibt sich (II'): $b + d - a^2 = 0$ bzw. (III'): $ad - ba = \frac{1}{2}$. Wenn es eine Lösung gibt, dann muss $a \neq 0$ sein, folglich können wir die erhaltenen Gleichungen umschreiben zu:

$$\text{(II')} \qquad b + d = a^2$$
$$\text{(III')} \qquad d - b = \frac{1}{2a}.$$

Addiert man (II') und (III') und teilt durch 2, erhält man $d = \frac{a^2}{2} + \frac{1}{4a}$. Löst man eine der Gleichungen schließlich nach b auf, erhält man $b = \frac{a^2}{2} - \frac{1}{4a}$.

Nun setzen wir b und d in Gleichung (IV) ein und erhalten $\left(\frac{a^2}{2} - \frac{1}{4a}\right)\left(\frac{a^2}{2} + \frac{1}{4a}\right) = 1 \Leftrightarrow \frac{a^4}{4} - \frac{1}{16a^2} = 1 \Leftrightarrow 4a^6 - 16a^2 - 1 = 0$. Nach dem Satz von Descartes muss $a \in \{-1, -\frac{1}{2}, -\frac{1}{4}, \frac{1}{4}, \frac{1}{2}, 1\}$ sein. Probiert man diese Werte durch, stellt man erneut fest, dass keiner passt. Diese Gleichung ist nicht lösbar, somit kann eine Zerlegung der obigen Form nicht existieren.

(2) Ja. Ein Beispiel ist das Polynom $f(X) = X^4 + 2X^2 + 1$. Dieses zerfällt in $f(X) = (X^2 + 1) \cdot (X^2 + 1)$. Wäre nun $a \in \mathbb{Q}$ eine Nullstelle, dann hieße das

$$f(a) = 0 \Leftrightarrow (a^2 + 1)^2 = 0 \Leftrightarrow (a^2 + 1) = 0 \Leftrightarrow a^2 = -1,$$

was aber nicht geschehen kann, sofern $a \in \mathbb{Q}$ ist.

(3) Ja. Hier ist das Polynom $f(X) = X^6 - 4X^3 + 4 = (X^3 - 2) \cdot (X^3 - 2)$ ein Beispiel. Ist $a \in \mathbb{Q}$ nämlich eine Nullstelle von f, so gilt:

$$f(a) = 0 \Leftrightarrow (a^3 - 2)^2 = 0 \Leftrightarrow a^3 - 2 = 0 \Leftrightarrow a^3 = 2,$$

allerdings gibt es keine rationale Lösung dieser Gleichung.