8.1. Gruppen

Das Zusammenzählen bzw. die **Addition natürlicher Zahlen** zum Zwecke der Vorratskontrolle ist in menschlichen Kulturen lange vor der Entwicklung der Schrift praktiziert worden. Um aufgenommene und abgegebene Mengen z.B. in einem Getreidespeicher unterscheiden zu können, wurden die **Subtraktion** und damit auch **negative Zahlen** entwickelt. Um die Addition vieler gleich großer (Steuer)beträge abzukürzen, kam man auf die **Multiplikation**, bei der gerechten Aufteilung von Ausgaben oder Einnahmen auf mehrere Personen auf die **Division** und damit die **rationalen Zahlen**.
Kurz: Die Beschreibung und Organisation immer komplexerer Systeme wurden mit neuen Rechenmethoden gelöst, die ihrerseits eine Erweiterung des Zahlbegriffes notwendig machten. Heute rechnen wir nicht mehr nur mit Zahlen, sonder verknüpfen z.B. **Vektoren** mit dem **Skalar- und Vektorprodukt**, **Matrizen** mit dem **Matrizenprodukt** und **Funktionen** mit der **Verkettung**.
Damit eine neue Rechenmethode für eine neue Menge von Rechenobjekten „funktioniert“, muss sie gewissen Mindestansprüchen genügen, die man unter dem Begriff der „Gruppe“ zusammenfasst.

Definition:

Eine Gruppe ist eine Menge G und eine Verknüpfung $\circ$ mit den folgenden Eigenschaften:

8.1.0. Wohldefiniertheit

Für alle $a, b \in G$ ist $a \circ b$ eindeutig definiert.
Beispiele:

- Auf der Menge $\mathbb{R}$ der reellen Zahlen ist die Division nicht wohl definiert, weil z.B. $3 : 0$ nicht definiert ist.
- Auf der Menge der Vektoren ist die Addition nicht wohl definiert, weil z.B. $\begin{pmatrix}1\\2\end{pmatrix} + \begin{pmatrix}3\\0\\2\end{pmatrix}$ nicht definiert ist.
- Auf der Menge der Matrizen ist die Multiplikation nicht wohl definiert, weil z.B. $\begin{pmatrix}1 & 2 & 3\\0 & 2 & 4\end{pmatrix} * \begin{pmatrix}0 & 1\\2 & 3\end{pmatrix}$ nicht definiert ist

Übungen: Aufgaben zu Gruppen Nr.1

8.1.1. Abgeschlossenheit

Für alle $a, b \in G$ ist auch $a \circ b \in G$.
Beispiele:

- Die Menge $\mathbb{N}$ der natürlichen Zahlen ist bezüglich der Subtraktion nicht abgeschlossen, weil z.B. $3 - 5 \notin \mathbb{N}$.
- Die Menge $\mathbb{Z}$ der ganzen Zahlen ist in Bezug auf die Division nicht abgeschlossen, weil z.B. $3 : 5 \notin \mathbb{Z}$.
- Auf der Menge der zweidimensionalen Vektoren ist das Skalarprodukt wohldefiniert, aber nicht abgeschlossen, weil z.B. $\begin{pmatrix}1\\2\end{pmatrix} * \begin{pmatrix}3\\4\end{pmatrix} = 11$ kein zweidimensionaler Vektor mehr ist.

Übungen: Aufgaben zu Gruppen Nr.2

8.1.2. Assoziativität

Für alle $a, b, c \in G$ ist auch $(a \circ b) \circ c = a \circ (b \circ c)$.
Beispiele:

- Auf den reellen Zahlen $\mathbb{R}$ ist die Subtraktion nicht assoziativ, weil z.B. $(1 - 2) - 3 \neq 1 - (2 - 3)$.
- Auf den reellen Zahlen $\mathbb{R}$ ist die Division nicht assoziativ, weil z.B. $(1 : 2) : 3 \neq 1 : (2 : 3)$.

Übungen: Aufgaben zu Gruppen Nr.3

8.1.3. Existenz eines neutralen Elements

Es gibt ein $n \in g$, so dass für all $a \in g$ gilt $n \circ a = a \circ n = a$.
Beispiele:

- Auf den reellen Zahlen $\mathbb{R}$ gibt es kein neutrales Element für die Subtraktion, weil z.B. $a - 0 \neq 0 - a \neq a$.
- Auf den reellen Zahlen $\mathbb{R}$ gibt es kein neutrales Element für die Division, weil z.B. $a : 1 \neq 1 : a \neq a$.
- Auf der Menge der dreidimensionalen Vektoren gibt es kein neutrales Element für das Vektorprodukt, da das Vektorprodukt zweier Vektoren immer orthogonal zu beiden Faktoren ist und damit niemals einem der beiden Faktoren gleich sein kann.

Übungen: Aufgaben zu Gruppen Nr.4

8.1.4. Existenz von inversen Elementen

Für jedes $a \in G$ existiert ein $a^{-1} \in G$, so dass $a^{-1} \circ a = a \circ a^{-1} = n$.
Beispiele:

- Auf den natürlichen Zahlen $\mathbb{N}$ gibt es kein inverses Element für die Addition, weil für alle $a, b \in \mathbb{N}$ gilt $a + b > a$.
- Auf den natürlichen Zahlen $\mathbb{N}$ gibt es kein inverses Element für die Multiplikation, weil für alle $a, b \in \mathbb{N}$ gilt $a \cdot b > a$.

Übungen: Aufgaben zu Gruppen Nr.5

8.1.5. Kommutativität

Eine Gruppe G heißt **kommutativ** oder **abelsch** nach dem norwegischen Mathematiker Nils Hendrik Abel (1802 – 1829), wenn außerdem die folgende Eigenschaft erfüllt ist: Für alle $a, b \in G$ gilt $a \circ b = b \circ a$.
Beispiele:

- Auf den reellen Zahlen $\mathbb{R}$ ist die Subtraktion nicht kommutativ, weil für alle $a, b \in \mathbb{R}/\{0\}$ gilt $a - b \neq b - a$.
- Auf den reellen Zahlen $\mathbb{R}$ ist die Division nicht kommutativ, weil für alle $a, b \in \mathbb{R}/\{0\}$ gilt $a : b \neq b : a$.

Übungen: Aufgaben zu Gruppen Nr.6

8.1.6. Untersuchung endlicher Gruppen mit Hilfe von Verknüpfungstafeln

Bei einer endlichen Menge lassen sich alle möglichen Ergebnisse der Verknüpfung auf einer Verknüpfungstafel darstellen. Aus der Verknüpfungstafel lassen sich alle Gruppeneigenschaften direkt ablesen.

Beispiele:

0. Wohldefiniertheit
Bleiben Felder der Verknüpfungstafel leer, so ist die Verknüpfung nicht wohl definiert:

:	0	1	2	3
0	-	0	0	0
1	-	1	0,5	$0,\overline{3}$
2	-	2	1	$0,\overline{6}$
3	-	3	1,5	1

1. Abgeschlossenheit
Enthält die Verknüpfungstafel Ergebnisse, die nicht auch in der ersten Zeile bzw. Spalte erscheinen, so ist die Verknüpfung nicht abgeschlossen:

−	0	1	2	3
0	0	−1	−2	−3
1	1	0	−1	−2
2	2	1	0	−1
3	3	2	1	0

2. Assoziativität
Weil die Assoziativität drei Elemente einbezieht, wäre sie nur in einem dreidimensionalen „Verknüpfungswürfel“ zu erkennen.

3. Neutrales Element

Sowohl die erste Spalte (n ∘ a) als auch die erste Zeile (a ∘ n) wiederholen sich an der Stelle des neutralen Elements:

−	0	1	2	3
0	0	−1	−2	−3
1	1	0	−1	−2
2	2	1	0	−1
3	3	2	1	0

Die erste Spalte wiederholt sich an der Stelle 0, d.h. a − 0 = a für alle a ∈ G. Leider wird aber die erste Zeile nicht wiederholt, d.h. die Bedingung 0 − a = a ist nicht erfüllt. 0 ist also kein neutrales Element der Subtraktion!

+	0	1	2	3
0	0	1	2	3
1	1	0	3	4
2	2	3	0	5
3	3	4	5	0

Sowohl die erste Spalte als auch die erste Zeile wiederholen sich an der Stelle 0. Es gilt also 0 + a = a + 0 für alle a ∈ G und 0 ist neutrales Element für die Addition. Da auch 4 und 5 als Ergebnisse erscheinen, ist die Addition auf der Menge {0; 1; 2; 3} allerdings nicht abgeschlossen!

4. Inverses Element
In der Verschlüsselungstechnik rechnet man oft mit Resten modulo n, die bei Division durch eine natürliche Zahl n entstehen. Die Menge der Reste modulo 5 besteht also aus den 5 Resten $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ und $\bar{4}$. Die Summe zweier Reste wird als der Rest der gewöhnlichen Summe der Reste definiert. Z.B. ist $\bar{2} + \bar{3} = \bar{0}$, weil 2 + 3 = 5 den Rest 0 besitzt:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

In jeder Zeile und in jeder Spalte erschein mindestens einmal das Ergebnis $\bar{0}$, d.h. für jedes Element a ∈ G gibt es ein inverses Element $a^{-1} \in G$ mit $a + a^{-1} = a^{-1} + a = \bar{0}$. Man liest ab: $\bar{1}^{-1} = \bar{4}$, $\bar{2}^{-1} = \bar{3}$, $\bar{3}^{-1} = \bar{2}$ und $\bar{4}^{-1} = \bar{1}$.

5. Kommutativität

Die Vertauschbarkeit a ∘ b = b ∘ a ist in der Verknüpfungstabelle an der Symmetrie zur grau schattierten Nebendiagonalen leicht zu erkennen:

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Übungen: Aufgaben zu Gruppen Nr. 7 - 10