

Lösung 1

Aufgabe 1

Es wird

$$(-r) \cdot s = (-r) \cdot s + r \cdot s - r \cdot s = ((-r) + r) \cdot s - r \cdot s = 0 \cdot s - r \cdot s = -(r \cdot s).$$

Analog wird

$$r \cdot (-s) = r \cdot (-s) + r \cdot s - r \cdot s = r \cdot ((-s) + s) - r \cdot s = r \cdot 0 - r \cdot s = -r \cdot s.$$

Vgl. Bemerkung 2.(3).

Aufgabe 2

- (1) Seien $(r_{i,j})_{i,j}, (r'_{i,j})_{i,j}, (s_{i,j})_{i,j}, (s'_{i,j})_{i,j}, (t_{i,j})_{i,j} \in R^{n \times n}$.

Wir setzen

$$\begin{aligned} (r_{i,j})_{i,j} + (s_{i,j})_{i,j} &:= (r_{i,j} + s_{i,j})_{i,j} \\ (r_{i,j})_{i,j} \cdot (s_{i,j})_{i,j} &:= \left(\sum_{j \in [1,n]} r_{i,j} s_{j,k} \right)_{i,k}. \end{aligned}$$

Zu (Ring 1). Es ist $(R^{n \times n}, +)$ eine abelsche Gruppe, wie sich aus punktweiser Anwendung der abelschen Gruppeneigenschaften von $(R, +)$ ergibt.

Zu (Ring 2). Es werden

$$\begin{aligned} (r_{i,j})_{i,j} \cdot ((s_{i,j})_{i,j} \cdot (t_{i,j})_{i,j}) &= (r_{i,j})_{i,j} \cdot \left(\sum_{k \in [1,n]} s_{j,k} t_{k,\ell} \right)_{j,\ell} \\ &= \left(\sum_{j \in [1,n]} \sum_{k \in [1,n]} r_{i,j} s_{j,k} t_{k,\ell} \right)_{i,\ell} \\ ((r_{i,j})_{i,j} \cdot (s_{i,j})_{i,j}) \cdot (t_{i,j})_{i,j} &= \left(\sum_{j \in [1,n]} r_{i,j} s_{j,k} \right)_{i,k} \cdot (t_{i,j})_{i,j} \\ &= \left(\sum_{k \in [1,n]} \sum_{j \in [1,n]} r_{i,j} s_{j,k} t_{k,\ell} \right)_{i,\ell}. \end{aligned}$$

Beide Klammerungen liefern also dasselbe Resultat.

Zu (Ring 3). Wir *behaupten*, daß $1_{R^{n \times n}} = (\partial_{i,j})_{i,j}$. Es werden

$$\begin{aligned} (r_{i,j})_{i,j} \cdot (\partial_{i,j})_{i,j} &= \left(\sum_{j \in [1,n]} r_{i,j} \partial_{j,k} \right)_{i,k} \\ &= (r_{i,k})_{i,k} \\ (\partial_{i,j})_{i,j} \cdot (r_{i,j})_{i,j} &= \left(\sum_{j \in [1,n]} \partial_{i,j} r_{j,k} \right)_{i,k} \\ &= (r_{i,k})_{i,k}. \end{aligned}$$

Zu (Ring 4). Es wird

$$\begin{aligned} &((r_{i,j})_{i,j} + (r'_{i,j})_{i,j}) \cdot ((s_{i,j})_{i,j} + (s'_{i,j})_{i,j}) \\ &= (r_{i,j} + r'_{i,j})_{i,j} \cdot (s_{i,j} + s'_{i,j})_{i,j} \\ &= \left(\sum_{j \in [1,n]} (r_{i,j} + r'_{i,j})(s_{j,k} + s'_{j,k}) \right)_{i,k} \\ &= \left(\sum_{j \in [1,n]} (r_{i,j} s_{j,k} + r_{i,j} s'_{j,k} + r'_{i,j} s_{j,k} + r'_{i,j} s'_{j,k}) \right)_{i,k} \\ &= \left(\sum_{j \in [1,n]} r_{i,j} s_{j,k} + \sum_{j \in [1,n]} r_{i,j} s'_{j,k} + \sum_{j \in [1,n]} r'_{i,j} s_{j,k} + \sum_{j \in [1,n]} r'_{i,j} s'_{j,k} \right)_{i,k} \\ &= \left(\sum_{j \in [1,n]} r_{i,j} s_{j,k} \right)_{i,k} + \left(\sum_{j \in [1,n]} r_{i,j} s'_{j,k} \right)_{i,k} + \left(\sum_{j \in [1,n]} r'_{i,j} s_{j,k} \right)_{i,k} + \left(\sum_{j \in [1,n]} r'_{i,j} s'_{j,k} \right)_{i,k} \\ &= (r_{i,j})_{i,j} (s_{i,j})_{i,j} + (r_{i,j})_{i,j} (s'_{i,j})_{i,j} + (r'_{i,j})_{i,j} (s_{i,j})_{i,j} + (r'_{i,j})_{i,j} (s'_{i,j})_{i,j}. \end{aligned}$$

(2) Wir betrachten folgende Matrizen $(r_{i,j})_{i,j}, (s_{i,j})_{i,j} \in R^{n \times n}$.

Sei $r_{i,j} := 1$, falls $i = 1$ und $j = 2$, und $r_{i,j} := 0$ sonst. Sei $s_{i,j} := 1$, falls $i = 2$ und $j = 1$, und $s_{i,j} := 0$ sonst.

Es ergibt sich der Eintrag bei $(1, 1)$ von $(r_{i,j})_{i,j} \cdot (s_{i,j})_{i,j}$ zu $\sum_{j \in [1,n]} r_{1,j} s_{j,1} = r_{1,2} s_{2,1} = 1$.

Es ergibt sich der Eintrag bei $(1, 1)$ von $(s_{i,j})_{i,j} \cdot (r_{i,j})_{i,j}$ zu $\sum_{j \in [1,n]} s_{1,j} r_{j,1} = 0$.

Da $1 \neq 0$, folgt $(r_{i,j})_{i,j} \cdot (s_{i,j})_{i,j} \neq (s_{i,j})_{i,j} \cdot (r_{i,j})_{i,j}$.

Vgl. Beispiel 3.(4).

Aufgabe 3

(1) Ist $r + I = r' + I$, so ist $r = r + 0 \in r + I = r' + I$. Somit gibt es ein $x \in I$ mit $r = r' + x$. Folglich ist $r - r' = x \in I$.

Sei umgekehrt $r - r' \in I$. Für $x \in I$ ist $r + x = r' + ((r - r') + x) \in r' + I$, und also $r + I \subseteq r' + I$. Auf der anderen Seite ist für $y \in I$ auch $r' + y = r + (-(r - r') + y) \in r + I$, und also $r' + I \subseteq r + I$. Insgesamt ist $r + I = r' + I$.

(2) Seien $r, \tilde{r}, r', \tilde{r}' \in R$ mit $r + I = \tilde{r} + I$ und $r' + I = \tilde{r}' + I$ gegeben.

Es ist $(r + r') + I = (\tilde{r} + \tilde{r}') + I$, da $(r + r') - (\tilde{r} + \tilde{r}') = (r - \tilde{r}) + (r' - \tilde{r}') \in I$. Folglich ist die angegebene Additionsabbildung auf R/I wohldefiniert.

Es ist $(r \cdot r') + I = (\tilde{r} \cdot \tilde{r}') + I$, da $r \cdot r' - \tilde{r} \cdot \tilde{r}' = r(r' - \tilde{r}') + (r - \tilde{r})\tilde{r}' \in I$. Folglich ist die angegebene Multiplikationsabbildung auf R/I wohldefiniert.

Die Ringeigenschaften für R/I vererben sich wie folgt von R . Seien $r, r', r'', s, s' \in R$.

Zu (Ring 1). Es ist

$$\begin{aligned} (r + I) + ((r' + I) + (r'' + I)) &= (r + I) + ((r' + r'') + I) \\ &= (r + (r' + r'')) + I \\ &= (r + r' + r'') + I, \end{aligned}$$

und genauso $((r + I) + (r' + I)) + (r'' + I) = (r + r' + r'') + I$.

Es ist $(r + I) + (r' + I) = (r + r') + I = (r' + r) + I = (r + I) + (r' + I)$.

Es ist $(0 + I) + (r + I) = (0 + r) + I = r + I$.

Es ist $((-r) + I) + (r + I) = ((-r) + r) + I = 0 + I$.

Zu (Ring 2). Es ist

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

und genauso $((r + I) \cdot (r' + I)) \cdot (r'' + I) = (r \cdot r' \cdot r'') + I$.

Zu (Ring 3). Es ist $(1 + I) \cdot (r + I) = (1 \cdot r) + I = r + I$. Es ist $(r + I) \cdot (1 + I) = (r \cdot 1) + I = r + I$.

Zu (Ring 4). Es ist

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

Vgl. Bemerkung 6.(2).

Aufgabe 4

- (1) Zeigen wir die Existenz von $n \in \mathbf{Z}_{\geq 0}$ mit $I = n\mathbf{Z}$. Sei $I \subseteq \mathbf{Z}$ ein Ideal. Ist $I = 0$, so ist $I = 0\mathbf{Z}$. Ist $I \neq 0$, so ist $I \cap \mathbf{Z}_{\geq 1}$ nicht leer, da mit jedem Element auch sein Negatives in I liegt. Sei $n := \min(I \cap \mathbf{Z}_{\geq 1})$. Wir behaupten, daß $I \stackrel{!}{=} n\mathbf{Z}$. Wegen $n \in I$ ist auch $n\mathbf{Z} \subseteq I$. Bleibt die Inklusion $I \stackrel{!}{\subseteq} n\mathbf{Z}$ zu zeigen. Sei $x \in I$. Dank Division mit Rest können wir $x = na + b$ schreiben mit $a, b \in \mathbf{Z}$ und $b \in [0, n - 1]$. Es ist $b = x - na \in I$. Wäre $b \neq 0$, so wäre $b \in I \cap \mathbf{Z}_{\geq 1}$, aber $b < n$, im Widerspruch zur Wahl von n . Also ist $b = 0$, und folglich $x = na \in n\mathbf{Z}$.

Zeigen wir die Eindeutigkeit eines solchen n . Seien also $n, \tilde{n} \in \mathbf{Z}_{\geq 0}$ mit $I = n\mathbf{Z} = \tilde{n}\mathbf{Z}$. Ist $I = 0$, so ist $n = 0 = \tilde{n}$. Ist $I \neq 0$, so sind $n, \tilde{n} \geq 1$. Ferner ist dann n ein Vielfaches von \tilde{n} , und \tilde{n} ein Vielfaches von n , was $n = \tilde{n}$ nach sich zieht.

- (2) Sei n prim. Zunächst ist $0 \neq 1$ in \mathbf{Z}/n . Sei ferner $x \in \mathbf{Z}$ mit $x \notin n\mathbf{Z}$, i.e. mit $x \neq 0$ in \mathbf{Z}/n gegeben. Um zu zeigen, daß x in \mathbf{Z}/n invertierbar ist, genügt es zu zeigen, daß $\mathbf{Z}/n \rightarrow \mathbf{Z}/n, y \mapsto xy$ surjektiv ist. Dafür wiederum genügt es wegen der Endlichkeit von \mathbf{Z}/n zu zeigen, daß $\mathbf{Z}/n \rightarrow \mathbf{Z}/n, y \mapsto xy$ injektiv ist. Seien also $y, y' \in \mathbf{Z}$ mit $xy = xy'$ in \mathbf{Z}/n gegeben. Dann ist n ein Teiler von $x(y - y')$. Da n prim ist und da n kein Teiler von x ist, ist n ein Teiler von $y - y'$. In anderen Worten, es ist $y = y'$ in \mathbf{Z}/n .

Sei n nicht prim. Ist $n = 1$, so ist $\mathbf{Z}/1\mathbf{Z}$ kein Körper, da darin $0 = 1$ gilt. Wir dürfen also $n \geq 2$ annehmen. Schreibt man $n = ab$ mit $a, b \in [1, n - 1]$, so ist a in \mathbf{Z}/n nicht invertierbar. Denn wäre $xa = 1$ in \mathbf{Z}/n für $x \in \mathbf{Z}$, so wäre $b = xab = 0$ in \mathbf{Z}/n , aber $b \neq 0$ in \mathbf{Z}/n , da $b \in [1, n - 1]$ in \mathbf{Z} .

- (3) Wir können $n \in \{15, 16, 20, 24, 30\}$ wählen.

Vgl. Beispiel 7.

Aufgabe 5

- (1) Die Aussage ist falsch. Sei etwa $R = \mathbf{Z}/8$, und sei $x = 3$. Dann ist $x^2 = 1$, aber $x \notin \{-1, +1\}$.
- (2) Die Aussage ist falsch. Seien etwa $n = 15$ und $x = 2$. Die Ordnung von 2 in $\mathbf{Z}/15$ ist 4, und das ist kein Teiler von $15 - 14$.