Theoretische Informatik I

Duale Hochschule Baden-Württemberg – Lörrach
Studiengang Informatik – TIF21

Januar 2022–März 2022

Teil I

Algebraische Strukturen

Übersicht

Mengen

Ein zentraler Begriff in der Mathematik ist der der Menge. Obwohl es möglich ist zu axiomatisieren, was man unter einer Menge versteht, wollen wir uns hier mit der Anschauung begnügen.

Intuition

- Eine **Menge** ist eine (gewissen Regeln unterliegende) Zusammenfassung von Objekten, den **Elementen** der Menge.
- Wir schreiben $x \in \mathscr{M}$, um auszudrücken, dass das Objekt x in der Menge $\mathscr{M}$ enthalten ist.
- Wir schreiben $x \notin \mathscr{M}$, um auszudrücken, dass das Objekt x nicht in der Menge $\mathscr{M}$ enthalten ist.
- Die **leere Menge** $\emptyset := \{\}$ ist die Menge, die kein Objekt enthält.

Elemente

Elemente von Mengen dürfen wir mit beliebigen Symbole bezeichnen, etwa $\clubsuit, b, J, \diamondsuit, A, \heartsuit, 25$ und $\circ$. Wir wollen uns allerdings darauf einigen, dass die Symbole »{« und » « und »,« und »}« keine Elemente sein sollen, um Verwechslungen zu vermeiden.

Ein Element ist höchstens einmal in einer Menge enthalten. $\{2, 2, 2\}$ ist dieselbe Menge wie $\{2\}$.

Die Reihenfolge der Elemente in der Menge ist nicht bestimmt. $\{1, 91, 351\}$ ist dieselbe Menge wie $\{91, 1, 351\}$.

Beschreibungen

Endliche Mengen können wir durch Aufzählen aller Elemente definieren.

Beispiele

$$M_1 := \{\clubsuit, b, J, \diamondsuit, A, \heartsuit, 25, \circ\}$$
$$M_2 := \{B, J, A, R\}$$
$$M_3 := \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Es gilt etwa: $\clubsuit \in M_1$, $\spadesuit \notin M_1$

Beschreibungen

Sofern klar ist, wie eine Aufzählung aufgebaut ist, dürfen wir Auslassungspunkte verwenden. Dies ist auch bei einigen unendlichen Mengen zulässig.

Beispiele

$$
\begin{aligned}
M_3 &= \{1, 2, 3, 4, \ldots, 10\} \\
M_4 &:= \{2, 4, 6, 8, 10, \ldots\} \\
M_5 &:= \{1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, \ldots\} \\
M_5 &= \{1!, 2!, 3!, 4!, 5!, 6!, 7!, 8!, 9!, 10!, \ldots\} \\
\mathbb{N} &= \{1, 2, 3, 4, \ldots\} \\
\mathbb{N}_0 &= \{0, 1, 2, 3, 4, \ldots\} \\
\mathbb{Z} &= \{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}
\end{aligned}
$$

Charakterisierende Eigenschaften

Mengen können auch durch die charakterisierenden Eigenschaften ihrer Elemente beschrieben werden.

Beispiele

$$\begin{aligned} M_3 &= \{x \in \mathbb{N} \mid 1 \leq x \leq 10\} \\ M_4 &= \{x \in \mathbb{N} \mid x \text{ gerade}\} \\ \mathbb{Z} &= \{x \in \mathbb{R} \mid x \in \mathbb{N} \text{ oder } -x \in \mathbb{N} \text{ oder } x = 0\} \end{aligned}$$

Hinweis

Die Variable x ist außerhalb von

$$\{x \in \mathbb{R} \mid x \in \mathbb{N} \text{ oder } -x \in \mathbb{N} \text{ oder } x = 0\}$$

nicht definiert. Wenn wir etwa in Beweisen etwas über diese Menge aussagen möchten, dürfen wir nicht ohne weiteres über ein x verfügen.

Charakterisierende Eigenschaften

Sofern es möglich ist, sollten wir allerdings eine passende Obermenge angeben, um Verwechslungen auszuschließen.

Beispiele

$$\{x \mid x \text{ gerade}\} \stackrel{?}{=} \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$$

$$\{x \mid x \text{ gerade}\} \stackrel{?}{=} \{2, 4, 6, 8, 10, \dots\}$$

$$\{x \in \mathbb{Z} \mid x \text{ gerade}\} = \{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}$$

$$\{x \in \mathbb{N} \mid x \text{ gerade}\} = \{2, 4, 6, 8, 10, \dots\}$$

Falls es nicht möglich ist, eine Obermenge anzugeben, sollten wir uns fragen wieso. Möglicherweise versuchen wir dann gerade eine Menge zu konstruieren, die gar nicht existiert.

Mengen von Mengen

Die Elemente von Mengen dürfen ebenfalls Mengen sein.

Beispiele

$$M_6 := \{M_1, Y, M_3\}$$
$$M_6 = \{\{\clubsuit, b, J, \diamondsuit, A, \heartsuit, 25, \circ\}, Y, \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\}$$

$$M_7 := \{\{x \in \mathbb{Z} \mid x \text{ gerade}\}, \{x \in \mathbb{Z} \mid x \text{ ungerade}\}\}$$
$$M_7 = \{\{\dots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}, \{\dots, -7, -5, -3, -1, 1, 3, 5, 7, 9, \dots\}\}$$

$$M_8 := \{\{\dots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \dots\}, \{\dots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \dots\}, \{\dots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \dots\}\}$$

Mengen von Mengen

Obacht: Wir müssen bei Mengen von Mengen sehr sorgfältig hinsehen.

Beispiele

- Die Menge $M_2 = \{B, J, A, R\}$ unterscheidet sich von $\{\{B\}, \{J\}, \{A\}, \{R\}\}$ und beide unterscheiden sich von $\{\{B\}, \{J\}, A, \{R\}\}$.
- Es gilt $3 \notin M_6$.
- Es gilt $\{3\} \notin M_6$.
- Es gilt $\{1\} \notin \{1\}$.
- Es gilt $\{1\} \in \{\{1\}\}$.
- Es gilt $\{1\} \in \{1, \{1\}\}$.

Grenzen

Mengen dürfen nicht beliebig aufgebaut sein. So darf sich eine Menge nicht selbst enthalten; weiter gibt es beispielsweise die »Menge aller Mengen« nicht.

Wir werden nun folgenden Satz beweisen:

Satz

$M := \{x \mid x \text{ ist Menge und } x \notin x\}$ ist keine Menge.

Grenzen

Beweis.

Wir nehmen an, dass M eine Menge sei und machen eine Fallunterscheidung.

- 1. Fall: Es gilt $M \in M$.
  M enthält als Elemente gerade alle Mengen x mit der Eigenschaft $x \notin x$. Diese Eigenschaft erfüllt M nach Voraussetzung im aktuellen Fall nicht, daher ist M nicht als Element enthalten in M. Also gilt $M \notin M$, im Widerspruch zur Voraussetzung dieses Falles.
- 2. Fall: Es gilt $M \notin M$.
  M enthält als Elemente gerade alle Mengen x mit der Eigenschaft $x \notin x$. Diese Eigenschaft erfüllt M nach Voraussetzung im aktuellen Fall, daher ist M als Element enthalten in M. Also gilt $M \in M$, im Widerspruch zur Voraussetzung dieses Falles.

Wir haben in beiden Fällen einen Widerspruch. Daher muss die Annahme, dass M eine Menge ist, falsch sein. $\square$

Beziehungen zwischen Mengen

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen.

- $\mathscr{N}$ heißt **Teilmenge** von $\mathscr{M}$, in Zeichen $\mathscr{N} \subseteq \mathscr{M}$, falls jedes Element von $\mathscr{N}$ auch Element von $\mathscr{M}$ ist.
  In dem Fall heißt $\mathscr{M}$ **Obermenge** von $\mathscr{N}$, in Zeichen $\mathscr{M} \supseteq \mathscr{N}$.
- $\mathscr{M}$ und $\mathscr{N}$ heißen **gleich**, in Zeichen $\mathscr{M} = \mathscr{N}$, falls sie die gleichen Elemente enthalten.
  Dies ist genau dann der Fall, wenn $\mathscr{M} \subseteq \mathscr{N}$ und $\mathscr{N} \subseteq \mathscr{M}$ gilt.
- $\mathscr{N}$ heißt **echte Teilmenge** von $\mathscr{M}$, in Zeichen $\mathscr{N} \subset \mathscr{M}$, falls $\mathscr{N} \subseteq \mathscr{M}$ und $\mathscr{N} \neq \mathscr{M}$.
- $\mathscr{M}$ und $\mathscr{N}$ heißen **disjunkt**, falls sie keine gemeinsamen Elemente besitzen.

Universum

Wenn wir Operationen auf Mengen ausführen, benötigen wir häufig eine Aussage, welche Elemente wir im Moment überhaupt verwenden.

Intuition

Das **Universum** ist die größte Menge, die wir untersuchen. Sie ist Obermenge aller anderen Mengen, die wir aktuell betrachten.

Operationen

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $\mathscr{U}$ das Universum, das heißt also insbesondere $\mathscr{M}, \mathscr{N} \subseteq \mathscr{U}$.

- Das **Komplement** von $\mathscr{M}$ bezüglich der Obermenge $\mathscr{U}$ ist $\mathscr{M}^C := \{x \in \mathscr{U} \mid x \notin \mathscr{M}\}$.
- Die **Vereinigung** von $\mathscr{M}$ und $\mathscr{N}$ ist $\mathscr{M} \cup \mathscr{N} := \{x \in \mathscr{U} \mid x \in \mathscr{M} \text{ oder } x \in \mathscr{N}\}$.
- Der **Schnitt** von $\mathscr{M}$ und $\mathscr{N}$ ist $\mathscr{M} \cap \mathscr{N} := \{x \in \mathscr{U} \mid x \in \mathscr{M} \text{ und } x \in \mathscr{N}\}$.
- Die **Differenz** von $\mathscr{M}$ und $\mathscr{N}$ ist $\mathscr{M} \backslash \mathscr{N} := \{x \in \mathscr{U} \mid x \in \mathscr{M} \text{ und } x \notin \mathscr{N}\}$.
  Es gilt $\mathscr{M} \backslash \mathscr{N} = \mathscr{M} \cap \mathscr{N}^C$.

Operationen

Beispiele

Es sei $U_1 := \{1, 2, 3, 4, 5\}$ das Universum.

$$\{1,2,3\}^C = \{4,5\}$$
$$\{1,2,3\} \cup \{2,5\} = \{1,2,3,5\}$$
$$\{1,2,3\} \cap \{2,5\} = \{2\}$$
$$\{1,2,3\} \backslash \{2,5\} = \{1,3\}$$

Es sei $U_2 := \mathbb{N}$ das Universum.

$$\{1,2,3\}^C = \{4,5,6,7,8,...\}$$
$$\{1,2,3\} \cup \{2,5\} = \{1,2,3,5\}$$
$$\{1,2,3\} \cap \{2,5\} = \{2\}$$
$$\{1,2,3\} \backslash \{2,5\} = \{1,3\}$$

Potenzmenge

Definition

Es sei $\mathscr{M}$ eine Menge.
Die **Potenzmenge** von $\mathscr{M}$ ist $\mathcal{P}(\mathscr{M}) := \{\mathscr{N} \mid \mathscr{N} \subseteq \mathscr{M}\}$.
Die Potenzmenge ist also die Menge aller Teilmengen von $\mathscr{M}$.
Beachte, dass immer $\emptyset \in \mathcal{P}(\mathscr{M})$ und $\mathscr{M} \in \mathcal{P}(\mathscr{M})$ gilt.
Manche Autoren schreiben $2^{\mathscr{M}}$ für $\mathcal{P}(\mathscr{M})$.

Potenzmenge

Beispiel

$$\begin{aligned}\mathcal{P}(\{1,2,3\}) = \{&\emptyset,\\ &\{1\},\{2\},\{3\},\\ &\{1,2\},\{1,3\},\{2,3\},\\ &\{1,2,3\}\}\end{aligned}$$

Gesetze

Es seien $\mathscr{M}, \mathscr{N}, \mathscr{O}$ Mengen und $\mathscr{U}$ das Universum. Dann gelten:

Idempotenzgesetze

$\mathscr{M} \cup \mathscr{M} = \mathscr{M}$
$\mathscr{M} \cap \mathscr{M} = \mathscr{M}$

Kommutativgesetze

$\mathscr{M} \cup \mathscr{N} = \mathscr{N} \cup \mathscr{M}$
$\mathscr{M} \cap \mathscr{N} = \mathscr{N} \cap \mathscr{M}$

Assoziativgesetze

$(\mathscr{M} \cup \mathscr{N}) \cup \mathscr{O} = \mathscr{M} \cup (\mathscr{N} \cup \mathscr{O})$
$(\mathscr{M} \cap \mathscr{N}) \cap \mathscr{O} = \mathscr{M} \cap (\mathscr{N} \cap \mathscr{O})$

Distributivgesetze

$\mathscr{M} \cup (\mathscr{N} \cap \mathscr{O}) = (\mathscr{M} \cup \mathscr{N}) \cap (\mathscr{M} \cup \mathscr{O})$
$\mathscr{M} \cap (\mathscr{N} \cup \mathscr{O}) = (\mathscr{M} \cap \mathscr{N}) \cup (\mathscr{M} \cap \mathscr{O})$

Komplementgesetze

$\mathscr{M} \cup \mathscr{M}^C = \mathscr{U}$
$\mathscr{M} \cap \mathscr{M}^C = \emptyset$

DeMorgansche Gesetze

$(\mathscr{M} \cup \mathscr{N})^C = \mathscr{M}^C \cap \mathscr{N}^C$
$(\mathscr{M} \cap \mathscr{N})^C = \mathscr{M}^C \cup \mathscr{N}^C$

Gesetze

Doppelkomplementgesetz

$(\mathscr{M}^C)^C = \mathscr{M}$

Merkwürdige Gesetze 1

$\mathscr{M} \cap (\mathscr{M} \cup \mathscr{N}) = \mathscr{M}$
$\mathscr{M} \cup (\mathscr{M} \cap \mathscr{N}) = \mathscr{M}$

Merkwürdige Gesetze 2

$\mathscr{U} \cup \mathscr{M} = \mathscr{U}$
$\mathscr{U} \cap \mathscr{M} = \mathscr{M}$

Merkwürdige Gesetze 3

$\emptyset \cup \mathscr{M} = \mathscr{M}$
$\emptyset \cap \mathscr{M} = \emptyset$

Kardinalität

Definition

Es sei $\mathscr{M}$ eine Menge.
Die **Kardinalität** von $\mathscr{M}$ ist die Anzahl der Elemente von $\mathscr{M}$.
Sie wird mit $|\mathscr{M}|$ bezeichnet.
Ist $\mathscr{M}$ endlich, so gilt $|\mathscr{M}| \in \mathbb{N}_0$, andernfalls schreiben wir $|\mathscr{M}| = \infty$.

Wir werden später auch noch eine genauere Unterscheidung von Mengen mit unendlich vielen Elementen einführen.

Kardinalität

Beispiele

$$M_2 = \{B, J, A, R\}$$
$$|M_2| = 4$$

$$M_6 = \{\{\clubsuit, b, J, \diamondsuit, A, \heartsuit, 25, \circ\}, Y, \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}\}$$
$$|M_6| = 3$$

$$\begin{aligned} M_7 = \{&\{\ldots, -8, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\},\\ &\{\ldots, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}\} \end{aligned}$$
$$|M_7| = 2$$

$$\begin{aligned} M_8 = \{&\{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\},\\ &\{\ldots, -11, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\},\\ &\{\ldots, -10, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}\} \end{aligned}$$
$$|M_8| = 3$$

Kardinalität

Beispiele

$$|\mathbb{N}| = \infty$$
$$|\mathbb{N}_0| = \infty$$
$$|\mathbb{Z}| = \infty$$
$$|\mathbb{Q}| = \infty$$
$$|\mathbb{R}| = \infty$$

Tupel

Intuition

Ein n-**Tupel** besitzt n Elemente (oder Einträge) und hat die Form

$$(x_1, x_2, \ldots, x_n)$$

Elemente dürfen hierbei mehrfach auftreten. Die Reihenfolge der Elemente ist wichtig: Zwei n-Tupel sind genau dann gleich, wenn an der gleichen Stelle das gleiche Element steht.

Beispiele

- $(1, 2, 3)$
- $(\clubsuit, A, 4, \gamma, \gamma, 4)$
- $(2, 2, 1) = (2, 2, 1) \neq (2, 1, 2)$
- $|\{A, 2, (3, 5)\}| = 3$

Kartesisches Produkt

Definitions-Vorläufer

Es seien $\mathscr{M}, \mathscr{N}$ Mengen. Dann heißt die Menge

$$\mathscr{M} \times \mathscr{N} := \{(x, y) \mid x \in \mathscr{M}, y \in \mathscr{N}\}$$

das **kartesische Produkt** von $\mathscr{M}$ und $\mathscr{N}$.

Beispiel

	a	b	c
1	$(1, a)$	$(1, b)$	$(1, c)$
2	$(2, a)$	$(2, b)$	$(2, c)$

Wir haben

$$\{1, 2\} \times \{a, b, c\} = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

Kartesisches Produkt

Beispiel

	$\square$	$\circ$	J
5	$(5, \square)$	$(5, \circ)$	$(5, J)$
$\bullet$	$(\bullet, \square)$	$(\bullet, \circ)$	$(\bullet, J)$

Wir haben

$$\{5, \bullet\} \times \{\square, \circ, J\} = \{(5, \square), (5, \circ), (5, J), (\bullet, \square), (\bullet, \circ), (\bullet, J)\}.$$

Kartesisches Produkt

Beispiel

	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$
2	$(2, \clubsuit)$	$(2, \diamondsuit)$	$(2, \heartsuit)$	$(2, \spadesuit)$
3	$(3, \clubsuit)$	$(3, \diamondsuit)$	$(3, \heartsuit)$	$(3, \spadesuit)$
4	$(4, \clubsuit)$	$(4, \diamondsuit)$	$(4, \heartsuit)$	$(4, \spadesuit)$
5	$(5, \clubsuit)$	$(5, \diamondsuit)$	$(5, \heartsuit)$	$(5, \spadesuit)$
6	$(6, \clubsuit)$	$(6, \diamondsuit)$	$(6, \heartsuit)$	$(6, \spadesuit)$
7	$(7, \clubsuit)$	$(7, \diamondsuit)$	$(7, \heartsuit)$	$(7, \spadesuit)$
8	$(8, \clubsuit)$	$(8, \diamondsuit)$	$(8, \heartsuit)$	$(8, \spadesuit)$
9	$(9, \clubsuit)$	$(9, \diamondsuit)$	$(9, \heartsuit)$	$(9, \spadesuit)$
10	$(10, \clubsuit)$	$(10, \diamondsuit)$	$(10, \heartsuit)$	$(10, \spadesuit)$
B	$(B, \clubsuit)$	$(B, \diamondsuit)$	$(B, \heartsuit)$	$(B, \spadesuit)$
D	$(D, \clubsuit)$	$(D, \diamondsuit)$	$(D, \heartsuit)$	$(D, \spadesuit)$
K	$(K, \clubsuit)$	$(K, \diamondsuit)$	$(K, \heartsuit)$	$(K, \spadesuit)$
A	$(A, \clubsuit)$	$(A, \diamondsuit)$	$(A, \heartsuit)$	$(A, \spadesuit)$

Kartesisches Produkt

Beispiel (fortgesetzt)

Wir haben

$$\begin{aligned}
&\{2,3,4,5,6,7,8,9,10,B,D,K,A\} \times \{\clubsuit,\diamondsuit,\heartsuit,\spadesuit\} \\
= &\{(2,\clubsuit),(2,\diamondsuit),(2,\heartsuit),(2,\spadesuit),(3,\clubsuit),(3,\diamondsuit),(3,\heartsuit),(3,\spadesuit), \\
&(4,\clubsuit),(4,\diamondsuit),(4,\heartsuit),(4,\spadesuit),(5,\clubsuit),(5,\diamondsuit),(5,\heartsuit),(5,\spadesuit), \\
&(6,\clubsuit),(6,\diamondsuit),(6,\heartsuit),(6,\spadesuit),(7,\clubsuit),(7,\diamondsuit),(7,\heartsuit),(7,\spadesuit), \\
&(8,\clubsuit),(8,\diamondsuit),(8,\heartsuit),(8,\spadesuit),(9,\clubsuit),(9,\diamondsuit),(9,\heartsuit),(9,\spadesuit), \\
&(10,\clubsuit),(10,\diamondsuit),(10,\heartsuit),(10,\spadesuit),(B,\clubsuit),(B,\diamondsuit),(B,\heartsuit),(B,\spadesuit), \\
&(D,\clubsuit),(D,\diamondsuit),(D,\heartsuit),(D,\spadesuit),(K,\clubsuit),(K,\diamondsuit),(K,\heartsuit),(K,\spadesuit), \\
&(A,\clubsuit),(A,\diamondsuit),(A,\heartsuit),(A,\spadesuit)\}.
\end{aligned}$$

Kartesisches Produkt

Definition

Es seien $\mathscr{M}_1, \ldots, \mathscr{M}_n$ Mengen. Dann heißt die Menge

$$\mathscr{M}_1 \times \ldots \times \mathscr{M}_n := \{(x_1, \ldots, x_n) \mid x_1 \in \mathscr{M}_1, \ldots, x_n \in \mathscr{M}_n\}$$

das **kartesische Produkt** von $\mathscr{M}_1, \ldots, \mathscr{M}_n$.
Für $\mathscr{M} \times \ldots \times \mathscr{M}$ schreiben wir auch kurz $\mathscr{M}^n$.
Wir setzen $\mathscr{M}^0 := \{()\}$.
Wir identifizieren $\mathscr{M}^1 = \mathscr{M}$.

Kartesisches Produkt

Beispiel

Wir haben

$$\begin{aligned}&\{1,2\}\times\{\triangle,\square,J\}\times\{a,b\}\\ =&\{(1,\triangle,a),(1,\triangle,b),(1,\square,a),(1,\square,b),(1,J,a),(1,J,b),\\ &(2,\triangle,a),(2,\triangle,b),(2,\square,a),(2,\square,b),(2,J,a),(2,J,b)\}.\end{aligned}$$

Beispiel

Es sei $\mathscr{M}$ eine Menge. Dann gilt

$$\mathscr{M}\times\emptyset=\emptyset.$$

Kartesisches Produkt

Beispiel

$$
\begin{aligned}
\{\circ\}^0 &= \{()\} \\
\{\circ\}^1 &= \{(\circ)\} = \{\circ\} \\
\{\circ\} \times \{\circ\} = \{\circ\}^2 &= \{(\circ, \circ)\} \\
\{\circ\} \times \{\circ\} \times \{\circ\} = \{\circ\}^3 &= \{(\circ, \circ, \circ)\}
\end{aligned}
$$

Beispiel

$$
\begin{aligned}
\{\circ, \bullet\}^0 &= \{()\} \\
\{\circ, \bullet\}^1 &= \{(\circ), (\bullet)\} = \{\circ, \bullet\} \\
\{\circ, \bullet\} \times \{\circ, \bullet\} = \{\circ, \bullet\}^2 &= \{(\circ, \circ), (\circ, \bullet), (\bullet, \circ), (\bullet, \bullet)\} \\
\{\circ, \bullet\} \times \{\circ, \bullet\} \times \{\circ, \bullet\} = \{\circ, \bullet\}^3 &= \{(\circ, \circ, \circ), (\circ, \circ, \bullet), (\circ, \bullet, \circ), (\circ, \bullet, \bullet), \\
&\qquad (\bullet, \circ, \circ), (\bullet, \circ, \bullet), (\bullet, \bullet, \circ), (\bullet, \bullet, \bullet)\}
\end{aligned}
$$

Kleenscher Abschluss

Definition

Es sei $\mathscr{M}$ eine Menge. Dann heißt

$$\mathscr{M}^* := \bigcup_{n=0}^{\infty} \mathscr{M}^n := \mathscr{M}^0 \cup \mathscr{M}^1 \cup \mathscr{M}^2 \cup \mathscr{M}^3 \cup \ldots$$

der **Kleensche Abschluss** von $\mathscr{M}$.

Beispiele

$$\{\circ\}^* = \{(), (\circ), (\circ, \circ), (\circ, \circ, \circ), (\circ, \circ, \circ, \circ), (\circ, \circ, \circ, \circ, \circ), \ldots\}$$
$$\{\circ, \bullet\}^* = \{(), (\circ), (\bullet), (\circ, \circ), (\circ, \bullet), (\bullet, \circ), (\bullet, \bullet), (\circ, \circ, \circ), \ldots\}$$

Positive Hülle

Definition

Es sei $\mathscr{M}$ eine Menge. Dann heißt

$$\mathscr{M}^+ := \bigcup_{n=1}^{\infty} \mathscr{M}^n := \mathscr{M}^1 \cup \mathscr{M}^2 \cup \mathscr{M}^3 \cup \ldots$$

die **positive Hülle** von $\mathscr{M}$.

Beispiele

$$\{\circ\}^+ = \{(\circ), (\circ,\circ), (\circ,\circ,\circ), (\circ,\circ,\circ,\circ), (\circ,\circ,\circ,\circ,\circ), \ldots\}$$
$$\{\circ,\bullet\}^+ = \{(\circ), (\bullet), (\circ,\circ), (\circ,\bullet), (\bullet,\circ), (\bullet,\bullet), (\circ,\circ,\circ), \ldots\}$$

Mengen

Aufgaben

Geben Sie die Elemente und die Kardinalität der folgenden Mengen an.

1. $[1, 10) \cap (\mathbb{N} \setminus \{5\})$
2. $[1, 10) \cap (\mathbb{N} \cup \{10\})$
3. $\{a, b\} \cup \{b, c\}$
4. $\{a, b\} \cap \{b, c\}$
5. $\{a, b\} \times \{b, c\}$
6. $\{1, 3\}^C$ für das Universum $\{1, 2, 3, 4\}$
7. $\{3\}^C$ für das Universum $\{1, 2, 3, 4\}$
8. $(\{a, b\} \times \{b, \{c\}\}) \cap (\{a\} \times \mathcal{P}(\{c\}))$

Übersicht

Definition

Definition

Es seien $\mathscr{M}_1, \dots, \mathscr{M}_n$ Mengen.
Eine **Relation** $\mathscr{R}$ über $\mathscr{M}_1, \dots, \mathscr{M}_n$ ist eine Teilmenge des kartesischen Produktes von $\mathscr{M}_1, \dots, \mathscr{M}_n$:

$$\mathscr{R} \subseteq \mathscr{M}_1 \times \dots \times \mathscr{M}_n$$

Im folgenden interessieren wir uns für zweistellige Relationen auf einer Menge.

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$.
Für $m \in \mathscr{M}$ und $n \in \mathscr{M}$ schreiben wir statt $(m, n) \in \mathscr{R}$ auch $m \ \mathscr{R} \ n$ und sagen »m steht in Relation zu n«.

Darstellungen

Relationen lassen sich in Mengenschreibweise, als Tabelle, als Matrix oder als Graph darstellen.

Exkurs – Graphen

Definition

Ein **Graph** $\mathscr{G} = (\mathscr{M}, \mathscr{R})$ besteht aus einer Eckenmenge $\mathscr{M}$ und einer Kantenmenge $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$.
Falls $\mathscr{R}$ symmetrisch ist, dann heißt $\mathscr{G}$ **ungerichtet**, andernfalls **gerichtet**.

Die Knotenmenge muss nicht endlich sein, ist es jedoch bei Informatikern in den allermeisten Fällen.

Es gibt eine ganze Flut von Anwendungsbeispielen, in denen man Graphen zur Modellierung verwendet, darunter Routenplanung für Automobile, Untersuchungen von Rechnernetzwerken und Analyse von Verkehrsströmen.

Beispiel

Beispiel

Wir betrachten als Grundmenge

$$M := \{A, B, C, D, E, F, G\}.$$

Wir betrachten die Menge

$$R := \{(A, A), (A, B), (C, C), (C, F), (E, C), (E, F), (F, E), (G, G)\}.$$

Es gilt $R \subseteq M \times M$, also ist R eine Relation auf M.

Beispiel

Beispiel (fortgesetzt)

Die Relation R als Liste dargestellt:

$$\begin{array}{c|l} A & A, B \\ B & \\ C & C, F \\ D & \\ E & C, F \\ F & E \\ G & G \end{array}$$

Beispiel

Beispiel (fortgesetzt)

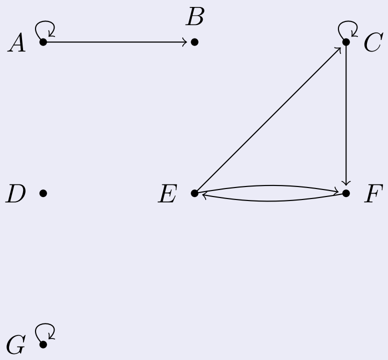
Die Relation R als Matrix dargestellt:

	A	B	C	D	E	F	G
A	X	X					
B							
C			X			X	
D							
E			X			X	
F					X		
G							X

Beispiel

Beispiel (fortgesetzt)

Die Relation R als Graph dargestellt:



Beispiel

Beispiel

Auf $\mathbb{N}$ gibt es die Relation

$$\begin{aligned}\leq = \{&(1,1),\\ &(1,2),(2,2),\\ &(1,3),(2,3),(3,3),\\ &(1,4),(2,4),(3,4),(4,4),...\} \subseteq \mathbb{N} \times \mathbb{N}\,.\end{aligned}$$

Obacht: $\leq$ ist hier ein Zeichen für eine Relation.

Beispiel

Beispiel

Auf $\mathbb{N}$ gibt es die Relation

$$R := \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y = x^2\}.$$

Aufgaben

1. Geben Sie 3 Elemente aus $\mathbb{N} \times \mathbb{N}$ an, die in R enthalten sind.
2. Geben Sie 3 Elemente aus $\mathbb{N} \times \mathbb{N}$ an, die nicht in R enthalten sind.

Beispiel

Beispiel

Auf $\mathbb{Z}$ gibt es die Relation

$$R := \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid \exists z \in \mathbb{N}_0 : y = x + z\}.$$

Aufgaben

1. Geben Sie 3 Elemente aus $\mathbb{Z} \times \mathbb{Z}$ an, die in R enthalten sind.
2. Geben Sie 3 Elemente aus $\mathbb{Z} \times \mathbb{Z}$ an, die nicht in R enthalten sind.

Eigenschaften

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$. $\mathscr{R}$ heißt

- **reflexiv**, wenn für alle $m \in \mathscr{M}$ gilt: $(m, m) \in \mathscr{R}$.

Eigenschaften

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$. $\mathscr{R}$ heißt

- **symmetrisch**, wenn für alle $m_1, m_2 \in \mathscr{M}$ gilt: aus $(m_1, m_2) \in \mathscr{R}$ folgt, dass $(m_2, m_1) \in \mathscr{R}$.

Eigenschaften

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$. $\mathscr{R}$ heißt

- **antisymmetrisch**, wenn für alle $m_1, m_2 \in \mathscr{M}$ gilt: aus $(m_1, m_2) \in \mathscr{R}$ und $(m_2, m_1) \in \mathscr{R}$ folgt, dass $m_1 = m_2$.

  Äquivalent: für alle $m_1, m_2 \in \mathscr{M}$ gilt: aus $m_1 \neq m_2$ folgt, dass $(m_1, m_2) \notin \mathscr{R}$ oder $(m_2, m_1) \notin \mathscr{R}$.

Eigenschaften

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$.
$\mathscr{R}$ heißt

- **transitiv**, wenn für alle $m_1, m_2, m_3 \in \mathscr{M}$ gilt:
  aus $(m_1, m_2) \in \mathscr{R}$ und $(m_2, m_3) \in \mathscr{R}$ folgt, dass $(m_1, m_3) \in \mathscr{R}$.

Eigenschaften

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$. $\mathscr{R}$ heißt

- **total**, wenn für alle $m_1, m_2 \in \mathscr{M}$ gilt: $(m_1, m_2) \in \mathscr{R}$ oder $(m_2, m_1) \in \mathscr{R}$.

Eigenschaften – mit mehr Symbolik

Definition

Es sei $\mathscr{M}$ eine Menge und $\mathscr{R} \subseteq \mathscr{M} \times \mathscr{M}$ eine Relation auf $\mathscr{M}$. $\mathscr{R}$ heißt

- **reflexiv** $:\Leftrightarrow \forall m \in \mathscr{M} : (m, m) \in \mathscr{R}$
- **symmetrisch** $:\Leftrightarrow$
  $\forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} : (m_1, m_2) \in \mathscr{R} \Rightarrow (m_2, m_1) \in \mathscr{R}$
- **antisymmetrisch** $:\Leftrightarrow \forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} :$
  $((m_1, m_2) \in \mathscr{R} \wedge (m_2, m_1) \in \mathscr{R}) \Rightarrow m_1 = m_2$
  Äquivalent: $\forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} :$
  $m_1 \neq m_2 \Rightarrow ((m_1, m_2) \notin \mathscr{R} \vee (m_2, m_1) \notin \mathscr{R})$
- **transitiv** $:\Leftrightarrow \forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} : \forall m_3 \in \mathscr{M} :$
  $((m_1, m_2) \in \mathscr{R} \wedge (m_2, m_3) \in \mathscr{R}) \Rightarrow (m_1, m_3) \in \mathscr{R}$
- **total** $:\Leftrightarrow$
  $\forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} : (m_1, m_2) \in \mathscr{R} \vee (m_2, m_1) \in \mathscr{R}$

Halbordnung

Definition

- Eine reflexive, antisymmetrische und transitive Relation $\mathscr{R}$ auf einer Menge $\mathscr{M}$ heißt **Halbordnung** (oder **partielle Ordnung**).
- $(\mathscr{M}, \mathscr{R})$ heißt **geordnete Menge**.

Halbordnung

Beispiele

- Auf den natürlichen Zahlen wird durch »|« eine Halbordnung definiert.
- Auf den natürlichen Zahlen wird durch »≤« eine Halbordnung definiert.
- Für eine beliebige Menge $\mathscr{M}$ wird auf $\mathcal{P}(\mathscr{M})$ durch »⊆« eine Halbordnung definiert. (In den folgenden Beispielen heißt die Relation $R_\subseteq$, da $\subseteq$ vielleicht etwas verwirrend ist.)

Teilmengenrelation auf Potenzmengen

Beispiel

Wir betrachten nun als Menge $N := \{\square, \triangledown\}$ und interessieren uns für eine Relation auf $M := \mathcal{P}(N)$. Wir halten zunächst fest:

$$M = \mathcal{P}(\{\square, \triangledown\}) = \{\emptyset, \{\square\}, \{\triangledown\}, \{\square, \triangledown\}\}.$$

Wir definieren nun eine Relation

$$R_{\subseteq} := \{(\mathscr{A}, \mathscr{B}) \in M \times M \mid \mathscr{A} \subseteq \mathscr{B}\}.$$

Teilmengenrelation auf Potenzmengen

Beispiel (fortgesetzt)

Wir haben

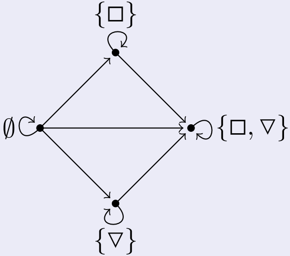
$$\begin{array}{rrrrr} M \times M = \{ & (\emptyset, \emptyset), & (\emptyset, \{\square\}), & (\emptyset, \{\triangledown\}), & (\emptyset, \{\square, \triangledown\}), \\ & (\{\square\}, \emptyset), & (\{\square\}, \{\square\}), & (\{\square\}, \{\triangledown\}), & (\{\square\}, \{\square, \triangledown\}), \\ & (\{\triangledown\}, \emptyset), & (\{\triangledown\}, \{\square\}), & (\{\triangledown\}, \{\triangledown\}), & (\{\triangledown\}, \{\square, \triangledown\}), \\ & (\{\square, \triangledown\}, \emptyset), & (\{\square, \triangledown\}, \{\square\}), & (\{\square, \triangledown\}, \{\triangledown\}), & (\{\square, \triangledown\}, \{\square, \triangledown\})\} \end{array}$$

$$\begin{array}{rrrrr} R_\subseteq = \{ & (\emptyset, \emptyset), & (\emptyset, \{\square\}), & (\emptyset, \{\triangledown\}), & (\emptyset, \{\square, \triangledown\}), \\ & & (\{\square\}, \{\square\}), & & (\{\square\}, \{\square, \triangledown\}), \\ & & & (\{\triangledown\}, \{\triangledown\}), & (\{\triangledown\}, \{\square, \triangledown\}), \\ & & & & (\{\square, \triangledown\}, \{\square, \triangledown\})\} \end{array}$$

Teilmengenrelation auf Potenzmengen

Beispiel (fortgesetzt)

Die Relation $R_\subseteq$ als Graph dargestellt:



Teilmengenrelation auf Potenzmengen

Beispiel

Wir betrachten nun als Menge $N := \{\square, \triangledown, \sharp\}$ und interessieren uns für eine Relation auf $M := \mathcal{P}(N)$. Wir halten zunächst fest:

$$\begin{aligned} M = \mathcal{P}(\{\square, \triangledown, \sharp\}) = \{&\emptyset, \\ &\{\square\}, \{\triangledown\}, \{\sharp\}, \\ &\{\square, \triangledown\}, \{\square, \sharp\}, \{\triangledown, \sharp\}, \\ &\{\square, \triangledown, \sharp\}\}. \end{aligned}$$

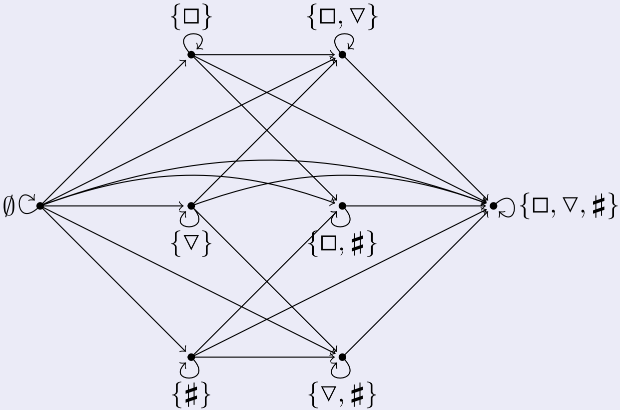
Wir definieren nun eine Relation

$$R_{\subseteq} := \{(\mathscr{A}, \mathscr{B}) \in M \times M \mid \mathscr{A} \subseteq \mathscr{B}\}.$$

Teilmengenrelation auf Potenzmengen

Beispiel (fortgesetzt)

Die Relation $R_\subseteq$ als Graph dargestellt:



Totalordnung

Definition

- Eine totale Ordnungsrelation $\mathscr{R}$ auf einer Menge $\mathscr{M}$ heißt **Totalordnung**.
- Eine Totalordnung ist also eine reflexive, antisymmetrische, transitive und totale Relation.
- $(\mathscr{M}, \mathscr{R})$ heißt **total geordnete Menge**.

Totalordnung

Beispiele

- Auf den natürlichen Zahlen wird durch »$\leq$« eine Totalordnung definiert.
- Obacht: Im Allgemeinen wird für eine beliebige Menge $\mathscr{M}$ auf $\mathcal{P}(\mathscr{M})$ durch »$\subseteq$« keine Totalordnung definiert.

Äquivalenzrelationen

Definition und Bemerkung

- Eine reflexive, symmetrische und transitive Relation $\mathscr{R}$ auf einer Menge $\mathscr{M}$ heißt **Äquivalenzrelation**.
- Äquivalenzrelationen induzieren eine Partitionierung der Grundmenge. Die Partitionen heißen **Äquivalenzklassen**.
- Die Äquivalenzklasse von $m \in \mathscr{M}$ wird mit $[m]_{\mathscr{R}} := \{n \in \mathscr{M} \mid (m, n) \in \mathscr{R}\}$ bezeichnet.
- Die Elemente einer Äquivalenzklasse heißen **Vertreter**.
- Mit $\mathscr{M}/\mathscr{R} := \{[m]_{\mathscr{R}} \mid m \in \mathscr{M}\}$ bezeichnen wir die Menge aller Äquivalenzklassen.
- Eine Äquivalenzrelation wird häufig mit $\sim$ bezeichnet.

Beitrag zur Allgemeinbildung

- Lat. »aequus« bedeutet in diesem Falle »gleich«.
- Lat. »valor« bedeutet in diesem Falle »Wert«.

Äquivalenzrelationen

Beispiel

Wir betrachten als Grundmenge

$$M := \{A, B, C, D, E, F\}.$$

Hierauf betrachten wir die Äquivalenzrelation

$$\begin{aligned} R := \{&(A, A), (A, D), (B, B), (C, C), (C, E), (C, F), (D, A), (D, D), \\ &(E, C), (E, E), (E, F), (F, C), (F, E), (F, F)\}. \end{aligned}$$

Wir haben folgende Äquivalenzklassen:

$$\begin{aligned} [A]_R &= \{A, D\} & [B]_R &= \{B\} & [C]_R &= \{C, E, F\} \\ [D]_R &= \{A, D\} & [E]_R &= \{C, E, F\} & [F]_R &= \{C, E, F\}. \end{aligned}$$

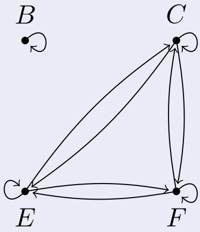
Die Menge der Äquivalenzklassen besteht damit aus

$$M/R = \{\{A, D\}, \{B\}, \{C, E, F\}\}.$$

Äquivalenzrelationen

Beispiel (fortgesetzt)

Zur Illustration R als Graph dargestellt:



Beispiel

Wir stellen uns die Frage, ob

$$\frac{1}{2} = \frac{3}{6}$$

gilt. Syntaktisch sind die beiden Seiten verschieden. Aber semantisch sollen die beiden Seiten gleich sein. Wir wollen nun versuchen, diese semantische Gleichheit zu formalisieren.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Um eine Gleichheit in den rationalen Zahlen zu überprüfen, können wir Äquivalenzumformungen anwenden, die uns eine Gleichheit auf den ganzen Zahlen liefern.

$$\frac{1}{2} = \frac{3}{6} \Leftrightarrow \frac{1}{2} \cdot 2 \cdot 6 = \frac{3}{6} \cdot 2 \cdot 6 \Leftrightarrow 1 \cdot 6 = 3 \cdot 2$$

Allgemeiner gilt:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a \cdot d = c \cdot b$$

Beispiel (fortgesetzt)

Wir wollen nun die rationalen Zahlen aus den ganzen Zahlen konstruieren. Hierzu setzen wir zunächst

$$M := \mathbb{Z} \times (\mathbb{Z} \backslash \{0\}) = \{(x, y) \mid x \in \mathbb{Z}, y \in \mathbb{Z}, y \neq 0\}$$

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir dürfen uns M etwa so vorstellen:

$$\begin{array}{cccccccccc}
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\
\cdots & (-2,-2) & (-2,-1) & (-2,1) & (-2,2) & (-2,3) & (-2,4) & (-2,5) & (-2,6) & \cdots \\
\cdots & (-1,-2) & (-1,-1) & (-1,1) & (-1,2) & (-1,3) & (-1,4) & (-1,5) & (-1,6) & \cdots \\
\cdots & (0,-2) & (0,-1) & (0,1) & (0,2) & (0,3) & (0,4) & (0,5) & (0,6) & \cdots \\
\cdots & (1,-2) & (1,-1) & (1,1) & (1,2) & (1,3) & (1,4) & (1,5) & (1,6) & \cdots \\
\cdots & (2,-2) & (2,-1) & (2,1) & (2,2) & (2,3) & (2,4) & (2,5) & (2,6) & \cdots \\
\cdots & (3,-2) & (3,-1) & (3,1) & (3,2) & (3,3) & (3,4) & (3,5) & (3,6) & \cdots \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

Beispiel (fortgesetzt)

In M gilt $(1,2) \neq (3,6)$.
Wir definieren auf M deshalb eine Relation $R \subseteq M \times M$ durch:

$$R := \{((a,b),(c,d)) \in M \times M \mid a \cdot d = c \cdot b\}.$$

Satz

R ist eine Äquivalenzrelation auf M.

Aufgabe

Zeigen Sie, dass R eine Äquivalenzrelation auf M ist.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir haben damit die Relation

$$
\begin{aligned}
R = \{&((-2,-4),(-2,-4)),((-2,-4),(-1,-2)),((-2,-4),(1,2)),\\
&((-2,-4),(2,4)),((-2,-4),(3,6)),((-2,-4),(4,8)),\dots,\\
&((1,2),(-2,-4)),((1,2),(-1,-2)),((1,2),(1,2)),\\
&((1,2),(2,4)),((1,2),(3,6)),((1,2),(4,8)),\dots,\\
&((3,6),(-2,-4)),((3,6),(-1,-2)),((3,6),(1,2)),\\
&((3,6),(2,4)),((3,6),(3,6)),((3,6),(4,8)),\dots,\\
&((5,7),(-15,-21)),((5,7),(-10,-14)),\dots,\\
&((-27,10),(54,-20)),\dots\}
\end{aligned}
$$

definiert.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Es gilt also beispielsweise

$$
\begin{aligned}
((1,2),(-2,-4)) &\in R \\
((1,2),(-1,-2)) &\in R \\
((1,2),(1,2)) &\in R \\
((1,2),(2,4)) &\in R \\
((1,2),(3,6)) &\in R \\
((1,2),(4,8)) &\in R \\
((3,6),(-1,-2)) &\in R \\
((5,7),(-10,-14)) &\in R
\end{aligned}
$$

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir setzen nun $Q := M/R$. Einige Elemente von Q (also Äquivalenzklassen von Elementen aus M) sind nun

$$
\begin{aligned}
[(1,2)]_R &= \{\dots, (-2,-4), (-1,-2), (1,2), (2,4), (3,6), (4,8), \dots\} \\
[(2,3)]_R &= \{\dots, (-4,-6), (-2,-3), (2,3), (4,6), (6,9) \dots, \} \\
[(4,8)]_R &= \{\dots, (-2,-4), (-1,-2), (1,2), (2,4), (3,6), (4,8), \dots\} \\
[(1,1)]_R &= \{\dots, (-3,-3), (-2,-2), (-1,-1), (1,1), (2,2), \dots\} \\
[(-1,1)]_R &= \{\dots, (-3,3), (-2,2), (-1,1), (1,-1), (2,-2), \dots\} \\
[(0,1)]_R &= \{\dots, (0,-3), (0,-2), (0,-1), (0,1), (0,2), \dots\} \\
[(3,6)]_R &= \{\dots, (-2,-4), (-1,-2), (1,2), (2,4), (3,6), (4,8), \dots\} \\
[(5,7)]_R &= \{\dots, (-10,-14), (-5,-7), (5,7), (10,14), (15,21), \dots\}
\end{aligned}
$$

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Es gilt also offenbar $[(1,2)]_R = [(3,6)]_R$. Wenn wir nun

$$\frac{a}{b} := [(a,b)]_R$$

definieren, dann haben wir unsere gewünschten Brüche. Wir erhalten also zum Beispiel

$$\frac{1}{2} = \{\dots, (-2,-4), (-1,-2), (1,2), (2,4), (3,6), (4,8), \dots\}$$

und

$$\frac{3}{6} = \{\dots, (-2,-4), (-1,-2), (1,2), (2,4), (3,6), (4,8), \dots\}.$$

An dieser Stelle könnte das Beispiel zu Ende sein. Ist es aber nicht.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir wollen unsere Brüche multiplizieren können. Wir wollen

$$\frac{m}{n} \cdot \frac{o}{p} := \frac{m \cdot o}{n \cdot p}$$

definieren, und für die Äquivalenzklassen bedeutet das, dass wir

$$[(m, n)]_R \cdot [(o, p)]_R := [(m \cdot o, n \cdot p)]_R$$

haben wollen. Damit diese Definition sinnvoll ist, müssen wir nachweisen, dass sie unabhängig von den Vertretern ist.

Äquivalenzrelationen
Das große Beispiel

Aufgabe

Zeigen Sie, dass die Multiplikation vertreterunabhängig ist.

Dafür muss für alle $m_1, m_2, o_1, o_2 \in \mathbb{Z}$ und $n_1, n_2, p_1, p_2 \in \mathbb{Z}\setminus\{0\}$ gelten:

aus $[(m_1, n_1)]_R = [(m_2, n_2)]_R$ und $[(o_1, p_1)]_R = [(o_2, p_2)]_R$ folgt $[(m_1 \cdot o_1, n_1 \cdot p_1)]_R = [(m_2 \cdot o_2, n_2 \cdot p_2)]_R$.

Aufgabe (Alternative Aufgabenstellung)

Zeigen Sie, dass die Multiplikation vertreterunabhängig ist.

Dafür muss für alle $m_1, m_2, o_1, o_2 \in \mathbb{Z}$ und $n_1, n_2, p_1, p_2 \in \mathbb{Z}\setminus\{0\}$ gelten:

aus $((m_1, n_1), (m_2, n_2)) \in R$ und $((o_1, p_1), (o_2, p_2)) \in R$ folgt $((m_1 \cdot o_1, n_1 \cdot p_1), (m_2 \cdot o_2, n_2 \cdot p_2)) \in R$.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir wollen die Brüche auch addieren können. Wir wollen

$$\frac{m}{n} + \frac{o}{p} := \frac{m \cdot p + o \cdot n}{n \cdot p}$$

definieren, und für die Äquivalenzklassen bedeutet das, dass wir

$$[(m, n)]_R + [(o, p)]_R := [(m \cdot p + o \cdot n, n \cdot p)]_R$$

haben wollen. Auch hier müssen wir die Vertreterunabhängigkeit nachweisen.

Äquivalenzrelationen
Das große Beispiel

Aufgabe

Zeigen Sie, dass die Addition vertreterunabhängig ist.

Dafür muss für alle $m_1, m_2, o_1, o_2 \in \mathbb{Z}$ und $n_1, n_2, p_1, p_2 \in \mathbb{Z} \backslash \{0\}$ gelten:

aus $[(m_1, n_1)]_R = [(m_2, n_2)]_R$ und $[(o_1, p_1)]_R = [(o_2, p_2)]_R$ folgt
$[(m_1 \cdot p_1 + o_1 \cdot n_1, n_1 \cdot p_1)]_R = [(m_2 \cdot p_2 + o_2 \cdot n_2, n_2 \cdot p_2)]_R$.

Aufgabe (Alternative Aufgabenstellung)

Zeigen Sie, dass die Addition vertreterunabhängig ist.

Dafür muss für alle $m_1, m_2, o_1, o_2 \in \mathbb{Z}$ und $n_1, n_2, p_1, p_2 \in \mathbb{Z} \backslash \{0\}$ gelten:

aus $((m_1, n_1), (m_2, n_2)) \in R$ und $((o_1, p_1), (o_2, p_2)) \in R$ folgt
$((m_1 \cdot p_1 + o_1 \cdot n_1, n_1 \cdot p_1), (m_2 \cdot p_2 + o_2 \cdot n_2, n_2 \cdot p_2)) \in R$.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Als Beispiel für eine nicht vertreterunabhängige Verknüpfung betrachten wir folgende (sinnlose) Definition:
Wir wollen

$$\frac{m}{n} \bigtriangleup \frac{o}{p} := \frac{m+o}{n \cdot p}$$

definieren, und für die Äquivalenzklassen bedeutet das, dass wir

$$[(m,n)]_R \bigtriangleup [(o,p)]_R := [(m+o, n \cdot p)]_R$$

haben wollen.

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Die Verknüpfung $\triangle$ ist nicht wohldefiniert. So ist

$$[(1,2)]_R \triangle [(2,5)]_R = [(3,10)]_R,$$

aber

$$[(3,6)]_R \triangle [(2,5)]_R = [(5,30)]_R.$$

Offenbar ist

$$[(1,2)]_R = [(3,6)]_R,$$

aber

$$[(3,10)]_R \neq [(5,30)]_R.$$

Also ist

$$\frac{1}{2} \triangle \frac{2}{5} \neq \frac{3}{6} \triangle \frac{2}{5}.$$

Äquivalenzrelationen
Das große Beispiel

Beispiel (fortgesetzt)

Wir dürfen also nicht davon ausgehen, dass jede beliebige Operation auf Äquivalenzklassen, die uns einfällt, sinnvoll ist. Wir müssen immer die Vertreterunabhängigkeit zeigen.

Moduloarithmetik

Für jede natürliche Zahl werden wir nun eine Äquivalenzrelation definieren.

Definition

Es sei $n \in \mathbb{N}$ fest gewählt. Wir definieren folgende Relation auf $\mathbb{Z}$:

$$\sim_n := \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \exists c \in \mathbb{Z} : a - b = c \cdot n\}.$$

Satz

$\sim_n$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Erinnerung

Außerhalb von

$$\{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \exists c \in \mathbb{Z} : a - b = c \cdot n\},$$

also etwa in Beweisen, ist zunächst kein a, b und c definiert.

Moduloarithmetik

Notation

- Wir schreiben statt $(a, b) \in \sim_n$ oder $a \sim_n b$ auch
$$a \equiv b \mod n$$
(und sagen: »a ist kongruent b modulo n«).
- Außerdem bezeichnen wir $\mathbb{Z}/{\sim_n}$ mit $\mathbb{Z}/n\mathbb{Z}$.
- Um Schreibarbeit zu sparen schreibt man manchmal $[a]_n$ statt $[a]_{\sim_n}$.

Wir wollen uns ein paar Beispiele zu dieser Relation ansehen.

Wir verwenden $n = 16$.

Moduloarithmetik

Wir haben die Relation

$$
\begin{aligned}
\sim_{16} = \{ \ldots,& \\
&(-31,-15), (-31,1), (-31,17), (-31,33), (-31,49), \ldots, \\
&(\ \ 0,-16), (\ \ 0,0), (\ \ 0,16), (\ \ 0,32), (\ \ 0,48), \ldots, \\
&(\ \ 1,-15), (\ \ 1,1), (\ \ 1,17), (\ \ 1,33), (\ \ 1,49), \ldots, \\
&(\ \ 3,-13), (\ \ 3,3), (\ \ 3,19), (\ \ 3,35), (\ \ 3,51), \ldots, \\
&(\ \ 17,-15), (\ \ 17,1), (\ \ 17,17), (\ \ 17,33), (\ \ 17,49), \ldots\}.
\end{aligned}
$$

Es gilt etwa

$$
\begin{array}{rcrcrl}
(0,16) \in \sim_{16} & \quad & 0 \sim_{16} 16 & \quad & 0 \equiv 16 & \mod 16 \\
(1,17) \in \sim_{16} & & 1 \sim_{16} 17 & & 1 \equiv 17 & \mod 16 \\
(1,49) \in \sim_{16} & & 1 \sim_{16} 49 & & 1 \equiv 49 & \mod 16 \\
(3,35) \in \sim_{16} & & 3 \sim_{16} 35 & & 3 \equiv 35 & \mod 16 \\
(11,43) \in \sim_{16} & & 11 \sim_{16} 43 & & 11 \equiv 43 & \mod 16 \\
(17,49) \in \sim_{16} & & 17 \sim_{16} 49 & & 17 \equiv 49 & \mod 16.
\end{array}
$$

Moduloarithmetik

Die Menge $\mathbb{Z}/16\mathbb{Z}$ besteht aus den folgenden Elementen:

$$
\begin{aligned}
[0]_{\sim 16} &= \{\dots, -48, -32, -16, 0, 16, 32, 48, 64, 80, \dots\} = [0]_{\sim 16} = [48]_{\sim 16}\\
[1]_{\sim 16} &= \{\dots, -47, -31, -15, 1, 17, 33, 49, 65, 81, \dots\} = [1]_{\sim 16} = [49]_{\sim 16}\\
[2]_{\sim 16} &= \{\dots, -46, -30, -14, 2, 18, 34, 50, 66, 82, \dots\} = [2]_{\sim 16} = [50]_{\sim 16}\\
[3]_{\sim 16} &= \{\dots, -45, -29, -13, 3, 19, 35, 51, 67, 83, \dots\} = [3]_{\sim 16} = [51]_{\sim 16}\\
[4]_{\sim 16} &= \{\dots, -44, -28, -12, 4, 20, 36, 52, 68, 84, \dots\} = [4]_{\sim 16} = [52]_{\sim 16}\\
[5]_{\sim 16} &= \{\dots, -43, -27, -11, 5, 21, 37, 53, 69, 85, \dots\} = [5]_{\sim 16} = [53]_{\sim 16}\\
[6]_{\sim 16} &= \{\dots, -42, -26, -10, 6, 22, 38, 54, 70, 86, \dots\} = [6]_{\sim 16} = [54]_{\sim 16}\\
[7]_{\sim 16} &= \{\dots, -41, -25, -9, 7, 23, 39, 55, 71, 87, \dots\} = [7]_{\sim 16} = [55]_{\sim 16}\\
[8]_{\sim 16} &= \{\dots, -40, -24, -8, 8, 24, 40, 56, 72, 88, \dots\} = [-8]_{\sim 16} = [56]_{\sim 16}\\
[9]_{\sim 16} &= \{\dots, -39, -23, -7, 9, 25, 41, 57, 73, 89, \dots\} = [-7]_{\sim 16} = [57]_{\sim 16}\\
[10]_{\sim 16} &= \{\dots, -38, -22, -6, 10, 26, 42, 58, 74, 90, \dots\} = [-6]_{\sim 16} = [58]_{\sim 16}\\
[11]_{\sim 16} &= \{\dots, -37, -21, -5, 11, 27, 43, 59, 75, 91, \dots\} = [-5]_{\sim 16} = [59]_{\sim 16}\\
[12]_{\sim 16} &= \{\dots, -36, -20, -4, 12, 28, 44, 60, 76, 92, \dots\} = [-4]_{\sim 16} = [60]_{\sim 16}\\
[13]_{\sim 16} &= \{\dots, -35, -19, -3, 13, 29, 45, 61, 77, 93, \dots\} = [-3]_{\sim 16} = [61]_{\sim 16}\\
[14]_{\sim 16} &= \{\dots, -34, -18, -2, 14, 30, 46, 62, 78, 94, \dots\} = [-2]_{\sim 16} = [62]_{\sim 16}\\
[15]_{\sim 16} &= \{\dots, -33, -17, -1, 15, 31, 47, 63, 79, 95, \dots\} = [-1]_{\sim 16} = [63]_{\sim 16}
\end{aligned}
$$

Moduloarithmetik

Wir dürfen die Äquivalenzklassen addieren, indem wir Vertreter aus den Klassen wählen, diese verknüpfen, und die Klasse des Ergebnisses nehmen.

Beispiel

$$\begin{aligned} &\{\ldots, -38, -22, -6, 10, 26, 42, 58, 74, 90, \ldots\} \\ +\ &\{\ldots, -41, -25, -9, 7, 23, 39, 55, 71, 87, \ldots\} \\ =\ &\{\ldots, -47, -31, -15, 1, 17, 33, 49, 65, 81, \ldots\} \end{aligned}$$

In anderer Schreibweise liest sich das als

Beispiel

$$\begin{aligned} &[10]_{\sim_{16}} \\ +\ &[7]_{\sim_{16}} \\ =\ &[17]_{\sim_{16}} \end{aligned}$$

Moduloarithmetik

Es gilt $[17]_{\sim_{16}} = [1]_{\sim_{16}}$, also dürfen wir genauso gut schreiben

Beispiel

$$\begin{array}{rr} & [10]_{\sim_{16}} \\ + & [7]_{\sim_{16}} \\ = & [1]_{\sim_{16}} \end{array}$$

Die Darstellung $[17]_{\sim_{16}}$ ist grundsätzlich nicht besser oder schlechter als die Darstellung $[1]_{\sim_{16}}$ oder auch die Darstellung $[49]_{\sim_{16}}$. Alle drei beschreiben dieselbe Menge, nämlich $\{\dots, -47, -31, -15, \ 1, 17, 33, 49, 65, 81, \dots\}$.

Moduloarithmetik

Wir dürfen die Äquivalenzklassen subtrahieren, indem wir Vertreter aus den Klassen wählen, diese verknüpfen, und die Klasse des Ergebnisses nehmen.

Beispiel

$$
\begin{aligned}
&\{\ldots, -38, -22, -6, 10, 26, 42, 58, 74, 90, \ldots\}\\
-\,&\{\ldots, -41, -25, -9, 7, 23, 39, 55, 71, 87, \ldots\}\\
=\,&\{\ldots, -45, -29, -13, 3, 19, 35, 51, 67, 83, \ldots\}
\end{aligned}
$$

In anderer Schreibweise liest sich das als

Beispiel

$$
\begin{aligned}
&[10]_{\sim_{16}}\\
-\,&[7]_{\sim_{16}}\\
=\,&[3]_{\sim_{16}}
\end{aligned}
\qquad\qquad
\begin{aligned}
&[10]_{\sim_{16}}\\
-\,&[7]_{\sim_{16}}\\
=\,&[-29]_{\sim_{16}}
\end{aligned}
$$

Moduloarithmetik

Wir dürfen die Äquivalenzklassen multiplizieren, indem wir Vertreter aus den Klassen wählen, diese verknüpfen, und die Klasse des Ergebnisses nehmen.

Beispiel

$$\begin{aligned} &\{\ldots, -38, -22, -\ \ 6, 10, 26, 42, 58, 74, 90, \ldots\} \\ \cdot\ &\{\ldots, -41, -25, -\ \ 9,\ \ 7, 23, 39, 55, 71, 87, \ldots\} \\ =\ &\{\ldots, -42, -26, -10,\ \ 6, 22, 38, 54, 70, 86, \ldots\} \end{aligned}$$

In anderer Schreibweise liest sich das als

Beispiel

$$\begin{aligned} &[10]_{\sim_{16}} \\ \cdot\ &\ [7]_{\sim_{16}} \\ =\ &[70]_{\sim_{16}} \end{aligned} \qquad\qquad \begin{aligned} &[10]_{\sim_{16}} \\ \cdot\ &\ [7]_{\sim_{16}} \\ =\ &\ [6]_{\sim_{16}} \end{aligned}$$

Moduloarithmetik

Nun wollen wir die Addition, Subtraktion und Multiplikation auf den Äquivalenzklassen definieren (bisher haben wir das noch nicht getan).

Definition

Es sei $n \in \mathbb{N}$. Für $[x]_{\sim_n}, [y]_{\sim_n} \in \mathbb{Z}/n\mathbb{Z}$ definieren wir

$$\begin{aligned}
[x]_{\sim_n} + [y]_{\sim_n} &:= [x+y]_{\sim_n}\\
[x]_{\sim_n} - [y]_{\sim_n} &:= [x-y]_{\sim_n}\\
[x]_{\sim_n} \cdot [y]_{\sim_n} &:= [x \cdot y]_{\sim_n}
\end{aligned}$$

Wir können die Äquivalenzklassen also vertreterweise addieren, subtrahieren und multiplizieren. Darüber hinaus gelten die aus $\mathbb{Z}$ bekannten Assoziativ-, Kommutativ- und Distributivgesetze.

Obacht: Wir haben am Beispiel der dritten Operation ($\triangle$) auf den Brüchen gesehen, dass es keineswegs selbstverständlich ist, dass eine vertreterweise Definition von Operationen sinnvoll ist.

Wir wissen nun

Beispiel

$$
\begin{aligned}
[10]_{\sim_{16}} + [7]_{\sim_{16}} &= [17]_{\sim_{16}} = [1]_{\sim_{16}} \\
[10]_{\sim_{16}} - [7]_{\sim_{16}} &= [3]_{\sim_{16}} = [-29]_{\sim_{16}} \\
[10]_{\sim_{16}} \cdot [7]_{\sim_{16}} &= [70]_{\sim_{16}} = [6]_{\sim_{16}}
\end{aligned}
$$

Wir können dies auch schreiben als

Beispiel

$$
\begin{aligned}
10 + 7 = 17 &\equiv 1 \mod 16 \\
10 - 7 = 3 &\equiv -29 \mod 16 \\
10 \cdot 7 = 70 &\equiv 6 \mod 16
\end{aligned}
$$

Moduloarithmetik

Die eben erklärte Äquivalenzrelation und die Rechenoperationen darauf sind für die Informatik ungemein wichtig. Unsere Rechner verarbeiten üblicherweise keineswegs Ganzzahlen, wie wir sie aus $\mathbb{Z}$ kennen. Die Standardaddition, -subtraktion und -multiplikation werden dort üblicherweise in $\mathbb{Z}/n\mathbb{Z}$ durchgeführt. Heute ist meist $n = 2^{64}$, früher $n = 2^{32}$. Oh, und noch viel früher $n = 2^{16}$. In Java ist meist $n = 2^{32}$.

Moduloarithmetik
Interessante Eigenschaften

Es ist

$$[10]_{\sim_{16}} \cdot [8]_{\sim_{16}} = [80]_{\sim_{16}} = [0]_{\sim_{16}},$$

oder in der anderen Notation

$$10 \cdot 8 = 80 \equiv 0 \mod 16.$$

In $\mathbb{Z}$ kann das Produkt zweier Zahlen niemals 0 sein, wenn keiner der beiden Faktoren 0 war.

Beitrag zur mathematischen Allgemeinbildung

Wenn das Produkt zweier Objekte 0 ergibt, so heißen die einzelnen Faktoren auch **Nullteiler** (die 0 selbst bezeichnet man meist nicht als Nullteiler).
Im Falle reell- oder komplexwertiger Matrizen sind dies genau die Matrizen mit Determinante 0.

Außerdem ist

$$[3]_{\sim_{16}} \cdot [11]_{\sim_{16}} = [33]_{\sim_{16}} = [1]_{\sim_{16}},$$

oder in der anderen Notation

$$3 \cdot 11 = 33 \equiv 1 \mod 16.$$

In $\mathbb{Z}$ kann eine Zahl ungleich ± 1 niemals durch Multiplikation mit einer anderen Zahl zu 1 werden.

Beitrag zur mathematischen Allgemeinbildung

Wenn das Produkt zweier Objekte 1 ergibt, so heißen die einzelnen Faktoren auch **multiplikative Einheiten** oder **multiplikativ invertierbare Elemente**.
Im Falle reell- oder komplexwertiger Matrizen sind dies genau die invertierbaren Matrizen, also genau die Matrizen mit Determinante $\neq 0$.

(Un-)Ordnung

Die Totalordnung $\leq$, die wir aus $\mathbb{Z}$ kennen, überträgt sich nicht ohne weiteres auf $\mathbb{Z}/n\mathbb{Z}$. Genauer ist es nicht möglich, die Ordnung vertreterweise zu übertragen.

Beispiel

In $\mathbb{Z}$ gilt $1 \leq 2$. Naiv wäre nun $[1]_{\sim_{16}} \leq [2]_{\sim_{16}}$. Weiter ist $[1]_{\sim_{16}} = [17]_{\sim_{16}}$. Damit wäre also $[17]_{\sim_{16}} \leq [2]_{\sim_{16}}$.
Da aber in $\mathbb{Z}$ $2 \leq 17$ gilt, hätten wir auch gerne $[2]_{\sim_{16}} \leq [17]_{\sim_{16}}$.
Wir verstricken uns in einen Widerspruch, denn aus der Antisymmetrie müsste nun $[17]_{\sim_{16}} = [2]_{\sim_{16}}$ folgen; das stimmt aber nicht.

Es ist aber möglich (und wird in unseren Rechnern auch so gemacht), die Totalordnung zu übertragen, sobald wir uns auf ein Vertretersystem festgelegt haben. Geläufig sind in unserem Falle die Systeme

$$-8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7$$

und

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.$$

Allerdings müssen wir auch dann noch aufpassen. Aus $\mathbb{Z}$ sind wir folgende Aussage gewohnt:

Für beliebige $w, x, y, z \in \mathbb{Z}$ gilt:

Wenn $w \leq x$ und $y \leq z$, dann ist $w + y \leq x + z$.

Beispiel

Es ist $1 \leq 9$ und $2 \leq 8$.
Damit ist auch $3 = 1 + 2 \leq 9 + 8 = 17$.

(Un-)Ordnung

Wenn wir nun versuchen, dies auf $\mathbb{Z}/n\mathbb{Z}$ zu übertragen, erhalten wir ein Problem. Wir legen uns hier auf das Vertretersystem $0, 1, \ldots, 15$ fest, das Problem tritt jedoch auch bei jedem anderen Vertretersystem auf.

Beispiel

Es ist $[1]_{\sim_{16}} \leq [9]_{\sim_{16}}$ und $[2]_{\sim_{16}} \leq [8]_{\sim_{16}}$.
Es ist aber $[3]_{\sim_{16}} = [1]_{\sim_{16}} + [2]_{\sim_{16}} \not\leq [9]_{\sim_{16}} + [8]_{\sim_{16}} = [1]_{\sim_{16}}$.

Das Phänomen des Überlaufes, das wir von unserem Rechner kennen, begegnet uns hier wieder. Wir müssen also sehr vorsichtig sein, wenn wir uns seit langem vertraute Sachverhalte auf die Arithmetik unseres Rechners, also auf $\mathbb{Z}/n\mathbb{Z}$, übertragen.

Moduloarithmetik
Zweimal modulo

Wir kennen von unserem Rechner ebenfalls eine Operation »Modulo«, die in Programmiersprachen manchmal mit % bezeichnet wird. Der Name »Modulo« ist für unsere Betrachtungsweise ungeschickt gewählt, aber üblich. Dummerweise verträgt sich die Operation auch nicht von vornherein mit unserer Moduloarithmetik.

Beispiel

Es gilt $4 \,\%\, 3 = 1$ und $20 \,\%\, 3 = 2$. Wir haben außerdem $[4]_{\sim_{16}} = [20]_{\sim_{16}}$.
Was soll nun $[4]_{\sim_{16}} \,\%\, [3]_{\sim_{16}}$ sein? Es muss dasselbe Ergebnis wie $[20]_{\sim_{16}} \,\%\, [3]_{\sim_{16}}$ sein, da $[4]_{\sim_{16}}$ und $[20]_{\sim_{16}}$ beide dasselbe Objekt bezeichnen.

Eine Definition der Form

Keine Definition

Es sei $n \in \mathbb{N}$. Für $[x]_{\sim_n}, [y]_{\sim_n} \in \mathbb{Z}/n\mathbb{Z}$ definieren wir

$$[x]_{\sim_n} \;\%\; [y]_{\sim_n} := [x \;\%\; y]_{\sim_n}$$

funktioniert also nicht.

Wenn wir uns auf ein Vertretersystem festlegen, etwa $0, 1, \dots, 15$, so ist das Ergebnis klar, im Beispiel also $[4]_{\sim_{16}} \;\%\; [3]_{\sim_{16}} = [1]_{\sim_{16}}$. Und genau das wird auch in unserem Rechner gemacht.

Moduloarithmetik
Exkurs – Teilbarkeit

Die Moduloarithmetik verschafft uns für die Frage, ob eine Zahl durch 11 teilbar ist, eine einfache Lösung.

Durch 11 teilbar zu sein, bedeutet ja, Vielfaches von 11 zu sein.

Und Vielfaches von 11 zu sein, bedeutet ja, kongruent 0 modulo 11 zu sein.

Wenn wir also einen einfachen Weg finden, um herauszufinden, ob eine Zahl kongruent 0 modulo 11 ist, haben wir damit auch einen einfachen Weg gefunden, um herauszufinden, ob sie durch 11 teilbar ist.

Sehen wir uns also an, wie wir einfach prüfen können, ob eine Zahl kongruent 0 modulo 11 ist.

Wir halten fest:

$$
\begin{array}{rrl@{\qquad\qquad}r}
1 \equiv & 1 & \mod 11 & (1, \quad 1) \in \sim_{11} \\
10 \equiv & -1 & \mod 11 & (10, -1) \in \sim_{11} \\
100 \equiv & 1 & \mod 11 & (100, \quad 1) \in \sim_{11} \\
1000 \equiv & -1 & \mod 11 & (1000, -1) \in \sim_{11} \\
\dots & & &
\end{array}
$$

Deshalb können wir die Frage nach »kongruent 0 modulo 11« beantworten, indem wir die alternierende Quersumme bilden und prüfen, ob das Ergebnis kongruent 0 modulo 11 ist.

Drei Beispiele sollen das illustrieren.

Moduloarithmetik
Exkurs – Teilbarkeit

Beispiel

Es gilt

$$\begin{aligned}3524 &= 3 \cdot 1000 + 5 \cdot 100 + 2 \cdot 10 + 4 \cdot 1 \\ &\equiv 3 \cdot (-1) + 5 \cdot 1 + 2 \cdot (-1) + 4 \cdot 1 \\ &= -3 + 5 - 2 + 4 \\ &= 4 \mod 11,\end{aligned}$$

also gilt

$$3524 \equiv 4 \mod 11,$$

also ist 3524 nicht durch 11 teilbar.
(Wir wissen sogar, dass 3524 durch 11 geteilt den Rest 4 gibt.)

Beispiel

Es gilt

$$\begin{aligned}5874 &= 5 \cdot 1000 + 8 \cdot 100 + 7 \cdot 10 + 4 \cdot 1\\ &\equiv 5 \cdot (-1) + 8 \cdot 1 + 7 \cdot (-1) + 4 \cdot 1\\ &= -5 + 8 - 7 + 4\\ &= 0 \mod 11,\end{aligned}$$

also gilt

$$5874 \equiv 0 \mod 11,$$

also ist 5874 durch 11 teilbar.

Beispiel

Es gilt

$$\begin{aligned}902 &= 9 \cdot 100 + 0 \cdot 10 + 2 \cdot 1 \\ &\equiv 9 \cdot 1 + 0 \cdot (-1) + 2 \cdot 1 \\ &= 9 - 0 + 2 \\ &= 11 \\ &\equiv 0 \mod 11,\end{aligned}$$

also gilt

$$902 \equiv 0 \mod 11,$$

also ist 902 durch 11 teilbar.

Übersicht

Abbildungen

Definition

- Eine **Abbildung** $\mathscr{f}$ von einer Menge $\mathscr{M}$ in eine Menge $\mathscr{N}$ ist eine Zuordnung, die jedem Element aus $\mathscr{M}$ genau ein Element aus $\mathscr{N}$ zuordnet. Wir schreiben hierfür $\mathscr{f} : \mathscr{M} \to \mathscr{N}$.
- $\mathscr{M}$ heißt **Definitionsbereich** (oder **Urbildbereich**), $\mathscr{N}$ heißt **Bildbereich** von $\mathscr{f}$.
- Falls $\mathscr{f}$ ein $m \in \mathscr{M}$ auf ein $n \in \mathscr{N}$ abbildet, so schreiben wir $\mathscr{f}(m) = n$.
- $\mathrm{Bild}(\mathscr{f}) := \{\mathscr{f}(m) \in \mathscr{N} \mid m \in \mathscr{M}\}$ heißt **Bild** von $\mathscr{f}$.
- $\mathrm{Abb}(\mathscr{M}, \mathscr{N}) := \{\mathscr{f} : \mathscr{M} \to \mathscr{N}\}$ ist die Menge aller Abbildungen von $\mathscr{M}$ nach $\mathscr{N}$.
- Falls $\mathscr{M} \subseteq \mathbb{C}^n$ und $\mathscr{N} \subseteq \mathbb{C}^m$, so spricht man von $\mathscr{f}$ häufig auch als **Funktion**.

Abbildungen

Beispiele

Wir betrachten die Abbildung

$$\begin{aligned} f_1 : \{a, b, c\} &\to \{1, 2, 3, 4\} \\ a &\mapsto 1 \\ b &\mapsto 4 \\ c &\mapsto 1. \end{aligned}$$

Es gilt

$$\begin{aligned} \mathrm{Bild}(f_1) &= \{f_1(a), f_1(b), f_1(c)\} \\ &= \{1, 4, 1\} \\ &= \{1, 4\}. \end{aligned}$$

Abbildungen

Beispiele

$$\begin{aligned} f_2 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^3 + x^2 + 3 \end{aligned}$$

$$\begin{aligned} f_3 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sin(x) \end{aligned}$$

Abbildungen

Vorsicht

$\cos(x)$ ist keine Abbildung, cos hingegen schon.

$\cos(x)$ könnte man, wenn man denn unbedingt wollte, als »abhängige Variable« bezeichnen. Es ist ein Wert, der von der Variablen x abhängt und damit in gewisser Weise auch eine Variable ist. Nur dürfen wir den Wert von $\cos(x)$ nicht beliebig wählen, vielmehr ergibt sich dieser aus dem Wert von x.

Der Unterschied ist vergleichbar mit dem Unterschied zwischen einer Reihung `R` und einem Reihungselement `R[n]` in einer Programmiersprache.

Abbildungen

Beispiele

$$
\begin{aligned}
f_4 : \{\square, \nabla, \sharp, *\} &\to \{\square, \nabla, \sharp, *\}\\
\square &\mapsto \square\\
\nabla &\mapsto \sharp\\
\sharp &\mapsto \square\\
* &\mapsto \nabla
\end{aligned}
$$

$$
\begin{aligned}
f_5 : \{\square, \nabla, \sharp, *\}^2 &\to \{\square, \nabla, \sharp, *\}\\
(x_1, x_2) &\mapsto \begin{cases} \square, & \text{falls } (x_1, x_2) = (\nabla, \sharp)\\ *, & \text{falls } x_1 = \sharp\\ \sharp, & \text{sonst} \end{cases}
\end{aligned}
$$

Abbildungen

Beispiele

$$
\begin{aligned}
f_6 : \mathbb{R}^2 &\to \mathbb{R} \\
(x_1, x_2) &\mapsto 2 \cdot x_1 + 5 \cdot x_2
\end{aligned}
$$

$$
\begin{aligned}
f_7 : \mathbb{R} &\to \mathbb{R} \\
x &\mapsto \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{sonst} \end{cases}
\end{aligned}
$$

Abbildungen

Kein Beispiel

$$f_8 : \mathbb{Q} \to \mathbb{Z}$$
$$\frac{p}{q} \mapsto p$$

$$f_8\left(\frac{1}{2}\right) = 1$$
$$f_8\left(\frac{2}{4}\right) = 2$$

Aber $\frac{1}{2} = \frac{2}{4}$. Also ist f_8 nicht wohldefiniert und damit keine Abbildung.

Abbildungen

Beispiele

$$\mathrm{Bild}(f_1) = \{1, 4\}$$
$$\mathrm{Bild}(f_2) = \mathbb{R}$$
$$\mathrm{Bild}(f_3) = [-1, 1]$$
$$\mathrm{Bild}(f_4) = \{\square, \triangledown, \sharp\}$$
$$\mathrm{Bild}(f_5) = \{\square, \sharp, *\}$$
$$\mathrm{Bild}(f_6) = \mathbb{R}$$
$$\mathrm{Bild}(f_7) = \mathbb{R}_{\geq 0}$$

Abbildungen

Beispiel

$$\begin{aligned} f_9 : \{1,2,3\} &\to \mathrm{Abb}(\mathbb{N}, \mathbb{N}) \\ 1 &\mapsto (n \mapsto n) \\ 2 &\mapsto (n \mapsto n^2) \\ 3 &\mapsto (n \mapsto n + 25) \end{aligned}$$

Wir haben $(f_9(2))(9) = 81$ und $(f_9(3))(7) = 32$.
Es gilt $f_9 \in \mathrm{Abb}(\{1,2,3\}, \mathrm{Abb}(\mathbb{N}, \mathbb{N}))$.

Erläuterungen

Beachte, dass $\mathbb{R} \subseteq \mathbb{C}$ gilt, also sind die handelsüblichen Funktionen aus der Schule auch bei uns Funktionen.

Beachte ferner, dass zu einer Abbildung immer ein Definitionsbereich und ein Bildbereich gehören. Selbst wenn die Vorschrift dieselbe ist, handelt es sich um zwei verschiedene Abbildungen, falls einer der Bereiche verschieden ist.

Beispiel

$$\begin{aligned} f_{10} : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

$$\begin{aligned} f_{11} : \mathbb{R} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto x^2 \end{aligned}$$

f_{10} und f_{11} sind verschiedene Abbildungen.

Abändern von Abbildungen

Zu Mengen $\mathscr{M}, \mathscr{N}$ und einer Abbildung $\mathscr{f} : \mathscr{M} \to \mathscr{N}$ erhalten wir für ein $\boldsymbol{m} \in \mathscr{M}$ und ein $\boldsymbol{n} \in \mathscr{N}$ eine modifizierte Abbildung $\mathscr{f}\,^{\boldsymbol{n}}_{m} : \mathscr{M} \to \mathscr{N}$, die wie folgt definiert ist:

$$\mathscr{f}\,^{\boldsymbol{n}}_{m}(x) := \begin{cases} \boldsymbol{n}, & \text{falls } x = \boldsymbol{m} \\ \mathscr{f}(x), & \text{falls } x \neq \boldsymbol{m}. \end{cases}$$

Abändern von Abbildungen

Beispiel

Wir betrachten die Abbildung

$$\begin{aligned} f : \{a, b, c\} &\to \{1, 2, 3, 4\} \\ a &\mapsto 1 \\ b &\mapsto 4 \\ c &\mapsto 1. \end{aligned}$$

Dann ist $f_c^3 : \{a, b, c\} \to \{1, 2, 3, 4\}$ und es gilt

$$\begin{aligned} f_c^3(a) &= 1 \\ f_c^3(b) &= 4 \\ f_c^3(c) &= 3. \end{aligned}$$

Schreibweisen

Bei Abbildungen mit zwei Argumenten (der Definitionsbereich ist von der Form $\mathscr{M} \times \mathscr{N}$) gibt es neben der Präfix-Schreibweise $\mathscr{f}(\mathscr{m}, \mathscr{n})$ auch die Infix-Schreibweise $\mathscr{m}\,\mathscr{f}\,\mathscr{n}$. Wir kennen dies etwa von der Addition. Wir schreiben meist nicht $+(2, 5)$ sondern $2 + 5$.

Daneben gibt es noch die Postfix-Schreibweise, etwa $\mathscr{m}\,\mathscr{n}\,\mathscr{f}$.

Rekursion

Die Vorschrift einer Abbildung $\mathbb{N} \to \mathcal{N}$ für eine Menge $\mathcal{N}$ kann auch rekursiv angegeben werden. Hierbei werden die Abbildungswerte für eine oder mehrere (meist kleine) Zahlen direkt definiert; die Abbildungswerte aller größeren Zahlen werden dann unter Zuhilfenahme der bereits definierten Werte definiert.

So können wir etwa statt der direkten Definition

$$\text{Fakultät}(n) := 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$$

auch die rekursive Definition

$$\begin{aligned} \text{Fakultät}(1) &:= 1 \\ \text{Fakultät}(n) &:= n \cdot \text{Fakultät}(n-1),\ n > 1 \end{aligned}$$

der Funktion »Fakultät« angeben.

Partielle Abbildungen

Definition

Es seien $\mathscr{M}, \mathscr{M}', \mathscr{N}$ Mengen, $f : \mathscr{M} \to \mathscr{N}$ eine Abbildung und $\mathscr{M} \subseteq \mathscr{M}'$.
Dann heißt

$$g : \mathscr{M}' \to \mathscr{N} \text{ mit } g(m) = \begin{cases} f(m), & m \in \mathscr{M} \\ \perp, & m \notin \mathscr{M} \end{cases}$$

eine **partielle Abbildung**.

Das Zeichen $\perp$ steht für »undefiniert«. Bei partiellen Abbildungen lassen wir also Definitionslücken ausdrücklich zu.

Partielle Abbildungen werden benötigt, wenn wir Algorithmen als Berechnungsvorschriften von Abbildungen begreifen. Dann kann es Eingaben für den Algorithmus geben, für die es keine Ausgabe gibt (Endlosschleife, Division durch 0, ...).

Partielle Abbildungen

Beispiel

Wir betrachten die Abbildung

$$\begin{aligned} f : \mathbb{R} \backslash \{0\} &\to \mathbb{R} \\ x &\mapsto \frac{1}{x}. \end{aligned}$$

Daraus erhalten wir beispielsweise die partielle Abbildung

$$\begin{aligned} g : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \begin{cases} \frac{1}{x}, & x \neq 0 \\ \perp, & x = 0. \end{cases} \end{aligned}$$

Gleichheit

Bemerkung

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$, $g : \mathscr{M} \to \mathscr{N}$ Abbildungen.

- Wenn für alle $m \in \mathscr{M}$ gilt $f(m) = g(m)$, dann gilt $f = g$.

Zwei Abbildungen zwischen denselben Mengen stimmen also überein, wenn sie elementweise übereinstimmen.

Identität

Definition

Es sei $\mathscr{M}$ eine Menge. Dann heißt

$$\begin{aligned} id_{\mathscr{M}} : \mathscr{M} &\to \mathscr{M} \\ m &\mapsto m \end{aligned}$$

die **Identität** auf $\mathscr{M}$.

Eigenschaften

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$ eine Abbildung.
f heißt

- **injektiv**, wenn für alle $m_1, m_2 \in \mathscr{M}$ gilt:
  aus $f(m_1) = f(m_2)$ folgt, dass $m_1 = m_2$.

  Äquivalent: für alle $m_1, m_2 \in \mathscr{M}$ gilt:
  aus $m_1 \neq m_2$ folgt, dass $f(m_1) \neq f(m_2)$.

  (Jedes Element aus $\mathscr{N}$ wird höchstens einmal getroffen.)

Abbildungen

Beispiel

Die Abbildung

$$\begin{aligned} f : \{\square, \triangledown, \sharp\} &\to \{a, b, c, d\} \\ \square &\mapsto c \\ \triangledown &\mapsto d \\ \sharp &\mapsto a \end{aligned}$$

ist injektiv.

Abbildungen

Kein Beispiel

Die Abbildung

$$\begin{aligned} f : \{\square, \nabla, \sharp\} &\to \{a, b, c, d\} \\ \square &\mapsto c \\ \nabla &\mapsto a \\ \sharp &\mapsto c \end{aligned}$$

ist nicht injektiv,
denn $f(\square) = f(\sharp)$, aber $\square \neq \sharp$.

Eigenschaften

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$ eine Abbildung.
f heißt

- **surjektiv**, wenn es für alle $n \in \mathscr{N}$ ein $m \in \mathscr{M}$ gibt mit $f(m) = n$.

  (Jedes Element aus $\mathscr{N}$ wird mindestens einmal getroffen.)

Zu einer Abbildung erhalten wir immer mit Gewalt eine surjektive Abbildung, indem wir den Bildbereich auf das Bild einschränken.

Abbildungen

Beispiel

Die Abbildung

$$
\begin{aligned}
f : \{\square, \triangledown, \sharp, *\} &\to \{a, b, c\} \\
\square &\mapsto c \\
\triangledown &\mapsto a \\
\sharp &\mapsto b \\
* &\mapsto a
\end{aligned}
$$

ist surjektiv.

Abbildungen

Kein Beispiel

Die Abbildung

$$
\begin{aligned}
f : \{\square, \triangledown, \sharp, *\} &\to \{a, b, c\} \\
\square &\mapsto c \\
\triangledown &\mapsto a \\
\sharp &\mapsto a \\
* &\mapsto c
\end{aligned}
$$

ist nicht surjektiv,
denn für $b \in \{a, b, c\}$ gibt es kein $m \in \{\square, \triangledown, \sharp, *\}$ mit $f(m) = b$.

Eigenschaften

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$ eine Abbildung.

- f heißt **bijektiv**, falls f injektiv und surjektiv ist.

  (Jedes Element aus $\mathscr{N}$ wird genau einmal getroffen.)

Bemerkung

Die Identität $id_{\mathscr{M}}$ auf einer Menge $\mathscr{M}$ ist immer bijektiv.

Eigenschaften – mit mehr Symbolik

Definition

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$ eine Abbildung.
f heißt

- **injektiv** $:\Leftrightarrow$
  $\forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} : f(m_1) = f(m_2) \Rightarrow m_1 = m_2$.
  Äquivalent:
  $\forall m_1 \in \mathscr{M} : \forall m_2 \in \mathscr{M} : m_1 \neq m_2 \Rightarrow f(m_1) \neq f(m_2)$.
- **surjektiv** $:\Leftrightarrow \forall n \in \mathscr{N} : \exists m \in \mathscr{M} : f(m) = n$.

Eigenschaften

Beispiele

	injektiv	nicht injektiv
surjektiv	$f_1 : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$	$f_2 : \mathbb{R} \to \mathbb{R}_{\geq 0}$, $x \mapsto x^2$
nicht surjektiv	$f_3 : \mathbb{R}_{\geq 0} \to \mathbb{R}$, $x \mapsto x^2$	$f_4 : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$

Charakterisierung unendlicher Mengen

Satz

Eine Menge $\mathscr{M}$ hat genau dann unendlich viele Elemente, wenn es eine injektive Abbildung von $\mathscr{M}$ in eine *echte* Teilmenge von $\mathscr{M}$ gibt.

Beispiel

Die Menge $\mathbb{N}$ hat unendlich viele Elemente; und die Abbildung

$$\begin{aligned} f : \mathbb{N} &\to \mathbb{N} \setminus \{1\} \\ n &\mapsto n + 1 \end{aligned}$$

ist eine injektive Abbildung von $\mathbb{N}$ in eine echte Teilmenge von $\mathbb{N}$.

Kardinalität

Satz

Für zwei endliche Mengen $\mathscr{M}, \mathscr{N}$ gilt:
$|\mathscr{M}| \leq |\mathscr{N}|$ genau dann, wenn es eine injektive Abbildung von $\mathscr{M}$ nach $\mathscr{N}$ gibt.

Satz

Für zwei endliche Mengen $\mathscr{M}, \mathscr{N}$ gilt:
$|\mathscr{M}| \geq |\mathscr{N}|$ genau dann, wenn es eine surjektive Abbildung von $\mathscr{M}$ nach $\mathscr{N}$ gibt.

Preisfrage

Wann haben zwei endliche Mengen gleich viele Elemente?

Mächtigkeit

Wir möchten nun wissen, ob alle Mengen mit unendlich vielen Elementen »gleich groß« sind (offenbar sind sie dies nicht, sonst gäbe es diese Folie nicht).

Definition

Zwei Mengen $\mathscr{M}, \mathscr{N}$ heißen **gleich mächtig**, wenn es eine bijektive Abbildung von $\mathscr{M}$ nach $\mathscr{N}$ gibt.

Satz

Endliche Mengen $\mathscr{M}, \mathscr{N}$ sind genau dann gleich mächtig, wenn $|\mathscr{M}| = |\mathscr{N}|$.

Abzählbarkeit

Definition

Eine Menge $\mathscr{M}$ heißt **abzählbar**, wenn $\mathbb{N}$ gleich mächtig wie $\mathscr{M}$ ist. Eine nicht-endliche, nicht-abzählbare Menge heißt **überabzählbar**.

Abzählbarkeit

Beispiele

- $\mathbb{N}, \{\circ\}^+, \mathbb{N}_0, \mathbb{Z}, \mathbb{Q}$ sind abzählbar.
- $\mathbb{R}, \mathbb{C}, [0,1)$ sind überabzählbar.

Satz

Die abzählbare Vereinigung abzählbarer Mengen ist abzählbar.

Verkettung

Definition

Es seien $\mathscr{M}, \mathscr{N}, \mathscr{O}$ Mengen und $f : \mathscr{M} \to \mathscr{N}$, $g : \mathscr{N} \to \mathscr{O}$ Abbildungen.
Dann heißt die Abbildung

$$\begin{aligned} g \circ f : \mathscr{M} &\to \mathscr{O} \\ m &\mapsto g(f(m)) \end{aligned}$$

die **Verkettung** (oder **Komposition**) von f und g (Sprechweise: »g nach f«).

$$\begin{tikzcd} \mathscr{M} \arrow[r, bend left, "f"] \arrow[rr, bend right, "g \circ f"'] & \mathscr{N} \arrow[r, bend left, "g"] & \mathscr{O} \end{tikzcd}$$

Verkettung

Bemerkung

Die Verkettung ist nichts anderes als die Hintereinanderausführung der Abbildungen.

Verkettung

Beispiel

Es seien

$$\begin{aligned} f_1 : \{1,2,3,4\} &\to \{a,b,c,d,e\} \\ 1 &\mapsto b \\ 2 &\mapsto d \\ 3 &\mapsto e \\ 4 &\mapsto b \end{aligned}$$

und

$$\begin{aligned} g_1 : \{a,b,c,d,e\} &\to \{\Box, \triangledown, \sharp\} \\ a &\mapsto \Box \\ b &\mapsto \sharp \\ c &\mapsto \triangledown \\ d &\mapsto \Box \\ e &\mapsto \sharp. \end{aligned}$$

Verkettung

Beispiel (fortgesetzt)

Dann gilt

$$\begin{aligned} g_1 \circ f_1 : \{1,2,3,4\} &\to \{\square, \triangledown, \sharp\} \\ 1 &\mapsto \sharp \\ 2 &\mapsto \square \\ 3 &\mapsto \sharp \\ 4 &\mapsto \sharp. \end{aligned}$$

Und wir bemerken, dass $f_1 \circ g_1$ nicht definiert ist.

Verkettung

Beispiel

Es seien

$$\begin{aligned} f_2 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 \end{aligned}$$

und

$$\begin{aligned} g_2 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x + 1. \end{aligned}$$

Verkettung

Beispiel (fortgesetzt)

Dann gilt

$$\begin{aligned} f_2 \circ g_2 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto (x+1)^2 \end{aligned}$$

und

$$\begin{aligned} g_2 \circ f_2 : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x^2 + 1. \end{aligned}$$

Wir bemerken

$$f_2 \circ g_2 \neq g_2 \circ f_2.$$

Verkettung

Bemerkung

Die Verkettung von Abbildungen ist assoziativ.
Das bedeutet, dass für Mengen $\mathscr{M}, \mathscr{N}, \mathscr{O}, \mathscr{P}$ und Abbildungen $f : \mathscr{M} \to \mathscr{N}$, $g : \mathscr{N} \to \mathscr{O}$ und $h : \mathscr{O} \to \mathscr{P}$ gilt:

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

$$\begin{tikzcd}
\mathscr{M} \arrow[r, "f"] \arrow[rr, bend left, "g \circ f"] & \mathscr{N} \arrow[r, "g"] \arrow[rr, bend right, "h \circ g"'] & \mathscr{O} \arrow[r, "h"] & \mathscr{P}
\end{tikzcd}$$

Inverse Abbildung

Definition und Bemerkung

Es seien $\mathcal{M}, \mathcal{N}$ Mengen und $f : \mathcal{M} \to \mathcal{N}$ eine Abbildung.

- Eine Abbildung $g : \mathcal{N} \to \mathcal{M}$ heißt **inverse Abbildung** (oder **Umkehrabbildung**) zu f, falls $g \circ f = id_{\mathcal{M}}$ und $f \circ g = id_{\mathcal{N}}$ gilt.

$$\begin{tikzcd} \mathcal{M} \arrow[loop left, "g \circ f"] \arrow[rr, bend left, "f"] & & \mathcal{N} \arrow[loop right, "f \circ g"] \arrow[ll, bend left, "g"] \end{tikzcd}$$

  In dem Fall heißen f und g **invers zueinander**.

- Falls eine inverse Abbildung zu f existiert, so ist sie eindeutig bestimmt und wir schreiben hierfür f^{-1}.
- f heißt **invertierbar** (oder **umkehrbar**), falls es eine inverse Abbildung zu f gibt.

Inverse Abbildung

Kein Beispiel

Die Abbildungen

$$\begin{aligned} f_1 : \{\square, \triangledown, \sharp, *\} &\to \{1, 2, 3, 4\} \\ \square &\mapsto 2 \\ \triangledown &\mapsto 4 \\ \sharp &\mapsto 1 \\ * &\mapsto 3 \end{aligned}$$

und

$$\begin{aligned} g_1 : \{1, 2, 3, 4\} &\to \{\square, \triangledown, \sharp, *\} \\ 1 &\mapsto \triangledown \\ 2 &\mapsto \square \\ 3 &\mapsto * \\ 4 &\mapsto \sharp \end{aligned}$$

sind **nicht** invers zueinander.

Inverse Abbildung

Beispiel

Die Abbildungen

$$
\begin{aligned}
f_2 : \{\Box, \triangledown, \sharp, *\} &\to \{1, 2, 3, 4\} \\
\Box &\mapsto 2 \\
\triangledown &\mapsto 4 \\
\sharp &\mapsto 1 \\
* &\mapsto 3
\end{aligned}
$$

und

$$
\begin{aligned}
g_2 : \{1, 2, 3, 4\} &\to \{\Box, \triangledown, \sharp, *\} \\
1 &\mapsto \sharp \\
2 &\mapsto \Box \\
3 &\mapsto * \\
4 &\mapsto \triangledown
\end{aligned}
$$

sind invers zueinander.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\begin{aligned} f_3 : \{\square, \triangledown, \sharp\} &\to \{1,2,3,4\} \\ \square &\mapsto 1 \\ \triangledown &\mapsto 2 \\ \sharp &\mapsto 3 \end{aligned}$$

und

$$\begin{aligned} g_3 : \{1,2,3,4\} &\to \{\square, \triangledown, \sharp\} \\ 1 &\mapsto \square \\ 2 &\mapsto \triangledown \\ 3 &\mapsto \sharp \\ 4 &\mapsto \square \end{aligned}$$

sind **nicht** invers zueinander.
Denn es gilt zwar $g_3 \circ f_3 = id_{\{\square, \triangledown, \sharp\}}$, aber $f_3 \circ g_3 \neq id_{\{1,2,3,4\}}$.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\begin{aligned} f_4 : [0,1] &\to [1,2] \\ x &\mapsto x+1 \end{aligned}$$

und

$$\begin{aligned} g_4 : [1,2] &\to [0,1] \\ x &\mapsto x-1 \end{aligned}$$

sind invers zueinander.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\begin{aligned} f_5 : [0,1] &\to [1,2] \\ x &\mapsto 2 - x \end{aligned}$$

und

$$\begin{aligned} g_5 : [1,2] &\to [0,1] \\ x &\mapsto 2 - x \end{aligned}$$

sind invers zueinander.

Inverse Abbildung

Hinweis

f_4 und f_5 sind beides invertierbare Abbildungen mit denselben Definitions- und Bildbereichen. Ebenso g_4 und g_5.

Inverse Abbildung

Kein Beispiel

Die Abbildungen

$$\begin{aligned} f_6 : [0,1] &\to [2,3] \\ x &\mapsto x+2 \end{aligned}$$

und

$$\begin{aligned} g_6 : [2,3] &\to [0,1] \\ x &\mapsto 3-x \end{aligned}$$

sind **nicht** invers zueinander. Sie sind aber beide invertierbar, haben also beide inverse Abbildungen.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\begin{aligned} f_7 : [0,1] &\to [0,5] \\ x &\mapsto 5 \cdot x \end{aligned}$$

und

$$\begin{aligned} g_7 : [0,5] &\to [0,1] \\ x &\mapsto \frac{1}{5} \cdot x \end{aligned}$$

sind invers zueinander.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\begin{aligned} f_8 : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto x^2 \end{aligned}$$

und

$$\begin{aligned} g_8 : \mathbb{R}_{\geq 0} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto \sqrt{x} \end{aligned}$$

sind invers zueinander.

Inverse Abbildung

Beispiel

Die Abbildungen

$$\sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$$

und

$$\sin^{-1} : [-1, 1] \to [-\frac{\pi}{2}, \frac{\pi}{2}]$$

sind invers zueinander.

Inverse Abbildung

Satz

Es seien $\mathscr{M}, \mathscr{N}$ Mengen und $\mathscr{f} : \mathscr{M} \to \mathscr{N}$ eine Abbildung. Dann gilt:
$\mathscr{f}$ ist umkehrbar genau dann, wenn $\mathscr{f}$ bijektiv ist.

Inverse Abbildung

Beweis.

$\Leftarrow$: Es sei f bijektiv. Die inverse Abbildung $g : \mathscr{N} \to \mathscr{M}$ zu f wird wie folgt definiert: Zu $y \in \mathscr{N}$ wähle das eindeutig bestimmte $x \in \mathscr{M}$ mit $f(x) = y$ (dies gibt es aufgrund der Bijektivität von f). Setze dann $g(y) := x$. Nun müssen wir noch nachrechnen, dass g tatsächlich die inverse Abbildung zu f ist.
Es gilt nun für beliebiges $m \in \mathscr{M}$

$$(g \circ f)(m) = g(f(m)) = m = id_{\mathscr{M}}(m), \text{ also } (g \circ f) = id_{\mathscr{M}},$$

und für beliebiges $n \in \mathscr{N}$

$$(f \circ g)(n) = f(g(n)) = n = id_{\mathscr{N}}(n), \text{ also } (f \circ g) = id_{\mathscr{N}}.$$

Inverse Abbildung

Beweis.

$\Rightarrow$: Es sei f umkehrbar, weiter sei $g : \mathcal{N} \to \mathcal{M}$ die inverse Abbildung zu f. Also $g \circ f = id_{\mathcal{M}}$ (1) und $f \circ g = id_{\mathcal{N}}$ (2).
f ist injektiv: Es seien $x, y \in \mathcal{M}$ mit $f(x) = f(y)$. Dann gilt aber auch $g(f(x)) = g(f(y))$, also $(g \circ f)(x) = (g \circ f)(y)$, also

$$x = id_{\mathcal{M}}(x) \overset{(1)}{=} (g \circ f)(x) = (g \circ f)(y) \overset{(1)}{=} id_{\mathcal{M}}(y) = y.$$

Also gilt $x = y$. Also ist f injektiv.
f ist surjektiv: Es sei $n \in \mathcal{N}$ beliebig. Dann gilt für $m := g(n) \in \mathcal{M}$:

$$f(m) = f(g(n)) = (f \circ g)(n) \overset{(2)}{=} id_{\mathcal{N}}(n) = n,$$

also $f(m) = n$. Also ist f surjektiv. $\square$