N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 2

Aufgabe 5

(1) Seien R, S und T Ringe. Seien $f : R \to S$ und $g : S \to T$ Ringmorphismen.
Man zeige: $g \circ f : R \to T$ ist ein Ringmorphismus.

(2) Seien R und S Ringe. Sei $f : R \to S$ ein Ringisomorphismus.
Man zeige: $f^{-1} : S \to R$ ist ein Ringisomorphismus.

(3) Man finde ein Ideal in $\mathbb{Q}[X]$, das maximal ist.

(4) Man finde ein Ideal in $\mathbb{Q}[X]$, das nicht maximal ist.

Lösung zu Aufgabe 5:

(1) Da $f(1_R) = 1_S$ und $g(1_S) = 1_T$, ist $(g \circ f)(1_R) = g(f(1_R)) = g(1_S) = 1_T$.
Es ist für $r, r' \in R$

$$(g \circ f)(r+r') = g(f(r+r')) = g(f(r)+f(r')) = g(f(r))+g(f(r')) = (g \circ f)(r)+(g \circ f)(r')$$

und

$$(g \circ f)(r \cdot r') = g(f(r \cdot r')) = g(f(r) \cdot f(r')) = g(f(r)) \cdot g(f(r')) = (g \circ f)(r) \cdot (g \circ f)(r') \ .$$

Somit ist $g \circ f$ ein Ringmorphismus.

(2) Da f bijektiv ist, ist auch f^{-1} bijektiv. Es bleibt zu zeigen, dass f^{-1} ein Ringmorphismus ist:

Da $f(1_R) = 1_S$ ist, ist $f^{-1}(1_S) = 1_R$.

Seien $s, s' \in S$. 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

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

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

(3) Das Ideal

$$(X) := \{u(X) \cdot X : u(X) \in \mathbb{Q}[X]\} = \{ \sum_{i \in [1,m]} a_i X^i : m \in \mathbb{Z}_{\geq 0}, a_i \in \mathbb{Q} \text{ für } i \in [1,m]\} \subseteq \mathbb{Q}[X]$$

ist ein maximal Ideal.
Annahme nicht: Dann gibt es ein Ideal I mit $(X) \subset I \lhd \mathbb{Q}[X]$ und darin ein Polynom $v(X)$ mit $v(X) \in I$, aber $v(X) \notin (X)$.
Schreibe $v(X) = \sum_{i\geq 0} a_i X^i$. Es ist $\sum_{i\geq 1} a_i X^i \in (X) \subset I$. Da I ein Ideal ist, ist auch

$$v(X) - \sum_{i\geq 1} a_i X^i = a_0 \in I \ .$$

Wegen $v(X) \notin (X)$, ist $0 \neq a_0 \in \mathbb{Q}$. Nun ist aber $a_0^{-1} \in \mathbb{Q}[X]$, und da I ein Ideal ist, somit auch $a_0 \cdot a_0^{-1} = 1 \in I$. Dann ist aber $I = \mathbb{Q}[X]$, im *Widerspruch* zu $I \lhd \mathbb{Q}[X]$.

(4) Z.B. ist $(X^2) = \{u(X) \cdot X^2 : u(X) \in \mathbb{Q}[X]\} \subset (X) \lhd \mathbb{Q}[X]$ ein nicht maximales Ideal in $\mathbb{Q}[X]$. Alternativ sind z.B. auch 0 oder $\mathbb{Q}[X]$ Ideale in $\mathbb{Q}[X]$, die nicht maximal sind.

Aufgabe 6

(1) Sei $f(X) := 3X^3 + 3X^2 + X + 2 \in \mathbb{Q}[X]$. Hat $f(X)$ eine positive Nullstelle in $\mathbb{R}$? Man bestimme alle Nullstellen von $f(X)$ in $\mathbb{Q}$.

(2) Sei $f(X) := X^4 - \frac{3}{2}X^3 - \frac{3}{2}X - 1$. Man bestimme alle Nullstellen von $f(X)$ in $\mathbb{Q}$.

Lösung zu Aufgabe 6:

(1) Es kann $f(X)$ keine positive Nullstelle in $\mathbb{R}$ haben, da $f(X)$ nur positive Koeffizienten hat und also $f(r) > 0$ ist für $r \in \mathbb{R}_{>0}$.

Wir zeigen mithilfe des Satzes von Descartes (Satz 10), dass $f(X) = 3X^3 + 3X^2 + X + 2$ keine Nullstelle $a \in \mathbb{Q}$ besitzt.

Eine Nullstelle $a \in \mathbb{Q}$ muss von der Form $\frac{u}{v}$ sein, wobei $u, v \in \mathbb{Z}$ teilerfremd sind, u ein Teiler von 2 ist und v ein Teiler von 3 ist, d.h. $u \in \{-2, -1, 1, 2\}$ und $v \in \{-3, -1, 1, 3\}$. Damit ist $\frac{u}{v} \in \{-2, -1, -\frac{2}{3}, -\frac{1}{3}, \frac{1}{3}, \frac{2}{3}, 1, 2\}$. Da $f(r) > 0$ ist für $r \in \mathbb{R}_{>0}$, genügt es $\frac{u}{v} \in \{-2, -1, -\frac{2}{3}, -\frac{1}{3}\}$ als mögliche Kandidaten zu betrachten. Nun ist

$$f(-2) = -12,\ f(-1) = 1,\ f(-\tfrac{2}{3}) = \tfrac{16}{9} \text{ und } f(-\tfrac{1}{3}) = \tfrac{17}{9}.$$

Es hat f also keine rationale Nullstelle.

(2) Ist $a \in \mathbb{Q}$ eine Nullstelle von $f(X)$, so auch von $2 \cdot f(X) = 2X^4 - 3X^3 - 3X - 2$.

Auf $2 \cdot f(X)$ können wir nun den Satz von Descartes (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 $f(X)$ ein, so sieht man, dass

$$f(-2) = 30,\ f(-1) = 3,\ f(-\tfrac{1}{2}) = 0,\ f(\tfrac{1}{2}) = -\tfrac{15}{8},\ f(1) = -3 \text{ und } f(2) = 0.$$

Es hat $f(X)$ also die rationalen Nullstellen $-\frac{1}{2}$ und 2.

Aufgabe 7 Sei $\mathbb{Q}(\sqrt{2}) := \{\, a + b\sqrt{2} \,:\, a,\, b \,\in\, \mathbb{Q} \,\} \subseteq \mathbb{R}$.

(1) Man zeige: Es ist $\mathbb{Q}(\sqrt{2})$ ein Teilring von $\mathbb{R}$ und ein $\mathbb{Q}$-Unterraum von $\mathbb{R}$. Dabei hat $\mathbb{Q}(\sqrt{2})$ die $\mathbb{Q}$-lineare Basis $(1, \sqrt{2})$.

(2) Sei $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}^{2\times 2} : a + b\sqrt{2} \mapsto \left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)$. Man weise nach, daß φ ein injektiver Ringmorphismus ist. Ist $\mathbb{Q}(\sqrt{2})$ isomorph zu einem Teilring von $\mathbb{Q}^{2\times 2}$?

(3) Sei $\psi : \mathbb{Q}[X] \to \mathbb{R} : f(X) \mapsto f(\sqrt{2})$. Man weise nach, daß ψ ein Ringmorphismus ist, welcher Bild $\mathbb{Q}(\sqrt{2})$ hat.

Man bestimme ein Ideal $I \trianglelefteq \mathbb{Q}[X]$ mit $\mathbb{Q}[X]/I \simeq \mathbb{Q}(\sqrt{2})$.

Lösung zu Aufgabe 7:

(1) Es ist $1_{\mathbb{R}} \in \mathbb{Q}(\sqrt{2})$. Für $a, a', b, b' \in \mathbb{Q}$ ist

$$(a + \sqrt{2}b) - (a' + \sqrt{2}b') = (a - a') + (b - b')\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

und

$$(a+\sqrt{2}b)\cdot(a'+\sqrt{2}b') = aa' + ab'\sqrt{2} + ba'\sqrt{2} + 2bb' = aa' + 2bb' + (ab' + ba')\sqrt{2} \in \mathbb{Q}(\sqrt{2}) \ .$$

Somit ist $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ ein Teilring. Da auch $\lambda \cdot (a + b\sqrt{2}) = \lambda \cdot a + \lambda \cdot b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ für $\lambda, a, b \in \mathbb{Q}$, ist $\mathbb{Q}(\sqrt{2})$ ein $\mathbb{Q}$-Unterraum von $\mathbb{R}$.

Das Tupel $(1, \sqrt{2})$ ist ein $\mathbb{Q}$-lineares Erzeugendensystem von $\mathbb{Q}(\sqrt{2})$, da sich jedes Element von $\mathbb{Q}(\sqrt{2})$ darstellen lässt als $a \cdot 1 + b \cdot \sqrt{2}$ mit $a, b \in \mathbb{Q}$. Da $\sqrt{2} \notin \mathbb{Q}$, ist $(1, \sqrt{2})$ linear unabhängig über $\mathbb{Q}$. Also ist $(1, \sqrt{2})$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2})$.

(2) Es ist $\varphi(1_{\mathbb{Q}(\sqrt{2})}) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = 1_{\mathbb{Q}^{2\times 2}}$. Für $a + b\sqrt{2}, a' + b'\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ ist

$$\varphi(a + b\sqrt{2} + a' + b'\sqrt{2}) = \left(\begin{smallmatrix} a+a' & 2(b+b') \\ b+b' & a+a' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right) = \varphi(a + b\sqrt{2}) + \varphi(a' + b'\sqrt{2})$$

und $\varphi((a + b\sqrt{2}) \cdot (a' + b'\sqrt{2})) = \varphi(aa' + 2bb' + (ab' + ba')\sqrt{2})$

$$= \left(\begin{smallmatrix} aa'+2bb' & 2(ab'+ba') \\ ab'+ba' & aa'+2bb' \end{smallmatrix}\right) = \left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right) = \varphi(a + b\sqrt{2}) \cdot \varphi(a' + b'\sqrt{2})$$

Somit ist φ ein Ringmorphismus.

Es ist $\mathrm{Kern}(\varphi) = \{a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}) : \left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\} = 0$. Nach Lemma 28.(3) ist φ injektiv. Eingeschränkt im Zielbereich auf sein Bild ist φ auch surjektiv. Nach Lemma 28.(3) ist $\varphi(\mathbb{Q}(\sqrt{2})) \subseteq \mathbb{Q}^{2\times 2}$ ein Teilring. Die Abbildung

$$\varphi_{|\varphi(\mathbb{Q}(\sqrt{2}))} : \mathbb{Q}(\sqrt{2}) \xrightarrow{\sim} \varphi(\mathbb{Q}(\sqrt{2})) = \{\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) : a, b \in \mathbb{Q}\}$$

ist ein Ringisomorphismus und also $\mathbb{Q}(\sqrt{2}) \cong \{\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) : a, b \in \mathbb{Q}\} \subseteq \mathbb{Q}^{2\times 2}$.

(3) Es ist $\psi(1_{\mathbb{Q}[X]}) = 1_{\mathbb{R}}$. Für $f(X), g(X) \in \mathbb{Q}[X]$ ist

$$\psi(f(X) + g(X)) = f(\sqrt{2}) + g(\sqrt{2}) = \psi(f(X)) + \psi(g(X))$$

und

$$\psi(f(X) \cdot g(X)) = f(\sqrt{2}) \cdot g(\sqrt{2}) = \psi(f(X)) \cdot \psi(g(X)) \ .$$

Somit ist ψ ein Ringmorphismus.

Für $a, b \in \mathbb{Q}$ ist $\psi(a + bX) = a + b\sqrt{2}$ und daher $\mathbb{Q}(\sqrt{2}) \subseteq \psi(\mathbb{Q}[X])$.

Sei $f(X) \in \mathbb{Q}[X]$. Schreibe $f(X) := \sum_{i\geq 0} a_i X^i$. Dann ist

$$\begin{aligned} \psi(f(X)) &= \textstyle\sum_{i\geq 0} a_i(\sqrt{2})^i = \sum_{k\geq 0} a_{2k}(\sqrt{2})^{2k} + \sum_{k\geq 0} a_{2k+1}(\sqrt{2})^{2k+1} \\ &= \textstyle\sum_{k\geq 0} a_{2k} \cdot 2^k + \sum_{k\geq 0} a_{2k+1} \cdot 2^k \cdot \sqrt{2} \in \mathbb{Q}(\sqrt{2}) \ . \end{aligned}$$

Somit ist auch $\psi(\mathbb{Q}[X]) \subseteq \mathbb{Q}(\sqrt{2})$. Insgesamt ist nun $\psi(\mathbb{Q}[X]) = \mathbb{Q}(\sqrt{2})$.

Nach dem Homomorphiesatz (Satz 31) ist $\mathbb{Q}[X]/\operatorname{Kern}(\psi) \xrightarrow{\sim} \psi(\mathbb{Q}[X]) = \mathbb{Q}(\sqrt{2})$ ein Ringisomorphismus. Es besteht $\operatorname{Kern}(\psi) = \{f(X) \in \mathbb{Q}[X] : f(\sqrt{2}) = 0\}$ gerade aus den Polynomen in $\mathbb{Q}[X]$, die $\sqrt{2}$ als Nullstelle besitzen. Wir zeigen $\operatorname{Kern}(\psi) \stackrel{!}{=} (X^2 - 2)$.

Zu $\supseteq$. Ein Element $u(X) \in (X^2 - 2)$ lässt sich schreiben als $(X^2 - 2) \cdot g(X)$ mit $g(X) \in \mathbb{Q}[X]$. Also hat $u(X)$ die Nullstelle $\sqrt{2}$. Somit ist $u(X) \in \operatorname{Kern}(\psi)$.

Zu $\subseteq$. Sei $v(X) \in \operatorname{Kern}(\psi)$. Mit Hilfe von Polynomdivision finden wir zwei Polynome $q(X), r(X) \in \mathbb{Q}[X]$ so, dass $v(X) = q(X) \cdot (X^2 - 2) + r(X)$ mit $\deg(r(X)) < 2$.

Nun ist

$$0 = v(\sqrt{2}) = q(\sqrt{2}) \cdot (\sqrt{2}^2 - 2) - r(\sqrt{2} = r(\sqrt{2}) \ .$$

Falls $r(X) = 0$, dann ist $v(X) = q(X) \cdot (X^2 - 2) \in (X^2 - 2)$.

Angenommen $r(X) \neq 0$.

Fall 1: $\deg(r(X)) = 1$. Dann ist $r(X) = a_1 \cdot X + a_0$ mit $0 \neq a_1, a_0 \in \mathbb{Q}$. Wir erhalten

$$0 = r(\sqrt{2}) = a_1 \cdot \sqrt{2} + a_0$$

und also $\sqrt{2} = -\frac{a_0}{a_1} \in \mathbb{Q}$. *Widerspruch.*

Fall 2: $\deg(r(X)) = 0$. Dann ist $r(X) = a_0$ mit $0 \neq a_0 \in \mathbb{Q}$. Aber $0 = r(\sqrt{2}) = a_0$. *Widerspruch.*

Aufgabe 8

(1) Man stelle die Additionstafel und die Multiplikationstafel von $\mathbb{F}_7$ auf.

(2) Man finde a, b, $c \in \mathbb{F}_7$ mit

$$\frac{1}{(X+1)^2 \cdot (1-X)} \ = \ \frac{a}{X-1} + \frac{b}{X+1} + \frac{c}{(X+1)^2} \ \in \ \mathbb{F}_7(X) \ .$$

Lösung zu Aufgabe 8:

(1) Additions- und Multiplikationstafel ergeben sich wie folgt.

$(+)$	-3	-2	-1	0	1	2	3
-3	1	2	3	-3	-2	-1	0
-2	2	3	-3	-2	-1	0	1
-1	3	-3	-2	-1	0	1	2
0	-3	-2	-1	0	1	2	3
1	-2	-1	0	1	2	3	-3
2	-1	0	1	2	3	-3	-2
3	0	1	2	3	-3	-2	-1

$(\cdot)$	-3	-2	-1	0	1	2	3
-3	2	-1	3	0	-3	1	-2
-2	-1	-3	2	0	-2	3	1
-1	3	2	1	0	-1	-2	-3
0	0	0	0	0	0	0	0
1	-3	-2	-1	0	1	2	3
2	1	3	-2	0	2	-3	-1
3	-2	1	-3	0	3	-1	2

(2) Durchmultiplizieren mit $(X+1)^2 \cdot (1-X)$ liefert

$$\begin{aligned} 1 &= -(X+1)^2 \cdot a + (X+1) \cdot (1-X) \cdot b + (1-X) \cdot c \\ &= -X^2 a - 2Xa - a - X^2 b + b + c - Xc \\ &= -(a+b)X^2 - (2a+c)X - a + b + c \end{aligned}$$

Daraus ergibt sich das folgende Gleichungssystem

$$\begin{aligned}
&\text{(I)} && a + b = 0 \\
&\text{(II)} && 2a + c = 0 \\
&\text{(III)} && -a + b + c = 1
\end{aligned}$$

Aus (I) folgt $b = -a$, aus (II) folgt $c = -2a$. Einsetzen in (III) liefert $3a = 1$. Somit folgt $a = -2$, $b = 2$ und $c = -3$.