UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

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

3. Präsenzblatt - Lösungen

Aufgabe P9 (Beispiele für Ringe und Körper).
Seien $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ und $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Es bezeichnen „+“ und „$\cdot$“ die übliche Addition und Multiplikation in $\mathbb{R}$.

$(\mathbb{Z}[\sqrt{2}], +, \cdot)$ und $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ sind kommutative Ringe mit 1.

(a) Geben Sie das neutrale Element bzgl. Addition, das inverse Element bzgl. Addition für ein beliebiges $x \in \mathbb{Z}[\sqrt{2}]$ und das Einselement in $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ an.

(b) Zeigen Sie: $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ ist kein Körper.

(c) Zeigen Sie: $(\mathbb{Q}[\sqrt{2}], +, \cdot)$ ist ein Körper.

Lösung: (a) Das neutrale Element ist $0 = 0 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, denn für beliebiges $x \in \mathbb{Z}[\sqrt{2}]$ gilt:

$$x + 0 = x = 0 + x$$

Das Einselement ist gegeben durch $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, denn für beliebiges $x \in \mathbb{Z}[\sqrt{2}]$ gilt:

$$1 \cdot x = x = x \cdot 1.$$

Das additiv inverse Element zu $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ ist gegeben durch $-x = -a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, denn:

$$x + (-x) = 0 = (-x) + x.$$

(b) Es handelt sich bei $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ um *keinen* Körper, da inverse Elemente in $(\mathbb{Z}[\sqrt{2}] \setminus \{0\}, \cdot)$ fehlen.
Angenommen es existiert ein inverses Element zu $2 = 2 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Dann gäbe es $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ mit:

$$1 = (2 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = 2a + 2b\sqrt{2}. \qquad (*)$$

Wäre $b \neq 0$, so würde aus (*) folgen:

$$\frac{1 - 2a}{2b} = \sqrt{2},$$

Widerspruch zu $\frac{1-2a}{2b} \in \mathbb{Q}$. Daher muss $b = 0$ gelten. Aus (*) folgt:

$$b = 0, \qquad 1 = 2a.$$

Die einzige Lösung ist $a = \frac{1}{2}$, $b = 0$, d.h. das inverse Element hätte die Form $\frac{1}{2} + 0\sqrt{2}$. Aber $\frac{1}{2} \notin \mathbb{Z}$, Widerspruch.

(c) Zum Körper fehlt nur noch die Existenz des inversen Elements bzgl. der Multiplikation. Sei $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \setminus \{0\}$.
Herleitung (muss nicht Bestandteil der Lösung sein): Suche $c, d \in \mathbb{Q}$ mit

$$\begin{aligned} 1 &= (a + b\sqrt{2})(c + d\sqrt{2}) \\ &= (ac + 2bd) + \sqrt{2}(bc + ad). \end{aligned}$$

Wegen $1 = 1 + 0\sqrt{2}$ muss folgendes Gleichungssystem in c, d gelöst werden:

$$(I) \quad 1 = ac + 2bd, \qquad (II) \quad 0 = bc + ad.$$

Addition von (II) $(-\frac{a}{b})$-mal auf (I) liefert:

$$1 = ac + 2bd + (-\frac{a}{b})(bc + ad) = d \cdot \Big(2b - \frac{a^2}{b}\Big) = d \cdot \Big(\frac{2b^2 - a^2}{b}\Big),$$

d.h. $d = -\frac{b}{a^2 - 2b^2}$. Durch Einsetzen in (I) erhält man $c = \frac{a}{a^2 - 2b^2}$.
Start geforderte Lösung: Dann ist das inverse Element gegeben über

$$c + d\sqrt{2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Es gilt stets $a^2 - 2b^2 \neq 0$ (würde Gleichheit gelten, wäre $a = \pm\sqrt{2}b$ und damit entweder a oder b nicht in $\mathbb{Q}$). Daher gilt $c, d \in \mathbb{Q}$. Weiter gilt

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (a + b\sqrt{2}) \cdot \Big(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}\Big) = ... = 1.$$

(wegen Kommutativität von $\cdot$ ist dann auch $(c + d\sqrt{2}) \cdot (a + b\sqrt{2}) = 1$ klar). Damit ist $(\mathbb{Q}, +, \cdot)$ ein Körper.

Aufgabe P10 (Beispiele / Gegenbeispiele für Ringe).
Gegeben seien die folgenden Strukturen $(R, +, \cdot)$:

(i) $(S, +, \cdot)$, wobei $S := \{\frac{a}{2^i} : a \in \mathbb{Z}, i \in \mathbb{N}\}$ mit der üblichen Addition und Multiplikation,

(ii) $(F_6, +_6, \cdot_6)$,

(iii) $(F_{13}, +_{13}, \cdot_{13})$,

(iv) $(S, \oplus, \odot)$, wobei $S := \{f : \mathbb{R} \to \mathbb{R} \text{ Abbildung}\}$ und für $f, g \in S$ die Abbildungen $f \oplus g, f \odot g : \mathbb{R} \to \mathbb{R}$ definiert werden durch

$$(f \oplus g)(x) := f(x) + g(x), \qquad (f \odot g)(x) := f(x) \cdot g(x)$$

(v) $(\mathbb{R}^2, \oplus, \odot)$, wobei

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

(vi) $(S, \Delta, \cap)$, wobei $S := \{A \subset \mathcal{P}(\mathbb{N}) : A \text{ endlich}\}$, $A\Delta B := (A \backslash B) \cup (B \backslash A)$. *Hinweis: Dies ist ein Ring.*

(vii) $(\mathbb{R}\backslash\{-1\}, \oplus, \cdot)$, wobei $a \oplus b := a + b + a \cdot b$ und „$\cdot$“ die übliche Multiplikation.

Gelten die folgenden Aussagen für die obigen Strukturen $(R, +, \cdot)$? Beantworten Sie die Fragen jeweils mit Ja/Nein. Geben Sie im Falle von 'Ja' *nur* die geforderten Größen an (keine weiteren Nachweise) und im Falle von 'Nein' 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.

(d) $(R, +, \cdot)$ ist ein Körper.

Lösung:

(a) (i) Ist ein Ring. Alle Eigenschaften (Assoziativität, Kommutativität) vererben sich von der Addition / Multiplikation in $\mathbb{R}$. Es ist nur zu zeigen, dass die Addition / Multiplikation abgeschlossen in S sind. Neutrales Element $0 = \frac{0}{2^1} \in S$, additiv inverses Element zu $\frac{a}{2^i} \in S$ ist $\frac{(-a)}{2^i} \in S$.

(ii) Ist ein Ring. Wird in Aufgabe 11 gezeigt bzw. bekannt aus Vorlesung. Neutrales Element ist $0 \in F_6$, das additiv inverse ist in P11 berechnet worden.

(iii) Ist ein Ring. Wird in Aufgabe 11 gezeigt bzw. bekannt aus Vorlesung. Neutrales Element ist $0 \in F_6$, das additiv inverse ist in P11 berechnet worden.

(iv) Ist ein Ring. Alle Eigenschaften (Assoziativität, Kommutativität) vererben sich von der Addition / Multiplikation in $\mathbb{R}$. Neutrales Element ist $f : \mathbb{R} \to \mathbb{R}, f(x) = 0$, additiv inverses Element zu $f \in S$ ist $f' : \mathbb{R} \to \mathbb{R}, f'(x) = -f(x)$.

(v) Ist ein Ring. Alle Eigenschaften (Assoziativität, Kommutativität) vererben sich von der Addition / Multiplikation in $\mathbb{R}$. Neutrales Element ist $(0, 0) \in \mathbb{R}^2$, additiv inverses Element zu $(a, b) \in \mathbb{R}^2$ ist $(-a, -b) \in \mathbb{R}^2$.

(vi) Dies ist ein Ring. Neutrales Element ist $\emptyset \in S$. Additiv inverses Element zu $A \in S$ ist $A \in S$ selbst.

(vii) Dies ist kein Ring, denn zum Beispiel sind die Distributivgesetze verletzt. Es gilt zum Beispiel $(1 \oplus 1) \cdot 2 = (1+1+1 \cdot 1) \cdot 2 = 6$, aber $1 \cdot 2 \oplus 1 \cdot 2 = 2 \oplus 2 = 2+2+2 \cdot 2 = 8$.

(b) (i) Ist ein Ring mit 1, denn $1 = \frac{2}{2^1} \in S$ ist das Einselement.

(ii) Ist ein Ring mit 1. Das Einselement ist $1 \in F_6$.

(iii) Ist ein Ring mit 1. Das Einelement ist $1 \in F_{13}$.

(iv) Ist ein Ring mit 1. Die Abbildung $e : \mathbb{R} \to \mathbb{R}, x \mapsto 1$ ist das Einselement.

(v) Ist ein Ring mit 1. Das Einselement ist $(1, 1) \in \mathbb{R}^2$. Für $(a_1, b_1) \in \mathbb{R}^2$ gilt $(a_1, b_1) \odot (1, 1) = a_1, b_1)$.

(vi) Ist kein Ring mit 1. Angenommen es gäbe ein Einselement $E \in S$. Dann müsste für alle $A \in S$ gelten: $A \cap E = A$ (*). Wähle nacheinander $A = \{n\}$, $n \in \mathbb{N}$, so folgt aus (*) jeweils $n \in E$. Damit muss aber $\mathbb{N} \subset E$ gelten. Damit ist E nicht endlich, d.h. $E \notin S$, Widerspruch.

(vii) NA.

(c) (i) Ist nullteilerfrei. Für $x, y \in S$ folgt aus $x \cdot y = 0$ direkt $x = 0$ oder $y = 0$ (Eigenschaft der Multiplikation in $\mathbb{R}$).

(ii) Ist nicht nullteilerfrei. Es gilt $2 \cdot 3 = 0$ in F_6.

(iii) Ist nullteilerfrei. Folgt aus der Vorlesung, da 13 Primzahl.

(iv) Ist nicht nullteilerfrei. Definiere

$$f : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 1, & \text{für } x = 0, \\ 0, & \text{sonst} \end{cases} \qquad \text{und} \qquad g : \mathbb{R} \to \mathbb{R}, x \mapsto \begin{cases} 0, & \text{für } x = 0, \\ 1, & \text{sonst.} \end{cases}$$

Dann sind $f, g \neq 0$, aber $f \cdot g = 0$

(v) Ist nicht nullteilerfrei. Wähle z.B. $x = (1, 0)$ und $y = (0, 1)$. Dann gilt $x \odot y = (0, 0)$.

(vi) Ist nicht nullteilerfrei. Wähle zum Beispiel $A = \{1\} \in S$, $B = \{2\} \in S$, dann gilt $A \cap B = \emptyset$, aber $A \neq \emptyset \neq B$.

(vii) NA

(d) (i) Ist kein Körper, denn zum Beispiel besitzt $x = \frac{7}{2^3} \in S$ kein inverses Element. Gäbe es ein inverses Element $y = \frac{a}{2^i} \in S$ (mit $a \in \mathbb{Z}$, $i \in \mathbb{N}$), so wäre
$1 = x \cdot y = \frac{7}{2^3} \cdot \frac{a}{2^i} = \frac{7a}{2^{3+i}}$
$\Rightarrow 7 \cdot a = 2^{3+i}$
Diese Gleichung wird für kein $a \in \mathbb{Z}$ erfüllt, denn die rechte Seite ist nicht durch 7 teilbar.

(ii) Ist kein Körper. Wäre F_6 ein Körper, so müsste F_6 nullteilerfrei sein.

(iii) Ist ein Körper. Dies folgt aus der Vorlesung, da 13 eine Primzahl ist.

(iv) Ist kein Körper, da nicht nullteilerfrei.

(v) Ist kein Körper, da nicht nullteilerfrei.

(vi) Ist kein Körper, da nicht nullteilerfrei.

(vii) NA

Aufgabe P11 (Eigenschaften von F_m).

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:

$$r_m(a) = r_m(b) \quad \Longleftrightarrow \quad \exists s \in \mathbb{Z} : a - b = s \cdot m.$$

(b) Für $a, b \in \mathbb{Z}$ gilt:

$$r_m(r_m(a) + b) = r_m(a + b) = r_m(a + r_m(b)) = r_m(r_m(a) + r_m(b)).$$

(c) $(F_m, +_m)$ ist eine Gruppe.

Lösung: (a) „⇒“: Seien $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ mit $r_1, r_2 \in \{0, ..., m-1\}$, so dass

$$a = q_1 \cdot m + r_1, \qquad b = q_2 \cdot m + r_2.$$

Voraussetzung $\Rightarrow r_1 = r_m(a) = r_m(b) = r_2$
$\Rightarrow a - b = (q_1 \cdot m + r_1) - (q_2 \cdot m + r_2) = (q_1 - q_2) \cdot m.$
Mit der Definition $s := q_1 - q_2$ folgt die Behauptung.
„⇐“: Es gebe $s \in \mathbb{Z}$ mit $a - b = s \cdot m$. Es sei $q_2 \in \mathbb{Z}$ so dass $b = q_2 \cdot m + r_m(b)$.
$\Rightarrow a = b + s \cdot m = (q_2 + s) \cdot m + r_m(b)$
$\Rightarrow r_m(a) = r_m(b)$.

(b) Wir nutzen die Äquivalenz aus (a).

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

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

  mit (a) folgt: $r_m(a + b) = r_m(r_m(a) + b)$.
- Die Gleichheit $r_m(a + b) = r_m(a + r_m(b))$ folgt analog.
- Anwendung der zweiten Gleichung auf die erste Gleichung (beachte: $r_m(a) \in \mathbb{Z}$) liefert

$$r_m(a + b) = r_m(r_m(a) + b) = r_m(r_m(a) + r_m(b)).$$

(c) Es ist zu zeigen: $(F_m, +_m)$ besitzt als Gruppe ein neutrales Element, ein inverses Element und die Verknüpfung ist assoziativ.

- Assoziativität: Seien $a, b, c \in F_m$ beliebig. Dann gilt:

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

- Das neutrale Element in $(F_m, +_m)$ ist $0 \in F_m$, denn: Sei $a \in F_m$ beliebig. Dann gilt $r_m(a) = a$ wegen $a \in F_m = \{0, ..., m-1\}$. Daher

$$a +_m 0 = r_m(a+0) \overset{0 \text{ neutr. El. in } \mathbb{Z}}{=} r_m(a) = a = r_m(a) \overset{0 \text{ neutr. El. in } \mathbb{Z}}{=} r_m(0+a) = 0 +_m a.$$

- Das inverse Element in $(F_m, +_m)$ zu $a \in F_m$ ist

$$a' := \begin{cases} m - a, a \neq 0, \\ 0, \qquad\qquad a = 0 \end{cases},$$

  denn: Fall 1 $a \neq 0$: Dann ist $r_m(m) = 0$ und daher

$$\begin{aligned}
a +_m a' &= r_m(a + a') = r_m(a + (m - a)) = r_m(m) = 0 = r_m(m) \\
&= r_m((m - a) + a) = r_m(a' + a) = a' +_m a.
\end{aligned}$$

  Fall 2: $a = 0$: Dann ist $a +_m a' = r_m(a+a') = r_m(0+0) = r_m(0) = 0 = ... = a' +_m a$.

Aufgabe P12 (Rechnen in F_m).

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_7 die Ausdrücke

$$4 \cdot (3^{-1} + 4), \qquad 2^{9568} \quad \text{und} \quad 3^p,$$

wobei $p = 5^{45}$.

(b) Sei $m \in \{7, 8\}$. Geben Sie alle $x \in F_m$ an, welche jeweils die Gleichungen $x^2 = 4$ und $4 \cdot x = 6$ lösen.

(c) Zeigen Sie, dass keine ganzzahligen Lösungen $x, y, z \in \mathbb{Z}$ mit $z > 1$ der Gleichung $x^2 + y^2 = 10^z - 1$ existieren.
Hinweis: Wenden Sie auf beiden Seiten der Gleichung $r_4(\cdot)$ an und untersuchen Sie die möglichen Werte der linken und der rechten Seite der Gleichung.

Lösung:

(i) In F_7 gilt $3^{-1} = 5$, da $r_7(3 \cdot 5) = 1$. In F_7 erhalten wir damit:

$$4 \cdot (3^{-1} + 4) = 4 \cdot (5 + 4) = 4 \cdot 2 = 1.$$

Hierbei haben wir genutzt: $r_7(5 + 4) = r_7(9) = 2$, $r_7(4 \cdot 2) = r_7(8) = 1$.

(ii) In F_7 gilt

$$2^3 = 2 \cdot 2 \cdot 2 = 4 \cdot 2 = 1,$$

da $r_7(4 \cdot 2) = r_7(8) = 1$.
Es gilt $9568 = 3 \cdot q + 1$ mit einem $q \in \mathbb{Z}$. Damit folgt in F_7:

$$2^{9568} = 2^{3 \cdot q + 1} = \underbrace{2^3 \cdot \ldots \cdot 2^3}_{q\text{-mal}} \cdot 2 = \underbrace{1 \cdot \ldots \cdot 1}_{q\text{-mal}} \cdot 2 = 2.$$

(iii) In F_7 gilt $3^6 = 1$, denn $r_7(3^6) = r_7(729) = 1$ (Wegen $729 = 700 + 28 + 1$).
Ansatz: Schreibe $p = 6 \cdot q + r$ mit $r \in \{0, 1, 2, 3, 4, 5\}$, dann gilt wie in (ii) in F_7:

$$3^p = \underbrace{3^6 \cdot \ldots \cdot 3^6}_{q\text{-mal}} \cdot 3^r = \underbrace{1 \cdot \ldots \cdot 1}_{q\text{-mal}} \cdot 3^r = 3^r.$$

Hilfsrechnung (Ansatz): Das bedeutet, wir müssen untersuchen, welchen Rest r die Zahl p beim Teilen durch 6 lässt. Dies entspricht einer Untersuchung von $p = 5^{45}$ in F_6. In F_6 gilt:

$$5^2 = 1,$$

da $r_6(5^2) = r_6(25) = 1$. Es gilt $45 = 2 \cdot 22 + 1$, daher gilt in F_6:

$$p = 5^{45} = 5^{2 \cdot 22} \cdot 5 = \underbrace{5^2 \cdot \ldots \cdot 5^2}_{22\text{-mal}} \cdot 5 = 5 =: r.$$

Zurück zum Ansatz: Es folgt insgesamt in F_7:

$$3^p = 3^r = 3^5 = 2 \cdot 2 \cdot 3 = 5,$$

denn $r_7(3 \cdot 3) = r_7(9) = 2$.

(iv) Da F_m jeweils nur endlich viele Elemente besitzt, können wir einfach alle Elemente $x \in F_m$ in die Gleichungen einsetzen, um die Lösungsmenge zu ermitteln.

Wir betrachten zuerst $m = 7$. In F_7 gilt

- $0^2 = 0$,
  $1^2 = 1$,
  $2^2 = 4$,
  $3^2 = 2$,
  $4^2 = 2$,
  $5^2 = 4$,
  $6^2 = 1$.
  Damit sind $x \in \{2, 5\}$ Lösungen von $x^2 = 4$.
- $4 \cdot 0 = 0$,
  $4 \cdot 1 = 4$,
  $4 \cdot 2 = 1$,
  $4 \cdot 3 = 5$,
  $4 \cdot 4 = 2$,
  $4 \cdot 5 = 6$,
  $4 \cdot 6 = 3$.
  Damit ist $x = 5$ die einzige Lösung von $4x = 6$.

Wir betrachten nun $m = 8$. In F_8 gilt

- $0^2 = 0$,
  $1^2 = 1$,
  $2^2 = 4$,
  $3^2 = 1$,
  $4^2 = 0$,
  $5^2 = 1$,
  $6^2 = 4$,
  $7^2 = 1$.
  Damit ist $x \in \{2, 6\}$ Lösungen von $x^2 = 4$.
- $4 \cdot 0 = 0$,
  $4 \cdot 1 = 4$,
  $4 \cdot 2 = 0$,
  $4 \cdot 3 = 4$,
  $4 \cdot 4 = 0$,
  $4 \cdot 5 = 4$,
  $4 \cdot 6 = 0$.
  $4 \cdot 7 = 4$.
  Damit besitzt die Gleichung $4x = 6$ keine Lösungen.

(v) Gäbe es Lösungen $x, y, z \in \mathbb{Z}$ mit $z > 1$, so wäre auch

$$r_4(x^2 + y^2) = r_4(10^z - 1) \quad (*)$$

Wir bestimmen zuerst, dass $r_4(x^2) \in \{0, 1\}$ für beliebiges $x \in \mathbb{Z}$.

Fall x gerade: Sei $k \in \mathbb{Z}$, also $x = 2k$. $\Rightarrow x^2 = 4k^2 \Rightarrow r_4(4 \cdot k^2) r_4(4) \cdot r_4(k^2) = 0 \cdot r_4(k^2) = 0$.

Fall x ungerade: Sei $k \in \mathbb{Z}$, also $x = 2k + 1 \Rightarrow x^2 = 4(k^2 + k) + 1 \Rightarrow r_4(4(k^2 + k) + 1) = r_4(4) \cdot r_4(k^2 + k) + r_4(1) = 1$.

Damit gilt $r_4(x^2 + y^2) \in \{0, 1, 2\}$.

Andererseits ist $r_4(10^z-1) = r_4(10^2 \cdot 10^{z-2}-1) = r_4(10^2) \cdot r_4(10^{z-2}) - r_4(1) = r_4(-1) = 3$, d.h. $r_4(10^z - 1) \in \{3\}$.

Damit gilt aber in (*):

$$\{0, 1, 2\} \ni r_4(x^2 + y^2) = r_4(10^z - 1) = 3,$$

Widerspruch.

Dieses Blatt ist **nicht abzugeben** und wird in den Übungsgruppen besprochen.

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