Lösung 3: Ringe, Körper, Vektorräume

1. **a)** *Bemerkung:* wir werden die notwendigen Eigenschaften der Verknüpfungen nur für die Addition beweisen. Wir zeigen zuerst, dass die Addition wohldefiniert ist, d.h. $[k+l]$ in der Definition ist unabhängig von der Wahl der Repräsentanten von $[k]$ und $[l]$. Seien $k, l, s, t \in \mathbb{Z}$, dann ist

$$(k + sn) + (l + tn) = k + l + (s + t)n \equiv k + l \mod n$$

Also ist $+$ wohldefiniert. Die Verknüpfung ist assoziativ, da $\mathbb{Z}$ ein Ring ist:

$$\begin{aligned}([k] + [l]) + [s] =& [k + l] + [s] = [(k + l) + s] = [k + (l + s)] \\ =& [k] + [l + s] = [k] + ([l] + [s])\end{aligned}$$

Die Verknüpfung ist kommutativ:

$$[k] + [l] = [k + l] = [l + k] = [l] + [k]$$

Wir finden ebenfalls:

$$[0] + [k] = [0 + k] = [k]$$

sowie

$$[k] + [-k] = [k - k] = [0]$$

Ähnlich folgt, dass $[1] \cdot [k] = [k]$, und die Distributivitätsgesetze folgen aus der Distributivität von $\mathbb{Z}$.

Also ist $\mathbb{Z}_n$ ein Ring *mit Eins* (d.h. es gilt K6) und kommutativ (d.h. es gilt K10). Falls $n \neq 1$, dann ist $[1] \neq [0]$ und $\mathbb{Z}_n$ ist nicht-trivial.

b) Wir sagen, zwei Elemente $e, f \in \mathbb{Z}$ sind *teilerfremd*, falls gilt:

$$\forall m \in \mathbb{Z} : m \mid e \wedge m \mid f \implies m = \pm 1$$

Zuerst stellen wir fest, dass wir o.B.d.A. annehmen können, dass $e, f > 0$, da $e \mid b$ genau dann wenn $-e \mid b$. Es ist klar, dass für $0 < e, f \leq 1$ die Aussage wahr ist, da $1 \mid b$ für alle $b \in \mathbb{Z}$. Sei nun $n \geq 1$ und die Aussage wahr für $e', f' \in \mathbb{N}$ mit $e', f' \leq n$.

Angenommen $e, f \in \mathbb{N}$ seien teilerfremd und $\max\{e, f\} \leq n + 1$, dann können wir o.B.d.A. annehmen, dass $e < f$. Division mit Rest liefert eindeutige $r \in \mathbb{N}$

Bitte wenden!

und $0 < s < e$ so dass $f = re + s$. Dies zeigt, dass jeder gemeinsame Teiler $m \in \mathbb{N}$ von s und e ein Teiler von f und somit ein gemeinsamer Teiler von e und f ist. Also sind s und e teilerfremd. Nach Einsetzen erhalten wir $ae = bf = bre + bs$, und also ist e ein Teiler von bs. Da nach Annahme $0 < s < e \leq n$ und s und e teilerfremd sind, folgt aus der Induktionsannahme, dass $e \mid b$.

c) Im Folgenden sei ein Teiler m von k und l *maximal*, wenn jeder andere Teiler von k und l ein Teiler von m ist. Die Behauptung ist also, dass jedes Paar von Null verschiedener Zahlen einen maximalen, gemeinsamen Teiler besitzt und der bis auf Vorzeichen durch k, l eindeutig bestimmt ist.

Wir beweisen dies per Induktion. Sei $\max\{|k|, |l|\} \leq 1$, dann gelten $1 \mid k \wedge 1 \mid l$ sowie $-1 \mid k \wedge -1 \mid l$. Sei $m \in \mathbb{Z} \setminus \{0\}$ mit $m \notin \{\pm 1\}$, dann gilt $m \nmid k \wedge m \nmid l$, und somit haben $1, -1$ die notwendigen Eigenschaften und der $\mathrm{ggT}(k, l)$ ist eindeutig bis auf Vorzeichen.

Angenommen es gibt $n \in \mathbb{N}$, $n \geq 2$, so dass die Existenz eines maximalen Teilers sowie seine Eindeutigkeit bis auf Vorzeichen für alle Paare (k', l') von Null verschiedener, ganzer Zahlen mit

$$\max\{|k'|, |l'|\} \leq n - 1$$

gelten und seien $k, l \in \mathbb{Z} \setminus \{0\}$ mit $\max\{|k|, |l|\} \leq n$. Falls $|k| = |l| = n$, dann ist n ein gemeinsamer Teiler von k und l und jeder gemeinsame Teiler von k und l ist ein Teiler von n, somit ist n ein maximaler Teiler.

Sei nun o.B.d.A. $|k| < n$. Wegen $1 \mid k \wedge 1 \mid l$, besitzt das Paar k, l einen gemeinsamen Teiler $a \in \mathbb{Z} \setminus \{0\}$. Des Weiteren gilt $a \mid k \implies |a| \leq |k|$ (siehe Analysisvorlesung). Also ist die Menge

$$T(k, l) := \{a \in \mathbb{Z} \mid a \mid k \wedge a \mid l\}$$

endlich und insbesondere

$$T(k, l) \subset \{a \in \mathbb{Z} \mid |a| < n\}$$

Sei $a \in T(k, l)$ so dass $|a|$ maximal (bezüglich Ordnung induziert von $\mathbb{R}$ – siehe Analysisvorlesung). Wir behaupten, dass a ein maximaler, gemeinsamer Teiler im Sinne der Aufgabenstellung ist. Um einen Widerspruch zu erzeugen, nehmen wir an, dass $b \in T(k, l)$ mit $b \nmid a$ und (o.B.d.A.) $0 < b < a$. Dann sind a und b teilerfremd. Um dies zu zeigen, sei $0 < m < b$ ein maximaler, gemeinsamer Teiler von a und b, dann sind $a = \alpha m$ und $b = \beta m$ mit teilerfremden $\alpha, \beta \in \mathbb{Z}$. Da $b \nmid m$, wissen wir $\beta \neq \pm 1$. Zusätzlich existieren $r, s, t, u \in \mathbb{Z}$, so dass $k = r\alpha m = s\beta m$ sowie $l = t\alpha m = u\beta m$. Aus der vorangehenden Teilaufgabe folgt $\beta \mid r$ und $\beta \mid t$, also existieren $r', t' \in \mathbb{Z}$ so dass $k = r'\beta a$ und $l = t'\beta a$. Also ist $|\beta| a \in T(k, l)$, im Widerspruch zur Maximalität von a. Da a, b teilerfremd sind, folgt aus der vorangehenden Aufgabe, dass ab ein gemeinsamer Teiler von k und l ist, und wegen Maximalität von a folgt $b = \pm 1$, im Widerspruch zu $b \nmid a$.

Siehe nächstes Blatt!

d) (1) $\Longrightarrow$ (2) Es ist klar, dass $(k,l) \mid sk+tl$ für alle $s,t \in \mathbb{Z}$.
(2) $\Longrightarrow$ (1) Da $\mathbb{N}$ wohlgeordnet ist, besitzt die Menge

$$\{d \in \mathbb{Z} | \exists s,t \in \mathbb{Z} : d = sk+tl\} \cap \mathbb{N}$$

ein minimales Element d^*. Aus $\mathrm{ggT}(k,l)|k \wedge \mathrm{ggT}(k,l)|l$ folgt $\mathrm{ggT}(k,l)|d^*$. Wir zeigen, dass $d^*|\,\mathrm{ggT}(k,l)$, woraus folgt, dass $d^* = \pm\,\mathrm{ggT}(k,l)$. Wir verwenden Division mit Rest und schreiben $k = pd^* + q$ mit $0 \leq q < d^*$. Es gilt

$$q = k - pd^* = k - p(sk+tl) = (1-ps)k - ptl$$

und wegen Minimalität von d^* folgt $q = 0$. Also ist d^* ein Teiler von k. Analog beweist man, dass d^* ein Teiler von l ist. Per definitionem von $\mathrm{ggT}(k,l)$ folgt $d^*|\,\mathrm{ggT}(k,l)$ und also $d^* = \pm\,\mathrm{ggT}(k,l)$.
Alternativ kann man auch hier Induktion verwenden: Es reicht zu zeigen, dass $s,t \in \mathbb{Z}$ existieren, so dass $(k,l) = sk+tl$. Sei nämlich $m = n(k,l)$, dann ist folglich $m = nsk + ntl$, wie gewünscht. Seien $k = \alpha(k,l)$ und $l = \beta(k,l)$ mit $\alpha, \beta \in \mathbb{Z}$ teilerfremd, dann müssen wir zeigen, dass $s,t \in \mathbb{Z}$ existieren, so dass

$$(k,l) = s\alpha(k,l) + t\beta(k,l)$$

Nach Divison mit (k,l) können wir im Folgenden also o.B.d.A. annehmen, dass k,l teilerfremd sind und es reicht zu zeigen, dass unter dieser Voraussetzung $s,t \in \mathbb{Z}$ existieren, mit $1 = sk+tl$. Hierfür verwenden wir einmal mehr Induktion. Für den Fall $|k|,|l| \leq 2$ ist die Aussage leicht überprüft, wegen $1 = 1 \cdot 2 + (-1) \cdot 1 = (-1) \cdot (-2) + (-1) \cdot 1$. Nehmen wir also an, dass für alle teilerfremden $k', l' \in \mathbb{Z} \setminus \{0\}$ mit $|k'|, |l'| < n$ die Aussage gelte, wobei $n > 2$. Seien $k, l \in \mathbb{Z} \setminus \{0\}$ teilerfremd mit $|k|, |l| \leq n$. Wir nehmen o.B.d.A. an, dass $0 < k < l$. Nach Division mit Rest existieren $0 \leq p$ und $0 < q < k$ so dass $l = pk + q$. Da l und k teilerfremd sind, sind k und q teilerfremd. Es existieren nach Induktionsannahme folglich $\alpha, \beta \in \mathbb{Z}$ so dass $1 = \alpha k + \beta q$ und also:

$$1 = \alpha k + \beta q = (\alpha - \beta p)k + \beta l$$

e) Sei $k \in \mathbb{Z}$, dann ist $[k]$ invertierbar in $\mathbb{Z}_n$ genau dann, wenn ein $l \in \mathbb{Z}$ existiert, so dass $lk \equiv 1 \mod n$, d.h. es gibt ein $s \in \mathbb{Z}$ mit $lk = sn + 1$, was wegen des Lemmas von Bézout genau dann gilt, wenn $(k,n) = \pm 1$. $\mathbb{Z}_n$ ist also ein Körper genau dann, wenn $(k,n) = \pm 1$ für alle $k \in \mathbb{Z}$ mit $k \not\equiv 0 \mod n$. Das ist der Fall genau dann, wenn n prim ist.

2. **a)** $(xy)^m = x^m y^m$**:** Falls $m = 0$ oder $m = 1$, dann ist die Aussage richtig per definitionem. Sei die Aussage bewiesen für ein $m \in \mathbb{Z}$ mit $m \geq 0$. Dann gilt

$$(xy)^{m+1} = (xy)^m (xy) = x^m y^m xy = x^{m+1} y^{m+1}$$

und die Aussage folgt aus dem Induktionsaxiom.

Bitte wenden!

$(x^m)^n = x^{mn}$**:** Keine Musterlösung

b) Seien $a, b, c, d \in \mathbb{Q}$, dann ist:

$$\begin{aligned}(a + b\sqrt{2}) + (c + d\sqrt{2}) =& (a + c) + (b + d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]\\ (a + b\sqrt{2})(c + d\sqrt{2}) =& (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]\end{aligned}$$

also ist $\mathbb{Q}[\sqrt{2}]$ abgeschlossen unter Addition und Multiplikation. Beachten Sie, dass

$$(a + b\sqrt{2}) + ((-a) + (-b)\sqrt{2}) = (a - a) + (b - b)\sqrt{2} = 0$$

und also folgt die Existenz additiver Inverser in $\mathbb{Q}[\sqrt{2}]$. Da $\mathbb{R}$ ein kommutativer Ring ist mit additivem neutralem Element 0 und multiplikativem neutralen Element 1, ist $\mathbb{Q}[\sqrt{2}]$ also ein kommutativer Ring mit Eins. Es bleibt zu zeigen, dass

$$a, b \in \mathbb{Q} : a \neq 0 \vee b \neq 0 \implies \exists c, d \in \mathbb{Q} : (a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

Nach oben gefundener Formel für das Produkt müssen wir also zeigen, dass für alle $a \neq 0 \vee b \neq 0$ existieren $c, d \in \mathbb{Q}$ so dass

$$ac + 2bd = 1 \text{ und } ad + bc = 0$$

Angenommen $a \neq 0$, dann folgt aus der zweiten Gleichung $d = -\frac{b}{a}c$ und aus der ersten also $ac - 2\frac{b^2}{a}c = 1$ oder dazu äquivalent:

$$(a^2 - 2b^2)c = a$$

Bekanntlich ist $\sqrt{2}$ (und folglich auch $-\sqrt{2}$) irrational, folglich ist $a^2 - 2b^2 = (a - b\sqrt{2})(a + b]sqrt2) \neq 0$ für alle $a, b \in \mathbb{Q}$ und also

$$c = \frac{a}{a^2 - 2b^2} \text{ und } d = -\frac{b}{a}c = \frac{-b}{a^2 - 2b^2}$$

Falls $a = 0$, dann ist $b \neq 0$. Seien $d = \frac{1}{2b}$ und $c = 0$. Es gilt:

$$b\sqrt{2}(c + d\sqrt{2}) = bc\sqrt{2} + 2bd = 1$$

Beachten Sie, dass auch in diesem Fall die Formeln gelten

$$c = \frac{a}{a^2 - 2b^2} \text{ und } d = \frac{-b}{a^2 - 2b^2}$$

Dies beweist die Existenz von Inversen bezüglich Multiplikation.

Siehe nächstes Blatt!

3. **a)** Für $k > n$ und $l > m$ seien $a_k := 0$ bzw. $b_l := 0$. Definiere

$$\forall 0 \leq k \leq m+n : c_k := \sum_{l=0}^{k} a_l b_{k-l} \tag{1}$$

Wir behaupten, dass

$$p(x) \cdot q(x) = \sum_{k=0}^{m+n} c_k x^k$$

Sei $m = 0$, dann ist $q(x) = b_0$ und $p(x)q(x) = \sum_{k=0}^{n} b_0 a_k x^k$. Andererseits gilt:

$$c_k = \sum_{l=0}^{k} a_l b_{k-l} = b_0 a_k + \sum_{l=0}^{k-1} a_l \underbrace{b_{k-l}}_{=0} = b_0 a_k$$

und die Behauptung stimmt punktweise. Angenommen, die Formel stimmt für ein $0 \leq m < n$, dann ist

$$\begin{aligned} p(x)\left(\sum_{l=0}^{m+1} b_l x^l\right) =& b_0 p(x) + x p(x)\left(\sum_{l=1}^{m+1} b_l x^{l-1}\right) \\ =& \sum_{k=0}^{m+n+1} d_k x^k + x \sum_{k=0}^{m+n} d'_k x^k \\ =& \sum_{k=0}^{m+n+1} d_k x^k + \sum_{k=0}^{m+n+1} d''_k x^k \\ =& \sum_{k=0}^{m+n+1} (d_k + d''_k) x^k \end{aligned}$$

wobei $d_k := b_0 a_k$ und

$$d'_k := \sum_{l=0}^{k} a_l b_{k+1-l}$$

sowie $d''_0 = 0$ sowie $d''_k = d'_{k-1}$ für $k > 0$. Es folgt

$$d_0 + d''_0 = d_0 = b_0 a_0 = \sum_{l=0}^{0} a_l b_{0-l}$$

sowie für $k \geq 1$:

$$d_k + d''_k = b_0 a_k + c'_{k-1} = b_0 a_k + \sum_{l=0}^{k-1} a_l b_{k-l} = \sum_{l=0}^{k} a_l b_{k-l}$$

wie gewünscht. Punktweise gilt also, dass $p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k$ mit den c_k wie in (1), also ist das Polynom $p \cdot q$ gleich dem Polynom mit Koeffizienten c_k wie in (1). Die Koeffizienten zu $p + q$ werden in dieser Lösung nicht bestimmt.

Bitte wenden!

b) Keine Musterlösung

c) Keine Musterlösung

d) Die Identitäten gelten allgemein für kommutative Ringe mit Eins und sollten zusätzlich in dieser Allgemeinheit bewiesen werden. Wir beweisen beispielhaft die zweite Identität. Seien $p, q \in P(\mathbb{R})$ beliebig, dann $p \cdot q + (-p) \cdot q = (p + (-p)) \cdot q = 0_R \cdot q = 0_R$ wegen der ersten Identität. Da die Inverse eindeutig ist, folgt $(-p) \cdot q = -(p \cdot q)$. Der Fall $q \cdot (-p) = -(p \cdot q)$ folgt aus der Kommutativität.

e) Keine Musterlösung

f) Falls $d < 0$, dann ist $P_0(\mathbb{R}) = \{0\}$ und $P_{=d}(\mathbb{R}) = \emptyset$, der erste also ein Vektorraum, der zweite nicht. Sei nun $d \geq 0$. Aus der Formel für Koeffizienten von $p+q$ in Teilaufgabe (a) folgt, dass $\deg(p+q) \leq \max\{\deg(p), \deg(q)\}$ und folglich ist $p + q \in P_d(\mathbb{R})$, falls $p, q \in P_d(\mathbb{R})$. Aus dem Beweis, dass die skalare Multiplikation wohldefiniert ist, folgt, dass

$$\deg(c \cdot p) = \begin{cases} \deg(p) & \text{falls } c \neq 0 \\ -\infty & \text{sonst} \end{cases}$$

Folglich ist $P_{=d}(\mathbb{R})$ kein Vektorraum, da die skalare Multiplikation nicht wohldefiniert ist ($0 \cdot p \notin P_{=d}(\mathbb{R})$ für alle $p \in P_{=d}(\mathbb{R})$). Andererseits ist $P_d(\mathbb{R})$ ein Vektorraum. Vektorraumaxiom VR3 ist erfüllt, da $\deg(0_R) = -\infty < d$ und in Teilaufgabe haben wir (c) gesehen, dass $\deg(-p) = \deg(p)$, also gilt auch Vektorraumaxiom VR4. Die restlichen Axiome gelten, da $P(\mathbb{R})$ ein Vektorraum ist.

4. Keine Musterlösung