Diskrete Mathematik für Informatiker

Evelina Viada
evelina.viada@mathematik.uni-goettingen.de
BITTE kontaktieren Sie mir via E-MAIL (nicht via Studip)

Wintersemester 2023/2024

Organizatorisches zur Vorlesung

Literatur:

- Skript von Markus Lohrey
  (https://www.eti.uni-siegen.de/ti/lehre/ws1415/diskrete_mathematik/)
  In Studip File: DMFolien2023MLohrey
- Lukas Pottmeyer, Diskrete Mathematik, Ein kompakter Einstieg, Springer-Verlag, 2019.

Weitere Literaturempfehlungen:

- Diekert, Kufleitner, Rosenberger, Elemente der diskreten Mathematik, De Gruyter
- Aigner, Diskrete Mathematik, Vieweg
- Hartmann, Mathematik für Informatiker, Vieweg

Die Übungen werden von Victoria Cantoral organisiert.

Diskrete Mathematik für Informatiker

Markus Lohrey

Universität Siegen

Wintersemester 2014/2015

Mengentheoretische Grundlagen

Naive Definition (Mengen, Elemente, $\in$, $\notin$)

Eine Menge ist die Zusammenfassung von bestimmten unterschiedlichen Objekten (die Elemente der Menge) zu einem neuen Ganzen.

Wir schreiben $x \in M$, falls das Objekt x zur Menge M gehört.
Wir schreiben $x \notin M$, falls das Objekt x nicht zur Menge M gehört.

Falls $x \in M$ und $y \in M$ gilt, schreiben wir auch $x, y \in M$.

Eine Menge, welche nur aus endlich vielen Objekten besteht (eine endliche Menge), kann durch explizite Auflistung dieser Elemente spezifiziert werden.

Beispiel: $M = \{2, 3, 5, 7\}$.

Hierbei spielt die Reihnfolge der Auflistung keine Rolle:
$\{2, 3, 5, 7\} = \{7, 5, 3, 2\}$.

Auch Mehrfachauflistungen spielen keine Rolle:
$\{2, 3, 5, 7\} = \{2, 2, 2, 3, 3, 5, 7\}$.

Mengentheoretische Grundlagen

Eine besonders wichtige Menge ist die leere Menge $\emptyset = \{\}$, die keinerlei Elemente enthält.

In der Mathematik hat man es häufig auch mit unendlichen Mengen zu tun (Mengen, die aus unendlich vielen Objekten bestehen).

Solche Mengen können durch Angabe einer Eigenschaft, welche die Elemente der Menge auszeichnet, spezifiziert werden.

Beispiele:

- $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$ (Menge der natürlichen Zahlen)
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (Menge der ganzen Zahlen)
- $\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$ (Menge der rationalen Zahlen)
- $P = \{n \in \mathbb{N} \mid n \geq 2, n \text{ ist nur durch 1 und } n \text{ teilbar}\}$ (Menge der Primzahlen)

Mengentheoretische Grundlagen

Beispiel: Eines der **ZFC**-Axiome besagt, dass zwei Mengen genau dann gleich sind, wenn sie die gleichen Elemente haben. Etwas formaler:

Für alle Mengen X und Y gilt: X und Y sind gleich, genau dann wenn für alle x gilt: $x \in X$ genau dann, wenn $x \in Y$.

Noch formaler:

$$\forall X \forall Y : (X = Y \longleftrightarrow (\forall x : x \in X \longleftrightarrow x \in Y))$$

Hierbei bedeutet $\forall$ "für alle" und $\exists$ "es existiert".

Bisher konnten Mathematiker kein schlüssiges mathematisches Argument finden, welches nicht mit den **ZFC**-Axiomen ableitbar ist.

Mengentheoretische Grundlagen

Die Notwendigkeit einer formalen Mengenlehre hat sich unter anderem aus diversen Paradoxien entwickelt. Eines der bekanntesten hiervon ist Russel's Paradoxon:

Elemente von Mengen können wieder Mengen sein. Also könnten wir doch die Menge aller Mengen, welche sich nicht selbst als Element haben, definieren:

$$Y = \{x \mid x \notin x\}$$

Gilt nun $Y \in Y$?

- Würde $Y \in Y$ gelten, so würde Y die Eigenschaft, welche die Menge Y definiert, erfüllen. Also müsste $Y \notin Y$ gelten.
- Würde $Y \notin Y$ gelten, so würde Y die Eigenschaft, welche die Menge Y definiert, nicht erfüllen. Also müsste $Y \in Y$ gelten.

Mengentheoretische Grundlagen

Definition ($\subseteq$, $\subsetneq$, Potenzmenge, $\cap$, $\cup$, $\setminus$, disjunkt)

Seien A und B zwei Mengen.

- $A \subseteq B$ bedeutet, dass jedes Element von A auch zu B gehört (A ist eine Teilmenge von B); formal:

$$\forall a : a \in A \to a \in B$$

- $A \subsetneq B$ bedeutet, dass $A \subseteq B$ und $A \neq B$ gilt. (echte Teilmenge)
- $2^A = \{B \mid B \subseteq A\}$ (Potenzmenge von A)
- $A \cap B = \{c \mid c \in A \text{ und } c \in B\}$ (Schnitt von A und B)
- $A \cup B = \{c \mid c \in A \text{ oder } c \in B\}$ (Vereinigung von A und B)
- $A \setminus B = \{c \in A \mid c \notin B\}$ (Differenz von A und B)
- Zwei Mengen A und B sind disjunkt, falls $A \cap B = \emptyset$ gilt.

Mengentheoretische Grundlagen

Beispiele und einige einfache Aussagen:

- $\emptyset \subseteq A$ und $A \subseteq A$ gilt für jede Menge A.
- Für alle Mengen A und B gilt $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$.
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$.
- $\{1, 2, 3\} \cap \{4, 5, 6\} = \emptyset$, d. h. die beiden Mengen sind disjunkt.
- $2^{\{1,2\}} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$ und $2^{\emptyset} = \{\emptyset\}$
- Für alle Mengen A gilt

$$A \cap \emptyset = \emptyset \text{ und } A \cup \emptyset = A.$$

- Für alle Mengen A, B, und C gilt:

$$\begin{aligned}
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \\
A \setminus (B \cup C) &= (A \setminus B) \cap (A \setminus C) \\
A \setminus (B \cap C) &= (A \setminus B) \cup (A \setminus C)
\end{aligned}$$

Mengentheoretische Grundlagen

Wir beweisen beispielhaft die Identität

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Hierzu zeigen wir:

(1) Jedes Element von $A \cup (B \cap C)$ gehört auch zu $(A \cup B) \cap (A \cup C)$.

(2) Jedes Element von $(A \cup B) \cap (A \cup C)$ gehört auch zu $A \cup (B \cap C)$.

zu (1). Sei $x \in A \cup (B \cap C)$.

Dann gilt also $x \in A$ oder $x \in (B \cap C)$.

Fall 1: Es gilt $x \in A$.

Dann gilt auch $x \in (A \cup B)$ sowie $x \in (A \cup C)$ und damit $x \in (A \cup B) \cap (A \cup C)$.

Fall 2: Es gilt $x \in (B \cap C)$, d. h. $x \in B$ und $x \in C$.

Wieder gilt $x \in (A \cup B)$ und $x \in (A \cup C)$ und damit $x \in (A \cup B) \cap (A \cup C)$.

zu (2). Sei $x \in (A \cup B) \cap (A \cup C)$

Dann gilt $x \in A \cup B$ und $x \in A \cup C$.

Fall 1: $x \in A$.

Dann gilt $x \in A \cup (B \cap C)$.

Fall 2: $x \notin A$.

Wegen $x \in A \cup B$ muss $x \in B$ gelten, und wegen $x \in A \cup C$ muss $x \in C$ gelten.

Also gilt $x \in B \cap C$, d.h. $x \in A \cup (B \cap C)$. $\square$

Mengentheoretische Grundlagen

Definition (beliebige Vereinigung und Schnitt)

Sei I eine Menge und für jedes $i \in I$ sei A_i wiederum eine Menge. Dann definieren wir:

$$\bigcup_{i \in I} A_i = \{a \mid \exists j \in I : a \in A_j\}$$

$$\bigcap_{i \in I} A_i = \{a \mid \forall j \in I : a \in A_j\}$$

Für Mengen $A_1, A_2, \ldots, A_n$ verwenden wir auch die Schreibweise

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i \in \{1,\ldots,n\}} A_i \text{ und } \bigcap_{i=1}^{n} A_i = \bigcap_{i \in \{1,\ldots,n\}} A_i.$$

Mengentheoretische Grundlagen

Beispiele:

$$\bigcup_{a \in A} \{a\} = A \text{ für jede Menge } A$$

$$\bigcap_{\varepsilon \in \mathbb{R} \setminus \{0\}} \{x \in \mathbb{R} \mid |x - \pi| \leq |\varepsilon|\} = \{\pi\}$$

$$\bigcap_{n \in \mathbb{N}} \{m \in \mathbb{N} \mid m \geq n\} = \emptyset$$

Einfache Aussagen:

$$\left(\bigcap_{i \in I} A_i\right) \cup B = \bigcap_{i \in I} (A_i \cup B)$$

$$\left(\bigcup_{i \in I} A_i\right) \cap B = \bigcup_{i \in I} (A_i \cap B)$$

Definition (Kartesisches Produkt)

Für zwei Mengen A und B ist

$$A \times B = \{(a,b) \mid a \in A \text{ und } b \in B\}$$

das kartesische Produkt von A und B.

Allgemeiner: Für Mengen $A_1, \ldots, A_n$ $(n \geq 2)$ sei

$$\begin{aligned}\prod_{i=1}^{n} A_i &= A_1 \times A_2 \times \cdots \times A_n \\ &= \{(a_1, \ldots, a_n) \mid \text{ für alle } 1 \leq i \leq n \text{ gilt } a_i \in A_i\}\end{aligned}$$

Falls $A_1 = A_2 = \cdots = A_n = A$ schreiben wir auch A^n für diese Menge.

Mengentheoretische Grundlagen

Beispiele und einige einfache Aussagen:

- $\{1,2,3\} \times \{4,5\} = \{(1,4),(1,5),(2,4),(2,5),(3,4),(3,5)\}$
- Für alle Mengen A, B, und C gilt:

$$
\begin{aligned}
(A \cup B) \times C &= (A \times C) \cup (B \times C)\\
A \times (B \cup C) &= (A \times B) \cup (A \times C)\\
(A \cap B) \times C &= (A \times C) \cap (B \times C)\\
A \times (B \cap C) &= (A \times B) \cap (A \times C)
\end{aligned}
$$

Definition (Relationen und Funktionen)

Seien A und B Mengen.

Eine Relation von A nach B ist eine Teilmenge $R \subseteq A \times B$.

Eine (binäre) Relation auf A ist eine Teilmenge $R \subseteq A \times A$.

Eine Funktion (oder Abbildung) von A (dem Definitionsbereich) nach B (dem Wertebereich) ist eine Relation $f \subseteq A \times B$, so dass für alle $a \in A$ genau ein $b \in B$ mit $(a, b) \in f$ existiert. Wir schreiben dann auch $f(a) = b$.

Wir schreiben auch $f : A \to B$ für eine Funktion f von A nach B.

Beispiel: Hier sind zwei Relationen von $\{a, b, c\}$ nach $\mathbb{N}$:

$$R = \{(a, 1), (b, 2), (c, 1)\} \text{ und } Q = \{(a, 1), (a, 2), (b, 2), (c, 1)\}$$

Mengentheoretische Grundlagen

Definition (Relationen und Funktionen)

Seien A und B Mengen.

Eine Relation von A nach B ist eine Teilmenge $R \subseteq A \times B$.

Eine (binäre) Relation auf A ist eine Teilmenge $R \subseteq A \times A$.

Eine Funktion (oder Abbildung) von A (dem Definitionsbereich) nach B (dem Wertebereich) ist eine Relation $f \subseteq A \times B$, so dass für alle $a \in A$ genau ein $b \in B$ mit $(a, b) \in f$ existiert. Wir schreiben dann auch $f(a) = b$.

Wir schreiben auch $f : A \to B$ für eine Funktion f von A nach B.

Beispiel: Hier sind zwei Relationen von $\{a, b, c\}$ nach $\mathbb{N}$:

$$R = \{(a, 1), (b, 2), (c, 1)\} \text{ und } Q = \{(a, 1), (a, 2), (b, 2), (c, 1)\}$$

Dann ist R eine Funktion, Q hingegen ist keine Funktion.

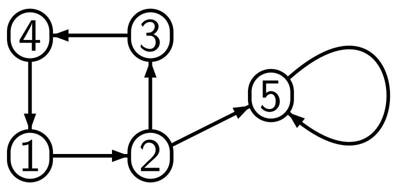
Mengentheoretische Grundlagen

Eine Relation $R \subseteq A \times A$ kann man sich graphisch veranschaulichen.

Beispiel: Sei $A = \{1, 2, 3, 4, 5\}$ und R die Relation

$$R = \{(1, 2), (2, 3), (3, 4), (4, 1), (2, 5), (5, 5)\}.$$

Diese Relation kann durch folgendes Diagram visualisiert werden.



Solche Diagramme werden wir im Kapitel über Graphentheorie noch genauer studieren.

Mengentheoretische Grundlagen

Definition

Für Mengen A und B sei B^A die Menge aller Funktionen von A nach B.

Definition (Bild und Urbild einer Funktion)

Sei $f : A \to B$ eine Funktion.

- Für $A' \subseteq A$ sei $f(A') = \{f(a) \mid a \in A'\}$ das Bild von A' unter f.
- Für $B' \subseteq B$ sei $f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$ das Urbild von B' unter f.

Beispiel: Sei $f : (\mathbb{N} \times \mathbb{N}) \to \mathbb{Z}$ definiert durch $f((n,m)) = n - m$ für $n, m \in \mathbb{N}$. Dann gilt:

- $f(\{(n,m) \mid n \leq m\}) = \{-a \mid a \in \mathbb{N}\}$
- $f^{-1}(\{0\}) = \{(a,a) \mid a \in \mathbb{N}\}$

Mengentheoretische Grundlagen

Einfache Aussagen:

- Für alle Funktionen $f : A \to B$ und alle $A_1, A_2 \subseteq A$ gilt
$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2).$$
- Für alle Funktionen $f : A \to B$ und alle $B_1, B_2 \subseteq B$ gilt
$$\begin{aligned} f^{-1}(B_1 \cup B_2) &= f^{-1}(B_1) \cup f^{-1}(B_2). \\ f^{-1}(B_1 \cap B_2) &= f^{-1}(B_1) \cap f^{-1}(B_2). \end{aligned}$$
- Im Allgemeinen gilt nicht $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

  Beispiel: Sei $a \neq b$ und $f(a) = c$ und $f(b) = c$. Dann gilt
$$f(\{a\} \cap \{b\}) = f(\emptyset) = \emptyset \text{ und } f(\{a\}) \cap f(\{b\}) = \{c\}.$$
- Für alle Funktionen $f : A \to B$ und $A' \subseteq A$, $B' \subseteq B$ gilt
$$A' \subseteq f^{-1}(f(A')) \text{ und } f(f^{-1}(B')) \subseteq B'.$$

Definition (injektive/surjektive/bijektive Funktionen)

Eine Funktion $f : A \to B$ is injektiv, falls für alle $a, b \in A$ gilt:
Wenn $a \neq b$ gilt, muss auch $f(a) \neq f(b)$ gelten
(verschiedene Elemente werden auf verschieden Elemente abgebildet).

Eine Funktion $f : A \to B$ is surjektiv, falls für alle $b \in B$ ein $a \in A$ mit $f(a) = b$ existiert (jedes Element aus B wird durch f getroffen).
Äquivalent: $f(A) = B$.

Eine Funktion $f : A \to B$ is bijektiv, falls sie injektiv und surjektiv ist.
Wir sagen auch, dass f eine Bijektion ist.

Eine Bijektion $f : A \to B$ ist eine 1-zu-1 Zuordnung zwischen den Elementen aus A und B.

Definition (Permutation)

Eine Permutation der Menge A ist eine Bijektion $f : A \to A$.

Beispiele:

- Die Funktion $f : \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \to \mathbb{Q}$ mit $f((a, b)) = \frac{a}{b}$ ist surjektiv (jede rationale Zahl ist Quotient zweier ganzer Zahlen) aber nicht injektiv (z. B. $f((1, 2)) = f((2, 4)) = 0.5$).
- Die Funktion $f : \mathbb{N} \to \mathbb{N}$ mit $f(n) = n + 1$ ist injektiv (aus $n + 1 = m + 1$ folgt $n = m$) aber nicht surjektiv (es gibt keine natürliche Zahl m mit $m + 1 = 0$).
- Die Funktion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = n + 1$ ist bijektiv (also eine Permutation).

Mengentheoretische Grundlagen

Einfache Aussagen:

- $f : A \to B$ is surjektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ nicht leer ist.
- $f : A \to B$ is injektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ höchstens ein Element enthält.
- $f : A \to B$ is bijektiv genau dann, wenn für alle $b \in B$ das Urbild $f^{-1}(b)$ genau ein Element enthält.
- Wenn $f : A \to B$ injektiv ist, dann gilt für alle $A' \subseteq A$ und $a \in A$: Aus $f(a) \in f(A')$ folgt $a \in A'$.

  Für nicht-injektive Funktionen ist dies im Allgemeinen falsch.
- Wenn $f : A \to B$ injektiv ist, dann gilt für alle $A_1, A_2 \subseteq A$: $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$.

Definition (Umkehrfunktion)

Für eine bijektive Funktion $f : A \to B$ kann man die Umkehrfunktion $f^{-1} : B \to A$ definieren durch folgende Vorschrift:

$$f^{-1}(b) = a \text{ genau dann, wenn } f(a) = b$$

Beachte: Wenn $f : A \to B$ bijektiv dann gibt es für jedes $b \in B$ genau ein Element a mit $f(a) = b$.

Daher ist die obige Definition von f^{-1} eindeutig!

Die Umkehrfunktion einer Bijektion ist wieder eine Bijektion.

Beispiel: Für die Bijektion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = n + 1$ gilt $f^{-1}(n) = n - 1$.

Beachte: Die Notation f^{-1} für die Umkehrfunktion ist konsistent mit der Notation $f^{-1}(A')$ für das Urbild.

Genauer: Ist $f : A \to B$ eine Bijektion, und ist $g = f^{-1}$ die Umkehrfunktion von f, so gilt für jede Teilmenge $B' \subseteq B$:

$$f^{-1}(B') = g(B').$$

In Worten: Das Urbild von B' unter f ist gleich dem Bild von B' unter der Umkehrfunktion von f.

Mengentheoretische Grundlagen

Mittels des Begriffs der Bijektion können wir definieren, wann zwei Mengen gleich groß sind.

Definition (gleich-mächtig)

Zwei Mengen A und B sind gleich-mächtig, kurz $|A| = |B|$, falls eine Bijektion $f : A \to B$ existiert.

Man schreibt auch $|A| \leq |B|$ (A is höchstens so mächtig wie B), falls eine injektive Funktion $f : A \to B$ existiert.

Den folgenden Satz beweisen wir später.

Satz 1 (Satz von Cantor, Schröder und Bernstein)

Für alle Mengen A und B gilt:

$$|A| = |B| \quad \textit{genau dann, wenn} \quad (|A| \leq |B| \textit{ und } |B| \leq |A|).$$

Mengentheoretische Grundlagen

In anderen Worten: Es existiert eine Bijektion von A nach B genau dann, wenn injektive Funktionen von A nach B sowie B nach A existieren.

Für endliche Mengen A und B gilt $|A| = |B|$ falls A und B im intuitiven Sinne gleich viele Elemente haben.

Der Begriff "gleich-mächtig" kann jedoch auch auf unendliche Mengen angewendet werden.

Beispiel: Die Mengen $\mathbb{N}$ und $\mathbb{Z}$ sind gleich-mächtig.

Wir definieren eine Bijektion $f : \mathbb{Z} \to \mathbb{N}$ wie folgt, wobei $m \in \mathbb{Z}$:

$$f(m) = \begin{cases} -(2m+1) & \text{falls } m < 0 \\ 2m & \text{falls } m \geq 0 \end{cases}$$

Übung: Zeigen Sie, dass f tatsächlich bijektiv ist.

Mengentheoretische Grundlagen

Ebenso sind die Mengen $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$ und $\mathbb{Q}$ gleich-mächtig.

Eine Bijektion zwischen $\mathbb{N} \times \mathbb{N}$ und $\mathbb{N}$ ist die Cantorsche Paarungsfunktion $p : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ mit

$$p(n_1, n_2) = \frac{1}{2}(n_1 + n_2 + 1)(n_1 + n_2) + n_2.$$

Alternativ kann man die Gleichmächtigkeit von $\mathbb{N}$ und $\mathbb{N} \times \mathbb{N}$ mittels des Satzes von Cantor, Schröder und Bernstein zeigen, indem man injektive Funktionen $i_1 : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ und $i_2 : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ angibt, z. B.

$$i_1(n) = (n, 0) \text{ und } i_2(n_1, n_2) = 2^{n_1} 3^{n_2}.$$

(Injektivität von i_2 folgt aus Satz 47.)

Man kann auch zeigen, dass die Mengen $2^{\mathbb{N}}$ und $\mathbb{R}$ (Menge der reellen Zahlen) gleich-mächtig sind.

Aber: Nicht alle unendlichen Mengen sind gleich-mächtig.

Satz 2 (Cantor 1891)

Für jede Menge A sind A und 2^A nicht gleich-mächtig.

Beweis (durch Widerspruch): Sei A eine beliebige Menge.

Angenommen es gäbe eine surjektive Funktion $f : A \to 2^A$.

Definiere die Menge

$$B = \{a \in A \mid a \notin f(a)\} \subseteq A.$$

Da f surjektiv ist, gibt es ein $b \in A$ mit $f(b) = B$.

Dann gilt:

$$b \in B \iff b \notin f(b) \iff b \notin B.$$

Also gibt es keine surjektive (und somit auch keine bijektive) Abbildung $f : A \to 2^A$. □

Mengentheoretische Grundlagen

Definition (abzählbar-unendlich, abzählbar, überabzählbar)

Eine Menge A ist abzählbar-unendlich, falls $|A| = |\mathbb{N}|$ gilt.

Eine Menge A ist abzählbar, falls A endlich oder abzählbar-unendlich ist.

Eine Menge A ist überabzählbar, falls A unendlich aber nicht abzählbar ist.

Beispiele:

Die Mengen $\mathbb{N}$, $\mathbb{N} \times \mathbb{N}$, $\mathbb{Z}$ und $\mathbb{Q}$ sind abzählbar-unendlich.

Die Mengen $2^{\mathbb{N}}$, $\mathbb{R}$ und $\mathbb{C}$ (Menge der komplexen Zahlen) sind überabzählbar.

Das eine Menge A abzählbar-unendlich ist, bedeutet, dass man die Elemente der Menge A auflisten kann als

$$a_1, a_2, a_3, a_4, \ldots$$

wobei in dieser Liste jedes Element von A genau einmal vorkommt.

Mengentheoretische Grundlagen

Es gibt in der Mengenlehre durchaus sehr schwierige Fragen.

Z. B. hat Georg Cantor folgende Vermutung aufgestellt:

Kontinuumshypothese (Cantor 1878)

Für jede unendliche Teilmenge $A \subseteq 2^{\mathbb{N}}$ gilt $|A| = |\mathbb{N}|$ oder $|A| = |2^{\mathbb{N}}|$.

Diese Vermutung konnte lange Zeit weder bewiesen noch widerlegt werden. Dies ist unvermeidbar:

- Die Verneinung der Kontinuumshypothese kann nicht aus dem Axiomensystem ZFC hergeleitet werden (Gödel 1938).
- Die Kontinuumshypothese kann nicht aus dem Axiomensystem ZFC hergeleitet werden (Cohen 1966).

Mengentheoretische Grundlagen

Für eine Relation $R \subseteq A \times A$ und $a, b \in A$ schreiben wir auch aRb für $(a, b) \in R$.

Definition ((ir)reflexive/(anti)symmetrische/transitive Relationen)

Sei A eine Menge und $R \subseteq A \times A$ eine Relation auf A.

- R ist reflexiv, falls aRa für alle $a \in A$ gilt.
- R ist irreflexiv, falls kein $a \in A$ mit aRa existiert.
- R ist symmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb, dann auch bRa.
- R ist antisymmetrisch, falls für alle $a, b \in A$ gilt:
  Wenn aRb und bRa, dann $a = b$.
- R ist transitiv, falls für alle $a, b, c \in A$ gilt:
  Wenn aRb und bRc, dann auch aRc.

Beispiel: Betrachte die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a + b = 43\}.$$

- Ist R reflexiv?

  Nein: Es gilt z.B. nicht $0 \; R \; 0$.
- Ist R irreflexiv?

  Ja: Würde $a \; R \; a$ gelten, so wäre $2a = 43$. Aber in $\mathbb{Z}$ gibt es eine solche Zahl a nicht.
- Ist R symmetrisch?

  Ja: Wenn $a \; R \; b$, dann $a + b = 43$. Dann gilt aber auch $b + a = 43$, d.h. $b \; R \; a$.
- Ist R antisymmetrisch?

  Nein: Es gilt z.B. $0 \; R \; 43$ und $43 \; R \; 0$ aber $0 \neq 43$.
- Ist R transitiv?

  Nein: Es gilt z.B. $0 \; R \; 43$ und $43 \; R \; 0$ aber nicht $0 \; R \; 0$.

Mengentheoretische Grundlagen

Definition (partielle Ordnung)

Eine Relation $R \subseteq A \times A$ ist eine partielle Ordnung (auf A), falls R reflexiv, antisymmetrisch, und transitiv ist.

Definition (lineare Ordnung)

Eine partielle Ordnung R auf A ist eine lineare Ordnung (auf A), falls für alle $a, b \in A$ gilt: aRb oder bRa.

Beispiel 1 (Teilmengenbeziehung oder Inklusion): Sei A eine beliebige Menge. Dann ist $\subseteq$ eine partielle Ordnung auf 2^A.

Falls A mindestens zwei Elemente enthält, ist jedoch $\subseteq$ keine lineare Ordnung auf 2^A: Sei $A = \{1, 2\}$. Dann gilt weder $\{1\} \subseteq \{2\}$ noch $\{2\} \subseteq \{1\}$.

Beispiel 2: Die Relation $\leq$ ist eine lineare Ordnung auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.

Beispiel 3 (Teilbarkeit): Wir definieren die binäre Relation $|$ auf den ganzen Zahlen $\mathbb{Z}$ wie folgt, wobei $a, b \in \mathbb{Z}$.

$$a|b \text{ genau dann, wenn } \exists q \in \mathbb{Z} : q \cdot a = b$$

Die Relation $|$ ist reflexiv und transitiv, sie ist jedoch nicht antisymmetrisch, denn für alle $a \in \mathbb{Z}$ gilt $a \mid -a$ und $-a \mid a$.

Betrachten wir jedoch $|$ als eine binäre Relation auf den natürlichen Zahlen $\mathbb{N}$, so ist $|$ eine partielle Ordnung, aber keine lineare Ordnung: Es gilt weder $2 \mid 3$ noch $3 \mid 2$.

Definition (Äquivalenzrelation)

Eine Relation $R \subseteq A \times A$ ist eine Äquivalenzrelation (auf A), falls R reflexiv, symmetrisch und transitiv ist.

Beispiel 1: Für jede Menge A ist die Relation

$$\mathrm{Id}_A = \{(a, a) \mid a \in A\}$$

(die Identitätsrelation) reflexiv, symmetrisch, antisymmetrisch, und transitiv. Insbesondere ist Id_A eine Äquivalenzrelation.

Beispiel 2: Sei $f : A \to B$ eine Funktion. Dann ist

$$\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$$

eine Äquivalenzrelation.

Beispiel 3: Sei $q \in \mathbb{Z} \setminus \{0\}$ eine ganze Zahl. Auf der Menge $\mathbb{Z}$ definieren wir die Relation

$$\equiv_q \;=\; \{(a,b) \mid a,b \in \mathbb{Z}, q|(a-b)\}.$$

Sprechweise für $a \equiv_q b$: a und b sind kongruent modulo q.

Es gilt $a \equiv_q b$ genau dann, wenn eine ganze Zahl $x \in \mathbb{Z}$ mit $a = b + x \cdot q$ existiert.

Beachte: $a \equiv_q b$ genau dann, wenn $a \equiv_{-q} b$.

Lemma 3

Für jede Zahl $q \in \mathbb{Z} \setminus \{0\}$ ist $\equiv_q$ eine Äquivalenzrelation auf $\mathbb{Z}$.

Beweis: Sei $q \in \mathbb{Z} \setminus \{0\}$.

(1) $\equiv_q$ ist reflexiv, denn $q|(a - a)$ (d. h. $q|0$) gilt für jede ganze Zahl a.

(2) $\equiv_q$ ist symmetrisch: Gelte $a \equiv_q b$, d. h. $q|(a - b)$.

Wegen $(b - a) = -(a - b)$ gilt dann auch $q|(b - a)$, d. h. $b \equiv_q a$.

(3) $\equiv_q$ ist transitiv: Seien $a, b, c \in \mathbb{Z}$ mit $a \equiv_q b$ und $b \equiv_q c$.

Also existieren ganze Zahlen $p, s \in \mathbb{Z}$ mit

$$a - b = qp \text{ und } b - c = qs.$$

Dann gilt

$$a - c = (a - b) + (b - c) = qp + qs = q(p + s).$$

Also gilt $a \equiv_q c$. $\square$

Mengentheoretische Grundlagen

Definition (Äquivalenzklassen)

Sei R eine Äquivalenzrelation auf der Menge A und sei $a \in A$. Dann ist $[a]_R = \{b \in A \mid aRb\}$ die Äquivalenzklasse von a (bzgl. R).

Beachte: Es gilt stets $a \in [a]_R$ (denn eine Aquivalenzrelation ist reflexiv).

Eine Äquivalenzklasse kann also nie leer sein, und jedes Element von A gehört zu einer Äquivalenzklasse.

Satz 4

Sei R eine Äquivalenzrelation auf der Menge A und seien $a, b \in A$. Dann sind folgende drei Aussagen äquivalent:

(1) aRb

(2) $[a]_R = [b]_R$

(3) $[a]_R \cap [b]_R \neq \emptyset$.

Beweis (durch Ringschluss):

(1) impliziert (2): Gelte aRb und damit auch bRa (R ist symmetrisch).

Wir zeigen zunächst $[a]_R \subseteq [b]_R$.

Sei also $c \in [a]_R$, d. h. es gilt aRc.

bRa, aRc und R transitiv $\rightarrow$ bRc, d. h. $c \in [b]_R$.

Analog kann man $[b]_R \subseteq [a]_R$ zeigen.

(2) impliziert (3): Gelte $[a]_R = [b]_R$.

Dann gilt $a \in [a]_R \cap [b]_R$ und damit $[a]_R \cap [b]_R \neq \emptyset$.

(3) impliziert (1): Gelte $[a]_R \cap [b]_R \neq \emptyset$.

Also gibt es ein c mit $c \in [a]_R$ und $c \in [b]_R$.

$\rightarrow$ aRc und bRc; und damit auch cRb (R ist symmetrisch).

$\rightarrow$ aRb, wegen R transitiv. $\square$

Beispiele:

- Die Äquivalenzklassen der Identitätsrelation Id_A sind die einelementigen Mengen $\{a\}$ mit $a \in A$.
- Die Äquivalenzklassen der Relation $\{(a_1, a_2) \in A \times A \mid f(a_1) = f(a_2)\}$ (für $f : A \to B$ eine Funktion) sind die Urbilder $f^{-1}(b)$ für $b \in B$.
- Die Äquivalenzklassen von $\equiv_q$ (für $q \in \mathbb{N} \setminus \{0\}$) sind die Mengen

$$\begin{gathered}\{0 + pq \mid p \in \mathbb{Z}\}\\ \{1 + pq \mid p \in \mathbb{Z}\}\\ \vdots\\ \{(q-1) + pq \mid p \in \mathbb{Z}\}\end{gathered}$$

Mengentheoretische Grundlagen

Sei R wieder eine Äquivalenzrelation auf der Menge A.

Seien $\{A_i \mid i \in I\}$ die Menge aller Äquivalenzklassen von R, d. h.

- Für jedes $a \in A$ gibt es ein $i \in I$ mit $[a]_R = A_i$
- Für alle $i, j \in I$ mit $i \neq j$ gilt $A_i \neq A_j$.

Aufgrund von Satz 4 bildet $\{A_i \mid i \in I\} \subseteq 2^A$ eine Partition von A, d. h.

- $\bigcup_{i \in I} A_i = A$
- $\forall i \in I : A_i \neq \emptyset$.
- $\forall i, j \in I : i \neq j \to A_i \cap A_j = \emptyset$ (verschiedene A_i sind disjunkt)

Ist umgekehrt $\{A_i \mid i \in I\}$ eine Partition von A, so kann man eine Äquivalenzrelation R auf A definieren durch:

$$R = \{(a, b) \mid a, b \in A, \exists i \in I : a, b \in A_i\}$$

Übung: Zeigen Sie, dass dies tatsächlich eine Äquivalenzrelation ist.

Da eine Relation $R \subseteq A \times B$ eine Menge (von Paaren) ist, können wir die Operationen $\cap$ und $\cup$ auch auf Relationen anwenden.

Es gibt aber noch zwei weitere wichtige Operationen auf Mengen:

Definition (R^{-1}, $R \circ S$)

Seien $R \subseteq A \times B$ und $S \subseteq B \times C$ binäre Relationen. Dann definieren wir:

- $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$
- $R \circ S = \{(a, c) \in A \times C \mid \exists b \in B : (a, b) \in R \text{ und } (b, c) \in S\}$

R^{-1} ist die Umkehrrelation von R.

$R \circ S$ ist die Komposition (oder Verknüpfung) von R und S.

Mengentheoretische Grundlagen

Beispiel 1: Sei

$$R = \{(a,1),(b,1),(b,2)\} \text{ und } S = \{(1,x),(1,y),(2,y)\}$$

Dann gilt:

- $R^{-1} = \{(1,a),(1,b),(2,b)\}$
- $R \circ S = \{(a,x),(a,y),(b,x),(b,y)\}$

Beispiel 2: Sei R eine lineare Ordnung auf der Menge A. Dann gilt

$$R \cap R^{-1} = \mathrm{Id}_A$$
$$R \cup R^{-1} = A \times A$$

Mengentheoretische Grundlagen

Ein wichtiger Spezialfall der Komposition von Relationen ist die Komposition von Funktionen:

Wenn $f : A \to B$ und $g : B \to C$ Funktionen sind, dann ist $f \circ g : A \to C$ eine Funktion und es gilt

$$(f \circ g)(a) = g(f(a))$$

für alle $a \in A$.

Vorsicht: Manchmal wird die Funktion $f \circ g$ auch durch die Vorschrift $(f \circ g)(a) = f(g(a))$ definiert.

Mengentheoretische Grundlagen

Bemerkungen: Sei $R \subseteq A \times A$ eine Relation auf A.

- R is reflexiv, genau dann, wenn $\mathrm{Id}_A \subseteq R$.
- R is irreflexiv, genau dann, wenn $\mathrm{Id}_A \cap R = \emptyset$.
- R ist symmetrisch, genau dann, wenn $R^{-1} = R$.
- R is transitiv, genau dann, wenn $R \circ R \subseteq R$.
- R is antisymmetrisch, genau dann, wenn $R \cap R^{-1} \subseteq \mathrm{Id}_A$.
- Für alle binären Relationen R, S und T auf der Menge A gilt:

$$R \circ \mathrm{Id}_A = \mathrm{Id}_A \circ R = R$$
$$(R \circ S) \circ T = R \circ (S \circ T)$$
$$(R \circ S)^{-1} = S^{-1} \circ R^{-1}$$

Mengentheoretische Grundlagen

- Ist die Relation $R \subseteq A \times B$ eine Bijektion (also insbesondere eine Funktion) dann ist die Umkehrrelation R^{-1} genau die Umkehrfunktion von R.
- Wenn $f : A \to B$ und $g : B \to C$ injektiv sind, dann ist auch $f \circ g$ injektiv.
- Wenn $f : A \to B$ und $g : B \to C$ surjektiv sind, dann ist auch $f \circ g$ surjektiv.
- Wenn $f : A \to B$ und $g : B \to C$ bijektiv sind, dann ist auch $f \circ g$ bijektiv.
- Konsequenz: Sei M eine Menge von Mengen. Dann ist Relation

$$\{(X, Y) \in M \times M \mid |X| = |Y|\}$$

eine Äquivalenzrelation.

Satz 5 (Prinzip der vollständigen Induktion)

Sei $A \subseteq \mathbb{N}$. Angenommen es gilt

- $0 \in A$ *und*
- *für alle* $n \in A$ *gilt auch* $n + 1 \in A$.

Dann gilt $A = \mathbb{N}$.

Beweis (durch Widerspruch): Angenommen für $A \subseteq \mathbb{N}$ gilt:

(1) $0 \in A$ und

(2) für alle $n \in A$ gilt auch $n + 1 \in A$.

Angenommen es gilt $A \neq \mathbb{N}$.

Wir leiten einen Widerspruch ab.

Da $\mathbb{N} \setminus A \neq \emptyset$ gilt, hat diese Menge ein kleinstes Element $m \notin A$ (jede nicht-leere Menge von natürlichen Zahlen hat ein kleinstes Element)

Da $0 \in A$ nach (1) gilt, muss $m > 0$ gelten.

Da m das kleinste Element von $\mathbb{N} \setminus A$ ist, muss $m - 1 \notin \mathbb{N} \setminus A$, d. h. $m - 1 \in A$ gelten.

Dann gilt aber nach (2) auch $m \in A$, was ein Widerspruch ist. $\square$

In Anwendungen ist häufig A die Menge aller natürlichen Zahlen mit einer gewissen Eigenschaft, und man will zeigen, dass alle natürlichen Zahlen diese Eigenschaft haben.

Beispiel 1: Wir beweisen mittels vollständiger Induktion, dass für alle natürlichen Zahlen n gilt:

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Hierbei ist $\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n$ die Summe der n ersten natürlichen Zahlen.

Induktionsanfang: Es gilt $\sum_{i=1}^{0} i = 0 = \frac{0 \cdot 1}{2}$.

Induktionsschritt: Angenommen es gilt

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}.$$

Dann gilt auch

$$\begin{aligned}
\sum_{i=1}^{n+1} i &= \Big(\sum_{i=1}^{n} i\Big) + n + 1 \\
&= \frac{n(n+1)}{2} + n + 1 \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}
\end{aligned}$$

Mengentheoretische Grundlagen

Beispiel 2: Wir beweisen mittels vollständiger Induktion, dass für alle natürlichen Zahlen $n \geq 1$ und alle reellen Zahlen $x_1, \ldots, x_n \geq 0$ gilt:

$$\prod_{i=1}^{n}(1 + x_i) \geq 1 + \sum_{i=1}^{n} x_i$$

Hierbei ist $\prod_{i=1}^{n}(1 + x_i) = (1 + x_1)(1 + x_2) \cdots (1 + x_n)$ das Produkt der Zahlen $1 + x_1, \ldots, 1 + x_n$

Induktionsanfang: Es gilt $\prod_{i=1}^{1}(1 + x_i) = 1 + x_1 = 1 + \sum_{i=1}^{1} x_i$.

Induktionsschritt: Angenommen es gilt

$$\prod_{i=1}^{n}(1 + x_i) \geq 1 + \sum_{i=1}^{n} x_i$$

Dann gilt:

$$\begin{aligned}
\prod_{i=1}^{n+1}(1+x_i) &= (1+x_{n+1})\cdot\prod_{i=1}^{n}(1+x_i)\\
&\geq (1+x_{n+1})\cdot(1+\sum_{i=1}^{n}x_i)\\
&= 1+(\sum_{i=1}^{n}x_i)+x_{n+1}+x_{n+1}\cdot(\sum_{i=1}^{n}x_i)\\
&\geq 1+\sum_{i=1}^{n+1}x_i
\end{aligned}$$

Bemerkung: Die Ungleichung $\prod_{i=1}^{n}(1+x_i)\geq 1+\sum_{i=1}^{n}x_i$ gilt auch für $n=0$, wenn man definiert

$$\prod_{i=1}^{0}a_i = 1.$$

Mengentheoretische Grundlagen

Die n-fache Komposition kann auch für eine Funktion $f : A \to A$ angewendet werden.

Dann ist f^n die n-fache Anwendung von f:

- $f^0(x) = x$ für alle $x \in A$.
- $f^{n+1}(x) = f(f^n(x))$ für alle $x \in A$ und $n \geq 0$.

Beispiel: Sei $R = \{(x, x+1) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$.

Dann gilt für alle $n \geq 0$:

$$R^n = \{(x, x+n) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}.$$

In diesem Fall ist R gleich der Funktion $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(x) = x + 1$.

Die Funktion $f^n : \mathbb{Z} \to \mathbb{Z}$ ist dann die n-fache Anwendung von f, d.h. $f^n(x) = x + n$.

Aussagenlogik

Sachverhalte der Realität werden in Form von Aussagen erfasst. Wir betrachten nur Aussagen, die entweder **wahr** oder **falsch** sind.
z.B.

- 7 ist kleiner als 9.
- Angela Merkel ist eine Frau.
- Ein Kreis hat vier Ecken.

Wobei es auch möglich ist, dass der Wahrheitsgehalt zum jetzigen Zeitpunkt noch nicht bestimmt werden kann.

- Der Weltklimakonferenz wird es gelingen, die Klimakatastrophe aufzuhalten.
- Jede gerade Zahl größer 2 ist Summe zweier Primzahlen (die Goldbach'sche Vermutung).

Aussagenlogik

Die Wahrheitswerte, wahr und falsch, sind die beiden Werte die eine Aussage annehmen kann.

Wir schreiben kurz:

- wahr $:=$ w
- falsch$:=$ f

Der Inhalt einer Aussage soll uns im Weiteren nicht mehr interessieren, deshalb ersetzen wir Sie durch Aussagevariablen die meistens die Form eines lateinischen großen Buchstabens A,B,C,... haben.

Aussagenlogik

In der Umgangssprache verknüpft man einzelne Aussagen mit “und”, “oder” oder ...

Wir verwenden die Zeichen:

Umgangssprache	Mathematik
und	$\wedge$
oder	$\vee$
nicht	$\neg$
wenn, dann	$\rightarrow$
genau dann, wenn	$\leftrightarrow$

Aussagenlogik

Wie bereits erwähnt: Jede Aussage ist entweder wahr oder falsch!
Um alle möglichen Varianten von Aussagen und ihren Verknüpfungen aufschreiben zu können, verwenden wir sogenannte Verknüpfungstabellen.

A	B	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
w	w	w	w	w	w
w	f	f	w	f	f
f	w	f	w	w	f
f	f	f	f	w	w

A	$\neg A$
w	f
f	w

Aussagenlogik

Aus diesen einfachen Aussagen, lassen sich beliebig komplizierte Aussagen mit den Verknüpfungen zusammenstellen.
Ähnlich wie in der Zahlenalgebra definieren wir in der Aussagenlogik einige Klammerregeln.

Definition (Klammerkonventionen)

$\wedge$, $\vee$ bindet stärker als $\rightarrow$, $\leftrightarrow$,
$\neg$ hat höchste Präferenz.

Beispiel:

$$((\neg A) \wedge B) \rightarrow (\neg(C \vee D))$$

und

$$\neg A \wedge B \rightarrow \neg(C \vee D)$$

sind äquivalent.

Aussagenlogik

Versuchen wir den Wahrheitswert einer Aussage zu ermitteln, so gehen wir schrittweise von innen nach außen vor.

Definition (gleichwertig)

Zwei Aussageformeln heißen gleichwertig, wenn sie für alle möglichen Belegungen mit Wahrheitswerten denselben Wahrheitswert haben.

Beispiel:

$$B \vee \neg A \leftrightarrow (A \rightarrow B)$$

A	B	$\neg A$	$B \vee \neg A$	$(A \rightarrow B)$	$B \vee \neg A \leftrightarrow (A \rightarrow B)$
w	w	f	w	w	w
w	f	f	f	f	w
f	w	w	w	w	w
f	f	w	w	w	w

Definition (Tautologie)

Eine Formel heißt allgemeingültig oder Tautologie, wenn sie für alle möglichen Einsetzungen von Wahrheitswerten wahr ist.

Satz 6 (Rechenregeln für Aussageformen)

Die folgenden Formeln sind Tautologien:

$A \vee B \rightarrow B \vee A$

$A \wedge B \rightarrow B \wedge A$

$(A \vee B) \vee C \rightarrow A \vee (B \vee C)$

$(A \wedge B) \wedge C \rightarrow A \wedge (B \wedge C)$

$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

$A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$

$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$

Aussagenlogik

Ein paar weitere wichtige Tautologien sind:

- $A \vee \neg A$
- $A \wedge (A \to B) \to B$
- $(A \to B) \wedge (B \to A) \leftrightarrow (A \leftrightarrow B)$
- $(A \to B) \leftrightarrow (\neg B \to \neg A)$

Es fällt auf, dass die Mengentheorie mit ihrem $\cup$ und $\cap$ sehr ähnliche Eigenschaften aufweist, wie die Aussagenlogik mit ihrem $\vee$ und $\wedge$. Deshalb versucht man eine abstrakte Struktur zu definieren, die von den gemeinsamen Eigenschaften bestimmt wird. Anschließend untersucht man dann diese Struktur und alle Ergebnisse gelten für beide Modelle.