UNIVERSITÄT HEIDELBERG
ZUKUNFT SEIT 1386

Lineare Algebra 1
Prof. Dr. R. Dahlhaus
Dr. S. Richter, N. Phandoidaen
Wintersemester 2018/2019

3. Abgabeblatt - Lösungen

Aufgabe 9	Aufgabe 10	Aufgabe 11	Aufgabe 12	Summe:

Übungsgruppe: Tutor(in):

Namen:

Aufgabe 9 (Beispiele für Ringe und Körper, 2 + 1 + 1 Punkte).
Auf $\mathbb{Z}$ definieren wir die Verknüpfungen $\oplus, \odot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ durch

$$a \oplus b := a + b - 1, \qquad a \odot b := a + b - a \cdot b.$$

Zeigen Sie:

(a) $(\mathbb{Z}, \oplus, \odot)$ ist kommutativer Ring mit 1.

(b) $(\mathbb{Z}, \oplus, \odot)$ ist nullteilerfrei, aber kein Körper.

(c) $(\mathbb{Q}, \oplus, \odot)$ ist ein Körper.
Hinweis: Die Verknüpfungen $\oplus$, $\odot$ werden wie oben angegeben auch auf $\mathbb{Q}$ definiert. Sie dürfen bereits nutzen, dass $(\mathbb{Q}, \oplus, \odot)$ ein kommutativer Ring mit 1 ist.

Lösung:

(a) Es handelt sich um einen Ring, denn:

- $\oplus$, $\odot$ sind offensichtlich abgeschlossen.
- $\oplus$ ist assoziativ, denn für $a, b, c \in \mathbb{Z}$ gilt:

  $$(a \oplus b) \oplus c = (a+b-1) \oplus c = (a+b-1)+c-1 = a+(b+c-1)-1 = a+(b \oplus c)-1 = a \oplus (b \oplus c).$$

- $\oplus$ ist kommutativ, denn für $a, b \in \mathbb{Z}$ gilt:

  $$a \oplus b = a + b - 1 = b + a - 1 = b \oplus a.$$

- Das neutrale Element bzgl. $\oplus$ ist $1 \in \mathbb{Z}$, denn: Für $a \in \mathbb{Z}$ gilt

  $$a \oplus 1 = a + 1 - 1 = a = 1 + a - 1 = 1 \oplus a.$$

- Für $a \in \mathbb{Z}$ ist das inverse Element gegeben durch $a' := -a + 2$, denn dann gilt

  $$a' \oplus a = (-a + 2) + a - 1 = 1 = a + (-a + 2) - 1 = a \oplus a'.$$

- Damit ist $(\mathbb{Z}, \oplus)$ abelsche Gruppe.
- Auch $\odot$ ist assoziativ, denn: Für $a, b, c \in \mathbb{Z}$ gilt:

$$\begin{aligned} a \odot (b \odot c) &= a \odot (b + c - b \cdot c) = a + (b + c - b \cdot c) - a \cdot (b + c - b \cdot c) \\ &= a + b + c - b \cdot c - a \cdot b - a \cdot c + a \cdot b \cdot c \\ &= (a + b - a \cdot b) + c - (a + b - a \cdot b) \cdot c \\ &= (a + b - a \cdot b) \odot c = (a \odot b) \odot c. \end{aligned}$$

- Es gelten weiter die Distributivgesetze, denn:

$$\begin{aligned} (a \oplus b) \odot c &= (a + b - 1) \odot c = (a + b - 1) + c - (a + b - 1) \cdot c \\ &= a + b + -a \cdot c - b \cdot c + 2c - 1 \\ &= (a + c - a \cdot c) + (b + c - b \cdot c) - 1 \\ &= a \odot c \oplus b \odot c, \end{aligned}$$

  analog das andere Distributivgesetz.
- $\odot$ ist kommutativ, denn für $a, b \in \mathbb{Z}$ gilt:

$$a \odot b = a + b - a \cdot b = b + a - b \cdot a = b \odot a.$$

- Es handelt sich sogar um einen Ring mit 1. Das neutrale Element der Multiplikation ist gegeben durch $0 \in \mathbb{Z}$, denn für alle $a \in \mathbb{Z}$ gilt:

$$0 \odot a = 0 + a - 0 \cdot a = a = a + 0 - a \cdot 0 = a \odot 0.$$

- Damit ist $(\mathbb{Z}, \oplus, \odot)$ ein kommutativer Ring mit 1.

(b)
- $(\mathbb{Z}, \oplus, \odot)$ ist nullteilerfrei, denn: Seien $a, b \in \mathbb{Z}$ mit $a \odot b = 1$ (beachte: 1 ist das neutrale Element bzgl. Addition!).
  $\Rightarrow a + b - a \cdot b = 1$
  $\Rightarrow (a - 1) \cdot (b - 1) = a \cdot b - a - b + 1 = 0$
  $\Rightarrow a = 1$ oder $b = 1$.
- Es gibt allerdings kein inverses Element zu $3 \in \mathbb{Z} \backslash \{1\}$, denn dann müsste es $b \in \mathbb{Z} \backslash \{1\}$ geben mit $0 = 3 \odot b = 3 + b - 3 \cdot b = 3 - 2b$, d.h. $b = \frac{3}{2} \notin \mathbb{Z}$. Daher ist $(\mathbb{Z}, \oplus, \odot)$ kein Körper.

(c) Zu $a \in \mathbb{Q} \backslash \{1\}$ ist das Inverse gegeben durch $a' := \frac{a}{a-1}$, denn:

$$a' \odot a = a' + a - a \cdot a' = \frac{a}{a-1} + a - a \cdot \frac{a}{a-1} = \frac{a + a(a-1) - a^2}{a-1} = 0.$$

(Herleitung: Gelöst werden muss die Gleichung

$$\begin{aligned} & 0 = a' \odot a = a' + a - a \cdot a' \\ \iff & 1 = a \cdot a' - a - a' + 1 = (a-1)(a'-1) \\ \iff & a' = 1 + \frac{1}{a-1} = \frac{a}{a-1}. \end{aligned}$$

)

Aufgabe 10 (Beispiele / Gegenbeispiele für Ringe, 4 = 2 + 1 + 1 Punkte).
Gegeben seien die folgenden Strukturen:

(i) $(2\mathbb{Z}, +, \cdot)$, wobei $2\mathbb{Z} := \{2 \cdot z : z \in \mathbb{Z}\}$ mit der üblichen Addition und Multiplikation,

(ii) $(S, \oplus, \circ)$, wobei $S := \{f : \mathbb{R} \to \mathbb{R} \text{ Abbildung}\}$ und für $f, g \in S$ die Abbildung $f \oplus g : \mathbb{R} \to \mathbb{R}$ definiert wird durch

$$(f \oplus g)(x) := f(x) + g(x).$$

(iii) $(\mathbb{Z}^2, \oplus, \odot)$, wobei

$$(a_1, b_1) \oplus (a_2, b_2) := (a_1 + a_2, b_1 + b_2), \qquad (a_1, b_1) \odot (a_2, b_2) := (a_1 \cdot a_2, b_1 \cdot b_2).$$

Stellen Sie jeweils fest, ob die folgenden Aussagen für die obigen Strukturen $(R, +, \cdot)$ gelten und antworten Sie mit wahr/falsch. Geben Sie im Falle von 'Wahr' *nur* die geforderten Größen an (keine weiteren Nachweise) und im Falle von 'Falsch' ein explizites Gegenbeispiel.

(a) $(R, +, \cdot)$ ist ein Ring.
Geben Sie das neutrale Element bzgl. Addition und das inverse Element bzgl. Addition für ein beliebiges $x \in R$ an.

(b) $(R, +, \cdot)$ ist ein Ring mit 1.
Geben Sie das Einselement an.

(c) $(R, +, \cdot)$ ist ein nullteilerfreier Ring.

Lösung:

(a) (i) Ist ein Ring. Neutrales Element $0_R = 0 = 2 \cdot 0 \in 2\mathbb{Z}$, denn: Für alle $x \in 2\mathbb{Z}$ gilt: $0 + x = x = x + 0$ (gewöhnliche Addition).
Inverses Element zu $z \in 2\mathbb{Z}$ ist $-z \in 2\mathbb{Z}$, denn: $z + (-z) = 0$. Es gilt $-z \in 2\mathbb{Z}$, denn: $z \in 2\mathbb{Z} \Rightarrow \exists a \in \mathbb{Z} : z = 2 \cdot a \Rightarrow -z = 2 \cdot (-a)$.

(ii) Ist kein Ring. Das Distributivgesetz wird verletzt: Im Allgemeinen gilt $f \circ (g \oplus h) \neq f \circ g \oplus f \circ h$ für $f, g, h \in S$. Konkretes Gegenbeispiel: Sei $g, h = \mathrm{id}_{\mathbb{R}}$ und $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$. Dann gilt für z.B. $x = 1$: $(f \circ (g \oplus h))(1) = f(g(1) + h(1)) = 4 \neq 2 = f(g(1)) + f(h(1)) = (f \circ g \oplus f \circ h)(1)$.

(iii) Ist ein Ring. Neutrales Element $0_R = (0, 0) \in \mathbb{Z}^2$, inverses Element zu $(a_1, b_1) \in \mathbb{Z}^2$ ist gegeben über $(-a_1, -b_1) \in \mathbb{Z}^2$.

(b) (i) Besitzt kein Einselement.
Angenommen, es gäbe ein Einselement, dann wäre $1_R \cdot z = z$ für alle $z \in 2\mathbb{Z}$.
Für $2 = 2 \cdot 1 \in 2\mathbb{Z}$ folgt: $1_R \cdot 2 = 2$, d.h. es muss $1_R = 1$ gelten. Aber $1 \notin 2\mathbb{Z}$, Widerspruch.

(ii) N.A.

(iii) Besitzt das Einselement $1_R := (1, 1) \in \mathbb{Z}^2$, denn für $(a_1, b_1) \in \mathbb{Z}^2$ gilt $(a_1, b_1) \odot (1, 1) = (a_1 \cdot 1, b_1 \cdot 1) = (a_1, b_1)$.

(c) (i) Nullteilerfrei (folgt aus Nullteilerfreiheit gewöhnliche Multiplikation)

(ii) N.A.

(iii) Nicht nullteilerfrei. Wähle z.B. $x = (1, 0)$ und $y = (0, 1)$. Dann gilt $x \odot y = (0, 0)$, aber $x \neq 0_R = (0, 0)$, $y \neq 0_R = (0, 0)$.

Aufgabe 11 (Eigenschaften von F_m, 4 = 1 + 1 + 1 + 1 Punkte).

Sei $m \in \mathbb{N}$, $m > 1$. Wie in der Vorlesung eingeführt gibt es für jedes $a \in \mathbb{Z}$ Zahlen $q, r \in \mathbb{Z}$ mit $r \in \{0, ..., m-1\}$ so dass $a = q \cdot m + r$, und man definiert $r_m(a) := r$.

Es sei $(F_m, +_m, \cdot_m)$ wie in der Vorlesung eingeführt, das heißt $F_m = \{0, ..., m-1\}$ und die Verknüpfungen sind durch

$$a +_m b := r_m(a + b), \qquad a \cdot_m b := r_m(a \cdot b),$$

gegeben. Zeigen Sie:

(a) Für $a, b \in \mathbb{Z}$ gilt:

$$r_m(r_m(a) \cdot b) = r_m(a \cdot b) = r_m(a \cdot r_m(b)) = r_m(r_m(a) \cdot r_m(b)).$$

(b) $\cdot_m$ ist assoziativ.

(c) $(F_m, +_m, \cdot_m)$ erfüllt die Distributivgesetze. Es wird nur der Nachweis eines Distributivgesetzes verlangt.

(d) $(F_m, +_m, \cdot_m)$ ist ein kommutativer Ring mit Einselement.

Hinweis: Sie dürfen für alle Aufgaben die Resultate aus Aufgabe P11 nutzen. Für (a) ist P11(a) hilfreich; für (c) die Resultate von (a) und P11(b); für (d) nutzen Sie P11(c).

Lösung: (a) Seien $a, b \in \mathbb{Z}$. Wir nutzen die Äquivalenz aus P11(a).

(i) Es gibt $q_1 \in \mathbb{Z}$ mit $a = q_1 \cdot m + r_m(a)$. Daher

$$(a \cdot b) - (r_m(a) \cdot b) = (q_1 \cdot m + r_m(a)) \cdot b - r_m(a) \cdot b = (q_1 \cdot b) \cdot m,$$

mit P11(a) folgt: $r_m(a \cdot b) = r_m(r_m(a) \cdot b)$.

(ii) (Analog:) Es gibt $q_2 \in \mathbb{Z}$ mit $b = q_2 \cdot m + r_m(b)$, daher

$$(a \cdot b) - (a \cdot r_m(b)) = a \cdot (q_1 \cdot m + r_m(a)) - a \cdot r_m(b) = (q_2 \cdot a) \cdot m,$$

mit P11(a) folgt: $r_m(a \cdot b) = r_m(a \cdot r_m(b))$.

(iii) Anwendung von (i), (ii) (hierbei wird (ii) auf $r_m(a), b$ anstelle von a, b angewandt):

$$r_m(a \cdot b) \overset{(i)}{=} r_m(r_m(a) \cdot b) \overset{(ii)}{=} r_m(r_m(a) \cdot r_m(b)).$$

(b) Seien $a, b, c \in F_m$ beliebig. Dann gilt:

$$\begin{aligned}
(a \cdot_m b) \cdot_m c &= r_m((a \cdot_m b) \cdot c) = r_m(r_m(a \cdot b) \cdot c) \overset{(a)}{=} r_m((a \cdot b) \cdot c) \\
&\overset{\text{Ass. in } \mathbb{Z}}{=} r_m(a \cdot (b \cdot c)) \overset{(a)}{=} r_m(a \cdot r_m(b \cdot c)) \\
&= r_m(a \cdot (b \cdot_m c)) = a \cdot_m (b \cdot_m c).
\end{aligned}$$

(c) Seien $a, b, c \in F_m$ beliebig. Dann gilt:

$$\begin{aligned}
(a +_m b) \cdot_m c &= r_m((a +_m b) \cdot c) = r_m(r_m(a + b) \cdot c) \overset{(a)}{=} r_m((a + b) \cdot c) \\
&\overset{\text{Distr. in } \mathbb{Z}}{=} r_m(a \cdot c + b \cdot c)) \overset{(P11(b))}{=} r_m(r_m(a \cdot c) + r_m(b \cdot c)) \\
&= r_m((a \cdot_m c) + (b \cdot_m c)) = a \cdot_m c +_m b \cdot_m c.
\end{aligned}$$

Der Beweis des zweiten Distributivgesetzes $c \cdot_m (a +_m b) = c \cdot_m a +_m c \cdot_m b$ funktioniert analog.

(d) Es wurde bereits in P11(d) gezeigt, dass $(F_m, +_m)$ eine Gruppe ist. In (c) wurde gezeigt, dass die Distributivgesetze gelten. In (b) wurde gezeigt, dass $\cdot_m$ assoziativ ist.
Es bleibt nur noch zu zeigen: $\cdot_m$ ist kommutativ und es gibt ein Einselement.

- Kommutativität von $\cdot_m$: Seien $a, b \in \mathbb{Z}$ beliebig. Dann gilt:

$$a \cdot_m b = r_m(a \cdot b) \overset{\text{Komm. in } \mathbb{Z}}{=} r_m(b \cdot a) = b \cdot_m a.$$

- Einselement: Da $m > 1$, gibt es $1 \in F_m = \{0, ..., m-1\}$. Wir weisen nach, dass $1 \in F_m$ tatsächlich das Einselement ist: Sei $a \in F_m$ beliebig. Da $a \in \{0, ..., m-1\}$, gilt $r_m(a) = a$ (*). Es folgt:

$$a \cdot_m 1 = r_m(a \cdot 1) \overset{1 \text{ neutral in } \mathbb{Z}}{=} r_m(a) \overset{(*)}{=} a \overset{(*)}{=} r_m(a) \overset{1 \text{ neutral in } \mathbb{Z}}{=} r_m(1 \cdot a) = 1 \cdot_m a.$$

Aufgabe 12 (Rechnen in F_m, 4 = 2 + 1 + 1 Punkte).

Für $m \in \mathbb{N}$, $m > 1$ sei $F_m = \{0, ..., m-1\}$ wie in der Vorlesung eingeführt. Im Folgenden schreiben wir kurz + für $+_m$ und · für $\cdot_m$. Für $x \in \mathbb{Z}$, $m \in \mathbb{N}$ definieren wir

$$x^m := \underbrace{x \cdot ... \cdot x}_{m\text{-mal}}.$$

(a) Berechnen Sie in F_5 die Ausdrücke

$$3 \cdot (4 + 2^{-1}), \qquad 3^{12345} \quad \text{und} \quad 2^p,$$

wobei $p = 7^{73}$.

(b) Sei $m \in \{5, 7\}$. Geben Sie alle $x \in F_m$ an, welche die Gleichung $x^3 = 1$ lösen.

(c) Finden Sie drei verschiedene Paare (x, y) mit $x, y \in F_9 \backslash \{0\}$, so dass $x \cdot y = 0$.

Lösung:

(a) (i) In F_5 gilt $2^{-1} = 3$, da $r_5(3 \cdot 2) = 1$. In F_5 erhalten wir damit:

$$3 \cdot (4 + 2^{-1}) = 3 \cdot (4 + 3) = 3 \cdot 2 = 1.$$

Hierbei haben wir genutzt: $r_5(4 + 3) = r_5(7) = 2$, $r_5(3 \cdot 2) = r_5(6) = 1$.

(ii) In F_5 gilt

$$3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = 4 \cdot 4 = 1,$$

da $r_5(3 \cdot 3) = r_5(9) = 4$ und $r_5(4 \cdot 4) = r_5(16) = 1$.
Es gilt $12345 = 4 \cdot q + 1$ mit einem $q \in \mathbb{Z}$ (es gilt $q = 3086$, aber das braucht man nicht hinzuschreiben). Damit folgt in F_5:

$$3^{12345} = 3^{4 \cdot q + 1} = \underbrace{3^4 \cdot ... \cdot 3^4}_{q\text{-mal}} \cdot 3 = \underbrace{1 \cdot ... \cdot 1}_{q\text{-mal}} \cdot 3 = 3.$$

(iii) In F_5 gilt $2^4 = 1$, denn $r_5(2^4) = r_5(16) = 1$.
Ansatz: Schreibe $p = 4 \cdot q + r$ mit $r \in \{0, 1, 2, 3\}$, dann gilt wie in (ii) in F_5:

$$2^p = \underbrace{2^4 \cdot ... \cdot 2^4}_{q\text{-mal}} \cdot 2^r = \underbrace{1 \cdot ... \cdot 1}_{q\text{-mal}} \cdot 2^r = 2^r.$$

Hilfsrechnung (Ansatz): Das bedeutet, wir müssen untersuchen, welchen Rest r die Zahl p beim Teilen durch 4 lässt. Dies entspricht einer Untersuchung von $p = 7^{73} = 3^{73}$ in F_4. In F_4 gilt:

$$3^2 = 1,$$

da $r_4(3^2) = r_4(9) = 1$. Es gilt $73 = 2 \cdot 36 + 1$, daher gilt in F_4:

$$p = 3^{73} = 3^{2 \cdot 36} \cdot 3 = \underbrace{3^2 \cdot \ldots \cdot 3^2}_{\text{36-mal}} \cdot 3 = 3 =: r.$$

Zurück zum Ansatz: Es folgt insgesamt in F_5:

$$2^p = 2^r = 2^3 = 4 \cdot 2 = 3,$$

denn $r_5(4 \cdot 2) = r_5(8) = 3$.

(b) Da F_m jeweils nur endlich viele Elemente besitzt, können wir einfach alle Elemente $x \in F_m$ in die Gleichung $x^3 = 1$ einsetzen, um die Lösungsmenge zu ermitteln.

- $m = 5$: In F_5 gilt:

$$\begin{aligned} 0^3 &= 0 \neq 1, \\ 1^3 &= 1, \\ 2^3 &= 4 \cdot 2 = 3 \neq 1, \\ 3^3 &= 4 \cdot 3 = 2 \neq 1, \\ 4^3 &= 1 \cdot 4 = 4 \neq 1. \end{aligned}$$

  Daher ist $x = 1$ die einzige Lösung.

- $m = 7$: In F_7 gilt:

$$\begin{aligned} 0^3 &= 0 \neq 1, \\ 1^3 &= 1, \\ 2^3 &= 4 \cdot 2 = 1, \\ 3^3 &= 2 \cdot 3 = 6 \neq 1, \\ 4^3 &= 2 \cdot 4 = 1, \\ 5^3 &= 4 \cdot 5 = 6 \neq 1, \\ 6^3 &= 1 \cdot 6 = 6 \neq 1. \end{aligned}$$

  Daher sind $x \in \{1, 2, 4\} \subseteq F_7$ Lösungen.

(c) In F_9 ist $3 \cdot 3 = 3 \cdot 6 = 6 \cdot 6 = 0$.

Abgabe:
In Zweiergruppen, bis spätestens Donnerstag, den **8. November 2018, 09:15 Uhr**.
(Die Zettelkästen für das Abgabeblatt sind im 1. OG, INF 205, vor dem Dekanat.)

Homepage der Vorlesung:
`https://ssp.math.uni-heidelberg.de/la1-ws2018/index.html`