D-MATH
Dr. Menny Akka Ginosar
Paula Truöl

HS 2020
ETH Zürich

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 und nur 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)

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 $b = c \Leftrightarrow a \circ b = a \circ c$.

   (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.

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

   (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.

   (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.

   (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 $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

   (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 $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$.

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

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

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

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.

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.

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

   (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 $\mathbb{C}$.

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

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

   (c) $\mathbb{R}$.

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

   (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.

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

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

9. (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 zum Beispiel die Assoziativität auch wirklich für alle Kombinationen erfüllt ist.

10. (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 bei Division durch 3 (bzw. 9) denselben Rest haben.

    (b) Finden Sie eine ähnliche Regel für die Teilbarkeit durch 11, und allgemeiner für den Rest bei Division durch 11.

(c) Finden Sie eine ähnliche Regel für die Teilbarkeit durch 7, und allgemeiner für den Rest bei Division durch 7.

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.

11. 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 des 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 schwierigere Richtung des Satzes zu beweisen, braucht man Zutaten des ganzen Mathematik-Bachelors.

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