2. Modellierung mit Wertebereichen — mathematische Grundlagen und Beweistechniken

Mathematische Notationen

$:=$	Definition eines Wertes, z.B.: $x := 5$, $M := \{1,2,3\}$
$:\Leftrightarrow$	Definition einer Eigenschaft oder einer Schreibweise z.B.: $m \in M :\Leftrightarrow$ m ist Element von M
ex.	es gibt, es existiert
f.a.	für alle, für jedes
$\Rightarrow$	impliziert z.B.: Regen $\Rightarrow$ nasse Straße
$\Leftrightarrow$	genau dann wenn z.B.: Klausur bestanden $\Leftrightarrow$ $z \geq 50\%$
$\square$	markiert das Ende eines Beweises
s.d.	Abkürzung für "so, dass"

Modellierung und Wertebereiche

In der Modellierung von Systemen / Aufgaben / Problemen / Lösungen kommen Objekte unterschiedlicher Art und Zusammensetzung vor.

Für Teile des Modells wird angegeben, aus welchem Wertebereich sie stammen, aber manchmal oft offen gelassen, welchen konkreten Wert sie haben.

Beispiel: Gegeben 3 Karten aus einem Kartenspiel; welches ist die höchste Karte?

Ein Wertebereich ist eine Menge gleichartiger Werte. Wertebereiche werden aus Mengen und Strukturen darüber gebildet.

Beispiel 2.1: Modellierung der Karten eines (Skat-) Kartenspiels

Wertebereich:

KartenArten := { Kreuz, Pik, Herz, Karo }

KartenSymbole := { 7, 8, 9, 10, Bube, Dame, König, Ass }

Karten := { (Kreuz, 7), (Kreuz, 8), ..., (Kreuz, Ass),
(Pik, 7), (Pik, 8), ..., (Pik, Ass),
(Herz, 7), (Herz, 8), ..., (Herz, Ass),
(Karo, 7), (Karo, 8), ..., (Karo, Ass) }

Übersicht über Begriffe, die in Kap 2 genauer betrachtet werden:

- Wertebereich: eine Menge gleichartiger Werte
- Grundlegender Kalkül: Mengenlehre — Mengen und Mengenoperationen
- Strukturen über Mengen zur Bildung von zusammengesetzten Wertebereichen:
  - Potenzmengen
  - Kartesische Produkte, Tupel
  - Relationen
  - Folgen, Wörter
  - Funktionen
- Verwendung dieses Kalküls
  - Modellierung von Strukturen und Zusammenhängen
  - Grundlage für alle anderen formalen Kalküle
  - abstrakte Grundlage für Typen in Programmiersprachen

Ziel von Kap 2 ist, diese Begriffe genauer zu betrachten und abgesehen davon einige wichtige mathematische Grundlagen und Beweistechniken zu erklären.

2.1 Mengen, Relationen und Funktionen

Was ist eine Menge?

Cantors naiver Mengenbegriff: (Georg Cantor, 1845–1918)

Eine Menge M ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche "Elemente der Menge M" genannt werden, zu einem Ganzen.

Notation: $m \in M :\Leftrightarrow m$ ist Element der Menge M

Die Russellsche Antinomie: (Bertrand Russell, 1872–1970)

Cantors Mengenbegriff ist problematisch und führt zu Widersprüchen.
Russel gab folgendes Beispiel:

Sei N die Menge aller Mengen M, die sich nicht selbst enthalten
(dh: $M \in N :\Leftrightarrow$ M ist eine Menge, für die gilt: $M \notin M$)

Frage: Enthält N sich selbst (dh gilt $N \in N$)?

klar: entweder gilt $N \in N$ oder es gilt $N \notin N$.

Fall 1: $N \notin N$. Gemäß Definition der Menge N gilt dann, dass $N \in N$. Das ist ein Widerspruch.

Fall 2: $N \in N$. Gemäß Definition der Menge N gilt dann, dass $N \notin N$. Das ist ein Widerspruch

Somit führen beide Fälle zu einem Widerspruch, obwohl wir wissen, dass eigentlich genau einer der beiden Fälle zutreffen müsste.

$\Longrightarrow$ Irgendwas stimmt nicht mit Cantors naivem Mengenbegriff!

Um Russells Beispiel und den daraus resultierenden Widerspruch besser zu verstehen, betrachte man folgende Geschichte vom Barbier von Sonnenthal.

Der Barbier von Sonnenthal:

Im Städtchen Sonnenthal (in dem bekanntlich viele seltsame Dinge passieren) wohnt ein Barbier, der genau diejenigen männlichen Einwohner von Sonnenthal rasiert, die sich nicht selbst rasieren.

Frage: Rasiert der Barbier sich selbst?

Um die Russellsche Antinomie zu vermeiden, muss man die Mengenlehre sehr vorsichtig axiomatisch aufbauen — dies sprengt allerdings den Rahmen dieser Vorlesung.

Sofern man sich der Problematik aber bewusst ist,

Kann man sie im "täglichen Gebrauch" von Mengen vermeiden. Wir arbeiten daher weiter mit einem naiven Mengenbegriff.

Beschreibung / Definition von Mengen

- durch Aufzählen der Elemente (extensional)

  z.B. $M_1 := \{0,1,2,3,4,5\}$
  $= \{0,1,2,\dots,5\}$

- durch Angabe von charakteristischen Eigenschaften der Elemente der Menge (intensional)

  z.B. $M_2 := \{x : x \in M_1 \text{ und } x \text{ ist gerade}\}$
  $= \{x \in M_1 : x \text{ ist gerade}\}$
  $= \{x : x \text{ ist eine natürliche Zahl und } x \text{ ist gerade und } 0 \leq x \leq 5\}$

  Intensional läßt sich M_2 folgendermaßen beschreiben: $M_2 = \{0,2,4\}$

  Oft schreibt man statt ":" auch "|" und statt "und" einfach ein "Komma",

  also $M_2 = \{x \mid x \in M_1, x \text{ gerade}\}$

Vorsicht:

(a) $\{x : 0 \leq x \leq 5\}$ definiert nicht eindeutig eine Menge, weil nicht festgelegt ist, ob x beispielsweise eine ganze oder eine reelle Zahl ist

(b) $\{M : M \text{ ist eine Menge}, M \notin M\}$ führt zur Russellschen Antinomie

Fazit:

Um solche Probleme zu vermeiden, sollte man bei intensionalen Mengendefinitionen immer angeben, aus welcher anderen Menge die ausgewählten Elemente kommen sollen, also:

$$\{x \in M : x \text{ hat Eigenschaft(en) } E\},$$

wobei M eine Menge und E eine Eigenschaft oder eine Liste von Eigenschaften ist, die jedes einzelne Element aus M haben kann oder nicht.

Wichtige grundsätzliche Eigenschaften von Mengen:

- Alle Elemente einer Menge sind verschieden.
  D.h. ein Wert ist entweder Element der Menge oder eben nicht – aber er kann nicht "mehrfach" in der Menge vorkommen

- Die Elemente einer Menge haben keine feste Reihenfolge.

- Dieselbe Menge kann auf verschiedene Weisen beschrieben werden, z.B.

$$\{1,2,3\} = \{1,2,2,3\} = \{2,1,3\}$$
$$= \{i : i \text{ ist eine ganze Zahl}, 0 < i \leq 3\}$$

Insbesondere können Mengen aus atomaren oder aus zusammengesetzten Elementen gebildet werden, und eine Menge kann auch verschiedenartige Elemente enthalten.

Beispiel: Die Menge $M := \{1, (\text{Pik}, 8), \{\text{rot}, \text{blau}\}, 5\}$

besteht aus 4 Elementen:
- den atomaren Werte 1 und 5
- dem Tupel (Pik, 8)
- der Menge {rot, blau}.

Notationen für bestimmte Zahlenmengen:

$\mathbb{N}$:= Menge der natürlichen Zahlen
$:= \{0, 1, 2, 3, \dots\}$

$\mathbb{N}_{>0}$:= Menge der positiven natürlichen Zahlen
$:= \{1, 2, 3, \dots\}$

$\mathbb{Z}$:= Menge der ganzen Zahlen
$:= \{0, 1, -1, 2, -2, 3, -3, \dots\}$

$\mathbb{Q}$:= Menge der rationalen Zahlen
$:= \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$

$\mathbb{R}$:= Menge der reellen Zahlen

Beobachtung: Es gibt genau eine Menge, die keine Elemente enthält

Definition 2.2:
Die **leere Menge** ist die (eindeutig bestimmte) Menge, die keine Element(e) enthält
Wir bezeichnen sie mit $\emptyset$.

□ Ende von Def. 2.2

Frage 23: Gibt es eine "Menge aller Mengen"?

Nein! Denn wäre U die Menge aller Mengen, so wäre auch $N := \{M \in U : M \notin M\}$ eine Menge. Dies führt aber wieder zur Russellschen Antinomie (da die Frage "Ist $N \in N$?" nicht geklärt werden kann).

Mengenalgebra

Definition 2.4 (Gleichheit von Mengen)

Zwei Mengen M und N sind gleich (kurz: $M = N$), falls sie dieselben Elemente enthalten, d.h. falls gilt:

- f.a. $x \in M$ gilt $x \in N$, und
- f.a. $x \in N$ gilt $x \in M$.

Beachte: $\emptyset \neq \{\emptyset\}$, denn $\emptyset$ ist die Menge, die keine Elemente enthält, während $\{\emptyset\}$ eine Menge ist, die ein Element (nämlich $\emptyset$) enthält.

Definition 2.5 (Teilmengen)

Seien M, N Mengen.

(a) M ist eine Teilmenge von N (kurz: $M \subseteq N$), wenn jedes Element von M auch ein Element von N ist.

(b) M ist eine echte Teilmenge von N (kurz: $M \subsetneq N$), wenn $M \subseteq N$ und $M \neq N$.

(c) M ist eine Obermenge von N (kurz: $M \supseteq N$), wenn $N \subseteq M$.

(d) M ist eine echte Obermenge von N (kurz: $M \supsetneq N$), wenn $M \supseteq N$ und $M \neq N$.

Satz 2.6

Seien M, N, P Mengen. Dann gilt:

(a) $M = N \iff M \subseteq N$ und $M \supseteq N$

(b) $M \subseteq N$ und $N \subseteq P \Rightarrow M \subseteq P$.

Beweis:

(a) $M = N$
$\overset{\text{Def 2.4}}{\iff}$ M und N enthalten dieselben Elemente
$\overset{\text{Def 2.4}}{\iff}$ f.a. $x \in M$ gilt $x \in N$ und
f.a. $x \in N$ gilt $x \in M$

$\iff$ jedes Element von M ist auch ein Element von N und
jedes Element von N ist auch ein Element von M

$\overset{\text{Def 2.5(a)}}{\iff}$ $M \subseteq N$ und $N \subseteq M$
$\overset{\text{Def 2.5(c)}}{\iff}$ $M \subseteq N$ und $M \supseteq N$.

(b) Es gelte $M \subseteq N$ und $N \subseteq P$.

Behauptung: $M \subseteq P$, d.h. f.a. $m \in M$ gilt $m \in P$

Beweis: Sei $m \in M$ beliebig. Wir zeigen, dass $m \in P$.

$$m \in M \overset{\text{nach Vor: } M \subseteq N}{\Longrightarrow} m \in N \overset{\text{nach Vor: } N \subseteq P}{\Longrightarrow} m \in P.$$

□

Definition 2.6:

Seien M und N Mengen.

(a) (Durchschnitt)

$$M \cap N := \{x : x \in M \text{ und } x \in N\}$$

(b) (Vereinigung)

$$M \cup N := \{x : x \in M \text{ oder } x \in N\}$$

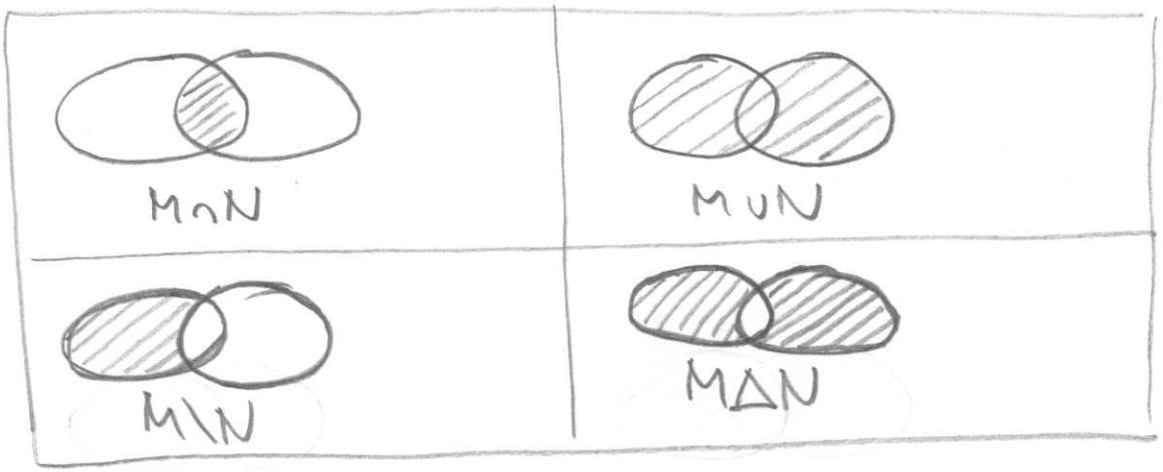
(c) (Differenz)

$$M \setminus N := M - N := \{x : x \in M \text{ und } x \notin N\}$$

(d) (Symmetrische Differenz)

$$M \Delta N := (M \setminus N) \cup (N \setminus M)$$

Veranschaulichung durch Venn Diagramme



Notation: Zwei Mengen M, N heißen disjunkt, falls $M \cap N = \emptyset$, dh falls sie keine gemeinsamen Elemente besitzen. Manchmal schreiben wir $M \dot{\cup} N$, um $M \cup N$ zu bezeichnen und gleichzeitig auszudrücken, dass $M \cap N = \emptyset$.

Rechenregeln für Durchschnitt und Vereinigung:

Satz 2.7:

Seien M, N, P Mengen. Dann gelten:

(a) (Idempotenz) $M \cap M = M$ und $M \cup M = M$

(b) (Kommutativität) $M \cap N = N \cap M$, $M \cup N = N \cup M$

(c) (Assoziativität) $M \cap (N \cap P) = (M \cap N) \cap P$,
$M \cup (N \cup P) = (M \cup N) \cup P$

(d) (Absorption) $M \cap (M \cup N) = M$,
$M \cup (M \cap N) = M$

(e) (Distributivität) $M \cap (N \cup P) = (M \cap N) \cup (M \cap P)$,
$M \cup (N \cap P) = (M \cup N) \cap (M \cup P)$.

anschaulich: (c): 

(d): 

(e): 

Beweis:

(a) $M \cap M \overset{\text{Def 2.6(a)}}{=} \{x : x \in M \text{ und } x \in M\}$
$= \{x : x \in M\}$
$= M$

analog: $M \cup M = M$

(b) $M \cap N \overset{\text{Def 2.6(a)}}{=} \{x : x \in M \text{ und } x \in N\}$
$= \{x : x \in N \text{ und } x \in M\}$
$\overset{\text{Def 2.6(a)}}{=} N \cap M$

analog: $M \cup N = N \cup M$

(c) $M \cap (N \cap P) \overset{\text{Def 2.6'(a)}}{=} \{x : x \in M \text{ und } x \in N \cap P\}$

$\overset{\text{Def 2.6'(a)}}{=} \{x : x \in M \text{ und } (x \in N \text{ und } x \in P)\}$

$= \{x : (x \in M \text{ und } x \in N) \text{ und } x \in P\}$

$\overset{\text{Def 2.6'(a)}}{=} \{x : x \in M \cap N \text{ und } x \in P\}$

$\overset{\text{Def 2.6'(a)}}{=} (M \cap N) \cap P$

analog: $M \cup (N \cup P) = (M \cup N) \cup P$

(d) Wir beweisen, dass $M \cap (M \cup N) = M$ in 2 Schritten:

Schritt 1: Zeige, dass $M \subseteq M \cap (M \cup N)$

Schritt 2: Zeige, dass $M \cap (M \cup N) \subseteq M$

Aus Satz 2.5 (a) folgt dann, dass $M \cap (M \cup N) = M$.

Zu Schritt 1: Behauptung: $M \subseteq M \cap (M \cup N)$, dh
f.a. $m \in M$ gilt $m \in M \cap (M \cup N)$

Beweis: Sei $m \in M$ beliebig. Zu zeigen: $m \in M \cap (M \cup N)$.
Wegen $m \in M$ gilt auch $m \in M \cup N$ (gemäß Def 2.6'(b)).
Wegen $m \in M$ und $m \in M \cup N$ gilt gemäß Def 2.6'(a),
dass $m \in M \cap (M \cup N)$ ✓

Zu Schritt 2: Behauptung: $M \cap (M \cup N) \subseteq M$, dh
f.a. $m \in M \cap (M \cup N)$ gilt $m \in M$.

Beweis: Sei $m \in M \cap (M \cup N)$ beliebig. Zu zeigen: $m \in M$.
Wegen $m \in M \cap (M \cup N)$ gilt gemäß Def 2.6'(a), dass
$m \in M$ und $m \in M \cup N$. Insbesondere ist also $m \in M$ ✓

Insgesamt haben wir damit gezeigt, dass

$M \cap (M \cup N) = M$

analog: $M \cup (M \cap N) = M$

(e) analog (Details: Übung). □

Komplemente:

Das Komplement einer Menge M, kurz: $\overline{M}$ soll die Menge aller Elemente sein, die nicht in M gehören. Bei der präzisen Definition von $\overline{M}$ ist allerdings wieder Vorsicht geboten, denn wenn wir einfach

$\overline{M} := \{x : x \notin M\}$ setzen, so gilt für die Leere Menge $\emptyset$, dass ihr Komplement $\overline{\emptyset}$ einfach alles enthält — und dann wäre

$\{M : M \in \overline{\emptyset}$ und M ist eine Menge$\}$

die "Menge aller Mengen" ... und dass es die nicht geben kann, haben wir in Frage 2.3 gesehen.

Daher betrachten wir Mengen stets innerhalb eines festen Universums U, das selber eine Menge ist.

Für $M \subseteq U$ setzen wir dann $\overline{M} := U \setminus M$

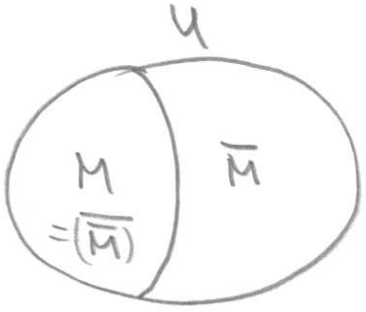
und bezeichnen $\overline{M}$ als das Komplement von M in U.

Rechenregeln für Komplemente:

Satz 2.8:
Sei U unser festes Universum, das selbst eine Menge ist, und seien $M, N \subseteq U$. Dann gelten:

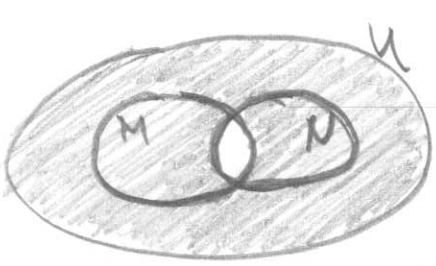
(a) (Doppelte Negation)

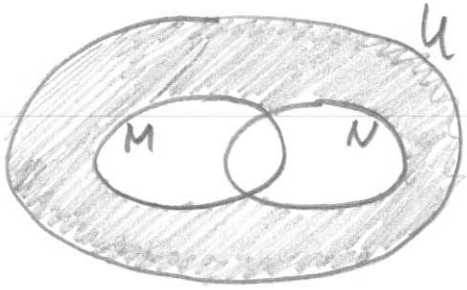
$$\overline{(\overline{M})} = M$$



(b) (De Morgansche Regeln)

$$\overline{(M \cap N)} = \overline{M} \cup \overline{N}, \qquad \overline{(M \cup N)} = \overline{M} \cap \overline{N}$$





(c) (Inversionsregeln)

$$M \cap \overline{M} = \emptyset, \qquad M \cup \overline{M} = U$$

(d) (Identitätsregeln)

$$M \cap U = M, \qquad M \cup \emptyset = M$$

Beweis: Übung.

Mächtigkeit / Kardinalität

Definition 2.9:

(a) Eine Menge heißt endlich, wenn sie nur endlich viele Elemente enthält

(b) Die Mächtigkeit (oder Kardinalität) einer Menge M ist

$$|M| := \begin{cases} \text{Anzahl der Elemente in } M, & \text{falls } M \text{ endlich} \\ \infty \text{ (unendlich)}, & \text{sonst.} \end{cases}$$

Notation: $\text{Card}(M) := |M|$.

Beispiel 2.10:

- $|\{2,4,6\}| = 3$
- $|\emptyset| = 0$
- $|\{\emptyset\}| = 1$
- $|\mathbb{N}| = \infty$
- $|\mathbb{Z}| = \infty$
- $|\{2,4,6,4\}| = 3$
- $|\{2,\{a,6\}\}| = 2$

Vorsicht beim Vergleich der Mächtigkeit unendlicher Mengen:

Hilberts Hotel (David Hilbert, 1862–1943)

Hilberts Hotel hat unendlich viele Zimmer, die fortlaufend mit 1, 2, 3, ... (also mit allen Zahlen aus $\mathbb{N}_{>0}$) nummeriert sind.

Obwohl alle Zimmer belegt sind, schafft der Angestellte an der Rezeption es, für jeden neuen Gast Platz zu schaffen.

Wie? — Er bittet alle Gäste, in das Zimmer mit der nächsthöheren Nummer umzuziehen und gibt dem neuen Gast das Zimmer mit der Nummer 1.

Fügt man also zu einer unendlichen Menge ein Element hinzu, so erhält man keine "wirklich größere" Menge.

Die Potenzmenge (engl: power set)

Definition 2.11

Die Potenzmenge einer Menge M (kurz: $\mathcal{P}(M)$) ist die Menge aller Teilmengen von M. D.h.:

$$\mathcal{P}(M) := \{ N : N \subseteq M \}$$

Notation: In manchen Büchern wird $\mathcal{P}(M)$ auch mit $\mathrm{Pow}(M)$ (für "power set") oder mit 2^M bezeichnet.

Beispiele 2.12:

- $\mathcal{P}(\{a,b\}) = \{ \emptyset, \{a\}, \{b\}, \{a,b\} \}$
- $\mathcal{P}(\{1,2,3\}) = \{ \emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\} \}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$

  Insbesondere: $\mathcal{P}(\emptyset) \neq \emptyset$.

Paare, Tupel und Kartesische Produkte

Definition 2.13 (Paare und Tupel)

(a) Für beliebige a, c bezeichnet (a,c) das (geordnete) Paar mit Komponenten a und c.

(b) Für $k \in \mathbb{N}$ und beliebige $a_1, \dots, a_k$ bezeichnet $(a_1, \dots, a_k)$ das k-Tupel mit Komponenten $a_1, \dots, a_k$

(c) (Gleichheit zweier Tupel):
F.a. $k, \ell \in \mathbb{N}$ und $a_1, \dots, a_k, b_1, \dots, b_\ell$ gilt

$$(a_1, \dots, a_k) = (b_1, \dots, b_\ell) \iff k = \ell \text{ und } a_1 = b_1 \text{ und } a_2 = b_2 \text{ und } \dots \text{ und } a_k = b_k$$

Bemerkung 2.14

(a) Für $k = 0$ gibt es genau ein k-Tupel, nämlich das leere Tupel $()$, das keine Komponente(n) hat.

(b) Beachte den Unterschied zwischen Tupeln und Mengen: z.B.:
- $(1,2) \neq (2,1)$, aber $\{1,2\} = \{2,1\}$
- $(1,1,2) \neq (1,2)$, aber $\{1,1,2\} = \{1,2\}$

Definition 2.14:

(a) Sei $k \in \mathbb{N}$ und sei M eine Menge.
Die k-te Potenz von M ist die Menge

$$M^k := \{ (m_1, \dots, m_k) : m_1 \in M, \dots, m_k \in M \}$$

Insbesondere: $M^0 = \{()\}$ besteht aus genau einem Element, dem leeren Tupel.

(b) Das kartesische Produkt zweier Mengen M, N ist die Menge

$$M \times N := \{ (m,n) : m \in M, n \in N \}$$

(c) Sei $k \in \mathbb{N}_{>0}$ und seien $M_1, \dots, M_k$ Mengen.
Das kartesische Produkt von $M_1, \dots, M_k$ ist die Menge

$$M_1 \times \dots \times M_k := \{ (m_1, \dots, m_k) : m_1 \in M_1, \dots, m_k \in M_k \}.$$

Beispiele:

Sei $M = \{a,b\}$, $N = \{1,2,3\}$.

- $M \times N = \{ (a,1), (a,2), (a,3), (b,1), (b,2), (b,3) \}$
- $M \times \{1\} = \{ (a,1), (b,1) \}$
- $M \times \emptyset = \emptyset$
- $M^2 = \{ (a,a), (a,b), (b,a), (b,b) \}$

- $M^1 = \{(a), (b)\}$
- $M^0 = \{()\}$
- $\emptyset^2 = \emptyset$
- $\emptyset^1 = \emptyset$
- $\emptyset^0 = \{()\}$
- Im Beispiel 2.1 hatten wir die Karten eines Skat-Kartenspiels durch folgende Wertebereiche modelliert:

  KartenArten = {Kreuz, Pik, Herz, Karo}

  KartenSymbole = {7, 8, 9, 10, Bube, Dame, König, Ass}

  Karten = KartenArten × KartenSymbole

- Uhrzeiten kann man repräsentieren durch Elemente der Menge

  Uhrzeiten := Stunden × Minuten × Sekunden,

  wobei

  Stunden := {0, 1, 2, ..., 23}
  Minuten := {0, 1, 2, ..., 59}
  Sekunden := {0, 1, 2, ..., 59}

  Das Tupel (9, 45, 00) repräsentiert dann die Uhrzeit "9 Uhr, 45 Minuten und 0 Sekunden" — d.h. den Beginn der Pause in der Vorlesung.

Die Mächtigkeit von kartesischen Produkten:

Satz 2.15:

(a) Seien M und N zwei endliche Mengen. Dann gilt:

$$|M \times N| = |M| \cdot |N|$$

(b) Sei $k \in \mathbb{N}_{>0}$ und seien $M_1, \dots, M_k$ endliche Mengen. Dann gilt:

$$|M_1 \times \dots \times M_k| = |M_1| \cdot \dots \cdot |M_k| = \prod_{i=1}^{k} |M_i|$$

(c) Sei $k \in \mathbb{N}$ und sei M eine endliche Menge. Dann gilt:

$$|M^k| = |M|^k.$$

Beweis:

(a) $$|M \times N| = \Big| \dot{\bigcup_{m \in M}} (\{m\} \times N) \Big| = \sum_{m \in M} |\{m\} \times N|$$

$$= \sum_{m \in M} |N| = \underbrace{|N| + \dots + |N|}_{|M|\text{-mal}} = |M| \cdot |N|$$

(b) analog.

(c) $$|M^k| = |\underbrace{M \times \dots \times M}_{k\text{-mal}}| \overset{(b)}{=} \underbrace{|M| \cdot \dots \cdot |M|}_{k\text{-mal}} = |M|^k.$$

□

Worte bzw. endliche Folgen

Bemerkung 2.16:

Sei A eine Menge

- Gelegentlich fassen wir ein Tupel $(a_1, \dots, a_k) \in A^k$ als Wort auf, dessen "Buchstaben" $a_1, \dots, a_k$ sind. Um diese Sichtweise zu betonen, schreiben wir oft $a_1 \cdots a_k$ an Stelle von $(a_1, \dots, a_k)$

  Beispiel: Das Tupel (m, o, d, e, l, l) identifizieren wir mit dem Wort modell

- A ist dann das Alphabet, über dem die Worte gebildet werden, und $a_1 \cdots a_k$ wird "Wort über A" genannt.
- Das leere Tupel $() \in A^0$ heißt auch leeres Wort und wird oft mit ε (epsilon) bezeichnet.
- Die Länge eines Wortes $a_1 \cdots a_k$ ist die Zahl

  $$|a_1 \cdots a_k| := k.$$

  Insbesondere ist $|\varepsilon| = 0$, d.h. das leere Wort hat die Länge 0.
- Sind $v = a_1 \cdots a_k$ und $w = b_1 \cdots b_\ell$ zwei Worte über A, so ist die Konkatenation von v und w das Wort

  $$vw := a_1 \cdots a_k b_1 \cdots b_\ell$$

- Manchmal wird ein Wort $a_1 \cdots a_k$ auch als Folge der Länge k aufgefasst.

Definition 2.17 (A^*, A^+, Sprache)

Sei A ein Alphabet (d.h. eine Menge).

(a) Die Menge aller Worte über A (von beliebiger endlicher Länge) bezeichnen wir mit A^*.

Es gilt also:

$$A^* = \bigcup_{k \in \mathbb{N}} A^k = \{ a_1 \cdots a_k : k \in \mathbb{N},\ a_1, \ldots, a_k \in A \}.$$

Beachte: Wegen $0 \in \mathbb{N}$ und $A^0 = \{()\} = \{\varepsilon\}$ enthält A^* insbesondere das leere Wort.

(b) Die Menge aller nicht-leeren Worte über A (von beliebiger endlicher Länge) bezeichnen wir mit A^+.

Es gilt also:

$$A^+ = A^* \setminus \{\varepsilon\} = \{ a_1 \cdots a_k : k \in \mathbb{N}_{>0},\ a_1, \ldots, a_k \in A \}.$$

(c) Eine Sprache über A ist eine Teilmenge von A^*.

Bemerkung: In vielen Büchern werden Sprachen mit dem Buchstaben L (für Language) oder Varianten wie L' oder L_1 bezeichnet.

Beispiel 2.18 (Natürliche Sprachen)

Alphabet: $A_{deutsch} := \{A, B, \ldots, Z, Ä, Ö, Ü,$
$a, b, \ldots, z, ä, ö, ü, ß,$
$., ,, :, ;, !, ?, „, ", -, \_, \}$

Sprachen über $A_{deutsch}$:

- L_1 := Menge aller grammatikalisch korrekten Sätze der deutschen Sprache (aufgefasst als Zeichenketten über $A_{deutsch}$)
- L_2 := Menge aller Wörter der deutschen Sprache

Beispiel 2.19 (Programmiersprachen)

Alphabet: ASCII := Menge aller ASCII-Symbole

Sprachen:

- L_1 := Menge aller JAVA-Schlüsselwörter
- L_2 := Menge aller erlaubten Variablennamen in JAVA
- L_3 := Menge aller syntaktisch korrekten JAVA-Programme

Relationen

Relationen sind Teilmengen aus kartesischen Produkten.
Präzise:

Definition 2.20

(a) Seien M, N Mengen. Eine Relation von M nach N ist eine Teilmenge von $M \times N$

(b) Sei $k \in \mathbb{N}_{>0}$ und seien $M_1, \dots, M_k$ Mengen.
Eine Relation auf $M_1, \dots, M_k$ ist eine Teilmenge von $M_1 \times \dots \times M_k$. Die Stelligkeit einer solchen Relation ist k.

(c) Sei M eine Menge und sei $k \in \mathbb{N}$.
Eine k-stellige Relation über M ist eine Teilmenge von M^k.

Beispiel 2.21:

Um Datumsangaben im Format (Tag, Monat, Jahr) anzugeben, nutzen wir die Wertebereiche

$$\text{TagWerte} := \{1, 2, \dots, 31\}$$
$$\text{MonatsWerte} := \{1, 2, \dots, 12\}$$
$$\text{JahresWerte} := \mathbb{Z}$$

Die Menge "Gültig" aller gültigen Daten ist dann eine Teilmenge von TagWerte × MonatsWerte × JahresWerte, d.h. eine Relation auf TagWerte, MonatsWerte, JahresWerte, zu der beispielsweise das Tupel (24, 12, 2007) gehört, nicht aber das Tupel (30, 2, 2008).

Notation 2.22:

- Ist R eine Relation von M nach N (für zwei Mengen M, N), so schreiben wir oft

  $$mRn \quad \text{anstatt} \quad (m,n) \in R$$

  Beispiel: • $m \leq n$, für natürliche Zahlen m, n
  • $m \neq n$.

- Ist R eine Relation auf $M_1, \dots, M_k$, so schreiben wir manchmal

  $$R(m_1, \dots, m_k) \quad \text{anstatt} \quad (m_1, \dots, m_k) \in R,$$

  Dies soll verdeutlichen, dass R eine "Eigenschaft" ist, die ein Tupel aus $M_1 \times \dots \times M_k$ haben kann — oder eben nicht haben kann.

Im Datums-Beispiel gilt:

$$\text{Gültig}(24,12,2007),$$

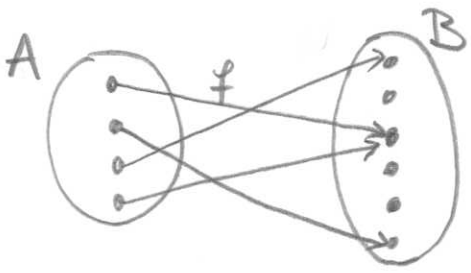
aber es gilt nicht: $\text{Gültig}(30,2,2008)$

Funktionen

Definition 2.23:

Seien A, B Mengen.
Eine Funktion (oder Abbildung) von A nach B ist eine Relation f von A nach B (d.h. $f \subseteq A \times B$) mit der Eigenschaft, dass für jedes $a \in A$ genau ein $b \in B$ mit $(a,b) \in f$ existiert.

anschaulich:



Notation 2.24:

(a) Wir schreiben $f: A \to B$, um auszudrücken, dass f eine Funktion von A nach B ist

(b) Ist $f: A \to B$ und ist $a \in A$, so bezeichnet $f(a)$ das (eindeutige) $b \in B$ mit $(a,b) \in f$.
Insbesondere schreiben wir meistens $f(a) = b$ an Stelle von $(a,b) \in f$.

(c) Für $f: A \to B$ und $A' \subseteq A$ sei

$$f(A') := \{ f(a) : a \in A' \}.$$

(d) Die Menge aller Funktionen von A nach B bezeichnen wir mit $Abb(A, B)$.

Beachte: In manchen Büchern wird $Abb(A,B)$ auch mit $A \to B$ oder mit B^A bezeichnet.

Bemerkung:
Zwei Funktionen $f: A \to B$ und $g: A \to B$ sind gleich (kurz: $f = g$), falls f.a. $a \in A$ gilt:
$f(a) = g(a)$.

Definition 2.25: (Definitionsbereich, Bildbereich, Bild)

Sei $f: A \to B$.
Der Definitionsbereich von f ist die Menge
$Def(f) := A$
Der Bildbereich von f ist die Menge B.
Das Bild von f (genauer: das Bild von A unter f) ist die Menge
$Bild(f) := f(A) \underset{Def}{=} \{ f(a) : a \in A \} \subseteq B$.

Definition 2.26 (Restriktionen)

Sei $f: A \to B$ eine Funktion und sei $A' \subseteq A$

Die Restriktion (oder Einschränkung) von f auf A' ist die Funktion

$$f_{|A'} : A' \to B \quad , \text{ die folgendermaßen}$$

definiert ist: f.a. $a \in A'$ ist $f_{|A'}(a) := f(a)$.

Partielle Funktionen

Definition 2.27

Eine partielle Funktion von einer Menge A in eine Menge B ist eine Funktion f mit $Def(f) \subseteq A$ und $Bild(f) \subseteq B$.

Bemerkung 2.28

(a) Im Gegensatz zu partiellen Funktionen nennt man Funktionen, wie wir sie in Definition 2.23 definiert haben, auch totale Funktionen.

Sprechen wir von "Funktionen", ohne sie explizit als "partiell" zu bezeichnen, so meinen wir in dieser Vorlesung immer "totale" Funktionen.

(b) Jede partielle Funktion von einer Menge A in eine Menge B lässt sich auch als totale Funktion von A nach $B \dot{\cup} \{\perp\}$ auffassen, wobei $\perp$ ein spezielles Zeichen ist, das für "undefiniert" steht (und das nicht zur Menge B gehört).

Eigenschaften von Funktionen

Definition 2.29:

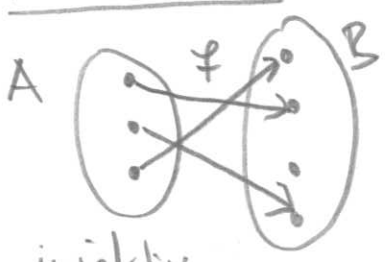
Sei $f: A \to B$.

(a) f heißt injektiv, falls es für jedes $b \in B$ höchstens ein $a \in A$ mit $f(a) = b$ gibt.

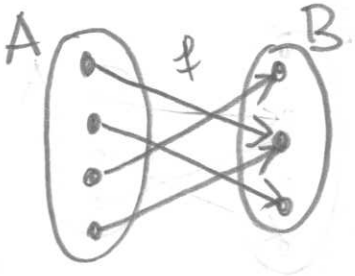
(b) f heißt surjektiv, falls es für jedes $b \in B$ mindestens ein $a \in A$ mit $f(a) = b$ gibt.

(c) f heißt bijektiv, falls es für jedes $b \in B$ genau ein $a \in A$ mit $f(a) = b$ gibt.

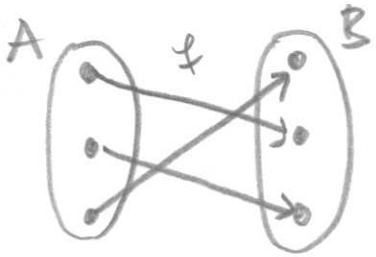
Anschaulich:



injektiv, nicht surjektiv, nicht bijektiv



nicht injektiv surjektiv nicht bijektiv



injektiv, surjektiv, bijektiv

Beobachtung 2.30:

(a) Für jede Funktion $f: A \to B$ gilt:

f ist bijektiv $\iff$ f ist injektiv und surjektiv.

(b) Seien A und B endliche Mengen. Dann gilt:

$|A| = |B|$ $\iff$ es gibt eine bijektive Funktion von A nach B.

Satz 2.31:

(a) Für jede Menge M gibt es eine bijektive Funktion von $\mathcal{P}(M)$ nach $\mathrm{Abb}(M, \{0,1\})$

(b) Sei B eine Menge, sei A eine endliche Menge und sei $k := |A|$.
Dann gibt es eine bijektive Funktion von $\mathrm{Abb}(A,B)$ nach B^k.

Beweis: (a) Repräsentiere jedes $M' \in \mathcal{P}(M)$ (d.h. $M' \subseteq M$) durch die so genannte charakteristische Funktion $\chi_{M'}: M \to \{0,1\}$

mit $\chi_{M'}(m) := \begin{cases} 1 & \text{falls } m \in M' \\ 0 & \text{sonst} \end{cases}$ (*)

Sei nun $f: \mathcal{P}(M) \to \mathrm{Abb}(M, \{0,1\})$ definiert durch

$f(M') := \chi_{M'}$, für jedes $M' \in \mathcal{P}(M)$ (**)

Behauptung: f ist bijektiv.

Wir zeigen dies in 2 Schritten (und nutzen Beobachtung 2.30(a)):

Schritt 1: f ist injektiv:

Seien $M', M'' \in \mathcal{P}(M)$ mit $f(M') = f(M'')$.

Ziel: Zeige, dass $M' = M''$.

Wegen $f(M') = f(M'')$ gilt gemäß (**), dass $\chi_{M'} = \chi_{M''}$.

D.h. f.a. $m \in M$ gilt $\chi_{M'}(m) = \chi_{M''}(m)$

Gemäß (*) gilt daher f.a. $m \in M$, dass

$m \in M' \iff m \in M''$.

Somit ist $M' = M''$.

Schritt 2: f ist surjektiv:

Sei $h \in \mathrm{Abb}(M, \{0,1\})$, d.h. $h: M \to \{0,1\}$.

Ziel: Finde ein $M' \in \mathcal{P}(M)$ mit $f(M') = h$.

Wir wählen

$M' := \{ m \in M : h(m) = 1 \}$. Klar: $M' \in \mathcal{P}(M)$.

Gemäß (*) gilt $\chi_{M'} = h$.

Gemäß (**) ist daher $f(M') = h$.

□ Beweis von (a)

(b) Idee: Sei $a_1, \dots, a_k$ eine Liste aller Elemente in A. Repräsentiere jede Funktion $h \in Abb(A,B)$ durch das k-Tupel $t_h := (h(a_1), \dots, h(a_k))$. Rest: Übung! □

Folgerung 2.32:

Seien A, B, M endliche Mengen. Dann gilt:

(a) $|Abb(A,B)| = |B|^{|A|}$

(b) $|\mathcal{P}(M)| = 2^{|M|}$.

Beweis:

(a) Gemäß Satz 2.31 (b) und Beobachtung 2.30 (b) gilt für $k := |A|$, dass

$$|Abb(A,B)| = |B^k|$$

Laut Satz 2.15 (c) ist $|B^k| = |B|^k$

Somit: $|Abb(A,B)| = |B|^k \overset{\text{Def. } k}{=} |B|^{|A|}$.

(b) Gemäß Satz 2.31 (a) und Beobachtung 2.30 (b) ist

$$|\mathcal{P}(M)| = |Abb(M, \{0,1\})|$$

Gemäß (a) ist $|Abb(M, \{0,1\})| = |\{0,1\}|^{|M|} = 2^{|M|}$.

□

Spezielle Funktionen:

Definition 2.33:
Die **Identitätsfunktion** auf einer Menge M ist die Funktion $id_M : M \to M$ mit

$id_M(m) := m$, f.a. $m \in M$.

Definition 2.34: (Multimenge, engl.: bag)
Eine **Multimenge über einer Menge M** ist eine Funktion $f : M \to \mathbb{N}$.

Mit solchen Funktionen kann man "Mengen" beschreiben, in denen einzelne Elemente mehrfach vorkommen können: Für jedes $m \in M$ gibt $f(m)$ an, wie oft m in der "Multimenge" vorkommt.

Beispiel 2.35: Ein Geldbeutel mit

- 3 1-cent-Münzen
- 0 2-cent-Münzen
- 0 5-cent-Münzen
- 2 10-cent-Münzen
- 4 20-cent-Münzen
- 1 50-cent-Münze
- 3 1-Euro-Münzen
- 2 2-Euro-Münzen

kann repräsentiert werden durch die Multimenge

Geldbeutelinhalt : MünzenArten $\to \mathbb{N}$,

wobei

$$\text{MünzenArten} := \{ 1c, 2c, 5c, 10c, 20c, 50c, 1€, 2€ \}$$

und

$$\begin{aligned}
&\text{GeldsäckelInhalt}(1c) := 3 \\
&\text{GeldsäckelInhalt}(2c) := 0 \\
&\text{GeldsäckelInhalt}(5c) := 0 \\
&\text{GeldsäckelInhalt}(10c) := 2 \\
&\text{GeldsäckelInhalt}(20c) := 4 \\
&\text{GeldsäckelInhalt}(50c) := 1 \\
&\text{GeldsäckelInhalt}(1€) := 3 \\
&\text{GeldsäckelInhalt}(2€) := 2 .
\end{aligned}$$

Bequemere Schreibweise:

$$\begin{aligned}
\text{GeldsäckelInhalt} := \{ &(1c,3), (2c,0), (5c,0), \\
&(10c,2), (20c,4), (50c,1), \\
&(1€,3), (2€,2) \}
\end{aligned}$$

2.2 Ein Beispiel zur Modellierung mit Wertebereichen

Beispiel 2.36: "Arbeitskreise der EU"

In der EU-Kommission sollen drei Arbeitskreise gebildet werden. Dazu entsendet jede der Nationen Deutschland, Frankreich, Österreich und Spanien drei Delegierte. Die Arbeitskreise sollen so gebildet werden, dass in jedem Arbeitskreis jede Nation vertreten ist und dass es unter Berücksichtigung der Fremdsprachenkenntnisse der Delegierten in jedem Arbeitskreis eine gemeinsame Sprache gibt, die alle beherrschen.

Aufgabe: Es soll nur die Situation modelliert werden — ein Lösungsverfahren wird hier erst mal nicht gesucht.

Formale Modellierung:

- Menge der Nationen:

  $$\text{Nationen} := \{D, F, Ö, S\},$$

  wobei D für Deutschland, F für Frankreich, Ö für Österreich und S für Spanien steht

- Die Delegierten können wir repräsentieren als Paare, die aus einer Nation und einem Index aus $\{1,2,3\}$ bestehen, so dass beispielsweise die drei Delegierten aus Deutschland durch die Paare $(D,1)$, $(D,2)$ und $(D,3)$ modelliert werden.

  Also:

  $$\text{Delegierte} := \text{Nationen} \times \text{DelegiertenIndex},$$

  wobei $\text{DelegiertenIndex} := \{1,2,3\}$

- Wir nutzen eine Funktion "spricht", die jedem Delegierten die Menge von Sprachen zuordnet, die er beherrscht. Formal:

  $$\text{spricht} : \text{Delegierte} \longrightarrow \mathcal{P}(\text{Sprachen}),$$

  wobei Sprachen := {deutsch, französisch, spanisch, englisch, italienisch, chinesisch, ...}

- Die drei Arbeitskreise bezeichnen wir mit AK1, AK2, AK3 und setzen

  Arbeitskreise := {AK1, AK2, AK3}

- Eine konkrete Besetzung der drei Arbeitskreise repräsentieren wir durch eine Funktion

  AK-Besetzung: Arbeitskreise → $\mathcal{P}$(Delegierte),

  die jedem der 3 Arbeitskreise die Menge der Delegierten zuordnet, die Mitglied des Arbeitskreises sind.

- Die Bedingung, dass jede Nation in jedem Arbeitskreis vertreten ist, lässt sich folgendermaßen formulieren:

  f.a. $a \in$ Arbeitskreise ist Vertretene_Nationen_in_a = Nationen,

  wobei Vertretene_Nationen_in_a :=
  {$n \in$ Nationen: es ex. ein $i \in$ Delegiertenindex
  s.d. $(n,i) \in$ AK-Besetzung(a)}

- Die Bedingung, dass es für jeden Arbeitskreis eine Sprache gibt, die alle Mitglieder des Arbeitskreises beherrschen, lässt sich folgendermaßen formulieren:

f.a. $a \in$ Arbeitskreise ist Gemeinsame_Sprachen_in_a $\neq \emptyset$,

wobei

Gemeinsame_Sprachen_in_a :=

$$\{ sp \in \text{Sprachen} : \text{f.a. } d \in \text{AK-Besetzung}(a) \text{ ist } sp \in \text{spricht}(d) \}$$

□Ende von Bsp 2.36

2.3 Beweise verstehen und selbst formulieren

Ziel dieses Abschnitts ist, einen kurzen Überblick über grundlegende Beweistechniken zu geben, insbesondere:

- direkter Beweis
- Beweis durch Kontraposition
- Beweis durch Widerspruch (indirekter Beweis)
- vollständige Induktion.

Was sind "Sätze" und "Beweise"?

Ein Satz (bzw. Theorem) besteht aus Voraussetzungen und einer Behauptung. Voraussetzungen und Behauptung sind Aussagen, so dass folgendes gilt: Wenn alle Voraussetzungen erfüllt sind, dann muss auch die Behauptung wahr sein.

Der Beweis eines Satzes muss nachweisen, dass die Behauptung des Satzes wahr ist und kann dabei verwenden:

- die Voraussetzungen des Satzes
- Definitionen und bereits bekannte Tatsachen und Sätze
- im Beweis selbst oder anderswo bereits als wahr bewiesene Aussagen
- logische Schlussregeln.

Typische Fehler, die man beim Versuch, Beweise zu formulieren, vermeiden sollte, sind:

- unzulässiges Argumentieren mit Beispielen
- Verwendung gleicher Symbole zur Bezeichnung verschiedener Dinge
- Hantieren mit nicht exakt oder gar widersprüchlich definierten Begriffsbildungen
- unzulässige Gedankensprünge beim Schlussfolgern
- Ausnützung von bis dahin noch unbewiesenen Behauptungen zur Begründung von einzelnen Beweisschritten.

Beweistechnik "direkter Beweis":

Ansatz: die Behauptung eines Satzes wird "direkt" (d.h. "ohne Umwege") bewiesen.

Beispiele für direkte Beweise haben wir in dieser Vorlesung bereits kennengelernt, z.B.

- der Beweis von Satz 2.6
- der Beweis von Satz 2.15
- der Beweis von Satz 2.31
- der Beweis von Folgerung 2.32

Beweistechnik "Beweis durch Kontraposition"

Beim Beweis durch Kontraposition wird ein Satz der Form "Falls Aussage A gilt, so gilt auch Aussage B" dadurch bewiesen, dass man zeigt: "Falls Aussage B nicht gilt, so kann auch Aussage A nicht gelten".

Als Beispiel für einen Beweis durch Kontraposition betrachten wir folgenden Satz:

Satz 2.37

Für jedes $n \in \mathbb{N}$ gilt: Falls n^2 eine ungerade Zahl ist, so ist auch n eine ungerade Zahl

Beweis: Durch Kontraposition.

Sei $n \in \mathbb{N}$ beliebig.

Wir zeigen: Falls n keine ungerade Zahl ist, so ist auch n^2 keine ungerade Zahl.

$n \in \mathbb{N}$ war beliebig gewählt. Falls n ungerade ist, so ist nichts weiter zu beweisen. Wir betrachten daher nun den Fall, dass n nicht ungerade ist (d.h. n ist gerade). und zeigen, dass dann auch n^2 gerade ist.

Beachte: Per Definition ist eine natürliche Zahl m genau dann gerade, wenn es ein $k \in \mathbb{N}$ gibt s.d. $m = 2 \cdot k$.

Daher gilt:

n ist gerade

$\Rightarrow$ es ex. $k \in \mathbb{N}$ s.d. $n = 2 \cdot k$ (gemäß Def. von "gerade")

$\Rightarrow$ es ex. $k \in \mathbb{N}$ s.d. $n^2 = n \cdot (2 \cdot k)$

$\Rightarrow$ es ex $k \in \mathbb{N}$ s.d. $n^2 = 2 \cdot (n \cdot k)$

$\Rightarrow$ es ex $k' \in \mathbb{N}$ s.d. $n^2 = 2 \cdot k'$

$\Rightarrow$ n^2 ist gerade (gemäß Def. von "gerade")

Somit ist n^2 gerade, d.h. n^2 ist keine ungerade Zahl. □

Beweistechnik "Beweis durch Widerspruch" (indirekter Beweis)

Beim Beweis durch Widerspruch wird ein Satz der Form "Falls die Voraussetzungen A erfüllt sind, so gilt Aussage B" dadurch bewiesen, dass man

- annimmt, dass die Voraussetzungen A erfüllt sind, aber die Aussage B <u>nicht</u> gilt, und
- daraus einen Widerspruch herleitet.

Als Beispiel für einen Beweis durch Widerspruch betrachten wir folgenden Satz:

<u>Satz 2.38</u>
Für alle geraden natürlichen Zahlen a und b gilt: $a \cdot b$ ist gerade.

<u>Beweis</u>: Durch Widerspruch
Angenommen, a und b sind gerade natürliche Zahlen, so dass $a \cdot b$ <u>nicht</u> gerade ist.
Da a und b gerade sind, gibt es $k, \ell \in \mathbb{N}$ s.d.
$a = 2 \cdot k$ und $b = 2 \cdot \ell$.
Dann ist $a \cdot b = (2 \cdot k) \cdot (2 \cdot \ell) = 2 \cdot (2 \cdot k \cdot \ell)$.
Insbes. gibt es also ein $k' \in \mathbb{N}$ s.d. $a \cdot b = 2 \cdot k'$.
Gemäß der Definition von "gerade" ist also $a \cdot b$ gerade.
Dies ist ein Widerspruch zur Annahme, dass $a \cdot b$ <u>nicht</u> gerade ist.

□

Ein weiteres, etwas anspruchsvolleres Beispiel für einen Beweis durch Widerspruch ist der Beweis des folgenden Satzes, der "anschaulich" besagt, dass die Potenzmenge von $\mathbb{N}$ viel größer ist als die Menge $\mathbb{N}$ selbst.

Satz 2.39: ("$\mathcal{P}(\mathbb{N})$ ist nicht abzählbar")

Es gibt keine surjektive Funktion von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$.

Beweis: Durch Widerspruch.

Angenommen, $f: \mathbb{N} \to \mathcal{P}(\mathbb{N})$ ist surjektiv.

Sei $M := \{ n \in \mathbb{N} : n \notin f(n) \}$. (*)

Klar: $M \in \mathcal{P}(\mathbb{N})$.

Da f surjektiv ist, muss es ein $m \in \mathbb{N}$ geben mit $f(m) = M$.

Klar: Entweder gilt $m \in M$ oder es gilt $m \notin M$.

Fall 1: $m \notin M$: Wegen $f(m) = M$ gilt also: $m \notin f(m)$.
Gemäß (*) für $n := m$ gilt also $m \in M$.
↯ (Wid. zu "Fall 1: $m \notin M$").

Fall 2: $m \in M$: Wegen $f(m) = M$ gilt also: $m \in f(m)$.
Gemäß (*) für $n := m$ gilt also $m \notin M$.
↯ (Wid. zu "Fall 2: $m \in M$").

Somit führen beide Fälle zu einem Widerspruch.
Daher kann es keine surjektive Funktion f von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$ geben.

□

Ein weiteres, sehr ähnliches Beispiel für einen Beweis durch Widerspruch haben wir bereits im Zusammenhang mit der Russellschen Antinomie kennengelernt:

Satz 2.40 ("Es gibt keine Menge aller Mengen")

Es gibt keine Menge U, so dass für jede Menge M gilt: $M \in U$.

Beweis: Durch Widerspruch. Angenommen, U ist eine Menge, so dass für jede Menge M gilt: $M \in U$.

Dann ist auch

(*) $N := \{ M \in U : M \text{ ist eine Menge und } M \notin M \}$

eine Menge.

Insbesondere gilt entweder $N \in N$ oder $N \notin N$.

Fall 1: $N \notin N$: Wir wissen: N ist eine Menge, also insbes. $N \in U$. Und da wir in Fall 1 sind, gilt außerdem: $N \notin N$. Gemäß (*) (für $M := N$) muss dann aber gelten: $N \in N$ ↯ (Wid. zu "Fall 1: $N \notin N$")

Fall 2: $N \in N$: Wegen $N \in N$ gilt gemäß (*) für $M := N$, dass $N \in U$ ist, dass N eine Menge ist, und dass $N \notin N$ ist. ↯ (Wid. zu "Fall 2: $N \in N$")

Somit führen beide Fälle zu einem Widerspruch.

Daher kann es keine Menge U geben, so dass für jede Menge M gilt: $M \in U$.

□

Beweistechnik "Beweis durch vollständige Induktion"

Grundidee der vollständigen Induktion:

Für $n \in \mathbb{N}$ sei $A(n)$ eine Aussage über die natürliche Zahl n.

Ziel: Zeige, dass für alle $n \in \mathbb{N}$ die Aussage $A(n)$ wahr ist.

Eine Möglichkeit, dies zu zeigen ist, sich das so genannte Induktionsprinzip zu Nutze zu machen.

Induktionsprinzip:
Man zeigt, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ wahr ist, indem man folgendermaßen vorgeht:

(1) Zuerst zeigt man, dass die Aussage $A(n)$ für die Zahl $n = 0$ gilt.
Diesen Schritt nennt man "Induktionsanfang" bzw. "Induktionsbasis".

(2) Danach zeigt man, dass für jede beliebige natürliche Zahl $n \in \mathbb{N}$ gilt:
Falls die Aussage $A(n)$ wahr ist, so ist auch die Aussage $A(n+1)$ wahr.
Diesen Schritt nennt man "Induktionsschritt".

Beachte: Wenn man die Schritte (1) und (2) bewiesen hat, so weiß man, dass die folgenden Aussagen wahr sind:

$A(0)$, $A(1)$, $A(2)$, $A(3)$, $A(4)$, ...

↑ Induktionsanfang

↑ Induktionsschritt für $n=0$

↑ Induktionsschritt für $n=1$

d.h., man hat gezeigt, dass für alle $n \in \mathbb{N}$ die Aussage $A(n)$ wahr ist.

Beispiel für einen Beweis durch vollständige Induktion:

Satz 2.41:
F.a. $n \in \mathbb{N}$ gilt: $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.

(Bemerkung: Die "Aussage $A(n)$", deren Gültigkeit hier f.a. $n \in \mathbb{N}$ bewiesen werden soll, besagt also: "$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$".

Zur Erinnerung: $\sum_{i=0}^{n} 2^i$ ist eine abkürzende Schreibweise für $2^0 + 2^1 + 2^2 + \cdots + 2^n$.)

Beweis: Per Induktion nach n.

Induktionsanfang: $n=0$:

Behauptung: $\sum_{i=0}^{0} 2^i = 2^{0+1} - 1$.

Beweis: • $\sum_{i=0}^{0} 2^i \underset{\text{Def. }\Sigma}{=} 2^0 = 1$

• $2^{0+1} - 1 = 2^1 - 1 = 2 - 1 = 1$

Also: $\sum_{i=0}^{0} 2^i = 1 = 2^{0+1} - 1$. ✓

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ beliebig.

Induktionsannahme: $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

(d.h. wir gehen davon aus, dass die Aussage $A(n)$ wahr ist)

Behauptung: $\sum_{i=0}^{n+1} 2^i = 2^{(n+1)+1} - 1$

(d.h. wir müssen zeigen, dass dann auch die Aussage $A(n+1)$ wahr ist).

Beweis:

$$\sum_{i=0}^{n+1} 2^i \underset{\text{Def } \Sigma}{=} \left(\sum_{i=0}^{n} 2^i\right) + 2^{n+1}$$

$$\underset{\text{Induktionsannahme}}{=} 2^{n+1} - 1 + 2^{n+1}$$

$$= 2 \cdot 2^{n+1} - 1$$

$$= 2^{n+2} - 1$$

$$= 2^{(n+1)+1} - 1. \quad ✓$$

□

Zwei nützliche Varianten des Induktionsprinzips

Um zu zeigen, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ wahr ist (wobei n_0 eine geeignete natürliche Zahl ist), kann man nach einem der beiden folgenden Schemata vorgehen:

Variante 1:

Induktionsanfang: $n = n_0$:

Behauptung: die Aussage $A(n_0)$ ist wahr

Beweis: ...

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ mit $n \geq n_0$ beliebig.

Induktionsannahme: die Aussage $A(n)$ ist wahr

Behauptung: die Aussage $A(n+1)$ ist wahr

Beweis: ...

Variante 2:

Induktionsanfang: $n = n_0$:

Behauptung: die Aussage $A(n_0)$ ist wahr

Beweis: ...

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ mit $n \geq n_0$ beliebig.

Induktionsannahme: die Aussagen $A(n_0), A(n_0+1), \ldots, A(n)$ sind wahr.

Behauptung: die Aussage $A(n+1)$ ist wahr

Beweis: ...

Beispiel 2.42:

Welche der Funktionen $f: \mathbb{N} \to \mathbb{Z}$ und $g: \mathbb{N} \to \mathbb{Z}$ mit $f(n) := n^2 - 7$ und $g(n) := 4 \cdot n$ (f.a. $n \in \mathbb{N}$) liefert größere Funktionswerte?

n	0	1	2	3	4	5	6	7	8	9
$f(n)$	-7	-6	-3	2	9	18	29	42	57	74
$g(n)$	0	4	8	12	16	20	24	28	32	36

Vermutung: F.a. $n \in \mathbb{N}$ mit $n \geq 6$ gilt: $f(n) > g(n)$.

Beweis: per Induktion nach n.

Induktionsanfang: $n = 6$

Behauptung: $f(6) > g(6)$

Beweis: • $f(6) = 6^2 - 7 = 29$

• $g(6) = 4 \cdot 6 = 24$

Also: $f(6) = 29 > 24 = g(6)$. ✓

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ mit $n \geq 6$ beliebig.

Induktionsannahme: $f(n) > g(n)$, d.h. $n^2 - 7 > 4 \cdot n$

Behauptung: $f(n+1) > g(n+1)$, d.h. $(n+1)^2 - 7 > 4 \cdot (n+1)$

Beweis:
$$\begin{aligned} (n+1)^2 - 7 &= n^2 + 2n + 1 - 7 \\ &= (n^2 - 7) + 2n + 1 \\ &\overset{\text{Ind.ann.}}{>} 4 \cdot n + 2n + 1 \\ &\geq 4 \cdot n + 4 \qquad \geq 4 \cdot (n+1). \end{aligned}$$

$n \geq 6$, also $2n+1 \geq 13 > 4$

□

Auf ähnliche Weise kann man per Induktion auch folgendes beweisen:

Satz 2.43

(a) F.a. $n \in \mathbb{N}$ mit $n \geq 1$ gilt: $\sum_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$

(b) F.a. $n \in \mathbb{N}$ mit $n \geq 1$ gilt: $\sum_{i=1}^{n} (2i-1) = n^2$

(d.h.: Die Summe der ersten n ungeraden Zahlen ergibt gerade die Zahl n^2).

(c) F.a. $n \in \mathbb{N}$ mit $n \geq 1$ gilt: $\sum_{i=1}^{n} i^2 = \frac{n \cdot (n+1) \cdot (2n+1)}{6}$

Beweis: Übung.

Das folgende Beispiel zeigt, dass man beim Führen von Induktionsbeweisen vorsichtig bzw. sehr sorgfältig sein sollte:

Beispiel 2.44

Der folgende Satz ist offensichtlicherweise nicht wahr – aber wo steckt der Fehler im Beweis?

"Satz": F.a. $n \in \mathbb{N}$ mit $n \geq 1$ gilt:
Ist M eine Menge von Menschen mit $|M| = n$, so haben alle Menschen in M die gleiche Größe.

"Beweis": per Induktion nach n.

Induktionsanfang: $n = 1$.

Behauptung: Ist M eine Menge von Menschen mit $|M| = 1$, so haben alle Menschen in M die gleiche Größe.

Beweis: Sei M eine Menge von Menschen mit $|M| = 1$. Dh, M besteht aus genau einem Menschen. Daher haben offensichtlich alle Menschen in M die gleiche Größe.

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ mit $n \geq 1$ beliebig.

Induktionsannahme: Ist M' eine Menge von Menschen mit $|M'| = n$, so haben alle Menschen in M' die gleiche Größe.

Behauptung: Ist M eine Menge von Menschen mit $|M| = n+1$, so haben alle Menschen in M die gleiche Größe.

Beweis: Sei M eine Menge von Menschen mit $|M| = n+1$.

Sei $a_1, a_2, \dots, a_n, a_{n+1}$ eine Liste aller Menschen in M, d.h. $M = \{a_1, a_2, \dots, a_n, a_{n+1}\}$.

Sei $M' := \{a_1, a_2, \dots, a_n\}$

und $M'' := \{a_2, \dots, a_n, a_{n+1}\}$

Offensichtlich sind M' und M'' Mengen von Menschen mit $|M'| = n$ und $|M''| = n$.

Gemäß der Induktionsannahme gilt daher:

(1) Alle Menschen in M' haben die gleiche Größe, und

(2) alle Menschen in M'' haben die gleiche Größe

Sei g' die Größe, die gemäß (1) jeder Mensch in M' hat, und sei g'' die Größe, die gemäß (2) jeder Mensch in M'' hat.

Laut Definition von M' und M'' gilt:

$a_2 \in M'$ und $a_2 \in M''$. Da jeder einzelne Mensch (und daher insbes. der Mensch a_2) nur eine Größe haben kann, gilt: $g' = g''$.

Wegen $M = M' \cup M''$ gilt daher, dass alle Menschen in M die gleiche Größe haben, nämlich die Größe $g := g' = g''$.

□

Frage: Wo steckt der Fehler im Beweis?

Antwort:

Der "Induktionsschritt $n \to n+1$" ist für den Wert $n = 1$ nicht schlüssig, denn in diesem Fall gilt $n+1 = 2$ und

- $M = \{a_1, a_2\}$
- $M' = \{a_1\}$
- $M'' = \{a_2\}$

Insbes gilt also zwar, dass $a_2 \in M''$, aber es gilt nicht, dass $a_2 \in M'$!

□ Ende von Bsp 2.44

2.4 Rekursive Definitionen von Funktionen und Mengen

Das Induktionsprinzip lässt sich auch zur "induktiven" (bzw. "rekursiven") Definition von Funktionen $f: \mathbb{N} \to M$ (wobei M eine beliebige Menge ist) nutzen, indem man folgendermaßen vorgeht:

(1): Definiere $f(0)$ ("Rekursionsanfang")

(2): Definiere, f.a. $n \in \mathbb{N}$, $f(n+1)$ unter Verwendung des Werts $f(n)$ (bzw. unter Verwendung der Werte $f(n), f(n-1), \dots, f(1), f(0)$) ("Rekursionsschritt")

Auch hier ist wieder eine Reihe von Varianten möglich

Beispiel 2.45:

(a) Rekursive Definition der Fakultätsfunktion $fak: \mathbb{N} \to \mathbb{N}$ durch:

- $fak(0) := 1$
- $fak(n+1) := (n+1) \cdot fak(n)$ (f.a. $n \in \mathbb{N}$)

Beachte: $fak(4) = 4 \cdot fak(3) = 4 \cdot 3 \cdot fak(2) = 4 \cdot 3 \cdot 2 \cdot fak(1)$
$= 4 \cdot 3 \cdot 2 \cdot 1 \cdot fak(0) = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1$

Allgemein gilt f.a. $n \in \mathbb{N}_{>0}$:
$fak(n) = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 2 \cdot 1 = \prod_{i=1}^{n} i$

Notation: $n! := fak(n)$.

(b) Rekursive Definition der so genannten Fibonacci-Folge $fib: \mathbb{N} \to \mathbb{N}$ durch

- $fib(0) := 0$
- $fib(1) := 1$
- $fib(n+1) := fib(n) + fib(n-1)$ f.a. $n \in \mathbb{N}_{>0}$.

Somit:

n	0	1	2	3	4	5	6	7	8	9	10
$fib(n)$	0	1	1	2	3	5	8	13	21	34	55

Um Aussagen über rekursiv definierte Funktionen zu beweisen, kann man wieder das Induktionsprinzip nutzen. Beispiel:

Satz 2.46:
Sei $fib: \mathbb{N} \to \mathbb{N}$ die Fibonacci-Folge.
Dann gilt f.a. $n \in \mathbb{N}$: $fib(n) \leq 2^n$.

Beweis: per Induktion nach n.

Induktionsanfang: betrachte $n=0$ und $n=1$.

Behauptung: $fib(0) \leq 2^0$ und $fib(1) \leq 2^1$.

Beweis: $fib(0) \underset{\text{Def.}}{=} 0 \leq 1 = 2^0$ ✓, $fib(1) \underset{\text{Def}}{=} 1 \leq 2 = 2^1$. ✓

Induktionsschritt: $n \to n+1$: Sei $n \in \mathbb{N}$ mit $n \geq 1$ beliebig.

Induktionsannahme: f.a. $i \in \mathbb{N}$ mit $i \leq n$ gilt: $fib(i) \leq 2^i$.

Behauptung: $fib(n+1) \leq 2^{n+1}$

Beweis:
$$fib(n+1) \underset{\text{Def}}{=} fib(n) + fib(n-1) \underset{\text{Ind.ann.}}{\leq} 2^n + 2^{n-1} \leq 2 \cdot 2^n = 2^{n+1}$$ ✓

□

Bemerkung 2.47

Es gibt auch eine "geschlossene Formel", mit der man den n-ten Wert der Fibonacci-Folge, d.h. die Zahl $fib(n)$ direkt ausrechnen kann, ohne dafür sämtliche Werte $fib(0), fib(1), \dots, fib(n-1)$ ausrechnen zu müssen:

F.a. $n \in \mathbb{N}$ gilt:

$$fib(n) = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Beweis: Übung (... per Induktion nach n).
(Details: siehe Buch von Meinel und Mundhenk)

Rekursive Definition von Mengen

Oft ist es nützlich, auch Mengen rekursiv (bzw induktiv) zu definieren.
Eine rekursive Definition einer Menge M besteht aus

(1) Basisregeln der Form "$m \in M$"
(d.h. die Basisregeln listen explizit bestimmte Elemente auf, die zur Menge M gehören)

(2) Rekursiven Regeln der Form:

"Wenn $m_1, \dots, m_k \in M$, dann $m \in M$",

wobei m von $m_1, \dots, m_k$ abhängt.

Die dadurch definierte Menge M ist dann die Menge aller Elemente, deren Zugehörigkeit zu M durch endlich-maliges Anwenden der Regeln gezeigt werden kann.

Beispiel 2.48: "Palindrome"

Betrachte das Alphabet $A := \{a, b\}$.

Die Menge $PAL \subseteq A^*$ sei wie folgt rekursiv definiert:

Basisregeln:
- $\varepsilon \in PAL$, (B1)
- $a \in PAL$, (B2)
- $b \in PAL$ (B3)

Rekursive Regeln:
- Ist $w \in PAL$, so ist auch $awa \in PAL$ (R1)
- Ist $w \in PAL$, so ist auch $bwb \in PAL$. (R2)

Beispiele für Worte, die zur Menge PAL gehören:

$\underbrace{\varepsilon, a, b}_{\text{durch Basisregeln}}$, $\underbrace{aa, bb}_{\text{durch rek. Regeln mit } w := \varepsilon}$, $\underbrace{aaa, bab}_{\text{durch rek. Regeln mit } w := a}$, $\underbrace{aba, bbb}_{\text{durch rek. Regeln mit } w := b}$

Es gilt beispielsweise auch: $aababaa \in PAL$

Beweis: $a \in PAL$ (Basisregel (B1))

Rek. Regel (R2) mit $w := a \Rightarrow bab \in PAL$.

Rek. Regel (R1) mit $w := bab \Rightarrow ababa \in PAL$.

Rek. Regel (R1) mit $w := ababa \Rightarrow aababaa \in PAL$. □

Aber beispielsweise $aab \notin PAL$, denn gemäß Basisregeln und rekursiven Regeln gilt für jedes Wort $w \in PAL$: der erste und der letzte Buchstabe von w sind identisch.

□ Bsp. 2.48

Induktionsprintip für rekursiv definierte Mengen:

Sei M eine rekursiv definierte Menge.
Dass eine Aussage $A(m)$ für alle $m \in M$ wahr ist, kann man folgendermaßen zeigen:

(1) Zuerst betrachtet man nacheinander jede Basisregel der Form "$m \in M$" und zeigt, dass die Aussage $A(m)$ wahr ist ("Induktionsanfang")

(2) Danach betrachtet man nacheinander jede rekursive Regel der Form
"Wenn $m_1, \dots, m_k \in M$, dann $m \in M$"
und zeigt folgendes: Wenn die Aussagen $A(m_1), \dots, A(m_k)$ wahr sind, dann ist auch die Aussage $A(m)$ wahr. ("Induktionsschritt")

Beachte: Wenn man die Schritte (1) und (2) bewiesen hat, so weiß man, dass die Aussage $A(m)$ für alle $m \in M$ wahr ist.

Beispiel 2.49:

Sei $A := \{a, b\}$.

Für jedes Wort $w \in A^*$ sei w^R das Wort, das durch "Rückwärtslesen" von w entsteht, d.h.:

- Ist $w = \varepsilon$, so ist $w^R = \varepsilon$
- Ist $w = w_1 \cdots w_k$ mit $k \in \mathbb{N}_{>0}$ und $w_1, \ldots, w_k \in A$, so ist $w^R := w_k \cdots w_1$.

(Bsp: $aaab^R = baaa$)

Sei PAL die in Beispiel 2.48 rekursiv definierte Teilmenge von A^*.

Behauptung 1: Für jedes Wort $w \in PAL$ gilt: $w = w^R$.

Beweis: Per Induktion über den Aufbau von PAL.

Induktionsanfang: Betrachte diejenigen Worte, die aufgrund von Basisregeln zur Menge PAL gehören:

Behauptung: $\varepsilon = \varepsilon^R$, $a = a^R$ und $b = b^R$

Beweis: Gemäß der Definition von w^R gilt offensichtlich, dass $\varepsilon = \varepsilon^R$, $a = a^R$ und $b = b^R$.

Induktionsschritt: betrachte die rekursiven Regeln:

- (R1):

  Sei $w \in PAL$ und sei $v := awa$.
  Nach (R1) ist damit auch $v \in PAL$.

  Induktionsannahme: $w = w^R$

  Behauptung: $v = v^R$

  Beweis: $v^R \underset{\text{Def } v}{=} (awa)^R \underset{\text{Def}(\cdot)^R}{=} aw^Ra \underset{\substack{\text{Ind.ann:} \\ w = w^R}}{=} awa \underset{\text{Def. } v}{=} v.$ ✓

- (R2):

  Sei $w \in PAL$ und sei $v := bwb$.
  Nach (R2) ist damit auch $v \in PAL$.

  Induktionsannahme: $w = w^R$

  Behauptung: $v = v^R$

  Beweis: $v^R \underset{\text{Def } v}{=} (bwb)^R \underset{\text{Def}(\cdot)^R}{=} bw^Rb = bwb \underset{\text{Def } v}{=} v.$ ✓

□ Beh 1

Behauptung 2: Für jedes $w \in A^*$ mit $w = w^R$ gilt: $w \in PAL$.

Beweisansatz: Zeige folgende Aussage per Induktion nach n:

Für alle $n \in \mathbb{N}$ gilt: Ist $w \in A^*$ mit $w = w^R$ und $|w| \leq n$, so gilt $w \in PAL$.

Im Induktionsanfang werden $n = 0$ und $n = 1$ betrachtet;
im Induktionsschritt $n \to n+1$ werden alle $n \geq 1$ betrachtet.

Details: Übung

Aus Beh 1 und Beh 2 folgt: $PAL = \{w \in A^* : w = w^R\}$.