D-MATH
Dr. Menny Akka Ginosar
Paula Truöl

HS 2020
ETH Zürich

Lösungen zu Serie 4

Gruppen, Ringe, Körper

Hinweis: Punkte können Sie in den Aufgaben 1, 2(a)-(e) und 5(b) bekommen. Wir erwarten, dass Sie nicht nur diese Aufgaben bearbeiten, sondern versuchen, die ganze Serie zu lösen. Eine Ausnahme bilden die Aufgaben, die mit (★) deklariert sind. Diese Markierung bedeutet, dass diese Aufgaben zum Spaß gedacht sind.

1. (Repetition) Sei $E = \{u + sv + tw \mid s, t \in \mathbb{R}\}$ für $u, v, w \in \mathbb{R}^n$ eine Ebene im n-dimensionalen Raum $\mathbb{R}^n$ und sei $u' \in E$. Zeigen Sie, dass $E = \{u' + sv + tw \mid s, t \in \mathbb{R}\}$ gilt, indem sie die beiden Inklusionen „ $\subseteq$ “ und „ $\supseteq$ “ zeigen. Um Punkte zu bekommen, müssen Sie diesen Beweis formal sauber aufschreiben. (2)

   Lösung:

   Behauptung: Sei $E' := \{u' + s'v + t'w \mid s', t' \in \mathbb{R}\}$. Dann gilt $E = E'$.

   Proof. Wir zeigen $E \subseteq E'$ und $E \supseteq E'$.
   Zunächst bemerken wir noch, dass es wegen $u' \in E$ (feste) $s_0, t_0 \in \mathbb{R}$ gibt, sodass $u' = u + s_0v + t_0w \quad (*)$.
   Wir beginnen mit $E \subseteq E'$. Sei $x = u + sv + tw \in E$ für $s, t \in \mathbb{R}$. Wegen $(*)$ gilt $u = u' - s_0v - t_0w$ und damit $x = u + sv + tw = u' - s_0v - t_0w + sv + tw = u' + (s - s_0)v + (t - t_0)w$. Somit ist $x = u' + s'v + t'w$ für $s' = s - s_0, t' = t - t_0 \in \mathbb{R}$, also $x \in E'$. Da wir $x \in E$ beliebig gewählt hatten, folgt $E \subseteq E'$.
   Bleibt noch $E' \subseteq E$ zu zeigen. Sei dazu $x = u' + s'v + t' \in E'$ für $s', t' \in \mathbb{R}$. Wegen $(*)$ gilt dann $x = u + s_0v + t_0w + s'v + t' = u + (s_0 + s')v + (t_0 + t')w$ mit $s_0 + s', t_0 + t' \in R$, also $x \in E$ und somit $E' \subseteq E$. □

2. In dieser Aufgabe können Sie je zwei Punkte in den Teilaufgaben (a)-(e) bekommen. (10)

   (a) Sei $(G, \circ)$ eine Gruppe und seien $a, b, c \in G$. Zeigen Sie $b = c \Leftrightarrow a \circ b = a \circ c$.

   Lösung:

   “⇒”: Es ist klar, dass $b = c \Rightarrow a \circ b = a \circ c$.

   “⇐”: Es gelte $a \circ b = a \circ c$. Da G eine Gruppe ist, existiert $x \in G$ mit $x \circ a = e$ (ein (links-)inverses Element von a), wobei e das neutrale Element ist. Also gilt wegen der Assoziativität der Verknüpfung $\circ$, dass

   $$\begin{aligned} b =& e \circ b = (x \circ a) \circ b = x \circ (a \circ b) \\ =& x \circ (a \circ c) = (x \circ a) \circ c = e \circ c = c. \end{aligned}$$

   (b) Seien $(G, \circ), (H, \triangle)$ Gruppen. Zeigen Sie, dass $G \times H$ mit der Verknüpfung

   $$(g_1, h_1) \star (g_2, h_2) := (g_1 \circ g_2, h_1 \triangle h_2) \qquad \text{für alle } g_1, g_2 \in G, h_1, h_2 \in H$$

   eine Gruppe ist.

   Lösung:
   Wir überprüfen die Gruppenaxiome. Seien $(g_1, h_1), (g_2, h_2), (g_3, h_3) \in G \times H$. Dann gilt wegen der Assoziativität in G bzw. H

   $$\begin{aligned} \big((g_1, h_1) \star (g_2, h_2)\big) \star (g_3, h_3) &= (g_1 \circ g_2, h_1 \triangle h_2) \star (g_3, h_3) = \big((g_1 \circ g_2) \circ g_3, (h_1 \triangle h_2) \triangle h_3\big) \\ &= \big(g_1 \circ (g_2 \circ g_3), h_1 \triangle (h_2 \triangle h_3)\big) = (g_1, h_1) \star \big(g_2 \circ g_3, h_2 \triangle h_3\big) \\ &= (g_1, h_1) \star \big((g_2, h_2) \star (g_3, h_3)\big). \end{aligned}$$

Wir behaupten, dass (e_G, e_H) das neutrale Element in $G \times H$ ist, wobei e_G das neutrale Element in G, e_H das neutrale Element in H bezeichne. Sei dazu $(g, h) \in G \times H$. Dann gilt

$$(e_G, e_H) \star (g, h) = (e_G \circ g, e_H \triangle h) = (g, h).$$

Sei nun $(g, h) \in G \times H$ und seien $g^{-1} \in G$ und $h^{-1} \in H$ die Inversen von g beziehungsweise h. Dann ist (g^{-1}, h^{-1}) das inverse Element von (g, h), denn es gilt

$$(g^{-1}, h^{-1}) \star (g, h) = (g^{-1} \circ g, h^{-1} \triangle h) = (e_G, e_H).$$

(c) Zeigen Sie, dass die Gruppe $\mathbb{Z}/6\mathbb{Z}$ isomorph ist zur Gruppe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Lösung:

Wir schreiben $[n]_m$ für die Restklasse von $n \in \mathbb{Z}$ in $\mathbb{Z}/m\mathbb{Z}$. Die Abbildung $\varphi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, $\varphi([n]_6) := ([n]_2, [n]_3)$ ist dann wohldefiniert. Denn seien $n, n' \in \mathbb{Z}$ mit $[n]_6 = [n']_6$. Dann existiert $k \in \mathbb{Z}$ mit $n = n' + 6k$, also gilt auch $n = n' + 2 \cdot (3k)$, also $[n]_2 = [n']_2$ und $n = n' + 3 \cdot (2k)$, also $[n]_3 = [n']_3$, und damit $\varphi([n]_6) = \varphi([n']_6)$.

Um zu zeigen, dass φ ein Gruppenhomomorphismus ist seien $[n]_6, [n']_6 \in \mathbb{Z}/6\mathbb{Z}$. Dann ist

$$\begin{aligned}\varphi([n]_6 + [n']_6) &= \varphi([n + n']_6) = ([n + n']_2, [n + n']_3) \\ &\overset{b)}{=} ([n]_2, [n]_3) + ([n']_2, [n']_3) = \varphi([n]_6) + \varphi([n']_6)\end{aligned}$$

per Definition von φ und der Addition in $\mathbb{Z}/m\mathbb{Z}$. Die Abbildung φ hätten wir auch allgemeiner als $\varphi\colon \mathbb{Z}/(mn)\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}, \varphi([k]_{mn}) := ([k]_m, [k]_n)$ für $m, n \in \mathbb{Z}$ definieren können. Diese Abbildung ist immer ein wohldefinierter Gruppenhomomorphismus, aber nicht immer bijektiv (Bonusaufgabe: überlegen Sie, welche Bedingung für m, n gelten muss, damit die Abbildung bijektiv ist). Um die Bijektivität unserer expliziten Abbildung $\varphi\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ zu zeigen, genügt es genau hinzusehen, welche Elemente wie abgebildet werden. Es gilt

$$\begin{aligned}\varphi\colon [0]_6 &\mapsto ([0]_2, [0]_3), \\ [1]_6 &\mapsto ([1]_2, [1]_3), \\ [2]_6 &\mapsto ([0]_2, [2]_3), \\ [3]_6 &\mapsto ([1]_2, [0]_3), \\ [4]_6 &\mapsto ([0]_2, [1]_3), \\ [5]_6 &\mapsto ([1]_2, [2]_3),\end{aligned}$$

somit ist φ bijektiv, also ein Isomorphismus.

(d) Die *Ordnung* $|G|$ einer Gruppe G ist definiert als die Mächtigkeit der Gruppe. Für eine *endliche Gruppe*, d.h. eine Gruppe mit $|G| < \infty$ ist die Ordnung also einfach die Anzahl der Elemente von G. Die *Ordnung* $\operatorname{ord}(a)$ eines Element $a \in G$ ist die kleinste Zahl $k \in \mathbb{N}$, so dass $a^k = e$, wobei $e \in G$ das neutrale Element ist. Wir schreiben $\operatorname{ord}(a) = \infty$, wenn $a^k \neq e$ für alle $k \in \mathbb{N}$.
Seien nun $(G, \circ), (H, \triangle)$ Gruppen und sei $\varphi\colon G \to H$ ein Gruppenisomorphismus. Zeigen Sie $\operatorname{ord}(\varphi(a)) = \operatorname{ord}(a)$ für alle $a \in G$.

Tipp: Benutzen Sie, dass φ das neutrale Element von G auf das neutrale Element von H abbildet.

Lösung:

Sei $a \in G$. Es gilt $\varphi(a^k) = (\varphi(a))^k$ für alle $k \in \mathbb{N}$. Falls $\operatorname{ord}(a) = \infty$ so gilt $a^k \neq e$ für alle $k \in \mathbb{N}$ und damit $(\varphi(a))^k = \varphi(a^k) \neq e$ für alle $k \in \mathbb{N}$, da φ injektiv ist. Folglich ist dann auch $\operatorname{ord}(\varphi(a)) = \infty$.
Ist nun $k = \operatorname{ord}(a) \in \mathbb{N}$, dann gilt $a^k = e$ also $e = (\varphi(a))^k$ und damit folgt $\operatorname{ord}(\varphi(a)) \leq k = \operatorname{ord}(a)$. Sein nun $\operatorname{ord}(\varphi(a)) = l$. Dann gilt $e = (\varphi(a))^l = \varphi(a^l)$. Da φ injektiv ist, folgt $a^l = e$, also auch $\operatorname{ord}(a) \leq l = \operatorname{ord}(\varphi(a))$. Es folgt $\operatorname{ord}(\varphi(a)) \leq \operatorname{ord}(a) \leq \operatorname{ord}(\varphi(a))$, also die Behauptung.

(e) Zeigen Sie, dass die zwei Gruppen $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ nicht isomorph sind.

Lösung:

Es ist $\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ und man überzeugt sich leicht, dass $\text{ord}(\overline{1}) = 4$. Allerdings gibt es in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\}$ kein Element der Ordnung 4, denn $\text{ord}((\overline{1}, \overline{1})) = 2$ und $\text{ord}((\overline{1}, \overline{0})) = \text{ord}((\overline{0}, \overline{1})) = 2$. Wegen der Aussage aus Teilaufgabe (d) kann es also keinen Gruppenisomorphismus $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ geben.

(f) Finden Sie einen surjektiven Homomorphismus $\mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$. Allgemeiner, seien $m, n \in \mathbb{N}$ mit $m|n$ (m *„teilt" n*, d.h. es existiert $d \in \mathbb{N}$ mit $n = dm$). Finden Sie dann einen surjektiven Homomorphismus $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Lösung:

Wir zeigen nur die allgemeine Aussage, der Spezialfall folgt dann aus $2|4$, denn $4 = 2 \cdot 2$. Wir benutzen die Notation aus (c) und setzen $\varphi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \varphi([k]_n) := [k]_m$. Dann ist φ wohldefiniert. Denn seien $k, k' \in \mathbb{Z}$ mit $[k]_n = [k']_n$, dann existiert $l \in \mathbb{Z}$ mit $k = k' + nl$. Nach Voraussetzung existiert $d \in \mathbb{N}$ mit $n = dm$, also gilt auch $k = k' + m \cdot (dl)$, also $[k]_m = [k']_m$ und somit $\varphi([k]_n) = \varphi([k']_n)$. Nun ist φ ein Gruppenhomomorphismus, denn für $[k]_n, [k']_n \in \mathbb{Z}/n\mathbb{Z}$ gilt

$$\varphi([k]_n + [k']_n) = \varphi([k + k']_n) = [k + k']_m = [k]_m + [k']_m = \varphi([k]_n) + \varphi([k']_n),$$

nach Definition von φ und der Addition in $\mathbb{Z}/n\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z}$. Außerdem ist φ surjektiv, denn für beliebiges $[k]_m \in \mathbb{Z}/m\mathbb{Z}$ mit $k \in \mathbb{Z}$ ist $\varphi([k]_n) = [k]_m$.

(g) Zeigen Sie, dass es weder einen surjektiven Homomorphismus $\mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ gibt noch einen surjektiven Homomorphismus $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$.

Lösung:

Angenommen, es gäbe einen surjektiven Gruppenhomomorphismus $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$. Dann gilt $\varphi(\overline{0}) = \overline{0}$, denn ein Gruppenhomomrphismus schickt immer das neutrale Element auf das neutrale Element. Falls $\varphi(\overline{1}) = \overline{0}$ ist, dann ist φ nicht surjektiv ($\overline{1}, \overline{2}$ wären nicht im Bild von φ), aber auch falls $\varphi(\overline{1}) \in \{\overline{1}, \overline{2}\}$ ist, dann ist φ nicht surjektiv (denn dann ist $\overline{2}$ bzw. $\overline{1}$ nicht im Bild von φ.
Nehmen wir nun an, dass $\varphi\colon \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ ein surjektiver Gruppenhomomorphismus ist. Dann ist $\varphi(\overline{1}) \in \{\overline{0}, \overline{1}\}$. Falls $\varphi(\overline{1}) = \overline{0}$ ist, dann gilt $\varphi(\overline{2}) = \varphi(\overline{1} + \overline{1}) = \overline{0} + \overline{0} = \overline{0}$, da φ ein Gruppenhomomorphismus ist, also ist $\varphi(\overline{n}) = \overline{0}$ für alle $\overline{n} \in \mathbb{Z}/3\mathbb{Z}$ und somit nicht surjektiv. Falls $\varphi(\overline{1}) = \overline{1}$ ist, dann folgt $\overline{0} = \varphi(\overline{0}) = \varphi(\overline{1} + \overline{1} + \overline{1}) = \overline{1} + \overline{1} + \overline{1} = \overline{1} \neq \overline{0}$, ein Widerspruch.

3. Betrachten Sie die Gruppe $S_3 = S(\{1, 2, 3\})$.

(a) Zeigen Sie, dass S_3 nicht abelsch ist.

Lösung:

Sei $f \in S_3 = S(\{1, 2, 3\})$ die bijektive Abbildung $f\colon \{1, 2, 3\} \to \{1, 2, 3\}, 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$, und sei $g \in S_3$ die bijektive Abbildung $g\colon \{1, 2, 3\} \to \{1, 2, 3\}, 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$. Dann gilt

$$g \circ f\colon 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2 \qquad \text{und}$$
$$f \circ g\colon 1 \mapsto 3, 2 \mapsto 2, 3 \mapsto 1,$$

also $g \circ f \neq f \circ g$ und S_3 ist nicht abelsch.

(b) Finden Sie jeweils eine Untergruppe von S_3, die Ordnung 2 bzw. 3 hat.

Lösung:

Wir behaupten, dass $B := \{f, h, \text{id}\}$ eine Untergruppe der Ordnung 3 von S_3 ist, wobei f die Abbildung aus (a) sei und $h\colon \{1, 2, 3\} \to \{1, 2, 3\}, 1 \mapsto 3, 2 \mapsto 1, 3 \mapsto 2$. Es gilt nämlich $f \circ h = \text{id}_{\{1,2,3\}}$, $h \circ f = \text{id}_{\{1,2,3\}}, f \circ f = h$ und $h \circ h = f$, also $j \circ k \in A$ für alle $j, k \in A$, und $f^{-1} = h, h^{-1} = f \in A$. Also ist B eine Untergruppe von S_3. $|B| = 3$ folgt direkt aus der Definition der Ordnung einer Gruppe und $|\{f, h, \text{id}_{\{1,2,3\}}\}| = 3$.
Die Teilmenge $A := \{\tau_{12}, \text{id}_{\{1,2,3\}}\}$ mit $\tau_{12}\colon 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$ ist eine Untergruppe von S_3 der

Ordnung 2. Denn es gilt $\tau_{12} \circ \tau_{12} = \mathrm{id}$, also $f \circ g \in A$ für alle $f, g \in A$, und $\tau_{12}^{-1} = \tau_{12} \in A$.

4. Betrachten Sie die Menge

$$G = (\mathbb{Z}/5\mathbb{Z})^* = (\mathbb{Z}/5\mathbb{Z}) \setminus \{0\} = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}\,.$$

(a) Zeigen Sie, dass G mit der Multiplikation $\overline{a} \cdot \overline{b} := \overline{a \cdot b}$ als Verknüpfung eine Gruppe bildet. Was sind die Inversen der 4 Elemente?

(b) Zeigen Sie, dass es einen eindeutigen Gruppenhomomorphismus

$$\varphi\colon \big(\mathbb{Z}/4\mathbb{Z}, +\big) \to G\,,$$

gibt, so dass $\varphi(\overline{1}) = \overline{2}$ gilt und φ ein Isomorphismus ist.

Lösung:

(a) Die Gruppenaxiome werden leicht nachgerechnet: Zunächst ist die Verknüpfung assoziativ, da das Produkt auf $\mathbb{Z}$ assoziativ ist. Das neutrale Element der Gruppe ist $\overline{1}$, und erfüllt offensichtlich das entsprechende Gruppenaxiom ($\overline{1}\overline{x} = \overline{1 \cdot x} = \overline{x}$). Die Inversen der 4 Elemente ergeben sich aus:

$$\overline{2} \cdot \overline{3} = \overline{1}\,, \qquad \overline{4} \cdot \overline{4} = \overline{1}\,.$$

Konkret: $\overline{2}^{-1} = \overline{3}$, $\overline{3}^{-1} = \overline{2}$, $\overline{4}^{-1} = \overline{4}$.

(b) Die Gruppe $\big(\mathbb{Z}/4\mathbb{Z}, +\big)$ wird vom Element $\overline{1}$ erzeugt. Das heisst, jedes Element ist ein Vielfaches von $\overline{1}$ (z.B. $\overline{3} = 3 \cdot \overline{1} = \overline{1} + \overline{1} + \overline{1}$ etc.). Damit ist ein Gruppenhomomorphismus φ schon eindeutig bestimmt durch Angabe des Bildes von $\overline{1}$, also $\varphi(\overline{1})(= \overline{2}$ in unserem Fall). Konkret sind die Bilder der Elemente

$$\begin{aligned}
&\varphi(\overline{0}) = \overline{1} && \text{(neutrales Element)}\\
&\varphi(\overline{1}) = \overline{2}\\
&\varphi(\overline{2}) = \varphi(\overline{1} + \overline{1}) = \varphi(\overline{1}) \cdot \varphi(\overline{1}) = \overline{2} \cdot \overline{2} = \overline{4}\\
&\varphi(\overline{3}) = \varphi(\overline{1}) \cdot \varphi(\overline{1}) \cdot \varphi(\overline{1}) = \overline{2} \cdot \overline{2} \cdot \overline{2} = \overline{3}.
\end{aligned}$$

Man kann explizit nachprüfen, dass dies ein Gruppenhomomorphismus ist, indem man „stumpfsinnig" alle möglichen Verknüfungen überprüft und zeigt $\varphi(a + b) = \varphi(a)\varphi(b)$. Da die Gruppen abelsch sind, muss man jeweils nur eine Reihenfolge der beiden verknüpften Elemente a, b beachten. Desweiteren gilt immer $\varphi(\overline{0} + a) = \varphi(a) = \varphi(\overline{0})\varphi(a)$, es reicht also $a, b \neq \overline{0}$ zu betrachten. Die verbleibenden Gleichungen sind schnell nachgerechnet:

$$\begin{aligned}
\varphi(\overline{1} + \overline{1}) &= \overline{4} = \varphi(\overline{1})\varphi(\overline{1})\\
\varphi(\overline{1} + \overline{2}) &= \overline{3} = \varphi(\overline{1})\phi(\overline{2})\\
\varphi(\overline{1} + \overline{3}) &= \overline{1} = \varphi(\overline{1})\varphi(\overline{3})\\
\varphi(\overline{2} + \overline{2}) &= \overline{1} = \varphi(\overline{2})\varphi(\overline{2})\\
\varphi(\overline{2} + \overline{3}) &= \overline{2} = \varphi(\overline{2})\varphi(\overline{3})\\
\varphi(\overline{3} + \overline{3}) &= \overline{4} = \varphi(\overline{3})\varphi(\overline{3})
\end{aligned}$$

Es ist außerdem aus der expliziten Beschreibung von φ oben klar, dass φ bijektiv ist, also ein Isomorphismus.

Hinweis: Mit mehr Erfahrung kann man den Beweis auch abkürzen. Die Gruppe $\mathbb{Z}/4\mathbb{Z}$ ist zyklisch, erzeugt von $\overline{1}$ mit der einzigen Relation $\overline{1}^4 = \overline{1} + \overline{1} + \overline{1} + \overline{1} = \overline{0}$. Um zu schließen, dass φ ein Gruppenhomomorphismus ist, reicht es deshalb zu prüfen, dass

$$\varphi(\overline{1})^4 = (\overline{2})^4 = \overline{1}\,.$$

5. Sei $\mathbb{F}$ ein Körper. Zeigen oder widerlegen Sie die folgenden Aussagen.

   Tipp: Für das Widerlegen genügt es, ein Gegenbeispiel zu finden.

   (a) Für alle $a, b \in \mathbb{F}$ folgt aus $a \cdot b = 0$, dass $a = 0$ oder $b = 0$ gilt.

   Lösung:

   Wir behaupten, dass die Aussage richtig ist.
   Seien $a, b \in \mathbb{F}$ mit $a \cdot b = 0$. Angenommen, es gilt $a \neq 0$ und $b \neq 0$. Dann existieren Inverse a^{-1}, b^{-1} von a, b und aus $ab = 0$ folgt $a^{-1}(ab) = a^{-1}0 = 0$ und daraus wegen der Assoziativität der Multiplikation $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}(ab)) = b^{-1}(0) = 0$. Nun ist aber $b^{-1}a^{-1}$ das inverse Element von ab, sodass wir $1 = 0$ bekommen. Dies ist ein Widerspruch, denn in Körpern gilt immer $1 \neq 0$. Unsere Annahme $a, b \neq 0$ war also falsch und es gilt $a = 0$ oder $b = 0$.

   (b) Für $a, b \in \mathbb{F}$ folgt aus $a \cdot a = b \cdot b$, dass $a = b$ oder $a = -b$ gilt. (2)

   Lösung:

   Wir behaupten wiederum, dass die Aussage richtig ist.
   Seien $a, b \in \mathbb{F}$ mit $a \cdot a = b \cdot b$. Dann gilt $a \cdot a + (-b \cdot b) = b \cdot b + (-b \cdot b) = 0$. Aus den Distibutivgesetzen in $\mathbb{F}$ folgt $(a - b)(a + b) = a \cdot a - b \cdot b$, also erhalten wir $(a - b)(a + b) = 0$. Teilaufgabe (a) impliziert nun $a - b = 0$, also $a = a - b + b = 0 + b = b$, oder $a + b = 0$, also $a = a + b - b = 0 - b = -b$, was zu zeigen war.

   (c) Für $a, b \in \mathbb{F}$ folgt aus $a \cdot a \cdot a = b \cdot b \cdot b$, dass $a = b$.

   Tipp: Denken Sie an die komplexen Zahlen $\mathbb{C}$.

   Lösung:

   Diese Aussage ist falsch. Sei $\mathbb{F} = \mathbb{C}$, $a = e^{2\pi i/3}$ und $b = 1$. Dann gilt

   $$a \cdot a \cdot a = \left(e^{2\pi i/3}\right)^3 = e^{2\pi i} = 1 = 1 \cdot 1 \cdot 1 = b \cdot b \cdot b,$$

   aber $a = e^{2\pi i/3} \neq b = 1$.

6. Lösen Sie das lineare Gleichungssystem

   $$\begin{aligned} x_1 + x_2 &= 1 \\ x_2 + x_3 &= 1 \\ x_1 + x_3 &= 1 \end{aligned}$$

   über dem Körper

   (a) $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$

   Lösung:

   Wir vereinfachen das lineare Gleichungssystem durch Zeilenumformungen, wobei wir beachten, dass $1 + 1 = 0$ gilt in $\mathbb{F}_2$:

   $$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right) \xrightarrow{L_3 + L_1 \to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right) \xrightarrow{L_3 + L_2 \to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

   Wegen $0 \neq 1 \in \mathbb{F}_2$ gibt es also keine Lösung.

   (b) $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$

   Lösung:

Unter Beachtung der Rechenregeln in $\mathbb{F}_3$ gehen wir vor wie in Teil (a):

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right) \xrightarrow{L_3+2L_1\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 2 & 1 & 0 \end{array}\right) \xrightarrow{L_3+L_2\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right)$$
$$\xrightarrow{2L_3\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{array}\right) \xrightarrow{L_2+2L_3\to L_2} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{array}\right) \xrightarrow{L_1+2L_2\to L_1} \left(\begin{array}{ccc|c} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{array}\right)$$

Die eindeutige Lösung des Gleichungssystems ist in diesem Fall also $x_1 = x_2 = x_3 = 2$.

(c) $\mathbb{R}$.

Lösung:

Wir vereinfachen das lineare Gleichungssystem wieder durch elementare Zeilenumforumgen, diesmal über $\mathbb{R}$:

$$\left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{array}\right) \xrightarrow{L_3-L_1\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & -1 & 1 & 0 \end{array}\right) \xrightarrow{L_3+L_2\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 \end{array}\right)$$
$$\xrightarrow{\frac{1}{2}L_3\to L_3} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & \frac{1}{2} \end{array}\right) \xrightarrow{L_2-L_3\to L_2} \left(\begin{array}{ccc|c} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{1}{2} \end{array}\right) \xrightarrow{L_1+-L_2\to L_1} \left(\begin{array}{ccc|c} 1 & 0 & 0 & \frac{1}{2} \\ 0 & 1 & 0 & \frac{1}{2} \\ 0 & 0 & 1 & \frac{1}{2} \end{array}\right)$$

Die eindeutige Lösung des Gleichungssystems ist in diesem Fall also $x_1 = x_2 = x_3 = \frac{1}{2}$.

7. (a) Lösen Sie die Gleichung $4x + 6 = 1$ in $\mathbb{F}_7$.

Lösung:

Es gilt $4x + 6 = 1 \iff 4x = 1 - 6 = -5 \equiv 2 \mod 7$. Nun ist $4^{-1} = 2$ in $\mathbb{F}_7$, denn $4 \cdot 2 = 8 \equiv 1 \mod 7$, also gilt

$$4x + 6 = 1 \iff 4x \equiv 2 \mod 7 \iff x = 4^{-1} \cdot 2 = 2 \cdot 2 = 4.$$

(b) Lösen Sie die Gleichung $3x + b = c$ in $\mathbb{F}_{17}$. *Achtung:* $\frac{c-b}{3}$ ist keine gute Antwort - verstehen Sie, was Teilen durch 3 in $\mathbb{Z}/17\mathbb{Z}$ bedeutet.

Lösung:

Das inverse Element von 3 in $\mathbb{F}_{17}$ ist 6, denn es gilt $6 \cdot 3 = 18 \equiv 1 \mod 17$. Es gilt also

$$3x + b = c \iff 3x = c - b \iff x = 3^{-1}(c - b) = 6(c - b) = 6c - 6b.$$

8. Betrachten Sie den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ und berechnen Sie

(a) $\overline{4}^{2020}$,

Lösung:

Wegen der Assoziativität der Multiplikation in $\mathbb{F}_5$ gilt $\overline{4}^{2020} = \left(\overline{4}^2\right)^{1010}$. Da $4^2 = 16 \equiv 1 \mod 5$ ist, gilt $\overline{4}^2 = \overline{1}$. Es folgt induktiv

$$\overline{4}^{2020} = \overline{1}^{1010} = \overline{1} \cdot \overline{1}^{1009} = \overline{1}^{1009} = \ldots = \overline{1},$$

da $\overline{1}$ das Einselement in $\mathbb{F}_5$ ist.

(b) $\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}}$.

Lösung:
Da

$$\overline{4} \cdot \overline{4} = \overline{1} \quad \text{und} \quad \overline{3} \cdot \overline{2} = \overline{1}$$

ist, folgt $\frac{\overline{1}}{\overline{4}} = \overline{4}$ und $\frac{\overline{1}}{\overline{3}} = \overline{2}$. Wir rechnen:

$$\begin{aligned} \frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} &= \overline{3} \cdot \overline{4} + \overline{1} \cdot \overline{2} \\ &= \overline{2} + \overline{2} \\ &= \overline{4}. \end{aligned}$$

Spaßaufgaben

Lösung:
Wir werden hier keine Lösungen für die Spaßaufgaben 9-11 angeben. Das Buch `https://www.springer.com/gb/book/9783030552329` beschäftigt sich mit diesen Aufgaben und Sie können jederzeit den Dozenten Menny Akka Ginosar ansprechen, um die Lösungen dieser Aufgaben zu diskutieren.

9. (Teilbarkeits-Tests) (★)
   (a) Zeigen Sie mittels Restklassenarithmetik, dass eine Zahl $n \in \mathbb{N}$ genau dann durch 3 teilbar ist, wenn ihre Quersumme durch 3 teilbar ist. Zeigen Sie auch, dass eine Zahl $n \in \mathbb{N}$ genau dann durch 9 teilbar ist, wenn ihre Quersumme durch 9 teilbar ist. Zeigen Sie allgemeiner mittels Restklassenarithmetik, dass eine Zahl $n \in \mathbb{N}$ und ihre Quersumme denselben Rest haben bei Division durch 3 (bzw. 9).
   (b) Finden Sie eine ähnliche Regel für Teilbarkeit durch 11, und allgemeiner für den Rest bei Division durch 11.
   (c) Finden Sie eine ähnliche Teilbarkeitsregel für die Zahl 7, und allgemeiner für den Rest bei Division durch 11.
   Tipp: Dies benutzt eine gewichtete Version der Quersumme. Überlegen Sie, was mit „gewichtete“ Version gemeint ist. Zum Beispiel benutzt der Teilbarkeitstest für 11 die „Gewichte“ 1 und -1.
   (d) Das erste Resultat bei Google für die Suchanfrage „divsibility test of 7“ ist die Website `https://www.mathsisfun.com/divisibility-rules.html`. Lesen Sie die Regel für Teilbarkeit durch 7 auf dieser Website und erklären Sie die Regel mit Restklassenarithmetik (nicht so einfach!). Zeigen Sie, dass sich diese Regel nicht einfach für Reste verallgemeinern lässt wie oben und begründen Sie, warum.

10. In dieser Aufgabe beschäftigen wir uns mit einigen einfachen Implikationen aus berühmten Theoremen aus dem Gebiet der Zahlentheorie. (★)
   (a) Der Zwei-Quadrate-Satz von Fermat lautet wie folgt: Sei p eine ungerade Primzahl. Dann kann p genau dann als Summe zweier Quadratzahlen $p = x^2 + y^2$ mit $x, y \in \mathbb{Z}$ geschrieben werden, wenn $p \equiv 1 \mod 4$. Zeigen Sie dass die Bedingung $p \equiv 1 \mod 4$ für die Existenz von x, y wie im Satz notwendig ist. Dies ist die einfache Richtung des Satzes.
   Für die schwierigere Richtung gibt es viele Beweise und sie ist der Anfang eines sehr schönen Gebiets der Mathematik. Wenn Sie daran interessiert sind und Zeit finden, schauen Sie sich dieses schöne Video an: `youtube.com/watch?v=DjI1NICfjOk`. Die visuelle Erklärung aus dem Video wird im Buch `https://link.springer.com/book/10.1007/978-3-030-55233-6` reproduziert. Die Geschichte des Zwei-Quadrate-Satzes von Fermat und wohin der Satz führt wird auch am Anfang dieses tollen Buches `http://www.math.toronto.edu/~ila/Cox-Primes_of_the_form_x2+ny2.pdf` besprochen.

(b) Der Drei-Quadrate-Satz von Legendre besagt folgendes: Eine natürliche Zahl n kann genau dann als Summe dreier Quadratzahlen

$$n = x^2 + y^2 + z^2$$

geschrieben werden, wenn n nicht von der Form $n = 4^a(8b + 7)$ mit natürlichen Zahlen a und b ist. Zeigen Sie eine einfachere Version der notwendigen Bedingung in diesem Satz: Falls $n = x^2+y^2+z^2$ ist, dann gilt $n \not\equiv 7 \mod 8$. Um die Umkehrung dieser Aussage zu beweisen, braucht man Zutaten des ganzen Mathematik-Bachelors.

11. Lösen Sie das Hut-Rätsel, siehe Aufgabe 3.56 im Buch `https://link.springer.com/book/10.1007/978-3-030-55233-6`. (★)

12. (Sudoku für Mathematiker) Sei G die Menge mit sechs verschiedenen Elementen $\{a, b, c, x, y, z\}$ und sei $\circ : G \times G \to G$ eine Verknüpfung, die über die folgende (unvollständige) Verknüpfungstafel beschrieben wird: (★)

$\circ$	a	b	c	x	y	z
a					c	b
b		x	z			
c		y				
x				x		
y						
z		a			x	

Hierbei bedeutet der Eintrag y in Zeile c und Spalte b, dass $c \circ b = y$ gilt. Die meisten Einträge dieser Tabelle fehlen noch. Ihre Aufgabe ist es, diese Tabelle zu vervollständigen und dabei die Gruppenaxiome zu erfüllen (Assoziativität der Verknüpfung, Existenz des neutralen Elements, Existenz der inversen Elemente).
Sie können davon ausgehen, dass eine Vervollständigung der Verknüpfungstafel existiert, die alle Gruppenaxiome erfüllt, d.h. Sie müssen am Ende nicht noch testen, ob z.B. die Assoziativität auch wirklich für alle Kombinationen erfüllt ist.

Lösung:

Zuerst versuchen wir das neutrale Element e der Gruppe zu erkennen. Dieses erfüllt $u \circ e = u$ oder $e \circ u = u$ für alle $u \in G$. Wenn wir in einer Zeile u den Eintrag $u \circ w = u$ finden, dann muss w das neutrale Element sein (folgt durch Multiplizieren mit der Links-Inverse von u). Analog kann man auch für die Spalten vorgehen.

Wir entdecken in der Tabelle den Eintrag $x \circ x = x$ und können also schliessen, dass $e = x$ das neutrale Element ist. Wir verwenden die Definition des neutralen Elements ($u \circ e = u$ und $e \circ u = u$ für alle u) und können die x-Zeile und x-Spalte auffüllen:

$\circ$	a	b	c	x	y	z
a				a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y				y		
z		a		z	x	

Jetzt verwenden wir die Definition des inversen Elements v von u: $u \circ v = e = v \circ u$. Wir finden den Eintrag $z \circ y = x$, also können wir $y \circ z = x$ ergänzen.

Um weiter fortzufahren müssen wir die Assoziativität anwenden: $(u \circ v) \circ w = u \circ (v \circ w)$. Damit wir mithilfe der Assiziativität einen Eintrag erzeugen, brauchen wir drei schon vorhandene Einträge in der Tabelle. Wissen wir z.B. $v \circ w = e$, $u \circ v = f$ und $u \circ s = g$, dann können wir den Eintrag $f \circ w = g$ in

die Tabelle eintragen. Solche Kombinationen zu finden ist zugegeben etwas mühsam, aber es gibt z.B. die folgenden Kombinationen

$$\begin{aligned}
a \circ b &= \underbrace{(z \circ b)}_{a} \circ b = z \circ \underbrace{(b \circ b)}_{x} = z, \\
x &= \underbrace{(a \circ z)}_{b} \circ b = a \circ \underbrace{(z \circ b)}_{a} = a \circ a, \\
y \circ b &= \underbrace{(c \circ b)}_{y} \circ b = c \circ \underbrace{(b \circ b)}_{x} = c, \\
z \circ c &= \underbrace{(a \circ b)}_{z} \circ c = a \circ \underbrace{(b \circ c)}_{z} = b.
\end{aligned}$$

Dann ergibt sich in unserer Tabelle

$\circ$	a	b	c	x	y	z
a	x	z		a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y		c		y		
z		a	b	z	x	

Wir finden weitere Einträge:

$$\begin{aligned}
z \circ y &= x = y \circ z \\
c \circ c &= (y \circ b) \circ c = y \circ (b \circ c) = y \circ z = x \\
a \circ (y \circ c) &= (a \circ y) \circ c = c \circ c = x, \text{ also } y \circ c = a. \\
c \circ y &= c \circ (c \circ b) = b \\
c \circ z &= c \circ (b \circ c) = y \circ c = a.
\end{aligned}$$

Da für alle Elemente $u \in G$ die Links- und Rechtsmultiplikation, nämlich

$$\begin{aligned}
u \circ \cdot &: G \to G, \quad v \mapsto u \circ v \\
\cdot \circ u &: G \to G, \quad v \mapsto v \circ u,
\end{aligned}$$

Bijektionen sind, folgt, dass in jeder Zeile und in jeder Spalte jedes Element genau einmal vorkommen muss. Wir schliessen deshalb

$$\begin{aligned}
a \circ c &= y \\
c \circ a &= z.
\end{aligned}$$

Es folgt weiter

$$\begin{aligned}
y \circ y &= (a \circ c) \circ y = a \circ (c \circ y) = a \circ b = z \\
b \circ y &= b \circ (c \circ b) = z \circ b = a \\
y \circ a &= y \circ (c \circ z) = az = b.
\end{aligned}$$

Wir erhalten

$\circ$	a	b	c	x	y	z
a	x	z	y	a	c	b
b		x	z	b	a	
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z		a	b	z	x	

Es folgt durch Assoziativität

$$b \circ a = b \circ (y \circ c) = (b \circ y) \circ c = a \circ c = y.$$

Da in jeder Zeile und Spalte jedes Element genau einmal stehen darf, folgt

$$z \circ a = c$$
$$b \circ z = c$$
$$z \circ z = y$$

und wir erhalten die vollständige Tabelle

$\circ$	a	b	c	x	y	z
a	x	z	y	a	c	b
b	y	x	z	b	a	c
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z	c	a	b	z	x	y

Ist dies jetzt eine Gruppe? Da wir in jedem Schritt zwingende Regeln angewendet haben, können wir aufgrund des Hinweises auf dem Übungsblatt davon ausgehen.

Wie kann man aber nachprüfen ob die Verknüpfungstabelle widerspruchslos ist? Eine Möglichkeit ist die Überprüfung aller möglicher Kombinationen; aufgrund der Anzahl Kombinationen ist dies aber sehr mühsam. Hier wissen wir aber, dass G (bei geeigneter Umbenennung der Elemente a, b, c, x, y, z) die symmetrische Gruppe S_3 ist, die Ihnen noch mehrmals im Laufe des Studium begegnen wird.