Algebraische Strukturen

1 Permutationen

Eine n-stellige *Permutation* ist eine bijektive (umkehrbar eindeutige) Abbildung einer n-elementigen Menge auf sich selbst.

Beispielsweise bildet die vierstellige Permutation

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

das erste Element auf das dritte, das zweite Element auf das erste, das dritte Element auf das zweite, und das vierte Element auf sich selbst ab.

Kurzschreibweise: $p(1) = 3$, $p(2) = 1$, $p(3) = 2$, $p(4) = 4$

Komposition von Permutationen

Auf der Menge aller n-stelligen Permutationen ist eine Operation definert, die jedem Paar von Permutationen p und q ihre Komposition $q \circ p$ zuordnet und zwar indem sie den Index i auf den Index $q(p(i))$ „schickt“: *Beispiele:*

(a) $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

(b) $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

Diese Art der Verknüfung garantiert, dass das Resultat wieder eine Permutation ist (*Abgeschlossenheit*).

Offenbar ist diese Operation nicht kommutativ.

Assoziativität

Hingegen hat die Komposition von Permutationen eine andere wichtige Eigenschaft. Bei der Verknüpfung von drei Permutationen spielt die Art des „Assoziierens“ (Zusammenfassens) keine Rolle:

$$r \circ (q \circ p) = (r \circ q) \circ p$$

Beweis: Setzt man für einen beliebigen Index $i \in \{1, 2, \ldots, n\}$ die Definition der Komposition $(q \circ p)(i) = q(p(i))$ ein, so erhält man für beide Ausdrücke den gleichen Wert:

- $(r \circ (q \circ p))(i) = r((q \circ p)(i)) = r(q(p(i)))$
- $((r \circ q) \circ p)(i) = (r \circ q)(p(i)) = r(q(p(i)))$

□

Das neutrale Element

(a) $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

(b) $\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix} \circ \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix} = \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$

Die identische Permutation

$$e = \begin{pmatrix}1&2&3&\dots&n-1&n\\1&2&3&\dots&n-1&n\end{pmatrix}$$

ist das *neutrale Element* der Komposition von Permutationen.

Inverse Elemente

Wie bei der Addition von ganzen Zahlen

$$7 + (-7) = (-7) + 7 = 0$$

lässt sich zu jeder Permutation p eine Permutation q finden, so dass $q \circ p = p \circ q = e$, die identische Permutation ist. *Beispiel:*

$$\underbrace{\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}}_{q} \circ \underbrace{\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}}_{p} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

$$\underbrace{\begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}}_{p} \circ \underbrace{\begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}}_{q} = \begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$$

2 Gruppen

Eine *Gruppe* ist ein Paar $(M, *)$, bestehend aus einer Menge M und einer Verknüpfung $*\colon M \times M \to M$, $(a, b) \mapsto a * b$ mit den folgenden Eigenschaften:

(1) *Assoziativität:* Für alle a, b, $c \in M$ gilt: $a * (b * c) = (a * b) * c$.

(2) *neutrales Element:* Es gibt ein Element $e \in M$, so dass für alle $a \in M$ gilt: $a * e = e * a = a$.

(3) *inverses Element:* Zu jedem Element $a \in M$ gibt es ein Element $a' \in M$, so dass $a * a' = a' * a = e$.

Gilt darüber hinaus $a * b = b * a$ für alle a, $b \in M$, so wird die Gruppe *kommutativ* oder *abelsch* genannt.

Bemerkungen

- Welche Symbole für die Verknüpfung $(*)$, für das neutrale Element (e) und für die inversen Elemente (a') verwendet werden, spielt im Grunde keine Rolle. Je nach verwendeter Menge und Art der Verknüpfung haben sich aber bestimmte Bezeichnungen etabliert.
- Ist die der Gruppe $(M, *)$ zugrunde liegende Menge M endlich, so wird die Anzahl der Elemente von M die *Ordnung* der Gruppe genannt.

Beispiele

- $(\mathbb{Z}, +)$ mit der Addition „$+$“, dem neutralen Element 0 und dem zu $a \in \mathbb{Z}$ inversen Element „$-a$“ ist eine kommutative Gruppe.
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ mit der Multiplikation „$\cdot$“, dem neutralen Element 1 und dem zu $a \in \mathbb{Q} \setminus \{0\}$ inversen Element a^{-1} ist eine kommutative Gruppe.
- Die Menge aller n-stelligen Permutationen $(S_n, \circ)$ mit der Komposition „$\circ$“, der identischen Permutation und der jeweils inversen Permutation ist eine (im Allgemeinen nicht kommutative) Gruppe der Ordnung $n!$. Diese Gruppe wird *symmetrische Gruppe* genannt.

Eindeutigkeit des neutralen Elements

Ist $(M, *)$ eine Gruppe, so ist das neutrale Element e eindeutig bestimmt.

Beweis: Sei e' ein zweites neutrales Element in M mit $e \neq e'$. Dann gilt aufgrund der Gruppenaxiome:

$$e' = e * e' = e' * e = e$$

im Widerspruch zur Annahme $e \neq e'$. $\square$

Eindeutigkeit des inversen Elements

Ist $(M, *)$ eine Gruppe, $a \in M$ und a' ein inverses Element von a, so ist a' eindeutig bestimmt.

Beweis: Sei a'' ein zweites inverses Element in M mit $a' \neq a''$. Dann gilt aufgrund der Gruppenaxiome:

$$a'' = e * a'' = (a' * a) * a'' = a' * (a * a'') = a' * e = a'$$

im Widerspruch zur Annahme $a'' \neq a'$. $\square$

3 Restklassen

Für $m \in \mathbb{N}$ definert man die *Kongruenz von* a, $b \in \mathbb{Z}$ *modulo* m wie folgt:

$$a \equiv b \pmod{m} \quad \Leftrightarrow \quad m \text{ teilt } a - b \text{ (ohne Rest)}$$

Beispiele:

- $7 \equiv 3 \pmod{2}$
- $2 \equiv 12 \pmod{5}$
- $-5 \equiv 4 \pmod{3}$

Die Menge aller Zahlen, die den gleichen Rest $r \in \mathbb{N}$ modulo m ergeben, bezeichnet man als Restklasse $\overline{r}$.

Beispiel: für $m = 5$

- $\overline{0} = \{\dots, -10, -5, 0, 5, 10, \dots\}$
- $\overline{1} = \{\dots, -9, -4, 1, 6, 11, \dots\}$
- $\overline{2} = \{\dots, -8, -3, 2, 7, 12, \dots\}$
- $\overline{3} = \{\dots, -7, -2, 3, 8, 13, \dots\}$
- $\overline{4} = \{\dots, -6, -1, 4, 9, 14, \dots\}$

$\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

Mit Restklassen können wir in „natürlicher Weise“ rechnen, indem wir die Operation mit zwei beliebigen Repräsentaten der Restklassen durchführen und als Ergebnis die Resklasse des Resultats wählen.

Beispiel ($m = 5$):

- $\overline{1} + \overline{2} = \overline{3}$ denn $1 + 2 = 3 \in \overline{3}$
- $\overline{2} + \overline{3} = \overline{0}$ denn $2 + 3 = 5 \in \overline{0}$
- $\overline{2} \cdot \overline{3} = \overline{1}$ denn $2 \cdot 3 = 6 \in \overline{1}$
- $\overline{2} - \overline{3} = \overline{4}$ denn $2 - 3 = -1 \in \overline{4}$

Dabei ist das Resultat unabhängig von der Wahl der Repräsentanten. Im letzten Beispiel hätte man statt $2 - 3 = -1$ auch $22 - 8 = 14$ rechnen können, da 22 in der gleichen Restklasse wie 2 und 8 in der gleichen Restklasse wie 3 liegt.

Verknüpfungstabelle von $\mathbb{Z}_4$

Für $\mathbb{Z}_4$ gilt: (die Überstriche wurden weggelassen)

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

In der ersten Spalte steht das erste Argument, in der ersten Zeile das zweite.

- $(\mathbb{Z}_4, +)$ ist eine kommutative Gruppe mit dem neutralen Element 0.
- $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ ist keine Gruppe, denn zur Restklasse von 2 gibt es keine multiplikative Inverse.

Verknüpfungstabelle von $\mathbb{Z}_5$

Für $\mathbb{Z}_5$ gilt: (die Überstriche wurden weggelassen)

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$+$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- $(\mathbb{Z}_5, +)$ ist eine kommutative Gruppe mit dem neutralen Element 0.
- $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit dem neutralen Element 1, denn alle Inversen existieren.

4 Körper

Eine *Körper* ist ein Tripel $(M, +, \cdot)$, bestehend aus einer Menge M und zwei abgeschlossenen Verknüpfungen $+$ bzw. $\cdot$ mit den folgenden Eigenschaften:

- *Addition:* $(M, +)$ ist eine kommutative Gruppe mit dem neutralen Element 0.
- *Multiplikation:* $(M \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit dem neutralen Element 1.
- *Distributivgesetz:* Für alle Elemente a, b, $c \in M$ gilt:
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$

Beispiele von Körpern

- $(\mathbb{Q}, +, \cdot)$ ist ein Körper
- $(\mathbb{R}, +, \cdot)$ ist ein Körper
- $(\mathbb{C}, +, \cdot)$ ist ein Körper
- $(\mathbb{Z}_m, +, \cdot)$ ist ein Körper, wenn m eine Primzahl ist.