Mathematische Grundlagen der Informatik 1

Mengen und Abbildungen

W. Gansterer, K. Schindlerova

2. Oktober 2019

Überblick

Mengenlehre

Begriffsdefinitionen

Was ist eine Menge?

Menge

[Georg Cantor, 1845-1918]

Eine Menge ist eine beliebige Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

- Schwierig exakt zu fassen!
- Barbier-Paradoxon: Man kann einen Barbier als einen definieren, der all jene und nur jene rasiert, die sich nicht selbst rasieren.
  Die Frage ist: *Rasiert der Barbier sich selbst*?
- Russellsche Antinomie (ein Paradoxon der naiven Mengenlehre): Betrachten Sie die „Menge aller Mengen, die sich nicht selbst als Element enthalten“ $\rightarrow$ enthält sich diese Menge selbst oder nicht? ...

Übliche Notationen

- Objekt x, Mengen M, N
- $x \in M$, $y \notin M$
- $M = N \Leftrightarrow M$ und N enthalten dieselben Elemente
  - Ansonsten $M \neq N$
- Leere Menge: $\emptyset := \{\}$
- Beschreibung von Mengen:
  - Explizite Auflistung: $\{1, 4, 8, 9\}$ – gleichbedeutend mit $\{8, 4, 9, 1\}$, $\{8, 8, 4, 9, 1, 9\}$, ...
  - Charakterisierende Eigenschaften:
    $\mathbb{N} := \{x \mid x \text{ ist eine natürliche Zahl}\} = \{1, 2, 3, 4, \ldots\}$;
    $\mathbb{N}_0 := \{0, 1, 2, 3, 4, \ldots\}$
- Mengen selbst sind Objekte, können also als Element in anderen Mengen enthalten sein!
  - $M := \{\mathbb{N}, -8, -2\}$, $N := \{\{\pi\}, \emptyset, \pi\}$
  - Achtung: $\{\pi\}$ und π sind zwei verschiedene Objekte!

Beziehungen zwischen Mengen

Teilmenge

Teilmenge

M heißt Teilmenge der Menge N ($M \subset N$, $N \supset M$) wenn jedes Element von M auch Element von N ist.

- M ist in N enthalten, N ist Obermenge von M

Graphische Darstellung der Beziehungen zwischen Mengen durch *Venn-Diagramme*:

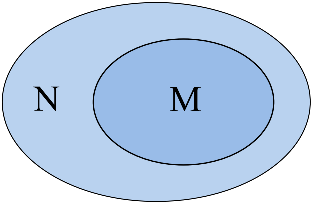


Abbildung: $M \subset N$

Teilmenge

Ist M nicht Teilmenge von N, dann schreibt man $M \not\subset N$

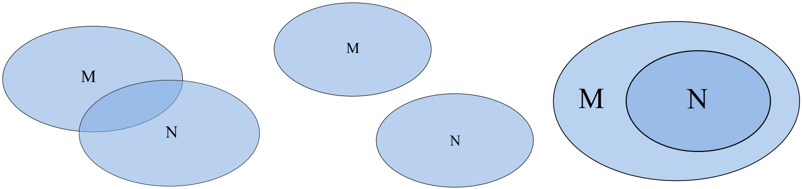


Abbildung: $M \not\subset N$

Vorsicht: Gilt $M \not\subset N \Rightarrow N \subset M$?

Teilmenge

- Echte Teilmenge: $M \subsetneq N \quad \Leftrightarrow \quad M \subset N \; und \; M \neq N$
- Gleichheit von Mengen: Ist $M \subset N \; und \; N \subset M$, so gilt $M = N$
  $\rightarrow$ für den Beweis der Gleichheit von zwei Mengen!
- Für alle Mengen M gilt $M \subset M$ und auch $\emptyset \subset M$
  (jedes Element der leeren Menge ist in M enthalten!)

Potenzmenge

Potenzmenge

$P(M)$, die Potenzmenge einer Menge M, ist die Menge aller Teilmengen von M.

Beispiele

- $M = \{1, 2\} \Rightarrow P(M) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
- $P(\mathbb{R})$ ist die Menge aller Teilmengen von $\mathbb{R} \Rightarrow \mathbb{N} \in P(\mathbb{R})$

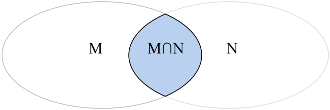
Operationen mit Mengen

Durchschnitt

Durchschnitt zweier Mengen

Der Durchschnitt zweier Mengen M und N ist die Menge der Elemente, die sowohl in M als auch in N enthalten sind:

$$M \cap N := \{x \,|\, x \in M \quad \textit{und} \quad x \in N\}$$



M und N heißen disjunkt, wenn $M \cap N = \emptyset$.

Durchschnitt

Beispiele

Gegeben seien $M = \{1, 3, 5\}$, $N = \{2, 3, 5\}$, $S = \{5, 7, 8\}$.

Dann gilt

- $M \cap N = \{3, 5\}$
- $N \cap S = \{5\}$
- $M \cap N \cap S = (M \cap N) \cap S = \{5\}$

Für jede Menge M gilt: $M \cap \emptyset = \emptyset$.

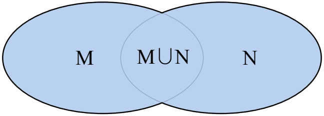
Vereinigung

Vereinigung zweier Mengen

Die Vereinigung zweier Mengen M und N ist die Menge der Elemente, die in M oder[a] in N enthalten sind:

$$M \cup N := \{x \,|\, x \in M \quad oder \quad x \in N\}$$

[a] "oder" ist hier nicht exklusiv gemeint – exklusiv wäre "entweder-oder".



Vereinigung

Beispiele

Gegeben seien $M = \{1, 3, 5\}$, $N = \{2, 3, 5\}$.

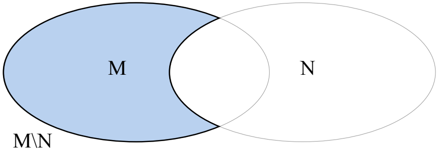
- $M \cup N = \{1, 2, 3, 5\}$
- $M \cup \emptyset = M$ (gilt für jede Menge M!)

Differenz, Differenzmenge

Differenzmenge zweier Mengen

Die Differenzmenge $M \backslash N$ (oder $M - N$) zweier Mengen M und N ist die Menge der Elemente, die in M, aber nicht in N enthalten sind:

$$M \backslash N := \{x \,|\, x \in M \quad \textit{und} \quad x \notin N\}$$



Für jede Menge M gilt: $M \backslash \emptyset = M$.

Komplement

Komplement von N in M

Ist $N \subset M$, so heißt $M \backslash N$ auch das Komplement von N in M.

Es wird mit $\overline{N}^M$ bezeichnet.

Rechenregeln für Mengenoperationen

Kommutativ-, Assoziativ-, Distributivgesetze

Seien M, N, S Mengen. Dann gilt:

- *Kommutativgesetze:*

$$\begin{aligned} M \cup N &= N \cup M \\ M \cap N &= N \cap M \end{aligned}$$

- *Assoziativgesetze:*

$$\begin{aligned} (M \cup N) \cup S &= M \cup (N \cup S) \\ (M \cap N) \cap S &= M \cap (N \cap S) \end{aligned}$$

- *Distributivgesetze:*

$$\begin{aligned} M \cap (N \cup S) &= (M \cap N) \cup (M \cap S) \\ M \cup (N \cap S) &= (M \cup N) \cap (M \cup S) \end{aligned}$$

Operationen mit mehreren Mengen

- Wir können definieren

$$M \cup N \cup S := (M \cup N) \cup S,$$

  und wegen des Assoziativgesetzes ist die Vereinigung dreier Mengen unabhängig davon, in welcher Reihenfolge sie durchgeführt wird.
- Analog für den Durchschnitt von drei Mengen.
- Analog für den Durchschnitt und die Vereinigung von mehr als drei Mengen.

Zum Distributivgesetz

Für Mengen gilt

$$\begin{aligned} M \cap (N \cup S) &= (M \cap N) \cup (M \cap S) \\ M \cup (N \cap S) &= (M \cup N) \cap (M \cup S) \end{aligned}$$

Erinnern wir uns in $\mathbb{R}$:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

Das gilt dort aber *nicht*, wenn man die Operationen vertauscht!

Wie können wir das Distributivgesetz für Mengen beweisen?

Beweis des Distributivgesetzes

Wir zeigen

$$\underbrace{S \cap (M \cup N)}_{:=A} = \underbrace{(S \cap M) \cup (S \cap N)}_{:=B},$$

indem wir zeigen, dass sowohl $A \subset B$ als auch $B \subset A$ gilt.

$A \subset B$: $x \in A \Rightarrow x \in S$ und gleichzeitig auch $x \in M$ oder $x \in N$.
Falls $x \in M$, dann gilt $x \in S \cap M \quad \Rightarrow \quad x \in B$.
Falls $x \in N$, dann gilt $x \in S \cap N \quad \Rightarrow \quad x \in B$.
$\Rightarrow \quad x \in B$ in jedem Fall

$B \subset A$: $x \in B \Rightarrow x \in S \cap M$ oder $x \in S \cap N$
Falls $x \in S \cap M$, dann ist $x \in S$ und $x \in M \quad \Rightarrow x \in M \cup N$ und daher $x \in S \cap (M \cup N) = A$.
Falls $x \in S \cap N$, dann ist $x \in S$ und $x \in N \quad \Rightarrow x \in M \cup N$ und daher $x \in S \cap (M \cup N) = A$.
$\Rightarrow \quad x \in A$ in jedem Fall

$\blacksquare$

Beweis des Distributivgesetzes

Probieren Sie selber, das andere Distributivgesetz zu beweisen!

Rechenregeln für die Komplementbildung

- $\overline{\overline{M}} = M$
- $M \subset N \quad \Rightarrow \quad \overline{N} \subset \overline{M}$
- $M \backslash N = M \cap \overline{N}$
- $\overline{M \cup N} = \overline{M} \cap \overline{N}$
- $\overline{M \cap N} = \overline{M} \cup \overline{N}$

Beweisen Sie diese Rechenregeln!

Unendliche Durchschnitte und Vereinigungen

Sei I eine Menge von Indizes (z. B., $I = \mathbb{N}$). Für jedes $i \in I$ sei eine Menge A_i gegeben. Dann definieren wir

- $\bigcup_{i \in I} A_i := \{x \mid x \in A_i \text{ für mindestens ein } i \in I\}$
- $\bigcap_{i \in I} A_i := \{x \mid x \in A_i \text{ für alle } i \in I\}$

Beachten Sie: Ist I eine *endliche* Menge (z. B., $I = \{1, 2, 3, \ldots, k\}$), dann stimmen diese Definitionen mit der bisherigen Definition von Vereinigung und Durchschnitt überein!

- $\bigcup_{i \in I} A_i := A_1 \cup A_2 \cup \ldots \cup A_k = \bigcup_{i=1}^{k} A_i$
- $\bigcap_{i \in I} A_i := A_1 \cap A_2 \cap \cdots \cap A_k = \bigcap_{i=1}^{k} A_i$

Unendliche Durchschnitte und Vereinigungen

Beispiel

$I = \mathbb{N}$, $A_i := \{x \in \mathbb{R} \mid 0 < x < \frac{1}{i}\} \quad \Rightarrow \quad \bigcap_{i \in \mathbb{N}} A_i = \emptyset$

Beachten Sie: Jeder endliche Durchschnitt ist nicht leer ($\bigcap_{i=1}^{k} A_i = A_k$), aber man findet keine reelle Zahl, die in allen A_i enthalten ist!

Das kartesische Produkt von Mengen

Kartesisches Produkt

Das kartesische Produkt von Mengen

Das kartesische Produkt zweier Mengen M und N besteht aus allen geordneten Paaren (x, y) mit $x \in M$ und $y \in N$:

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

Beachten Sie: $\{5, 3\} = \{3, 5\}$, aber die geordneten Paare $(3, 5)$ und $(5, 3)$ sind verschieden!

Kartesisches Produkt

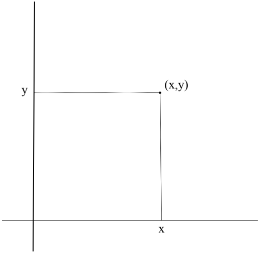
Beispiele

- $M = \{1, 2\}$, $N = \{a, b, c\}$
  - Frage: Gilt $M \times N = N \times M$?
  - *Im allgemeinen nicht!*
    - $M \times N = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$
    - $N \times M = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$
- $M \times \emptyset = \emptyset$ für alle Mengen M.

Kartesisches Produkt

Beispiele

- $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R} = \{(x, y) \,|\, x, y \in \mathbb{R}\}$
    - Das sind die kartesischen Koordinaten.
    - Jeden Punkt im zweidimensionalen Raum kann man im kartesischen Koordinatensystem darstellen.



- $P := \{(x, y) \in \mathbb{R}^2 \,|\, y = x^2\} = \{(x, x^2) \,|\, x \in \mathbb{R}\}$ ... Parabel im $\mathbb{R}^2$

Kartesisches Produkt

Beispiele

- $\mathbb{R}_{\leq} := \{(x, y) \in \mathbb{R}^2 \mid x \leq y\}$ . . . eine Halbebene

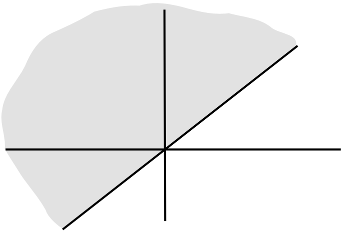
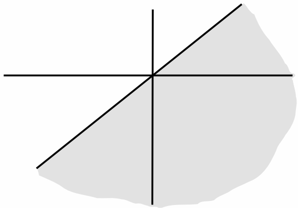


Abbildung: Halbebene $\mathbb{R}_{\leq}$

Kartesisches Produkt

Beispiele

- Wie kann man diese Halbebene definieren?



$\rightarrow \quad \mathbb{R}_{\geq} := \{(x, y) \in \mathbb{R}^2 \,|\, x \geq y\}$

Die Mächtigkeit von Mengen

Mächtigkeit

Mächtigkeit einer Menge M

Die Mächtigkeit (Kardinalität) einer Menge M ist die Anzahl der Elemente in M.

Sie wird mit $|M|$ bezeichnet.

$|M| = |N| \quad \Leftrightarrow \quad M$ und N heissen *gleichmächtig* und es gibt eine *bijektive Abbildung* zwischen M und N.

Endliche Mächtigkeit $k \in \mathbb{N}$

Eine Menge M hat endliche Mächtigkeit $k \Leftrightarrow |M| = |\{1, 2, 3, \ldots, k\}|$

Spezielle Mengen: Zahlenmengen

Die natürlichen Zahlen

Axiomensysteme

- Standardvorgang in der Mathematik: aus gegebenen Aussagen mithilfe logischer Schlussfolgerungen neue Aussagen (*Sätze*) gewinnen
- Wie kann dieser Prozess beginnen?

- An den Anfang wird eine Reihe von Tatsachen gestellt, die als wahr/richtig angenommen werden, ohne dass sie selber bewiesen werden.
- Unbewiesene Grundtatsachen einer Theorie = Axiome

Axiomensysteme

- Aufstellen von Axiomensystemen ist eine schwierige Aufgabe
- Anforderungen:
  - Möglichst wenige und einfache (plausible!) Axiome;
    aber genügend, um die Theorie vollständig beschreiben zu können!
  - Axiome müssen unabhängig voneinander sein
  - Axiome müssen widerspruchsfrei sein

Die Axiome der natürlichen Zahlen

- Intuitiv sind die natürlichen Zahlen und ihre Eigenschaften jedem Menschen vertraut
- Aber welches Axiomensystem ist als Fundament für die Theorie der natürlichen Zahlen geeignet?

$\rightarrow$ *Axiomensystem von Guiseppe Peano* (Ende des 19. Jhdts)

Die Axiome der natürlichen Zahlen

Peano Axiome

Die Menge $\mathbb{N}$ der natürlichen Zahlen ist durch folgende Eigenschaften charakterisiert:

(P1) $1 \in \mathbb{N}$

(P2) *Jede natürliche Zahl hat genau einen von 1 verschiedenen Nachfolger, der selbst eine natürliche Zahl ist.*

(P3) *Verschiedene natürliche Zahlen haben verschiedene Nachfolger.*

(P4) *Wenn eine Teilmenge $M \subset \mathbb{N}$ die beiden folgenden Eigenschaften hat:*

- $1 \in M$
- $n \in M \Rightarrow$ *der Nachfolger von n ist ebenfalls Element von M,*

dann gilt $M = \mathbb{N}$.

Anmerkung: P4 wird durch "Ausprobieren" plausibel!
$(1 \in M \Rightarrow 2 \in M \Rightarrow 3 \in M \Rightarrow \cdots)$

Die Axiome der natürlichen Zahlen

- Wir bezeichnen den Nachfolger der natürlichen Zahl n mit $n + 1$.
- Aus diesen vier Axiomen kann man alles folgern, was wir über die natürlichen Zahlen wissen.

Die vollständige Induktion

Das Beweisprinzip der vollständigen Induktion

Sei $A(n)$ eine Aussage über die natürliche Zahl n.

Wenn gilt

- $A(1)$ ist wahr.
- für alle $n \in \mathbb{N}$: $A(n)$ ist wahr $\Rightarrow A(n+1)$ ist wahr,

dann ist $A(n)$ wahr *für alle* $n \in \mathbb{N}$.

Das Beweisprinzip der vollständigen Induktion

Beispiel

Sei $A(n)$ die Aussage $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$.

- $A(1) : 1 = \frac{1 \cdot 2}{2}$
- $A(2) : 1 + 2 = \frac{2 \cdot 3}{2}$
- $A(3) : 1 + 2 + 3 = \frac{3 \cdot 4}{2}$
- ...
- Aber gilt es auch für $n = 1000$, $n = 10^{27}$, ...? Wir können nicht unendlich viele Fälle überprüfen!

Das Beweisprinzip der vollständigen Induktion

Induktionsprinzip: Wenn wir ganz allgemein von einer Zahl auf ihren Nachfolger schliessen können, dann gilt die Aussage für alle natürlichen Zahlen.

Beweis für eine von einer natürlichen Zahl n abhängigen Aussage $A(n)$ erfolgt in drei Schritten:

- **Induktionsanfang**: Beweise, dass die Aussage $A(n)$ für die kleinste natürliche Zahl, für die die Aussage wahr sein soll (im Normalfall $n = 1$) wahr ist.
- **Induktionsannahme**: Nimm an, dass $A(n)$ wahr ist.
- **Induktionsschluss**: Beweise, dass unter dieser Annahme auch $A(n + 1)$ wahr ist.

Das Beweisprinzip der vollständigen Induktion

Beispiel:

Für alle natürlichen Zahlen n gilt: $2^n > n$

Induktionsanfang: $n = 1 \qquad 2^1 > 1 \quad w.A.$
Induktionsannahme: Nehmen wir an, $2^n > n$.
Induktionsschritt:

$$2^{n+1} = 2^n \cdot 2 \overset{?}{>} n + 1$$

$$2^n \cdot 2 > n \cdot 2 = n + n \geq n + 1$$

$\rightarrow w.A. \quad \forall n \geq 1, n \in \mathbb{N}$

Das Beweisprinzip der vollständigen Induktion

Warum stimmt das Beweisprinzip der vollständigen Induktion?

Die Voraussetzungen 1,2 des Beweisprinzips seien erfüllt:

- $A(1)$ ist wahr.
- für alle $n \in \mathbb{N}$: $A(n)$ ist wahr $\Rightarrow A(n+1)$ ist wahr,

Definieren wir die Menge $M := \{n \in \mathbb{N} \,|\, A(n)\,\text{ist eine wahre Aussage}\}$.
Nun gilt:

- $1 \in M$ wegen Voraussetzung 1.
- Ist $n \in M$, dann ist auch $n + 1 \in M$ wegen Voraussetzung 2.

Wegen Axiom P4 gilt also: $M = \mathbb{N}$. ■

Weitere wichtige Zahlenmengen

- $\mathbb{Z} := \{x \mid x \text{ ist ganze Zahl}\} = \{0, +1, -1, +2, -2, \ldots\} = \{y \mid y = 0 \text{ oder } y \in \mathbb{N} \text{ oder } -y \in \mathbb{N}\}$
- $\mathbb{Q} := \{x \mid x \text{ ist ein Bruch}\} := \{x \mid x = \frac{p}{q},\ p \in \mathbb{Z}, q \in \mathbb{N}\}$
- $\mathbb{R} := \ldots$ *später (2. Semester)*