M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 1

Aufgabe 1 Wir betrachten den Teilring $R := \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ 0 & 0 & \mathbb{Q} \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \end{smallmatrix}\right) = \mathbb{Q}^{3\times 3}$.
Wir betrachten dazuhin den Ring $S := \mathbb{Q}^{2\times 2} \times \mathbb{Q}$.

(1) Man finde ein Linksideal in R, das kein Ideal in R ist.

(2) Man bestimme einen Ringmorphismus $\varphi : R \to S$, für welchen gilt: $\mathrm{U}(R) = \varphi^{-1}(\mathrm{U}(S))$.

Lösung.

Zu (1). Etwa ist $I := \left(\begin{smallmatrix} \mathbb{Q} & 0 & 0 \\ \mathbb{Q} & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \subseteq \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ 0 & 0 & \mathbb{Q} \end{smallmatrix}\right) = R$ ein Linksideal, aber kein Ideal.

Linksideal: Seien $\left(\begin{smallmatrix} x & 0 & 0 \\ y & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} x' & 0 & 0 \\ y' & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in I$. Seien $\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right) \in R$. Dann wird

$$\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right)\left(\begin{smallmatrix} x & 0 & 0 \\ y & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right)\left(\begin{smallmatrix} x' & 0 & 0 \\ y' & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} ax+by & 0 & 0 \\ dx+ey & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) + \left(\begin{smallmatrix} a'x'+b'y' & 0 & 0 \\ d'x'+e'y' & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in I .$$

Um zu zeigen, daß I kein Ideal in R ist, zeigen wir, daß es kein Rechtsideal ist.
In der Tat ist zwar $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in I$ und $\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \in R$, aber $\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{smallmatrix}\right) \notin I$.

Zu (2). Sei

$$\begin{array}{rcl} R = \left(\begin{smallmatrix} \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ \mathbb{Q} & \mathbb{Q} & \mathbb{Q} \\ 0 & 0 & \mathbb{Q} \end{smallmatrix}\right) & \xrightarrow{\varphi} & \mathbb{Q}^{2\times 2} \times \mathbb{Q} = S \\ \left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right) & \mapsto & (\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right), g) \end{array}$$

Dann ist

$$\varphi(1_R) = \varphi(\left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)) = (\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), 1) = 1_S .$$

Ferner ist für $\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right), \left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right) \in R$ zum einen

$$\begin{aligned} \varphi(\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right)) &= \varphi(\left(\begin{smallmatrix} a+a' & b+b' & c+c' \\ d+d' & e+e' & f+f' \\ 0 & 0 & g+g' \end{smallmatrix}\right)) \\ &= (\left(\begin{smallmatrix} a+a' & b+b' \\ d+d' & e+e' \end{smallmatrix}\right), g+g') \\ &= (\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right), g) + (\left(\begin{smallmatrix} a' & b' \\ d' & e' \end{smallmatrix}\right), g') \\ &= \varphi(\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right)) + \varphi(\left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right)) , \end{aligned}$$

zum anderen

$$\begin{aligned} \varphi(\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right)) &= \varphi(\left(\begin{smallmatrix} aa'+bd' & ab'+be' & ac'+bf'+cg' \\ da'+ed' & db'+ee' & dc'+ef'+fg' \\ 0 & 0 & gg' \end{smallmatrix}\right)) \\ &= (\left(\begin{smallmatrix} aa'+bd' & ab'+be' \\ da'+ed' & db'+ee' \end{smallmatrix}\right), gg') \\ &= (\left(\begin{smallmatrix} a & b \\ d & e \end{smallmatrix}\right), g)(\left(\begin{smallmatrix} a' & b' \\ d' & e' \end{smallmatrix}\right), g') \\ &= \varphi(\left(\begin{smallmatrix} a & b & c \\ d & e & f \\ 0 & 0 & g \end{smallmatrix}\right)) \cdot \varphi(\left(\begin{smallmatrix} a' & b' & c' \\ d' & e' & f' \\ 0 & 0 & g' \end{smallmatrix}\right)) . \end{aligned}$$

Also ist φ ein Ringmorphismus.

Es bleibt $\mathrm{U}(R) \overset{!}{=} \varphi^{-1}(\mathrm{U}(S))$ zu zeigen.

Zu $\overset{!}{\subseteq}$. Ist $r \in R$ invertierbar, dann ist wegen $\varphi(r) \cdot \varphi(r^{-1}) = \varphi(r \cdot r^{-1}) = \varphi(1) = 1$ und $\varphi(r^{-1}) \cdot \varphi(r) = \varphi(r^{-1} \cdot r) = \varphi(1) = 1$ auch $\varphi(r)$ invertierbar.

Zu $\overset{!}{\supseteq}$. Wir betrachten $r = \left(\begin{smallmatrix} A & x \\ 0 & g \end{smallmatrix}\right) \in R$, geschrieben in Blockmatrixschreibweise, wobei $A \in \mathbb{Q}^{2\times 2}$, $x \in \mathbb{Q}^{2\times 1}$ und $g \in \mathbb{Q}$.
Sei $\varphi(r) = (A, g)$ invertierbar. Dann ist A invertierbar und $g \neq 0$. Es wird $r^{-1} = \left(\begin{smallmatrix} A & x \\ 0 & g \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} A^{-1} & -A^{-1}xg^{-1} \\ 0 & g^{-1} \end{smallmatrix}\right) \in R$, da sowohl $\left(\begin{smallmatrix} A & x \\ 0 & g \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} A^{-1} & -A^{-1}xg^{-1} \\ 0 & g^{-1} \end{smallmatrix}\right) = \left(\begin{smallmatrix} \mathrm{E}_2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ als auch $\left(\begin{smallmatrix} A^{-1} & -A^{-1}xg^{-1} \\ 0 & g^{-1} \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} A & x \\ 0 & g \end{smallmatrix}\right) = \left(\begin{smallmatrix} \mathrm{E}_2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ ist. Also ist r invertierbar.

Aufgabe 2

(1) Man erstelle die Multiplikationstafel von $\mathbb{Z}/8\mathbb{Z}$.

(2) Man bestimme $\{\, x \in \mathbb{Z}/8\mathbb{Z} \,:\, x^2 - 1 = 0 \,\}$.

(3) Ist $\mathbb{Z}/8\mathbb{Z}$ ein Körper? Man entscheide anhand (1).

Lösung.
Zu (1). Die Multiplikationstafel von

$$\mathbb{Z}/8\mathbb{Z} \;=\; \{0+8\mathbb{Z}, 1+8\mathbb{Z}, 2+8\mathbb{Z}, 3+8\mathbb{Z}, 4+8\mathbb{Z}, 5+8\mathbb{Z}, 6+8\mathbb{Z}, 7+8\mathbb{Z}\} \overset{\text{kurz}}{=} \{0,1,2,3,4,5,6,7\}$$

ergibt sich wie folgt.

$(\cdot)$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Zu (2). Der Diagonale der Multiplikationstafel kann man entnehmen, daß

$$\{\, x \in \mathbb{Z}/8\mathbb{Z} \,:\, x^2 - 1 = 0 \,\} \;=\; \{1,3,5,7\}$$

ist.
Zu (3). Nein, es ist $\mathbb{Z}/8\mathbb{Z}$ kein Körper. Denn es ist z.B. $2 \in (\mathbb{Z}/8\mathbb{Z})^{\times}$, wohingegen $2 \notin \mathrm{U}(\mathbb{Z}/8\mathbb{Z})$ liegt. Denn in der Multiplikationstafel taucht in der Zeile zur 2 das Element 1 nicht auf.
Insgesamt ist hier

$$\mathrm{U}(\mathbb{Z}/8\mathbb{Z}) \;=\; \{1,3,5,7\} \;\subset\; \{1,2,3,4,5,6,7\} \;=\; (\mathbb{Z}/8\mathbb{Z})^{\times}\ .$$

In (2) haben wir also gesehen: Ein normiertes Polynom kann also in $\mathbb{Z}/8\mathbb{Z}$ mehr Nullstellen haben, als sein Grad anzeigt.
Aber, wie in (3) gesehen, es ist ja $\mathbb{Z}/8\mathbb{Z}$ auch kein Körper.

Aufgabe 3

(1) Sei $f(X) := X^4 + \frac{2}{3}X^3 - \frac{10}{3}X^2 - 2X + 1 \in \mathbb{Q}[X]$.
Man bestimme alle Nullstellen von $f(X)$, die in $\mathbb{Q}$ liegen.

(2) Man zeige unter Verwendung des Satzes von Descartes: $\sqrt{2} \notin \mathbb{Q}$.

Lösung.
Zu (1). Wir wollen alle Nullstellen von

$$3 \cdot f(X) \;=\; 3X^4 + 2X^3 - 10X^2 - 6X + 3 \;\in\; \mathbb{Z}[X]$$

bestimmen, die in $\mathbb{Q}$ liegen. Jede solche Nullstelle ist von der Form $\pm\frac{u}{v}$, mit $u,\, v \in \mathbb{Z}^\times$ teilerfremd und mit u ein Teiler des konstanten Terms 3 und v ein Teiler des Leitterms 3. Also ist jede Nullstelle, die in $\mathbb{Q}$ liegt, enthalten in

$$\left\{ -\frac{1}{3},\, \frac{1}{3},\, -1,\, 1,\, -3,\, 3 \right\} .$$

Es wird

$$\begin{array}{lcr} 3\cdot f(-\frac{1}{3}) & = & \frac{104}{27} \\ 3\cdot f(\frac{1}{3}) & = & 0 \\ 3\cdot f(-1) & = & 0 \\ 3\cdot f(1) & = & -8 \\ 3\cdot f(-3) & = & 120 \\ 3\cdot f(3) & = & 192 \end{array}$$

Also sind die Nullstellen von $f(X)$, die in $\mathbb{Q}$ liegen, gegeben durch $\frac{1}{3}$ und -1.

Zu (2). *Annahme*, es ist $\sqrt{2} \in \mathbb{Q}$. Dann hat $g(X) := X^2 - 2 \in \mathbb{Z}[X]$ wenigstens eine Nullstelle, die in $\mathbb{Q}$ liegt, nämlich $\sqrt{2}$.

Eine solche Nullstelle ist laut Descartes von der Form $\frac{u}{v}$, mit $u,\, v \in \mathbb{Z}^\times$ teilerfremd und mit u Teiler von -2 und v Teiler von 1. Somit sind alle solchen Nullstellen von $X^2 - 2$ enthalten in

$$\{ -1,\, 1,\, -2,\, 2 \} .$$

Aber es ist

$$\begin{array}{lcr} g(-1) & = & -1 \\ g(1) & = & -1 \\ g(-2) & = & 3 \\ g(2) & = & 3\,. \end{array}$$

Also hat $g(X)$ keine Nullstelle, die in $\mathbb{Q}$ liegt. *Widerspruch.*

Aufgabe 4

(1) Man zeige: $\mathrm{U}(\mathbb{Z}) \subset \mathrm{U}(\mathbb{Z}_{(5)}) \subset \mathrm{U}(\mathbb{Q})$.
Hierbei heiße $(M \subset N) :\Leftrightarrow (M \subseteq N \wedge M \neq N)$.

(2) Man zeige unter Verwendung der Multiplikationstafel von $\mathbb{Z}/5\mathbb{Z}$:
Für jedes $v \in \mathbb{Z}$ mit $v \not\equiv_5 0$ gibt es ein $w \in \mathbb{Z}$ mit $wv \equiv_5 1$.

(3) Wir betrachten den injektiven Ringmorphismus

$$\varphi \;:\; \mathbb{Z}/5\mathbb{Z} \;\to\; \mathbb{Z}_{(5)}/5\mathbb{Z}_{(5)} \;:\; z + 5\mathbb{Z} \;\mapsto\; z + 5\mathbb{Z}_{(5)} \;.$$

Man zeige unter Verwendung von (2): Es ist φ ein Ringisomorphismus.

(4) Seien R und S Ringe.
Sei $\varphi : R \to S$ ein Ringisomorphismus, d.h. ein bijektiver Ringmorphismus.
Man zeige: $\varphi^{-1} : S \to R$ ist ein Ringisomorphismus.

Lösung.

Zu (1). Da $\mathbb{Z} \subseteq \mathbb{Z}_{(5)} \subseteq \mathbb{Q}$, ist auch $\mathrm{U}(\mathbb{Z}) \subseteq \mathrm{U}(\mathbb{Z}_{(5)}) \subseteq \mathrm{U}(\mathbb{Q})$.
Wir haben zu zeigen, daß die Inklusionen echt sind.

Zu $\mathrm{U}(\mathbb{Z}) \overset{!}{\subset} \mathrm{U}(\mathbb{Z}_{(5)})$. Es ist $2 \in \mathrm{U}(\mathbb{Z}_{(5)})$, mit inversem Element $\frac{1}{2} \in \mathbb{Z}_{(5)}$.
Aber es ist $2 \notin \mathrm{U}(\mathbb{Z}) = \{-1, +1\}$.

Zu $\mathrm{U}(\mathbb{Z}_{(5)}) \overset{!}{\subset} \mathrm{U}(\mathbb{Q})$. Es $5 \in \mathrm{U}(\mathbb{Q})$, mit inversem Element $\frac{1}{5} \in \mathbb{Q}$.
Aber es ist $5 \notin \mathrm{U}(\mathbb{Z}_{(5)}) = \{ \frac{u}{v} \;:\; u,\, v \in \mathbb{Z}^\times,\; u \not\equiv_5 0,\; v \not\equiv_5 0 \}$.

Zu (2). Die Multiplikationstafel von

$$\mathbb{Z}/8\mathbb{Z} \;=\; \{0+5\mathbb{Z}, 1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}5\} \;\stackrel{\text{kurz}}{=}\; \{0,1,2,3,4\}$$

ergibt sich wie folgt.

$(\cdot)$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Da in jeder Zeile, die nicht zu 0 gehört, eine 1 auftritt, gilt: Für jedes $x \in \mathbb{Z}/5$ mit $x \neq 0$ gibt es ein $y \in \mathbb{Z}$ mit $xy = 1$.
Für jedes $v \in \mathbb{Z}$ mit $v \not\equiv_5 0$ ist $x := v + 5\mathbb{Z} \neq 0$. Also gibt es ein $y \in \mathbb{Z}$ mit $xy = 1$. Schreiben wir $y = w + 5\mathbb{Z}$ für ein $w \in \mathbb{Z}$, so folgt $vw + 5\mathbb{Z} = xy = 1 = 1 + 5\mathbb{Z}$, also $vw \equiv_5 1$.
Zu (3). Nach Aufgabenstellung dürfen wir als bekannt voraussetzen, daß φ ein injektiver Ringmorphismus ist.
Zu zeigen bleibt die Surjektivität von φ. Sei $\frac{u}{v} \in \mathbb{Z}_{(5)}$ gegeben, wobei $u,\, v \in \mathbb{Z}^\times$ mit $v \not\equiv_5 0$.
Gesucht ist ein $z \in \mathbb{Z}$ mit $z + 5\mathbb{Z}_{(5)} \stackrel{!}{=} \frac{u}{v} + 5\mathbb{Z}_{(5)}$, also mit $5\mathbb{Z}_{(5)} \stackrel{!}{\ni} z - \frac{u}{v} = \frac{zv-u}{v}$.
Es genügt, ein $z \in \mathbb{Z}$ mit $zv - u \stackrel{!}{\equiv}_5 0$ zu finden.
Da $v \not\equiv_5 0$, finden wir gemäß (2) ein $w \in \mathbb{Z}$ mit $vw \equiv_5 1$, also mit $vw - 1 \equiv_5 0$.
Sei $z := uw$. Dann wird

$$zv - u \;=\; uwv - u \;=\; u(vw-1) \;\equiv_5\; 0\,.$$

Zu (4). Zu zeigen ist, daß auch die Umkehrabbildung φ^{-1} ein Ringmorphismus ist.
Es ist

$$\varphi^{-1}(1_S) \;=\; \varphi^{-1}(\varphi(1_R)) \;=\; 1_R\,.$$

Für $x,\, y \in S$ wird

$$\varphi^{-1}(x+y) \;=\; \varphi^{-1}(\varphi(\varphi^{-1}(x)) + \varphi(\varphi^{-1}(y))) \;=\; \varphi^{-1}(\varphi(\varphi^{-1}(x) + \varphi^{-1}(y))) \;=\; \varphi^{-1}(x) + \varphi^{-1}(y)$$

und

$$\varphi^{-1}(x \cdot y) \;=\; \varphi^{-1}(\varphi(\varphi^{-1}(x)) \cdot \varphi(\varphi^{-1}(y))) \;=\; \varphi^{-1}(\varphi(\varphi^{-1}(x) \cdot \varphi^{-1}(y))) \;=\; \varphi^{-1}(x) \cdot \varphi^{-1}(y)\,.$$