Lösung 3:
Gruppen, Ringe und Körper

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 $\mathbb{Z}/n\mathbb{Z}$ 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 $\mathbb{Z}/n\mathbb{Z}$ ist nicht-trivial.

Bitte wenden!

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 $e < f$. Um dies zu rechtfertigen, sei $f < e$ und setze voraus, dass wir bereits wissen, dass daraus $f \mid a$ folgt. Also ist $a = kf$ für ein $k \in \mathbb{N}$ und folglich haben wir die Gleichung $ke = b$. Insbesondere gilt also $e \mid b$ und es folgt die Behauptung. Nach Voraussetzung ist zudem $e \neq f$. Sei im Folgenden also $e < f$. Division mit Rest liefert eindeutige $r \in \mathbb{N}$ 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

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

Siehe nächstes Blatt!

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 $b \nmid a$.

d) (1) $\implies$ (2) Es ist klar, dass $(k,l) \mid sk + tl$ für alle $s, t \in \mathbb{Z}$.

(2) $\implies$ (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.

Bitte wenden!

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 $\mathbb{Z}/n\mathbb{Z}$ 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 $(k, n) = \pm 1$. $\mathbb{Z}n\mathbb{Z}$ 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)** 1. **"⇒":** Falls $b = c$, dann ist sicherlich $a \circ b = a \circ c$.
"⇐": Das ist die Kürzungsregel: Angenommen $a, b, c \in G$ erfüllen $a \circ b = a \circ c$. Da G eine Gruppe ist, existiert $a^{-1} \in G$, sodass $a^{-1} \circ a = e$ gilt, wobei e ein linksneutrales ELement ist. Unter Verwendung der Assoziativität der Verknüpfung folgt

$$b = e \circ b = (a^{-1} \circ a) \circ b = a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) = (a^{-1} \circ a) \circ c = e \circ c = c.$$

2. Seien $a', a'' \in G$, sodass $a' \circ a = a'' \circ a = e$ ist. Wir wissen aus der Vorlesung, dass sowohl a' als auch a'' Rechtsinverse von a sind. Es folgt

$$a' = a' \circ (a \circ a') = (a' \circ a) \circ a' = (a'' \circ a) \circ a' = a'' \circ (a \circ a') = a''.$$

Da a beliebig war, ist somit für beliebige $a \in G$ das inverse Element von a eindeutig durch a bestimmt.

3. Unter Verwendung der obigen Aufgabe reicht es zu zeigen, dass $b^{-1} \circ a^{-1}$ eine Linksinverse von $a \circ b$ ist. Es gilt unter Verwendung der Assoziativität von $\circ$

$$\begin{aligned}(b^{-1} \circ a^{-1}) \circ (a \circ b) &= \big((b^{-1} \circ a^{-1}) \circ a\big) \circ b = \big(b^{-1} \circ (a^{-1} \circ a)\big) \circ b \\ &= (b^{-1} \circ e) \circ b = b^{-1} \circ b = e,\end{aligned}$$

und somit folgt die Behauptung.

b) 1. Sei $g \in G$ beliebig, dann gilt

$$\varphi(g) = \varphi(g \circ e_G) = \varphi(g) * \varphi(e_G) \implies e_H = \varphi(e_G)$$

aufgrund der Kürzungsregel. Es folgt

$$e_H = \varphi(e_G) = \varphi(g^{-1} \circ g) = \varphi(g^{-1}) * \varphi(g)$$

und somit $\varphi(g)^{-1} = \varphi(g^{-1})$, da $\varphi(g)^{-1}$ durch die Eigenschaft $e_H = \varphi(g)^{-1} \circ \varphi(g)$ eindeutig bestimmt ist.

Siehe nächstes Blatt!

2. Sei $\mathrm{Im}(\varphi) \subset H$ das Bild von φ. Wir zeigen zuerst, dass die Verknüpfung $* : \mathrm{Im}(\varphi) \times \mathrm{Im}(\varphi) \to \mathrm{Im}(\varphi)$ wohldefiniert ist, d.h. für alle $h_1, h_2 \in \mathrm{Im}(\varphi)$ gilt $h_1 * h_2 \in \mathrm{Im}(\varphi)$. Da $h_1, h_2 \in \mathrm{Im}(\varphi)$ nach Voraussetzung, existieren $g_1, g_2 \in G$, sodass $h_1 = \varphi(g_1)$ und $h_2 = \varphi(g_2)$ gelten. Insbesondere ist also

$$h_1 * h_2 = \varphi(g_1) * \varphi(g_2) = \varphi(g_1 \circ g_2) \in \mathrm{Im}(\varphi).$$

Seien h_1, h_2, h_3 im Bild von φ, dann sind insbesondere $h_1, h_2, h_3 \in H$ und folglich ist die Verknüpfung auf $\mathrm{Im}(\varphi)$ assoziativ, denn

$$(h_1 * h_2) * h_3 = h_1 * (h_2 * h_3)$$

nach Voraussetzung.
Wir zeigen, dass $\mathrm{Im}(\varphi)$ ein neutrales Element enthält. Wir haben vorhin gezeigt, dass $\varphi(e_G) = e_H$ und folglich ist $e_H \in \mathrm{Im}(\varphi)$. Da e_H das neutrale Element in H ist, folgt $e_H * h = h$ für alle $h \in \mathrm{Im}(\varphi)$.
Wir beweisen die Existenz der Inversen. Sei $h \in \mathrm{Im}(\varphi)$ beliebig, dann existiert nach Voraussetzung ein $g \in G$, sodass $h = \varphi(g)$ gilt. Es ist, wie wir oben gezeigt haben, $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \mathrm{Im}(\varphi)$.

3. Im Folgenden sei $\mathrm{Ker}(\varphi)$ der Kern von φ. Wir zeigen wieder zuerst, dass die Verknüpfung wohldefiniert ist. Seien $g_1, g_2 \in \mathrm{Ker}(\varphi)$. Dann gilt

$$\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2) = e_H * e_H = e_H,$$

und folglich ist $g_1 \circ g_2 \in \mathrm{Ker}(\varphi)$. Das heisst, die Verknüpfung ist wohldefiniert auf $\mathrm{Ker}(\varphi)$.
Wie oben folgt die Assoziativität der Verknüpfung auf $\mathrm{Ker}(\varphi)$ sofort aus der Assoziativität der Verknüpfung auf G.
Wir zeigen, dass Ker ein neutrales Element enthält. Tatsächlich wissen wir bereits, dass $\varphi(e_G) = e_H$ und somit $e_G \in \mathrm{Ker}(\varphi)$. Das $\mathrm{Ker}(\varphi) \subset G$ ist, folgt insbesondere $e_g \circ g = g$ für alle $g \in \mathrm{Ker}(\varphi)$.
Wir beweisen die Existenz von Inversen. Sei $g \in \mathrm{Ker}(\varphi)$ beliebig und sei g^{-1} die Inverse von g in G. Wir zeigen, dass $g^{-1} \in \mathrm{Ker}(\varphi)$ gilt. Tatsächlich gilt wie oben gezeigt $\varphi(g^{-1}) = \varphi(g)^{-1} = e_H^{-1}$ und aus $e_H * e_H = e_H$ folgt $e_H = e_H^{-1}$. Insbesondere ist also $\varphi(g^{-1}) = e_H$ und somit $g^{-1} \in \mathrm{Ker}(\varphi)$.

c) "1. $\Longrightarrow$ 2.": Da H eine Untergruppe ist, enthält H ein neutrales Element und ist somit nicht leer. Seien nun $g, h \in H$, dann ist $h^{-1} \in H$, da H eine Gruppe ist. Nach Voraussetzung ist $g \circ h^{-1} \in H$, da die Restriktion der verknüpfung auf H wohldefiniert ist.

"2. $\Longrightarrow$ 1.": Da H nicht-leer ist, existiert ein $g \in H$ und nach Voraussetzung ist $e_G = g \circ g^{-1} \in H$. Somit enthält H ein neutrales Element. Insbesondere folgt für alle $h \in H$, dass $h^{-1} = e_G \circ h^{-1} \in H$, und H enthält Inverse. Seien $g, h \in H$, dann ist wie eben gezeigt auch $h^{-1} \in H$ und somit folgt $g \circ h = g \circ (h^{-1})^{-1} \in H$, und die Verknüpfung ist wohldefiniert auf H.

Bitte wenden!

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 $k \geq 1$:

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

Siehe nächstes Blatt!

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).

Für die Addition gilt

$$\sum_{k=0}^{\infty} a_k x^k + \sum_{k=0}^{\infty} b_k x^k = \sum_{k=0}^{\infty} (a_k + b_k) x^k,$$

wann immer $a_k = 0$ und $b_k = 0$ für alle bis auf endlich viele $k \in \mathbb{N}$ gilt. Insbesondere gilt also für $p(x) = \sum_{k=0}^{m} a_k x^k$, $q(x) = \sum_{k=0}^{n} b_k x^k$ punktweise

$$p(x) + q(x) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k) x^k, \tag{2}$$

wobei wir für $k > m$ bzw. für $k > n$ jeweils $a_k = 0$ bzw. $b_k = 0$ setzen.

b) Wir machen eine Fallunterscheidung. Falls $p = 0$, d.h. falls alle Koeffizienten von p gleich 0 sind, dann folgt aus (1), dass alle Koeffizienten von $p \cdot q$ gleich 0 sind und somit ist $\deg(p \cdot q) = -\infty = \deg(p) + \deg(q)$ (wobei wir implizit die Definition $-\infty + c = -\infty$ für alle $c \in \mathbb{R} \cup \{-\infty\}$ verwenden). Da $p \cdot q = q \cdot p$ können wir im Folgenden also annehmen, dass sowohl p als auch q von 0 verschiedene Koeffizienten besitzen. Sei $p \cdot q = \sum_{k \geq 0} c_k x^k$. Für $k > \deg(p) + \deg(q)$ gilt

$$c_k = \sum_{l=0}^{k} a_l b_{k-l} = \sum_{l=0}^{\deg(p)} a_l \underbrace{b_{k-l}}_{=0} + \sum_{l=\deg(p)+1}^{k} \underbrace{a_l}_{=0} b_{k-l} = 0$$

und folglich ist $\deg(p \cdot q) \leq \deg(p) + \deg(q)$. Sei $k = \deg(p) + \deg(q)$, dann ist

$$c_k = \sum_{l=0}^{k} a_l b_{k-l} = \sum_{l<\deg(p)} a_l \underbrace{b_{k-l}}_{=0} + a_{\deg(p)} b_{\deg(q)} + \sum_{l>\deg(p)} \underbrace{a_l}_{=0} b_{k-l} = a_{\deg(p)} b_{\deg(q)} \neq 0$$

und somit $\deg(p \cdot q) \geq \deg(p) + \deg(q)$. Es folgt

$$\deg(p \cdot q) = \deg(p) + \deg(q).$$

c) Sei p_0 das Polynom mit Koeffizienten alle gleich 0. Dann gilt nach Formel (2), dass $p_0 + p = p$ ist für alle $p \in \mathbb{R}[x]$. Es ist also $0_R = p_0$.

Sei $p_1 = \sum_{k=0}^{m} a_k x^k$ das Polynom gegeben durch $a_0 = 1$ und $a_k = 0$ wann immer $k \neq 0$. Sei $p = \sum_{k=0}^{n} b_k x^k \in \mathbb{R}[x]$ beliebig, dann ist nach Formel (1)

$$(p_1 \cdot p)(x) = \sum_{k \geq 0} \left(\sum_{l=0}^{k} a_l b_{k-l} \right) x^k = \sum_{k \geq 0} a_0 b_k x^k = \sum_{k \geq 0} b_k x^k = p(x).$$

Es ist also $1_R = p_1$.

Bitte wenden!

d) Die Identitäten gelten allgemein für Ringe mit Eins und sollten zusätzlich in dieser Allgemeinheit bewiesen werden.

1. Es gilt aufgrund der Distributivität $0_R \cdot p = (0_R + 0_R) \cdot p = 0_R \cdot p + 0_R \cdot p$ und da $(R, +, 0_R)$ eine abelsche Gruppe ist, folgt aus der Kürzungsregel, dass $0_R = 0_R \cdot p$. Analog gilt $p \cdot 0_R = p \cdot 0_R + p \cdot 0_R$ und somit $p \cdot 0_R = 0_R$.
2. Seien $p, q \in \mathbb{R}[x]$ 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 analog.
3. Es gilt

$$\begin{aligned}(-p) \cdot (-q) + (-(p \cdot q)) &= (-p) \cdot (-q) + (-p) \cdot q = (-p) \cdot ((-q) + q) \\ &= (-p) \cdot 0_R = 0_R\end{aligned}$$

   und somit ist $(-p) \cdot (-q)$ die additive Inverse von $-(p \cdot q)$. Andererseits ist $p \cdot q$ ebenfalls die additive Inverse von $-(p \cdot q)$ und somit folgt aus der Eindeutigkeit der Inversen, dass $(-p) \cdot (-q) = p \cdot q$ ist.
4. Es gilt unter Verwendung der vorangehenden Resultate

$$(-1_R) \cdot p = -(1_R \cdot p) = -p = -(p \cdot 1_R) = p \cdot (-1_R).$$

4. a) Sei $G = \{e, a, b\}$ mit Verknüpfung $\circ$ und neutralem Element e. Dann wissen wir

$\circ$	e	a	b
e	e	a	b
a	a	$*$	$*$
b	b	$*$	$*$

wobei die "$*$" Platzhalter für noch nicht bestimmte Einträge sind. Beachte, dass in jeder Spalte und jeder Zeile jedes Element von G genau einmal auftaucht. Andernfalls existiert (allgemein für endliche G) ein $h \in G$, das zweimal auftaucht und also $g_i, g_j, g \in G$ mit $g_i \neq g_j$ und $g_i \circ g = g_j \circ g = h$ (bzw. $g \circ g_i = g \circ g_j = h$), was absurd ist (siehe Aufgabe 2). Wir wissen also $a \circ a \in \{e, b\}$. Falls $a \circ b = b = e \circ b$, dann gilt ebenfalls wegen der Kürzungsregel $a = e$. Also ist $a \circ b = e$ und $a \circ a = b$ und somit

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

b) Die Vorgehensweise ist wie in Teilaufgabe (a). Im Folgenden sei $G = \{e, a, b, c\}$. Wir verwenden im Folgenden häufig die Kürzungsregel, welche impliziert, dass

Siehe nächstes Blatt!

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Tabelle 1 – Die Gruppentafel von $\mathbb{Z}/4\mathbb{Z}$.

$x \in G : x \circ x = x \Rightarrow x = e$ und dass in jeder Zeile und in jeder Spalte jedes Gruppenelement genau einmal auftaucht.

Eine Gruppe mit vier Elementen ist gegeben durch $(\mathbb{Z}/4\mathbb{Z}, +)$ und die zugehörige Gruppentafel ist gegeben in 1. Diese Gruppe heisst *zyklisch*. Man beachte, dass in diesem Falle die Gruppe durch $a \circ a = b$ vollständig beschrieben ist, denn daraus folgt, dass $a \circ b \in \{e, c\}$. Falls $a \circ b = e$ ist, dann folgt $a \circ c = c$ und somit $a = e$, was absurd ist. Wir wissen also $a \circ b = c$ und $a \circ c = e$. Da in jeder Spalte jedes Element genau einmal auftaucht, folgt aus $e \circ b = b$ und $a \circ b = c$, dass $b \circ b \in \{e, a\}$ ist. Falls $b \circ b = a$ ist, folgt $c \circ b = e$. Dies impliziert aber $b = a$, da die Inverse von c durch c eindeutig bestimmt ist, und das ist absurd. Also ist $b \circ b = e$ und somit $c \circ b = a$. Die Zeilen von e und a sowie die Spalten von e und b sind also vollständig bestimmt. Da in jeder Zeile jedes Element genau einmal auftaucht, reicht es, die Spalte von a zu bestimmen. Wir wissen bereits, dass $e \circ a = a$ und $a \circ a = b$, somit ist $c \circ a \in \{e, c\}$. Da $a \circ c = e$ ist, folgt $c \circ a = e$ und somit ist $b \circ a = c$ und die Spalte von a vollständig bestimmt. Dies zeigt, dass die Gruppentafel durch $a \circ a = b$ vollständig bestimmt ist.

Man beachte, dass nach Umbenennung der Elemente b und c der Fall $a \circ a$ notwendigerweise bis auf Umbenennung der Element dieselbe Gruppentafel liefert, wie der Fall $a \circ a = b$, da im Falle der zyklischen Gruppe die Annahme, dass $a \circ a \neq e$ die Gruppe vollständig beschrieben hat.

Es bleibt also, den Fall $a \circ a = e$ zu bestimmen. In diesem Falle ist $a \circ b \in \{b, c\}$ und somit $a \circ b = c$ sowie $a \circ c = b$. Die Zeile von a ist also vollständig bestimmt. Es folgt $b \circ b \in \{a, e\}$. Falls $b \circ b = a$, dann folgt $c \circ b = e = b \circ c$ und somit $c \circ c = a$. Somit sind die Spalten von e, b und c vollständig bestimmt und wir erhalten die Tafel 2. Nach Umbenennung $a \mapsto b'$, $b \mapsto c'$ und $c \mapsto a'$, sehen wir, dass dies die Tafel der zyklischen Gruppe ist.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

$\circ$	e	b'	c'	a'
e	e	b'	c'	a'
b'	b'	e	a'	c'
c'	c'	a'	b'	e
a'	a'	c'	e	b'

Tabelle 2 – Tafel, welche aus $a \circ a = e$ und $b \circ b = a$ resultiert vor und nach Umbenennung.

Bitte wenden!

Wir können also annehmen, dass $a \circ a = e$, $a \circ b = c$, $a \circ c = b$ sowie $b \circ b = e$ gelten. Daraus folgt $c \circ b = a$ und, da e, a, b somit alles nicht Inverse von c sind, schliesslich $c \circ c = e$. Es folgt $b \circ c = a$ und somit sind die Spalten von e, b, c vollständig bestimmt und wir erhalten die Tafel 3. Diese Gruppe heisst *Kleinsche Vierergruppe* und ist von der zyklischen Gruppe verschieden, da in der zyklischen Gruppe genau zwei Elemente x existieren, sodass $x \circ x = e$. Das heisst, es existiert keine Umbenennung, die die Kleinsche Vierergruppe mit der zyklischen Gruppe identifiziert.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Tabelle 3 – Tafel der Kleinschen Vierergruppe.

Es existieren also zwei Gruppen mit vier ELementen, die zyklische Gruppe, sowie die Kleinsche Vieregruppe.

c) G ist abelsch genau dann, wenn $g_i \circ g_j = g_j \circ g_i$ für alle i, j genau dann, wenn die Gruppentafel symmetrisch ist.

d) Wir führen die folgende Notation ein: Gegeben ein Winkel $\phi \in [0, 2\pi)$ bezeichne r_ϕ die Rotation der Ebene um den Mittelpunkt M um den Winkel ϕ im Gegenuhrzeigersinn. Die Menge solcher Rotationen, die das Quadrat auf sich selber abbilden, ist

$$\mathcal{R} := \left\{ r_\phi \mid \phi = \frac{k\pi}{2} \text{ für } 0 \leq k < 4 \right\}$$

Im folgenden bezeichnen wir $r := r_{\pi/2}$ und man sieht leicht, dass

$$\mathcal{R} = \{ r^k \mid 0 \leq k < 4 \}$$

wobei $r^k := \mathrm{id}$ falls $k = 0$ und $r^k := r^{k-1} \circ r$ falls $k \geq 1$. Man beachte, dass $\mathcal{R}$ bereits eine Gruppe bildet, mit neutralem Element id und Inversen $(r^k)^{-1} = r^{4-k}$. Wir bezeichnen im Gegenuhrzeigersinn mit S_k, $0 \leq k < 4$, die Symmetrieachsen des Quadrats, beginnend mit der horizontalen Symmetrieachse und wir bezeichnen mit s_k die Spiegelung der Ebene entlang der Achse S_k. Zur Vereinfachung der Notation schreiben wir $s := s_0$. Im Folgenden sei $s_n := s_k$ für $n \in \mathbb{Z}$, wobei $0 \leq k < 4$ so dass $n \sim_4 k$.

Als erstes bemerken wir drei spezielle Relationen, die wir verwenden werden, um die gewünschte Beschreibung der Gruppe D_4 zu erhalten. Zuerst überprüft man für die vier Spiegelungen explizit, dass

$$s_k = r^k s \quad \forall 0 \leq k < 4 \tag{3}$$

Siehe nächstes Blatt!

Andererseits gilt aber auch

$$s_k = r_{\pi/4}^k s r_{\pi/4}^{-k} \quad \forall k \in \mathbb{Z} \tag{4}$$

Falls $0 \leq k < 3$, dann überlegt man sich das konkret anhand des Quadrates. Andernfalls sei $k \in \mathbb{Z}$ und sei $k = 4l + n$ für $l \in \mathbb{Z}$ und $0 \leq n < 3$. Beachte, dass $r_{\pi/4}^2 = r$. Dann ist per Definition $s_k = s_n = r_{\pi/4}^n s r_{\pi/4}^{-n}$. Des Weiteren ist $r^2 s r^{-2}$ eine Rotation um Winkel π um den Nullpunkt, gefolgt von einer Spiegelung entlang der x-Achse, gefolgt von einer Rotation um π um den Nullpunkt dasselbe wie eine Spiegelung entlang der x-Achse, denn die Rotation um Winkel π ist eine Spiegelung am Nullpunkt und sendet (x, y) nach $(-x, -y)$, während die Spiegelung s den Punkt (x, y) auf $(x, -y)$ abbildet, also

$$(x, y) \overset{r^{-2}}{\mapsto} (-x, -y) \overset{s}{\mapsto} (-x, y) \overset{r^2}{\mapsto} (x, -y)$$

Also ist $r^{4l} s r^{-4l} = s$ und folglich

$$s_k = s_n = r_{\pi/4}^n s r_{\pi/4}^{-n} = r_{\pi/4}^n (r_{\pi/4}^{4l} s r_{\pi/4}^{-4l}) r_{\pi/4}^{-n} = r^k s r^{-k}$$

wie behauptet.

Wir zeigen nun, unter Verwendung dieser Relationen, dass sich jedes Element in D_4 in der Form $s^l r^k$ mit $l \in \{0, 1\}$ und $0 \leq k < 4$ schreiben lässt. Seien $0 \leq i < 4$ und $k \in \mathbb{Z}$, dann bemerken wir zuerst, dass

$$s_i r^k \overset{(3)}{=} (r^i s) r^k = r^{i+k} (r^{-k} s r^k) = r^{i+k} (r_{\pi/4}^{-2k} s r_{\pi/4}^{2k}) = r^{i+k} s_{-2k} = r^{i-k} s \tag{5}$$

Falls nun $\sigma = s_i$ oder $\sigma = r^k$, dann sind wir fertig, denn wegen $s^2 = \mathrm{id}$ und (5) hat

$$\sigma = s_i = r^i s = (s r^{-i})^{-1} \overset{(5)}{=} (r^i s)^{-1} = s r^{-i} = s r^{4-i}$$

die gewünschte Form und im Falle $\sigma = r^k$ ist nichts zu zeigen. Seien nun also $m \geq 1$ und τ_i, $1 \leq i \leq m + 1$, Rotationen und Spiegelungen. Angenommen, die Behauptung gilt für Kompositionen von m oder weniger Rotationen und Spiegelungen, dann folgt aus der Assoziativität, dass

$$\tau_{m+1} \circ \cdots \circ \tau_1 = \tau_{m+1} \circ (\tau_m \cdots \circ \tau_1) = \tau_{m+1} \circ (s^l r^k)$$

für $0 \leq k < 4$ und $l \in \{0, 1\}$. Wenn τ_{m+1} eine Spiegelung ist, dann sind wir fertig. Sei also $\tau_{m+1} = r^n$ für $0 \leq n < 4$. Falls $l = 0$, dann sind wir fertig. Andernfalls folgt

$$\tau_{m+1} \circ \cdots \circ \tau_1 = r^n s r^k \overset{(5)}{=} s r^{-n+k}$$

wie gewünscht, da $r^{-n+k} = r^{k'}$ für $0 \leq k' < 4$. Dies löst die Aufgabe. Wir zeigen zusätzlich, dass $|D_4| = 8$, d.h. dass die $s^l r^k$ tatsächlich alle verschieden sind. Angenommen $l, l' \in \{0, 1\}$ und $0 \leq k, k' < 4$ so dass $s^l r^k = s^{l'} r^{k'}$, dann ist auch $s^{l-l'} = r^{k'-k}$, und da r die Orientierung der Ebene erhält während s die Orientierung ändert, gilt $l = l'$. Es folgt $k' \sim_4 k$, und also ist $k = k'$.

e) Suchen Sie ein Gegenbeispiel, d.h. zwei Elemente $\tau, \sigma \in D_4$ so dass $\tau \circ \sigma \neq \sigma \circ \tau$.