Kapitel 2

Mathematische Grundbegriffe und Beweistechniken

Folie 18

Symbol	Bedeutung
$:=$	Definition eines Wertes, z.B. $x := 5$, $M := \{1, 2, 3\}$
$:\iff$	Definition einer Eigenschaft oder einer Schreibweise z.B. $m \in M \;:\iff m$ ist Element von M
ex.	Abkürzung für “es gibt”, “es existiert”
f.a.	Abkürzung für “für alle”, “für jedes”
s.d.	Abkürzung für “so, dass”
$\Longrightarrow$	Abkürzung für “impliziert” z.B.: Regen $\Longrightarrow$ nasse Straße
$\iff$	Abkürzung für “genau dann, wenn” z.B.: Übungsschein erhalten $\iff$ mindestens 40% der erreichbaren Übungspunkte erreicht
$\square$	markiert das Ende eines Beweises

Folie 19

Modellierung und Wertebereiche

In der Modellierung von Systemen, Aufgaben, Problemen oder Lösungen kommen *Objekte unterschiedlicher Art und Zusammensetzung* vor. Für Teile des Modells wird angegeben, aus welchem Wertebereich sie stammen, es wird zumeist aber offen gelassen, welchen konkreten Wert sie annehmen.

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

Folie 20

Beispiel 2.1 (Modellierung der Karten eines (Skat-)Kartenspiels)**.**
Die Karten eines Skat-Kartenspiels lassen sich durch folgende Wertebereiche darstellen:

$$\begin{aligned}
\text{KartenArten} &:= \{ \text{Kreuz}, \text{Pik}, \text{Herz}, \text{Karo} \} \\
\text{KartenSymbole} &:= \{ 7, 8, 9, 10, \text{Bube}, \text{Dame}, \text{König}, \text{Ass} \} \\
\text{Karten} &:= \{ (\text{Kreuz}, 7), (\text{Kreuz}, 8), \ldots, (\text{Kreuz}, \text{Ass}), \\
&\qquad (\text{Pik}, 7), (\text{Pik}, 8), \ldots, (\text{Pik}, \text{Ass}), \\
&\qquad (\text{Herz}, 7), (\text{Herz}, 8), \ldots, (\text{Herz}, \text{Ass}), \\
&\qquad (\text{Karo}, 7), (\text{Karo}, 8), \ldots, (\text{Karo}, \text{Ass}) \}.
\end{aligned}$$

$\square$Ende Beispiel 2.1

Folie 21

Wertebereiche sind u.a. wichtig

- zur Modellierung von Strukturen und Zusammenhängen,
- als Grundlage für alle anderen formalen Kalküle und
- als *abstrakte Grundlage für Typen in Programmiersprachen.*

Folie 22

Der grundlegende Kalkül zur Handhabung von Wertebereichen ist die *Mengenlehre*, bei der Mengen und Mengenoperationen betrachtet werden. Zur Modellierung von "zusammengesetzten Wertebereichen" kann man z.B.

- Potenzmengen,
- kartesische Produkte und Tupel,

- Relationen,
- Folgen bzw. Wörter und
- Funktionen

nutzen. Ziel dieses Kapitels ist, diese Begriffe zu präzisieren und darüber hinaus auch einige wichtige mathematische Grundlagen und Beweistechniken zu erklären.

2.1 Mengen

Was ist eine Menge?

Folie 23

Cantors naiver Mengenbegriff

Cantors naiver Mengenbegriff besagt Folgendes: *(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.

Wir schreiben

$$m \in M$$

um auszusagen, dass M eine Menge ist und dass m ein Element in der Menge M ist.
Wir schreiben

$$m \notin M$$

um auszusagen, dass m kein Element in der Menge M ist.

Künftig werden wir solche Notationen festlegen, indem wir kurz Folgendes schreiben:

Notation.
$m \in M \quad :\Longleftrightarrow \quad m$ ist Element der Menge M.
$m \notin M \quad :\Longleftrightarrow \quad m$ ist kein Element der Menge M.

Folie 24

Die Russellsche Antinomie

Cantors Mengenbegriff ist problematisch und führt zu Widersprüchen. Russell gab folgende Beispiel:

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

Sei X die Menge aller Mengen M, die sich nicht selbst als Element enthalten (d.h.: $M \in X \;:\Longleftrightarrow\; M$ ist eine Menge, für die gilt: $M \notin M$).

Frage: Enthält X sich selbst — d.h. gilt $X \in X$?

Klar ist: Entweder es gilt $X \in X$ oder es gilt $X \notin X$.

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

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

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

Fazit: *Irgendetwas stimmt nicht mit Cantors naivem Mengenbegriff!*

Folie 25

Der Barbier von Sonnenthal

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?

Folie 26

Um die Russellsche Antinomie zu vermeiden, muss man die Mengenlehre sehr sorgfältig axiomatisch aufbauen (siehe z.B. [Ebb03]) — dies sprengt allerdings den Rahmen dieser Vorlesung.

Sofern man sich der Problematik bewusst ist, kann man sie im „täglichen Gebrauch“, den Informatiker*innen von Mengen machen, vermeiden.
Wir arbeiten daher weiter mit einem naiven Mengenbegriff, den wir nach den im Folgenden beschriebenen Grundsätzen verwenden werden.

Folie 27

Beschreibung bzw. Definition von Mengen

Wir beschreiben bzw. definieren Mengen

- *extensional*, durch Aufzählen der Elemente, z.B.

  $$M_1 \ := \ \{0,1,2,3,4,5\} \qquad\qquad \text{oder}$$

- *intensional*, durch Angabe von charakteristischen Eigenschaften der Elemente der Menge, z.B.

  $$\begin{aligned} M_2 \ &:= \ \{x : x \in M_1 \text{ und } x \text{ ist gerade}\} \\ &= \ \{x \in M_1 : x \text{ ist gerade}\} \\ &= \ \{x : x \text{ ist eine natürliche Zahl und } x \text{ ist gerade und } 0 \leqslant x \leqslant 5\}. \end{aligned}$$

Extensional lässt sich die Menge M_2 folgendermaßen beschreiben:

$$M_2 \ = \ \{0,2,4\}.$$

Oft schreibt man statt “:” auch “|” und statt “und” einfach ein “Komma”, also

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

Folie 28

Vorsicht.

- $\{x : 0 \leqslant x \leqslant 5\}$ definiert nicht eindeutig eine Menge, weil nicht festgelegt ist, ob x beispielsweise eine ganze Zahl oder eine reelle Zahl ist.

- $\{M : M \text{ ist eine Menge}, M \notin M\}$ führt zur Russellschen Antinomie.

Fazit: *Um solche Probleme zu vermeiden, müssen wir 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.

Folie 29

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.
$$\begin{aligned}\{1,2,3\} &= \{1,2,2,3\} = \{2,1,3\} \\ &= \{i : i \text{ ist eine ganze Zahl, } 0 < i \leqslant 3\}.\end{aligned}$$
- Mengen können aus „atomaren“ oder aus „zusammengesetzten“ Elementen gebildet werden. Eine Menge kann auch „verschiedenartige“ Elemente enthalten. *Beispiel:* Die Menge
$$M \;:=\; \{\ 1,\ (\text{Pik}, 8),\ \{\text{rot}, \text{blau}\},\ 5,\ 1\ \}$$
besteht aus 4 Elementen: dem atomaren Wert 1, dem Tupel $(\text{Pik}, 8)$, der Menge $\{\text{rot}, \text{blau}\}$ und dem atomaren Wert 5.

Folie 30

Einige konkrete Zahlenmengen

$$\begin{aligned}
\mathbb{N} &:= \text{die Menge der natürlichen Zahlen} := \{0,1,2,3,...\} \\
\mathbb{N}_{\geqslant 1} &:= \text{die Menge der positiven natürlichen Zahlen} := \{1,2,3,...\} \\
\mathbb{Z} &:= \text{die Menge der ganzen Zahlen} := \{0,1,-1,2,-2,3,-3,...\} \\
\mathbb{Q} &:= \text{die Menge der rationalen Zahlen} := \{\tfrac{a}{b} : a,b \in \mathbb{Z},\ b \neq 0\} \\
\mathbb{R} &:= \text{die Menge der reellen Zahlen}
\end{aligned}$$

Folie 31

Die leere Menge und die „Menge aller Mengen“

Beobachtung. Es gibt genau eine Menge, die kein(e) Element(e) enthält.

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

Frage 2.3. Gibt es eine "Menge aller Mengen"?

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

Mengenalgebra

Folie 32

In diesem Abschnitt werden einige grundlegende Operationen auf Mengen betrachtet. Nebenbei werden auch einige (sehr einfache) Beispiele von mathematischen Beweisen gegeben.

Folie 33

Definition 2.4 (Gleichheit von Mengen)**.**
Zwei Mengen X und Y sind gleich (kurz: $X = Y$), falls sie dieselben Elemente enthalten, d.h. falls gilt:

- f.a. $z \in X$ gilt $z \in Y$, und
- f.a. $z \in Y$ gilt $z \in X$.

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

Folie 34

Definition 2.5 (Teilmengen)**.** Seien X, Y Mengen.

(a) X ist eine *Teilmenge* von Y (kurz: $X \subseteq Y$), wenn jedes Element von X auch ein Element von Y ist.

(b) X ist eine *echte Teilmenge* von Y (kurz: $X \subsetneqq Y$), wenn $X \subseteq Y$ und $X \neq Y$.

(c) X ist eine *Obermenge* von Y (kurz: $X \supseteq Y$), wenn $Y \subseteq X$.

(d) X ist eine *echte Obermenge* von Y (kurz: $X \supsetneqq Y$), wenn $X \supseteq Y$ und $X \neq Y$.

Satz 2.6. *Seien X, Y, Z Mengen. Dann gilt:*

(a) $X = Y \iff X \subseteq Y$ *und* $X \supseteq Y$.

(b) $X \subseteq Y$ *und* $Y \subseteq Z \implies X \subseteq Z$.

Beweis:

(a) Es gilt:

$$\begin{aligned} X = Y \quad &\overset{\text{Def. 2.4}}{\iff} \quad \text{f.a. } z \in X \text{ gilt } z \in Y \text{ und} \\ &\qquad\quad \text{f.a. } z \in Y \text{ gilt } z \in X \\ &\iff \quad \text{jedes Element von } X \text{ ist auch ein Element von } Y \text{ und} \\ &\qquad\quad \text{jedes Element von } Y \text{ ist auch ein Element von } X \\ &\overset{\text{Def. 2.5(a)}}{\iff} \quad X \subseteq Y \text{ und } Y \subseteq X \\ &\overset{\text{Def. 2.5(c)}}{\iff} \quad X \subseteq Y \text{ und } X \supseteq Y. \end{aligned}$$

(b) Es gelte $X \subseteq Y$ und $Y \subseteq Z$.

Behauptung: $X \subseteq Z$, d.h. f.a. $x \in X$ gilt $x \in Z$.

Beweis: Sei $x \in X$ beliebig. Wir zeigen, dass $x \in Z$:

$$x \in X \quad \overset{\text{nach Vor.: } X \subseteq Y}{\implies} \quad x \in Y \quad \overset{\text{nach Vor.: } Y \subseteq Z}{\implies} \quad x \in Z.$$

$\square$

Folie 35

Definition 2.7. Seien X und Y Mengen.

(a) Der *Durchschnitt* von X und Y ist die Menge

$$X \cap Y \; := \; \{z : z \in X \text{ und } z \in Y\}.$$

(b) Die *Vereinigung* von X und Y ist die Menge

$$X \cup Y \; := \; \{z : z \in X \text{ oder } z \in Y\}.$$

(c) Die *Differenz* von X und Y ist die Menge

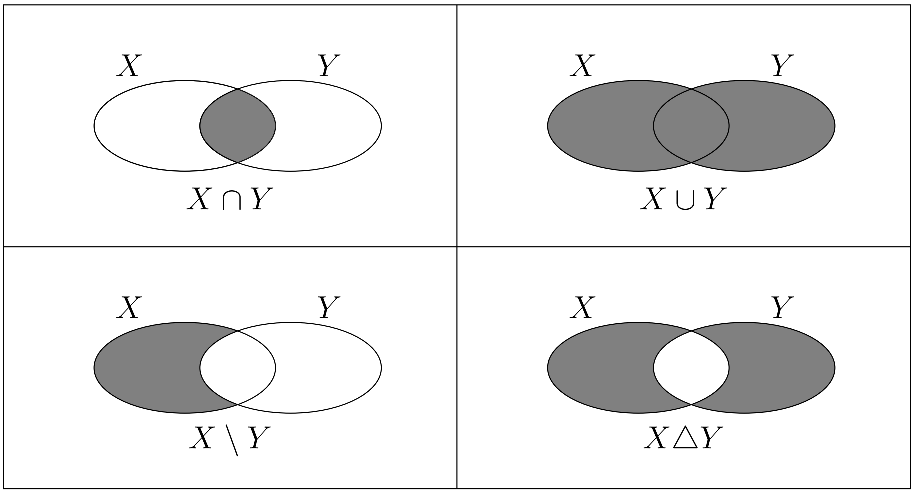
$$X \setminus Y \; := \; X - Y := \{z : z \in X \text{ und } z \notin Y\}.$$

(d) Die *symmetrische Differenz* von X und Y ist die Menge

$$X \triangle Y \; := \; (X \setminus Y) \cup (Y \setminus X).$$

Folie 36

Veranschaulichung durch Venn-Diagramme



Folie 37

Notation 2.8 (disjunkt)**.**
Zwei Mengen X und Y heißen *disjunkt*, falls $X \cap Y = \emptyset$, d.h. falls sie keine gemeinsamen Elemente besitzen.Manchmal schreiben wir

$$X \dot{\cup} Y,$$

um die Menge $X \cup Y$ zu bezeichnen und gleichzeitig auszudrücken, dass $X \cap Y = \emptyset$.

Folie 38

Rechenregeln für Durchschnitt und Vereinigung

Satz 2.9. *Seien X, Y, Z Mengen. Dann gelten:*

(a) Idempotenz:

$$X \cap X \ = \ X \qquad \textit{und} \qquad X \cup X \ = \ X.$$

(b) Kommutativität:

$$X \cap Y \ = \ Y \cap X \qquad \textit{und} \qquad X \cup Y \ = \ Y \cup X.$$

(c) Assoziativität:

$$X \cap (Y \cap Z) \;=\; (X \cap Y) \cap Z \qquad \textit{und} \qquad X \cup (Y \cup Z) \;=\; (X \cup Y) \cup Z.$$

(d) Absorption:

$$X \cap (X \cup Y) \;=\; X \qquad \textit{und} \qquad X \cup (X \cap Y) \;=\; X.$$

(e) Distributivität:

$$X \cap (Y \cup Z) \;=\; (X \cap Y) \cup (X \cap Z) \qquad \textit{und} \qquad X \cup (Y \cap Z) \;=\; (X \cup Y) \cap (X \cup Z).$$

Beweis:

(a)

$$\begin{array}{rcl} X \cap X & \overset{\text{Def. 2.7(a)}}{=} & \{x : x \in X \text{ und } x \in X\} \\ & = & \{x : x \in X\} \\ & = & X. \end{array}$$

Analog: $X \cup X = X$.

(b)

$$\begin{array}{rcl} X \cap Y & \overset{\text{Def. 2.7(a)}}{=} & \{z : z \in X \text{ und } z \in Y\} \\ & = & \{z : z \in Y \text{ und } z \in X\} \\ & \overset{\text{Def. 2.7(a)}}{=} & Y \cap X. \end{array}$$

Analog: $X \cup Y = Y \cup X$.

(c)

$$\begin{array}{rcl} X \cap (Y \cap Z) & \overset{\text{Def. 2.7(a)}}{=} & \{x : x \in X \text{ und } x \in Y \cap Z\} \\ & \overset{\text{Def. 2.7(a)}}{=} & \{x : x \in X \text{ und } (x \in Y \text{ und } x \in Z)\} \\ & = & \{x : (x \in X \text{ und } x \in Y) \text{ und } x \in Z\} \\ & \overset{\text{Def. 2.7(a)}}{=} & \{x : x \in X \cap Y \text{ und } x \in Z\} \\ & \overset{\text{Def. 2.7(a)}}{=} & (X \cap Y) \cap Z. \end{array}$$

Analog: $X \cup (Y \cup Z) = (X \cup Y) \cup Z$.

(d) Wir beweisen, dass $X \cap (X \cup Y) = X$ in zwei Schritten:

Schritt 1: Zeige, dass $X \cap (X \cup Y) \supseteq X$.

Schritt 2: Zeige, dass $X \cap (X \cup Y) \subseteq X$.

Aus Satz 2.6(a) folgt dann, dass $X \cap (X \cup Y) = X$.

Zu Schritt 1:

Behauptung: $X \cap (X \cup Y) \supseteq X$, d.h. f.a. $x \in X$ gilt $x \in X \cap (X \cup Y)$.

Beweis: Sei $x \in X$ beliebig. Zu zeigen: $x \in X \cap (X \cup Y)$. Wegen $x \in X$ gilt auch $x \in X \cup Y$ (gemäß Definition 2.7(b)). Wegen $x \in X$ und $x \in X \cup Y$ gilt gemäß Definition 2.7(a), dass $x \in X \cap (X \cup Y)$.

Zu Schritt 2:

Behauptung: $X \cap (X \cup Y) \subseteq X$, d.h. f.a. $z \in X \cap (X \cup Y)$ gilt $z \in X$.

Beweis: Sei $z \in X \cap (X \cup Y)$ beliebig. Zu zeigen: $z \in X$. Wegen $z \in X \cap (X \cup Y)$ gilt gemäß Definition 2.7(a), dass $z \in X$ und $z \in X \cup Y$. Insbesondere ist also $z \in X$.

Insgesamt haben wir damit gezeigt, dass $X \cap (X \cup Y) = X$.

Analog: $X \cup (X \cap Y) = X$.

(e) Analog; Details: Übung.

□

Das Komplement einer Menge

Folie 39

Das *Komplement* einer Menge M (kurz: $\overline{M}$) soll die Menge aller Elemente sein, die *nicht* zu 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

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

die "Menge aller Mengen" — und dass es die nicht geben kann, haben wir bereits bei der Beantwortung von Frage 2.3 gesehen.

Daher betrachten wir Mengen stets innerhalb eines festen Universums U, das selbst eine Menge ist (die wir jeweils im Kontext angeben müssen). Für $M \subseteq U$ setzen wir dann $\overline{M} := U \setminus M$ und bezeichnen $\overline{M}$ als das Komplement von M in U.

Folie 40

Rechenregeln für Komplemente

Satz 2.10.
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:

$$\overline{M \cap N} \;=\; \overline{M} \cup \overline{N} \qquad \textit{und} \qquad \overline{M \cup N} \;=\; \overline{M} \cap \overline{N}.$$

(c) Inversionsregeln:

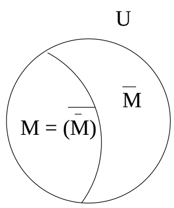
$$M \cap \overline{M} \;=\; \emptyset \qquad \textit{und} \qquad M \cup \overline{M} \;=\; U.$$

(d) Identitätsregeln:

$$M \cap U \;=\; M \qquad \textit{und} \qquad M \cup \emptyset \;=\; M.$$

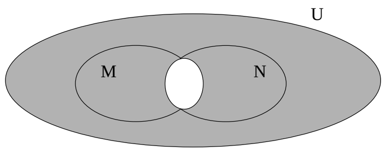
Beweis. Übungsaufgabe. □

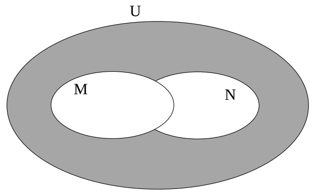
Veranschaulichung durch Venn-Diagramme:

- Doppelte Negation: 

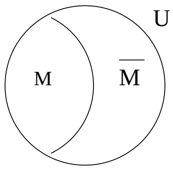
- De Morgansche Regeln:

$$\overline{M \cap N} = \overline{M} \cup \overline{N} \qquad\qquad \overline{M \cup N} = \overline{M} \cap \overline{N}$$





- Inversionsregel:



Mächtigkeit bzw. Kardinalität einer Menge

Folie 41

Definition 2.11.

(a) Eine Menge heißt *endlich*, wenn sie nur endlich viele Elemente enthält, d.h. wenn es eine Zahl $n \in \mathbb{N}$ gibt, so dass die Menge genau n verschiedene Elemente enthält.

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

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

Man beachte, dass “∞” keine natürliche Zahl ist (d.h. $\infty \notin \mathbb{N}$), sondern lediglich eine Abkürzung für das Wort “unendlich”.

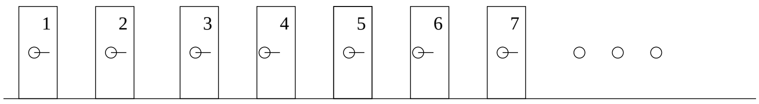
Beispiel 2.12.

$$\begin{array}{rcl@{\qquad}rcl@{\qquad}rcl} |\{2,4,6\}| &=& 3\,, & |\mathbb{N}| &=& \infty\,, & |\emptyset| &=& 0\,, \\ |\{2,4,6,4\}| &=& 3\,, & |\mathbb{Z}| &=& \infty\,, & |\{\emptyset\}| &=& 1\,. \\ |\{2,\{a,b\}\}| &=& 2\,, & & & & & & \end{array}$$

Folie 42

Vorsicht beim Vergleich der Mächtigkeit unendlicher Mengen

Hilberts Hotel (David Hilbert, 1862–1943)
Hilberts Hotel hat unendlich viele Zimmer, die fortlaufend mit $1, 2, 3, \ldots$ (also mit allen Zahlen aus $\mathbb{N}_{\geqslant 1}$) 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.

Es ist nicht schwer, zu sehen, dass im vollbesetzten Hotel sogar unendlich viele neue Gäste, die mit den Zahlen 1, 2, 3, ... durchnummeriert sind, einquartiert werden können. Dazu muss einfach jeder der bisherigen Gäste in das Zimmer umziehen, dessen Nummer das Doppelte der bisherigen Zimmernummer ist. Danach sind alle "alten" Gäste in den Zimmern mit geraden Zimmernummern untergebracht, und die neuen Gäste können in die Zimmer mit ungeraden Zimmernummern einziehen.

Die Potenzmenge

Folie 43

Definition 2.13.
Die *Potenzmenge* (engl.: power set) einer Menge M (kurz: $\mathcal{P}(M)$) ist die Menge aller Teilmengen von M. D.h.:

$$\mathcal{P}(M) \quad = \quad \{X : X \subseteq M\}.$$

Beispiel 2.14.

- $\mathcal{P}(\{a, b\}) = \{\ \emptyset, \{a\}, \{b\}, \{a, b\}\ \}$.
- $\mathcal{P}(\{1, 2, 3\}) = \{\ \emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\ \}$.
- $\mathcal{P}(\emptyset) = \{\ \emptyset\ \}$.
  Insbesondere gilt: $\mathcal{P}(\emptyset) \neq \emptyset$.

Notation 2.15.
In manchen Büchern wird $\mathcal{P}(M)$ auch mit *Pow(M)* (für "power set") oder mit 2^M bezeichnet.
Später, in Folgerung 2.39, werden wir nachweisen, dass für jede endliche Menge M gilt:

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

2.2 Kartesische Produkte und Relationen

Paare, Tupel und kartesische Produkte

Folie 44

Definition 2.16 (Paare und Tupel)**.**

(a) Für beliebige Objekte a und b bezeichnet (a, b) das geordnete *Paar* mit Komponenten a und b.

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

(c) Die *Gleichheit* zweier Tupel ist wie folgt definiert:
F.a. $k, \ell \in \mathbb{N}$ und $a_1, \ldots, a_k, b_1, \ldots, b_\ell$ gilt:

$$\begin{aligned} & (a_1, \ldots, a_k) = (b_1, \ldots, b_\ell) \\ :\Longleftrightarrow\quad & k = \ell \text{ und } a_1 = b_1 \text{ und } a_2 = b_2 \text{ und } \cdots \text{ und } a_k = b_k. \end{aligned}$$

Bemerkung 2.17.

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

(b) Man 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 $\{1, 1, 2\} = \{1, 2\}$.

Folie 45

Definition 2.18.

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

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

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

(b) Das *kartesische Produkt* (bzw. *Kreuzprodukt*) zweier Mengen X, Y ist die Menge

$$X \times Y \;:=\; \{(x, y) : x \in X,\; y \in Y\}.$$

(c) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \dots, M_k$ Mengen. Das kartesische Produkt von $M_1, \dots, M_k$ ist die Menge

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

Folie 46

Beispiel 2.19. Sei $X = \{a, b\}$ und $Y = \{1, 2, 3\}$. Dann gilt:

- $X \times Y = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.
- $X \times \{1\} = \{(a, 1), (b, 1)\}$.
- $X \times \emptyset = \emptyset$.
- $X^2 = \{(a, a), (a, b), (b, a), (b, b)\}$.
- $X^1 = \{(a), (b)\}$.
- $X^0 = \{()\}$.
- $\emptyset^2 = \emptyset$.
- $\emptyset^1 = \emptyset$.
- $\emptyset^0 = \{()\}$.

Folie 47

- In Beispiel 2.1 hatten wir die *Karten eines Skat-Kartenspiels* durch folgende Wertebereiche modelliert:

$$\begin{aligned}
\text{KartenArten} &= \{\text{Kreuz}, \text{Pik}, \text{Herz}, \text{Karo}\},\\
\text{KartenSymbole} &= \{7, 8, 9, 10, \text{Bube}, \text{Dame}, \text{König}, \text{Ass}\},\\
\text{Karten} &= \text{KartenArten} \times \text{KartenSymbole}.
\end{aligned}$$

- *Uhrzeiten* kann man repräsentieren durch Elemente der Menge

  $$\text{Uhrzeiten} \ := \ \text{Stunden} \times \text{Minuten} \times \text{Sekunden},$$

  wobei

  $$\begin{aligned} \text{Stunden} &:= \{0, 1, 2, ..., 23\}, \\ \text{Minuten} &:= \{0, 1, 2, ..., 59\}, \\ \text{Sekunden} &:= \{0, 1, 2, ..., 59\}. \end{aligned}$$

  Das Tupel $(9, 45, 0)$ repräsentiert dann die Uhrzeit “9 Uhr, 45 Minuten und 0 Sekunden”.

Folie 48

Notation 2.20.

- Ist $k \in \mathbb{N}_{\geqslant 1}$ und sind $z_1, \ldots, z_k$ Zahlen, so schreiben wir

  $$\sum_{i=1}^{k} z_i \qquad \text{bzw.} \qquad \sum_{i \in \{1,\ldots,k\}} z_i$$

  um die Summe der Zahlen $z_1, \ldots, z_k$ zu bezeichnen (d.h. die Zahl $z_1 + \cdots + z_k$).

  Wir schreiben

  $$\prod_{i=1}^{k} z_i \qquad \text{bzw.} \qquad \prod_{i \in \{1,\ldots,k\}} z_i$$

  um das Produkt der Zahlen $z_1, \ldots, z_k$ zu bezeichnen (d.h. die Zahl $z_1 \cdot \cdots \cdot z_k$).

Folie 49

- Sind $M_1, \ldots, M_k$ Mengen, so schreiben wir

  $$\bigcup_{i=1}^{k} M_i \qquad \text{bzw.} \qquad \bigcup_{i \in \{1,\ldots,k\}} M_i$$

  um die Vereinigung der Mengen $M_1, \ldots, M_k$ zu bezeichnen (d.h. die Menge $M_1 \cup \cdots \cup M_k$).

  Wir schreiben

  $$\bigcap_{i=1}^{k} M_i \qquad \text{bzw.} \qquad \bigcap_{i \in \{1,\ldots,k\}} M_i$$

  um den Durchschnitt der Mengen $M_1, \ldots, M_k$ zu bezeichnen (d.h. die Menge $M_1 \cap \cdots \cap M_k$).

Folie 50

- Ist K eine Menge, deren Elemente Teilmengen einer Menge U sind (d.h.: $K \subseteq \mathcal{P}(U)$), so ist

$$\bigcup_{M \in K} M \quad := \quad \{x \in U \ : \ \text{ex. } M \in K \text{ s.d. } x \in M\}$$

die Vereinigung aller Mengen $M \in K$ (d.h. die Menge aller Elemente x, die in mindestens einer Menge $M \in K$ liegen).

Analog ist

$$\bigcap_{M \in K} M \quad := \quad \{x \in U \ : \ \text{f.a. } M \in K \text{ gilt } x \in M\}$$

der Durchschnitt aller Mengen $M \in K$ (d.h. die Menge aller Elemente x, die in jeder Menge $M \in K$ liegen).

Folie 51

Die Mächtigkeit von kartesischen Produkten

Satz 2.21.

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

$$|A \times B| \ = \ |A| \cdot |B|.$$

(b) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_k$ endliche Mengen. Dann gilt:

$$|M_1 \times \cdots \times M_k| \ = \ \prod_{i=1}^{k} |M_i|.$$

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

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

Beweis:

(a) Es gilt:

$$A \times B \ = \ \{(a,b) : a \in A,\ b \in B\} \ = \ \bigcup_{a \in A} \{(a,b) : b \in B\} \ = \ \bigcup_{a \in A} \big(\{a\} \times B\big).$$

Außerdem gilt für alle $a, a' \in A$ mit $a \neq a'$, dass die Mengen $\{a\} \times B$ und $\{a'\} \times B$ disjunkt sind. Ferner gilt für beliebige disjunkte endliche Mengen X und Y, dass $|X \cup Y| = |X| + |Y|$ ist. Insgesamt folgt daraus, dass

$$\begin{aligned} |A \times B| \ &= \ \big|\bigcup_{a \in A} \big(\{a\} \times B\big)\big| \ = \ \sum_{a \in A} |\{a\} \times B| \\ &= \ \sum_{a \in A} |B| \ = \ \underbrace{|B| + \cdots + |B|}_{|A|\text{-mal}} \ = \ |A| \cdot |B|. \end{aligned}$$

(b) Analog; Details: Übung.

(c) $|M^k| \ = \ \underbrace{|M \times \cdots \times M|}_{k\text{-mal}} \ \stackrel{(b)}{=} \ \prod_{i=1}^{k} |M| \ = \ \underbrace{|M| \cdot \ \cdots \ \cdot |M|}_{k\text{-mal}} \ = \ |M|^k.$

□

Folie 52

Bemerkung. Satz 2.21(c) besagt, dass

$$|M^k| \ = \ |M|^k \tag{2.1}$$

für jedes $k \in \mathbb{N}$ und jede endliche Menge M gilt.

Speziell für $M := \emptyset$ gilt:
$|M| = |\emptyset| = 0$. Aus Beispiel 2.19 wissen wir, dass $M^0 = \emptyset^0 = \{()\}$, also $|M^0| = |\emptyset^0| = 1$; und für alle $k \in \mathbb{N}$ mit $k \geqslant 1$ ist $M^k = \emptyset^k = \emptyset$, also $|\emptyset^k| = 0$.
Gemeinsam mit (2.1) rechtfertigt dies die Konvention, dass

$$0^0 \ = \ 1 \qquad \text{und} \qquad 0^k \ = \ 0 \quad \text{f.a. } k \in \mathbb{N} \text{ mit } k \geqslant 1.$$

Worte bzw. endliche Folgen

Folie 53

Bemerkung 2.22. Sei A eine Menge.

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

  Beispiel: Das Tupel $(\mathrm{S}, \mathrm{t}, \mathrm{r}, \mathrm{u}, \mathrm{k}, \mathrm{t}, \mathrm{u}, \mathrm{r})$ identifizieren wir mit dem Wort Struktur.

- 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 als ε (epsilon, für "empty word") 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.

Folie 54

Definition 2.23 (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:

$$A^+ \;=\; A^* \setminus \{\varepsilon\} \;=\; \{\, a_1 \cdots a_k \;:\; k \in \mathbb{N}_{\geqslant 1},\, a_1, \ldots, a_k \in A \,\}.$$

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

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

Folie 55

Beispiel 2.24 (Natürliche Sprachen)**.**
Wir betrachten das Alphabet

$$\begin{aligned} A_{deutsch} \;:=\; \{\; & \mathrm{A}\,,\ \mathrm{B}\,,\ \ldots,\ \mathrm{Z}\,,\ \mathrm{\ddot{A}}\,,\ \mathrm{\ddot{O}}\,,\ \mathrm{\ddot{U}}\,, \\ & \mathrm{a}\,,\ \mathrm{b}\,,\ \ldots,\ \mathrm{z}\,,\ \mathrm{\ddot{a}}\,,\ \mathrm{\ddot{o}}\,,\ \mathrm{\ddot{u}}\,,\ \text{ß}\,, \\ & .\,,\ ,\,,\ :\,,\ ;\,,\ !\,,\ ?\,,\ \text{-}\,,\ \_\ \}. \end{aligned}$$

Beispiele für Sprachen über $A_{deutsch}$ sind:

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

Folie 56

Beispiel 2.25 (Programmiersprachen)**.**
Wir betrachten das Alphabet

$$\text{ASCII} \;:=\; \text{die Menge aller ASCII-Symbole}$$

Beispiele für Sprachen über Alphabet ASCII sind:

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

Relationen

Folie 57

Relationen sind Teilmengen von kartesischen Produkten. Präzise:

Definition 2.26.

(a) Seien A, B Mengen. Eine *Relation* von A nach B ist eine Teilmenge von $A \times B$.

(b) Sei $k \in \mathbb{N}_{\geqslant 1}$ und seien $M_1, \ldots, M_k$ Mengen. Eine *Relation auf* $M_1, \ldots, M_k$ ist eine Teilmenge von $M_1 \times \cdots \times M_k$. 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.

Folie 58

Beispiel 2.27. Um Datumsangaben im Format (Tag, Monat, Jahr) anzugeben, nutzen wir die Wertebereiche

$$\begin{aligned} \text{TagWerte} &:= \{1, 2, \ldots, 31\} \\ \text{MonatsWerte} &:= \{1, 2, \ldots, 12\} \\ \text{JahresWerte} &:= \mathbb{Z}. \end{aligned}$$

Die Menge "Gültig" aller *gültigen* Daten ist dann eine *Teilmenge* von

$$\text{TagWerte} \times \text{MonatsWerte} \times \text{JahresWerte},$$

d.h. eine *Relation* auf TagWerte, MonatsWerte, JahresWerte, zu der beispielsweise das Tupel $(23, 6, 1912)$ gehört,[1] nicht aber das Tupel $(30, 2, 1912)$.

Folie 59

Notation 2.28.

- Ist R eine Relation von A nach B (für zwei Mengen A, B), so schreiben wir oft
$$a\,R\,b \quad \text{statt} \quad (a, b) \in R.$$
Beispiel:

[1] Der 23. Juni 1912 ist der Geburtstag von *Alan M. Turing*, einem der einflussreichsten Pioniere der Informatik.

  – $a \leqslant b$, für natürliche Zahlen a und b
  – $a \neq b$, für ganze Zahlen a und b

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

$$R(m_1, \ldots, m_k) \qquad \text{statt} \qquad (m_1, \ldots, m_k) \in R.$$

  Das soll verdeutlichen, dass R eine "Eigenschaft" ist, die ein Tupel aus $M_1 \times \cdots \times M_k$ haben kann — oder eben nicht haben kann. Im Datums-Beispiel gilt: $\text{Gültig}(23, 6, 1912)$, aber es gilt *nicht*: $\text{Gültig}(30, 2, 1912)$.

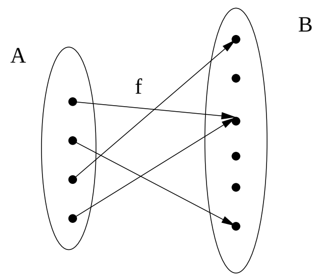
2.3 Funktionen

Totale Funktionen und partielle Funktionen

Folie 60

Definition 2.29. 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:



Folie 61

Notation 2.30.

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

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

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

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

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

(e) In manchen Büchern wird $\mathrm{Abb}(A, B)$ auch mit B^A bezeichnet. Später, in Folgerung 2.39, werden wir sehen, dass für endliche Mengen A, B gilt:

$$|\mathrm{Abb}(A, B)| \;=\; |B|^{|A|}.$$

Folie 62

Definition 2.31.
Zwei Funktionen $f\colon A \to B$ und $g\colon A \to B$ sind *gleich* (kurz: $f = g$), falls f.a. $a \in A$ gilt: $f(a) = g(a)$.

Definition 2.32 (Definitionsbereich, Bildbereich, Bild)**.** Sei $f\colon A \to B$.

(a) Der *Definitionsbereich* von f ist die Menge $\mathrm{Def}(f) := A$.

(b) Der *Bildbereich* von f ist die Menge B.

(c) Das *Bild* von f (genauer: das Bild von A unter f) ist die Menge

$$\mathit{Bild}(f) \;:=\; f(A) \;=\; \{f(a) : a \in A\} \;\subseteq\; B.$$

Definition 2.33 (Restriktionen)**.**
Sei $f\colon A \to B$ eine Funktion und sei $A' \subseteq A$. Die *Restriktion* (oder *Einschränkung*) von f auf A' ist die Funktion

$$f|_{A'} \;:\; A' \to B,$$

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

Folie 63

Definition 2.34.
Eine *partielle Funktion* von einer Menge A in eine Menge B ist eine Funktion f mit $\mathrm{Def}(f) \subseteq A$ und $\mathit{Bild}(f) \subseteq B$.

Bemerkung 2.35.

(a) Im Gegensatz zu partiellen Funktionen nennt man Funktionen, wie wir sie in Definition 2.29 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

Folie 64

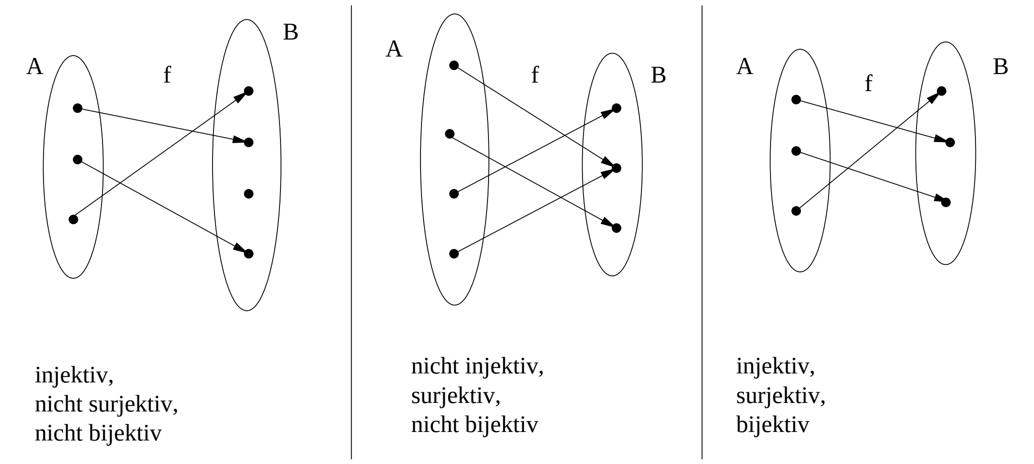
Definition 2.36. Sei $f\colon A \to B$.

(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:



Beobachtung 2.37.

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

$$f \text{ ist bijektiv} \iff f \text{ ist injektiv und surjektiv.}$$

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

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

Folie 65

Satz 2.38.

(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 $Z \in \mathcal{P}(M)$ (d.h. $Z \subseteq M$) durch die so genannte *charakteristische Funktion* $\chi_Z\colon M \to \{0,1\}$ mit

$$\chi_Z(m) \ := \ \begin{cases} 1, & \text{falls } m \in Z \\ 0, & \text{sonst.} \end{cases} \tag{*}$$

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

$$f(Z) \ := \ \chi_Z, \quad \text{für jedes } Z \in \mathcal{P}(M). \tag{**}$$

Behauptung. f ist bijektiv.

Wir zeigen dies in 2 Schritten (und nutzen Beobachtung 2.37(a)).

Schritt 1: f ist injektiv:

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

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

Wegen $f(Z) = f(Z')$ gilt gemäß (**), dass $\chi_Z = \chi_{Z'}$. D.h. f.a. $m \in M$ gilt $\chi_Z(m) = \chi_{Z'}(m)$. Gemäß (*) gilt daher f.a. $m \in M$, dass

$$m \in Z \iff m \in Z'.$$

Somit ist $Z = Z'$.

Schritt 2: f ist surjektiv:

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

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

Wir wählen

$$Z \ := \ \{m \in M \ : \ h(m) = 1\}.$$

Dann ist klar: $Z \in \mathcal{P}(M)$. Gemäß (*) gilt $\chi_Z = h$. Gemäß (**) ist daher $f(Z) = h$.

(b) *Idee:* Sei $a_1, \ldots, a_k$ eine Liste aller Elemente in A. Repräsentiere jede Funktion $h \in \text{Abb}(A, B)$ durch das k-Tupel $t_h := \big(h(a_1), \ldots, h(a_k)\big)$.

Rest: Übungsaufgabe.

$\square$

Folie 66

Folgerung 2.39. *Seien A, B, M endliche Mengen. Dann gilt:*

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

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

Beweis:

(a) Gemäß Satz 2.38(b) und Beobachtung 2.37(b) gilt für $k := |A|$, dass

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

Laut Satz 2.21(c) ist $|B^k| = |B|^k$. Somit $|\text{Abb}(A, B)| = |B|^k = |B|^{|A|}$.

(b) Gemäß Satz 2.38(a) und Beobachtung 2.37(b) ist

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

Gemäß (a) ist

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

$\square$

Spezielle Funktionen

Folie 67

Definition 2.40. Die *Identitätsfunktion* auf einer Menge M ist die Funktion

$$\mathrm{id}_M\colon M \to M$$

mit $\mathrm{id}_M(m) := m$, f.a. $m \in M$.

Definition 2.41. Eine *Permutation* einer Menge M ist eine *bijektive* Funktion $f : M \to M$.

Definition 2.42. Eine *Multimenge* (engl.: *bag*) über einer Menge M ist eine Funktion $f\colon M \to \mathbb{N}$.

Mit solchen Multimengen 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.

Folie 68

Beispiel 2.43. Ein Geldbeutel mit

- 3 1-Cent-Münzen
- 2 10-Cent-Münzen
- 4 20-Cent-Münzen
- 1 50-Cent-Münzen
- 3 1-Euro-Münzen
- 2 2-Euro-Münzen

kann repräsentiert werden durch die Multimenge

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

wobei

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

und

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

Bequemere Schreibweise (die konsistent ist mit Definition 2.29):

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

2.4 Beweise verstehen und selbst formulieren

Folie 69

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.

Nebenbei werden wir einige interessante mathematische Aussagen beweisen, die es sich zu merken lohnt.

Folie 70

Was sind *Sätze* und *Beweise*?

Ein *Satz* (bzw. *Theorem*) ist eine formale Aussage, die man sich merken sollte. Sie 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.

Folie 71

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,
- Ausnutzung von bis dahin noch unbewiesenen Behauptungen zur Begründung von einzelnen Beweisschritten.

Folie 72

Die Begriffe *Definition*, *Lemma*, *Korollar*, *Folgerung* und *Proposition*

Eine *Definition* führt einen neuen Begriff ein und legt dessen Bedeutung fest.

Ein *Lemma* (Plural: Lemmas oder Lemmata) ist so etwas ähnliches wie ein Satz. Es bezeichnet meistens einen „technischen Hilfssatz“, dessen Aussage man sich nicht unbedingt dauerhaft merken muss, die aber nützlich ist, um ein Theorem zu beweisen.

Ein *Korollar* (bzw. eine *Folgerung*) ist eine formale Aussage (ähnlich wie ein Satz), die man sich merken sollte, und deren Beweis relativ leicht aus einem bereits vorher bewiesenen Sachverhalt folgt.

Eine *Proposition* ist eine formale Aussage (ähnlich wie ein Satz oder ein Lemma). Der Begriff wird auf unterschiedliche Art verwendet — manchmal, um eine Aussage zu bezeichnen, die man sich merken sollte und die ganz leicht zu beweisen ist; und manchmal um einen „technischen Hilfssatz“ zu bezeichnen, der schwer zu beweisen ist, den man sich aber nicht unbedingt merken muss.

Beweistechnik "direkter Beweis"

Folie 73

Bei einem *direkten Beweis* wird die Behauptung eines Satzes "direkt", d.h. ohne "Umwege", bewiesen.

Beispiele für direkte Beweise haben wir bereits kennengelernt, z.B. der Beweis von Satz 2.6, der Beweis von Satz 2.21, der Beweis von Satz 2.38, der Beweis von Folgerung 2.39.

Es folgt ein weiteres Beispiel für einen direkten Beweis.

Folie 74

Gaußsche Summenformel

Satz 2.44. *Für alle $n \in \mathbb{N}$ gilt:* $\displaystyle\sum_{i=0}^{n} i \;=\; \frac{n \cdot (n+1)}{2}$.

Beweis: Sei $n \in \mathbb{N}$ beliebig. Es gilt:

$$
\begin{aligned}
2 \cdot \sum_{i=0}^{n} i \;&=\; \sum_{i=0}^{n} i \;+\; \sum_{j=0}^{n} j \;&=\; \sum_{i=0}^{n} i \;+\; \sum_{i=0}^{n} (n-i) \\
&=\; \sum_{i=0}^{n} \bigl(i + (n-i)\bigr) \;&=\; \sum_{i=0}^{n} n \qquad\qquad =\; n \cdot (n+1)\,.
\end{aligned}
$$

Es gilt also:

$$2 \cdot \sum_{i=0}^{n} \;=\; n \cdot (n+1)\ .$$

Somit gilt:

$$\sum_{i=0}^{n} \;=\; \frac{n \cdot (n+1)}{2}\ .$$

□

Beweistechnik "Beweis durch Kontraposition"

Folie 75

Man beachte, dass für beliebige Aussagen A und B das Folgende gilt:

$$\begin{array}{rl} & \text{die folgende Aussage ist wahr:} \\ & \text{“Falls Aussage } A \text{ gilt, so gilt auch Aussage } B\text{”} \\ \iff & \text{Aussage } B \text{ gilt oder Aussage } A \text{ gilt nicht} \\ \iff & \text{die folgende Aussage ist wahr:} \\ & \text{“Falls Aussage } B \text{ \textit{nicht} gilt, so gilt auch Aussage } A \text{ \textit{nicht}.”} \end{array}$$

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.”

Folie 76

Als Beispiel für einen Beweis durch Kontraposition betrachten wir den folgenden Satz.

Definition 2.45. Eine *gerade* Zahl ist eine Zahl z, für die gilt: es gibt ein $y \in \mathbb{Z}$ so dass $z = 2 \cdot y$ ist. Eine *ungerade* Zahl ist eine Zahl $z \in \mathbb{Z}$, die nicht gerade ist.

Satz 2.46.
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 nur den Fall, dass n *keine* ungerade Zahl ist (d.h. n ist gerade). Wir müssen zeigen, dass dann auch n^2 *keine* ungerade Zahl ist (d.h. n^2 ist eine gerade Zahl).

Es gilt:

$$\begin{array}{rll} n \text{ ist gerade} & \Longrightarrow & \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n = 2 \cdot y \quad \text{(gemäß Def. 2.45)} \\ & \Longrightarrow & \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n^2 = n \cdot (2 \cdot y) \\ & \Longrightarrow & \text{es ex. } y \in \mathbb{Z} \text{ s.d. } n^2 = 2 \cdot (n \cdot y) \\ & \Longrightarrow & \text{es ex. } y' \in \mathbb{Z} \text{ s.d. } n^2 = 2 \cdot y' \\ & \Longrightarrow & n^2 \text{ ist gerade} \quad \text{(gemäß Def. 2.45).} \end{array}$$

Somit ist n^2 gerade, d.h. n^2 ist keine ungerade Zahl. $\square$

Beweistechnik Beweis durch Widerspruch *(indirekter Beweis)*

Folie 77

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 *nicht* gilt und
- daraus einen Widerspruch herleitet.

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

Satz 2.47. *Für alle geraden natürlichen Zahlen a und b gilt: $a \cdot b$ ist gerade.*

Beweis: Durch Widerspruch.
Angenommen, a und b sind gerade natürlichen Zahlen, so dass $a \cdot b$ *nicht* gerade ist.
Da a und b gerade sind, gibt es $k, \ell \in \mathbb{Z}$ s.d. $a = 2 \cdot k$ und $b = 2 \cdot \ell$.
Dann ist $a \cdot b = (2 \cdot k) \cdot (2 \cdot \ell)$. Insbesondere gibt es also ein $m \in \mathbb{Z}$, s.d. $a \cdot b = 2 \cdot m$ (nämlich $m = 2{\cdot}k{\cdot}\ell$).
Gemäß Definition 2.45 ist also $a \cdot b$ gerade. Dies ist ein Widerspruch zur Annahme, dass $a \cdot b$ *nicht* gerade ist. □

Folie 78

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 2.48 (“$\mathcal{P}(\mathbb{N})$ ist nicht abzählbar”)**.**
Es gibt keine surjektive Funktion von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$.

Beweis: Durch Widerspruch. Angenommen, $f\colon \mathbb{N} \to \mathcal{P}(\mathbb{N})$ ist surjektiv. Sei

$$X \;:=\; \{\, n \in \mathbb{N} \;:\; n \notin f(n) \,\}. \qquad (*)$$

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

Da f surjektiv ist, muss es ein $m \in \mathbb{N}$ geben mit $f(m) = X$.
Klar: Entweder gilt $m \in X$ oder es gilt $m \notin X$.

Fall 1: $m \notin X$:
Wegen $f(m) = X$ gilt also $m \notin f(m)$.
Gemäß (*) für $n := m$ folgt, dass $m \in X$. $\lightning$ (Widerspruch zu "Fall 1: $m \notin X$").

Fall 2: $m \in X$:
Wegen $f(m) = X$ gilt also: $m \in f(m)$.
Gemäß (*) für $n := m$ folgt, dass $m \notin X$. $\lightning$ (Widerspruch zu "Fall 2: $m \in X$").

Somit führen beide Fälle zu einem Widerspruch. Daher muss unsere Annahme, dass es eine surjektive Funktion f von $\mathbb{N}$ nach $\mathcal{P}(\mathbb{N})$ gibt, falsch gewesen sein. $\square$

Folie 79

Cantors zweites Diagonalargument

Bemerkung 2.49.
Die in diesem Beweis verwendete Technik ist unter dem Namen *Diagonalisierung* (oder *Cantors zweites Diagonalargument*) bekannt.

Die Grundidee des obigen Beweises lässt sich nämlich folgendermaßen veranschaulichen: Eine Funktion $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ können wir durch folgende Tabelle repräsentieren

	0	**1**	**2**	**3**	**4**	**5**	$\cdots$
0	$a_{0,0}$	$a_{0,1}$	$a_{0,2}$	$a_{0,3}$	$a_{0,4}$	$a_{0,5}$	$\cdots$
1	$a_{1,0}$	$a_{1,1}$	$a_{1,2}$	$a_{1,3}$	$a_{1,4}$	$a_{1,5}$	$\cdots$
2	$a_{2,0}$	$a_{2,1}$	$a_{2,2}$	$a_{2,3}$	$a_{2,4}$	$a_{2,5}$	$\cdots$
3	$a_{3,0}$	$a_{3,1}$	$a_{3,2}$	$a_{3,3}$	$a_{3,4}$	$a_{3,5}$	$\cdots$
4	$a_{4,0}$	$a_{4,1}$	$a_{4,2}$	$a_{4,3}$	$a_{4,4}$	$a_{4,5}$	$\cdots$
5	$a_{5,0}$	$a_{5,1}$	$a_{5,2}$	$a_{5,3}$	$a_{5,4}$	$a_{5,5}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

wobei der Eintrag $a_{i,j}$ in Zeile i und Spalte j folgendermaßen gewählt ist:

$$a_{i,j} \ := \ \begin{cases} 1 & \text{falls } j \in f(i) \\ 0 & \text{falls } j \notin f(i). \end{cases}$$

Folie 80

Somit repräsentiert jede Zeile i dieser Tabelle die Menge $f(i)$, und es gilt

$$f(i) \;=\; \{j \in \mathbb{N} \;:\; a_{i,j} = 1\}.$$

Wir wählen nun die Folge

$$b_0 \;\; b_1 \;\; b_2 \;\; b_3 \;\; b_4 \;\; b_5 \;\; \cdots$$

so, dass sich, für jedes $j \in \mathbb{N}$, der Wert b_j von dem Eintrag $a_{j,j}$ in der Diagonalen der Tabelle unterscheidet. D.h., wir wählen

$$b_j \;:=\; \begin{cases} 0 & \text{falls } a_{j,j} = 1 \\ 1 & \text{falls } a_{j,j} = 0, \end{cases}$$

für alle $j \in \mathbb{N}$.
Anhand dieser Wahl von $b_0, b_1, b_2, \ldots$ wissen wir, dass diese Folge in keiner Zeile der Tabelle stehen kann, denn für jede Zeile i unterscheidet sich der in Spalte i stehende Wert $a_{i,i}$ vom Wert b_i. Somit gilt für die Menge

$$X \;:=\; \{j \in \mathbb{N} \;:\; b_j = 1\},$$

dass X nicht im Bild der Funktion f liegen kann, und dass f daher nicht surjektiv sein kann.

Folie 81

Man kann sich leicht davon überzeugen, dass die hier gewählte Menge X mit der im Beweis von Satz 2.48 gewählten Menge X übereinstimmt, denn

$$\begin{aligned} X \;&=\; \{j \in \mathbb{N} \;:\; b_j = 1\} \;&&=\; \{j \in \mathbb{N} \;:\; a_{j,j} = 0\} \\ &=\; \{j \in \mathbb{N} \;:\; j \notin f(j)\} \;&&=\; \{n \in \mathbb{N} \;:\; n \notin f(n)\}. \end{aligned}$$

Folie 82

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

Satz 2.50 ("Es gibt keine Menge aller Mengen")**.**
Es gibt keine Menge U, so dass für jede Menge M gilt: $M \in U$.

Folie 83

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

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

eine Menge. Insbesondere gilt entweder $X \in X$ oder $X \notin X$.

Fall 1: $X \notin X$:
Wir wissen: X ist eine Menge, also insbesondere $X \in U$.
Da wir in Fall 1 sind, gilt außerdem: $X \notin X$.
Gemäß (*) (für $M := X$) muss dann aber gelten: $X \in X$. $\lightning$ (Widerspruch zu "Fall 1: $X \notin X$").

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

Somit führen beide Fälle zu einem Widerspruch. Daher kann es keine Menge U geben, so dass für jede Menge M gilt: $M \in U$. $\square$

Folie 84

Bemerkung 2.51. Jede Aussage, die durch einen *Beweis durch Kontraposition* bewiesen werden kann, kann auch durch einen *Beweis durch Widerspruch* nachgewiesen werden.
Um zu zeigen, dass die Aussage

"Falls Aussage A gilt, so gilt auch Aussage B"

wahr ist, kann man in einem Beweis durch Widerspruch folgendermaßen vorgehen: Man nimmt an, dass Aussage A gilt und Aussage B nicht gilt und leitet aus dieser Annahme dann einen Widerspruch her.

Übungsaufgabe: Beweisen Sie Satz 2.46 durch einen "Beweis durch Widerspruch".

Beweistechnik "Beweis durch vollständige Induktion"

Folie 85

Das Induktionsprinzip

Um die Grundidee der vollständigen Induktion zu erklären, sei $A(n)$ eine Aussage über die natürliche Zahl n. Das Ziel ist, zu zeigen, dass die Aussage $A(n)$ für jedes $n \in \mathbb{N}$ wahr ist.

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

Folie 86

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

(i) $A(0)$ ist wahr gemäß Schritt (1).

(ii) $A(1)$ ist wahr gemäß (i) und Schritt (2) für $n = 0$,

(iii) $A(2)$ ist wahr gemäß (ii) und Schritt (2) für $n = 1$,

(iv) $A(3)$ ist wahr gemäß (iii) und Schritt (2) für $n = 2$,

(v) $A(4)$ ist wahr gemäß (iv) und Schritt (2) für $n = 3$,

(vi) $A(5)$ ist wahr gemäß (v) und Schritt (2) für $n = 4$,

(vii) usw.

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

Folie 87

Als Beispiel für einen Beweis durch vollständige Induktion betrachten wir den folgenden Satz:

Satz 2.52. *F.a.* $n \in \mathbb{N}$ *gilt:*

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1\,.$$

Beweis: Per Induktion nach n.

Die "Aussage $A(n)$", deren Gültigkeit hier f.a. $n \in \mathbb{N}$ bewiesen werden soll, besagt:

$$\sum_{i=0}^{n} 2^i \quad = \quad 2^{n+1} - 1.$$

INDUKTIONSANFANG: $n = 0$

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

Beweis:
Es gilt: $\sum_{i=0}^{0} 2^i \;=\; 2^0 \;=\; 1.$
Außerdem gilt: $2^{0+1} - 1 \;=\; 2^1 - 1 \;=\; 2 - 1 \;=\; 1.$
Somit: $\sum_{i=0}^{0} 2^i \;=\; 1 \;=\; 2^{0+1} - 1.$

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:

$$\begin{aligned}
\sum_{i=0}^{n+1} 2^i \quad &\overset{\text{Not.2.20}}{=} \quad \left(\sum_{i=0}^{n} 2^i \right) + 2^{n+1} \\
&\overset{\text{Ind.ann.}}{=} \quad (2^{n+1} - 1) + 2^{n+1} \\
&= \quad 2 \cdot 2^{n+1} - 1 \\
&= \quad 2^{(n+1)+1} - 1.
\end{aligned}$$

$\square$

Zwei nützliche Varianten des Induktionsprinzips

Um zu zeigen, dass eine Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geqslant n_0$ 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 $n \geqslant n_0$ beliebig.

Induktionsannahme: Die Aussage $A(n)$ ist wahr.

Behauptung: Die Aussage $A(n{+}1)$ ist wahr.

Beweis: ...

Folie 89

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 $n \geqslant n_0$ beliebig.

Induktionsannahme: Für jede natürliche Zahl i mit $n_0 \leqslant i \leqslant n$ ist die Aussage $A(i)$ wahr.

Behauptung: Die Aussage $A(n{+}1)$ ist wahr.

Beweis: ...

Folie 90

Beispiel 2.53.
Wir nutzen Variante 1, um die folgende Frage zu beantworten: Welche der Funktionen $f\colon \mathbb{N} \to \mathbb{Z}$ und $g\colon \mathbb{N} \to \mathbb{Z}$ mit $f(n) := n^2 - 7$ und $g(n) := 4 \cdot n$ (f.a. $n \in \mathbb{N}$) liefert größere Funktionswerte?

Um eine Vermutung darüber zu bekommen, welche der beiden Funktionen die größeren Werte liefert, stellen wir zunächst eine Tabelle auf, die die Funktionswerte für $n = 0$, $n = 1$, $n = 2$, etc. enthält:

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

Anhand dieser Tabelle drängt sich die Vermutung auf, dass f.a. $n \in \mathbb{N}$ mit $n \geqslant 6$ gilt: $f(n) > g(n)$. Die Korrektheit dieser Vermutung weisen wir im Folgenden per Induktion nach n nach.

INDUKTIONSANFANG: $n = 6$

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

Beweis:

Es gilt: $f(6) = 6^2 - 7 = 29$.

Außerdem gilt: $g(6) = 4 \cdot 6 = 24$.

Also: $f(6) = 29 > 24 = g(6)$.

INDUKTIONSSCHRITT: $n \to n{+}1$

Sei $n \in \mathbb{N}$ mit $n \geqslant 6$ 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:

$$\begin{aligned}
(n+1)^2 - 7 &= n^2 + 2n + 1 - 7 \\
&= (n^2 - 7) + 2n + 1 \\
&\overset{\text{Ind.ann}}{>} 4n + 2n + 1 \\
&\overset{n \geqslant 6,\text{ also } 2n+1 \geqslant 13 > 4}{\geqslant} 4n + 4 \\
&= 4(n{+}1).
\end{aligned}$$

Insgesamt haben wir damit bewiesen, dass f.a. $n \in \mathbb{N}$ mit $n \geqslant 6$ gilt: $f(n) > g(n)$.

$\square$Ende Beispiel 2.53

Folie 91

Auf ähnliche Weise kann man per Induktion auch Folgendes beweisen:

Satz 2.54.

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

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

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

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

(d) F.a. $n \in \mathbb{N}$ *gilt:* $2^n > n$.

Beweis. Übungsaufgabe □

Folie 92

Das folgende Beispiel zeigt, dass man beim Führen von Induktionsbeweisen sehr sorgfältig sein muss:

Beispiel 2.55.
Der folgende Satz ist offensichtlich nicht wahr — aber wo steckt der Fehler im Beweis?

"Satz": *F.a.* $n \in \mathbb{N}$ *mit* $n \geqslant 1$ *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 $|M| = 1$. D.h. 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 $n \geqslant 1$ 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 $a_1, a_2, \ldots, a_n, a_{n+1}$ eine Liste aller Menschen in M, d.h. $M = \{a_1, a_2, \ldots, a_n, a_{n+1}\}$. Sei

$$M' \;:=\; \{a_1, a_2, \ldots, a_n\} \quad \text{und} \quad M'' \;:=\; \{a_2, \ldots, a_n, a_{n+1}\}.$$

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? □Ende Beispiel 2.55

2.5 Rekursive Definition von Funktionen und Mengen

Folie 93

Rekursive Definitionen von Funktionen

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

(1) Definiere $f(0)$.
Diesen Schritt bezeichnet man als *Rekursionsanfang*.

(2) Definiere, f.a. $n \in \mathbb{N}$, $f(n{+}1)$ unter Verwendung des Werts $f(n)$ (bzw. unter Verwendung der Werte $f(n), f(n{-}1), \ldots, f(1), f(0)$).
Diesen Schritt bezeichnet man als *Rekursionsschritt*.

Auch hier sind wieder eine Reihe von Varianten möglich.

Folie 94

Beispiel 2.56.

(a) *Frage:* Wie viele Möglichkeiten gibt es, n Studierende so an n PCs zu verteilen, dass an jedem PC genau ein Studierender sitzt?

Antwort: $\text{fak}(n)$, wobei

- $\text{fak}(1) \;=\; 1$ und
- $\text{fak}(n{+}1) \;=\; (n{+}1) \cdot \text{fak}(n)$ (für alle $n \in \mathbb{N}_{\geqslant 1}$).

Insbesondere ist fak eine Funktion von $\mathbb{N}_{\geqslant 1}$ nach $\mathbb{N}_{\geqslant 1}$, d.h. $\text{fak}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$.

Beispielsweise ist

$$\text{fak}(4) \;=\; 4 \cdot \text{fak}(3) \;=\; 4 \cdot 3 \cdot \text{fak}(2) \;=\; 4 \cdot 3 \cdot 2 \cdot \text{fak}(1) \;=\; 4 \cdot 3 \cdot 2 \cdot 1 \;=\; 24.$$

Allgemein gilt f.a. $n \in \mathbb{N}_{\geqslant 1}$:

$$\text{fak}(n) \;=\; n \cdot (n-1) \cdot (n-2) \cdot \cdots \cdot 2 \cdot 1 \;\overset{\text{Not.2.20}}{=}\; \prod_{i=1}^{n} i.$$

Notation.
Die Funktion fak wird *Fakultätsfunktion* genannt. Meistens schreibt man $n!$ um die Zahl $\text{fak}(n)$ zu bezeichnen.

Folie 95

(b) *Fragestellung:* Ein Bauer züchtet Kaninchen. Jedes weibliche Kaninchen bringt im Alter von zwei Monaten ein weibliches Kaninchen zur Welt und danach jeden Monat ein weiteres.
Wie viele weibliche Kaninchen hat der Bauer zu Beginn des n-ten Monats, wenn er mit einem neu geborenen weiblichen Kaninchen startet?

Antwort: $\text{fib}(n)$, wobei die Funktion $\text{fib}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$ rekursiv wie folgt definiert ist:

- $\text{fib}(1) \;:=\; 1$,
- $\text{fib}(2) \;:=\; 1$ und
- $\text{fib}(n{+}1) \;:=\; \text{fib}(n) + \text{fib}(n{-}1)$ (f.a. $n \in \mathbb{N}$ mit $n \geqslant 2$).

Somit gilt:

n	1	2	3	4	5	6	7	8	9	10	11	12
$\text{fib}(n)$	1	1	2	3	5	8	13	21	34	55	89	144

Die Funktion fib wird auch *Fibonacci-Folge* genannt; sie ist benannt nach italienischen Mathematiker Leonardo Fibonacci (13. Jh.). Die Zahl $\text{fib}(n)$ heißt auch *n-te Fibonacci-Zahl*.

Folie 96

Um Aussagen über rekursiv definierte Funktionen zu beweisen, kann man wieder das Induktionsprinzip nutzen. Der folgende Satz gibt dazu ein Beispiel.

Satz 2.57. *Sei* $\mathrm{fib}\colon \mathbb{N}_{\geqslant 1} \to \mathbb{N}_{\geqslant 1}$ *die Fibonacci-Folge. Dann gilt f.a.* $n \in \mathbb{N}_{\geqslant 1}$*:* $\mathrm{fib}(n) \leqslant 2^n$.

Beweis: Per Induktion nach n.

INDUKTIONSANFANG: Betrachte $n = 1$ und $n = 2$.

Behauptung: $\mathrm{fib}(1) \leqslant 2^1$ und $\mathrm{fib}(2) \leqslant 2^2$.

Beweis: Es gilt: $\mathrm{fib}(1) \overset{\text{Def.}}{=} 1 \leqslant 2 = 2^1$ und $\mathrm{fib}(2) \overset{\text{Def.}}{=} 1 \leqslant 4 = 2^2$.

INDUKTIONSSCHRITT: $n \to n{+}1$

Sei $n \in \mathbb{N}$ mit $n \geqslant 2$ beliebig.

Induktionsannahme: F.a. $i \in \mathbb{N}_{\geqslant 1}$ mit $i \leqslant n$ gilt: $\mathrm{fib}(i) \leqslant 2^i$.

Behauptung: $\mathrm{fib}(n{+}1) \leqslant 2^{n+1}$.

Beweis:

$$\mathrm{fib}(n{+}1) \overset{\text{Def.}}{=} \mathrm{fib}(n) + \mathrm{fib}(n{-}1) \overset{\text{Ind.ann.}}{\leqslant} 2^n + 2^{n-1} \leqslant 2 \cdot 2^n = 2^{n+1}. \qquad \Box$$

Folie 97

Vergleich der Laufzeit zweier Algorithmen

Bemerkung 2.58. Ein möglicher Algorithmus, um für eine Zahl $n \in \mathbb{N}_{\geqslant 1}$ den Wert $\mathrm{fib}(n)$ der Fibonacci-Folge zu berechnen, ist:

Algo 1 (bei Eingabe einer Zahl $n \in \mathbb{N}_{\geqslant 1}$):

1. Falls $n = 1$ oder $n = 2$, dann gib 1 als Ergebnis zurück.
2. Falls $n \geqslant 3$, dann:
3. Sei x_1 die Ausgabe von *Algo 1* bei Eingabe der Zahl $n{-}1$.
4. Sei x_2 die Ausgabe von *Algo 1* bei Eingabe der Zahl $n{-}2$.
5. Gib den Wert $(x_1 + x_2)$ als Ergebnis zurück.

Der Algorithmus benötigt bei Eingabe einer Zahl n höchstens $g_1(n)$ Schritte, wobei

$$\begin{aligned} g_1(1) &= 2 \quad \text{und} \quad g_1(2) \;=\; 3 \quad \text{und} \\ g_1(n) &= 3 + g_1(n{-}1) + g_1(n{-}2) + 2 \\ &= 5 + g_1(n{-}1) + g_1(n{-}2) \quad \text{für alle } n \in \mathbb{N} \text{ mit } n \geqslant 3 \end{aligned}$$

(wir zählen hier jede Addition, jeden Vergleich, und jedes Zurückgeben eines Ergebnisses als einen Schritt).

Folie 98

Ein anderer Algorithmus, der für eine Zahl $n \in \mathbb{N}_{\geqslant 1}$ den Wert $\text{fib}(n)$ berechnet, ist:

Algo 2 (bei Eingabe einer Zahl $n \in \mathbb{N}_{\geqslant 1}$):

1. Falls $n = 1$ oder $n = 2$, dann gib 1 als Ergebnis zurück.
2. Seien $a_0 := 0$, $a_1 := 1$ und $a_2 := 1$.
3. Wiederhole für alle i von 3 bis n:
4. Ersetze a_0 durch a_1 und a_1 durch a_2.
5. Ersetze a_2 durch $a_0 + a_1$.
6. Gib den Wert a_2 als Ergebnis zurück.

Dieser Algorithmus benötigt bei Eingabe $n \in \mathbb{N}_{\geqslant 1}$ höchstens $g_2(n)$ Schritte, wobei

$$g_2(1) := 2, \quad g_2(2) := 3, \quad \text{und} \quad g_2(n) := 6 + 6 \cdot (n{-}2) \quad \text{f.a. } n \geqslant 3$$

(ähnlich wie oben zählen wir jeden Vergleich, jedes Zurückgeben eines Werts und jedes Setzen eines Werts als einen Schritt. Für jeden Schleifendurchlauf berechnen wir zusätzlich 2 Schritte, um i um eins zu erhöhen und zu testen, ob das Ergebnis kleiner oder gleich n ist).

Folie 99

Frage: Welcher der beiden Algorithmen läuft im Allgemeinen schneller? D.h. welche der beiden Funktionen g_1 und g_2 liefert kleinere Funktionswerte?

Mit den in diesem Kapitel bereitgestellten Werkzeugen können wir eine Antwort auf diese Frage finden, und wir können sogar beweisen, dass die Antwort korrekt ist. Hierzu können wir ähnlich vorgehen wie in Beispiel 2.53.

Folie 100

Bemerkung 2.59. Es gibt auch eine "geschlossene Formel", mit der man die n-te Fibonacci-Zahl, d.h. die Zahl $\text{fib}(n)$, direkt ausrechnen kann, ohne dafür sämtliche Werte $\text{fib}(1)$, $\text{fib}(2)$, $\ldots$, $\text{fib}(n{-}1)$ ausrechnen zu müssen:
F.a. $n \in \mathbb{N}_{\geqslant 1}$ gilt:

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

Beweis: Übungsaufgabe (per Induktion nach n; Details finden sich in [MM00]). □

Folie 101

Rekursive Definitionen von Mengen

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

(a) *Basisregeln* der Form "$m \in M$".

(D.h. die Basisregeln listen explizit bestimmte Elemente auf, die zur Menge M gehören.)

(b) *Rekursiven Regeln* der Form:

$$\text{"Wenn } m_1, \ldots, m_k \in M, \text{ dann } m \in M\text{"},$$

wobei m von $m_1, \ldots, m_k$ 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.

Folie 102

Beispiel 2.60 (Die Menge PAL)**.**
Betrachte das Alphabet $A := \{a, b\}$.
Die Menge $\text{PAL} \subseteq A^*$ sei wie folgt rekursiv definiert:

Basisregeln:

(B1): $\varepsilon \in \text{PAL}$

(B2): $a \in \text{PAL}$

(B3): $b \in \text{PAL}$

Rekursive Regeln:

(R1): Ist $w \in \text{PAL}$, so ist auch $awa \in \text{PAL}$.

(R2): Ist $w \in \text{PAL}$, so ist auch $bwb \in \text{PAL}$.

Beispiele für Worte, die zur Menge PAL gehören:

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

Es gilt beispielsweise auch: $aababaa \in \text{PAL}$.

Beweis:

- $a \in \text{PAL}$ (gemäß Basisregel (B2)).
- Regel (R2) mit $w := a \implies bab \in \text{PAL}$.
- Regel (R1) mit $w := bab \implies ababa \in \text{PAL}$.
- Regel (R1) mit $w := ababa \implies aababaa \in \text{PAL}$.

$\square$

Aber beispielsweise gilt

$$aab \notin \text{PAL},$$

denn aus den Basisregeln und den rekursiven Regeln folgt, dass für jedes Wort $w \in \text{PAL}$ der erste und der letzte Buchstabe von w identisch sind. $\square$Ende Beispiel 2.60

Folie 103

Induktionsprinzip 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.
Dieser Schritt heißt *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.
Dieser Schritt heißt *Induktionsschritt*.

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

Folie 104

Im Folgenden betrachten wir ein Beispiel dafür, wie das Induktionsprinzip dazu genutzt werden kann, Eigenschaften von rekursiv definierten Mengen nachzuweisen.

Beispiel 2.61 (Palindrome)**.**
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 $k \in \mathbb{N}_{\geqslant 1}$ und $w_1, \dots, w_k \in A$, so ist $w^R := w_k \cdots w_1$.

Beispiel: $aaab^R = baaa$.

Definition: Ein Wort $w \in A^*$ heißt *Palindrom*, wenn gilt: $w = w^R$.

Sei PAL die in Beispiel 2.60 rekursiv definierte Teilmenge von A^*.

Behauptung 1: Für jedes Wort $w \in \text{PAL}$ 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 $w \in \mathrm{PAL}$ und sei $v := awa$. Gemäß (R1) ist $v \in \mathrm{PAL}$.

  Induktionsannahme: $w = w^R$.

  Behauptung: $v = v^R$.

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

- (R2): Sei $w \in \mathrm{PAL}$ und sei $v := bwb$. Gemäß (R2) ist $v \in \mathrm{PAL}$.

  Induktionsannahme: $w = w^R$.

  Behauptung: $v = v^R$.

  Beweis: $v^R \overset{\text{Def. } v}{=} (bwb)^R \overset{\text{Def. } (\cdot)^R}{=} bw^Rb \overset{\text{Ind.ann.: } w = w^R}{=} bwb \overset{\text{Def. } v}{=} v$.

$\square_{\text{Beh. 1}}$

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

Beweisansatz: Zeige folgende Aussage per Induktion nach n:

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

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

Details: Übungsaufgabe. $\square_{\text{Beh. 2}}$

Aus Behauptung 1 und Behauptung 2 folgt, dass $\mathrm{PAL} = \{w \in A^* : w = w^R\}$.

$\square_{\text{Ende Beispiel 2.61}}$

2.6 Größenvergleich von Mengen

Folie 105

Definition 2.62. Seien A und B beliebige Mengen.

(a) A heißt *höchstens so mächtig wie* B, wenn es eine injektive Abbildung von A nach B gibt.

(b) A und B heißen *gleichmächtig*, wenn es eine bijektive Abbildung von A nach B gibt.

(c) B heißt *echt mächtiger* als A, wenn gilt: A ist höchstens so mächtig wie B, und A und B sind nicht gleichmächtig.

Beispiel 2.63 ($\mathcal{P}(\mathbb{N})$ ist echt mächtiger als $\mathbb{N}$)**.**
$\mathbb{N}$ ist höchstens so mächtig wie $\mathcal{P}(\mathbb{N})$. Dies wird belegt durch die injektive Abbildung $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ mit $f(n) := \{n\}$ f.a. $n \in \mathbb{N}$.

$\mathbb{N}$ und $\mathcal{P}(\mathbb{N})$ sind nicht gleichmächtig. Dies folgt direkt aus Satz 2.48.

Somit ist $\mathcal{P}(\mathbb{N})$ echt mächtiger als $\mathbb{N}$.

Folie 106

Satz 2.64. *Für jede Menge M gilt:*

(a) $\mathcal{P}(M)$ ist echt mächtiger als M.

(b) $\mathcal{P}(M)$ und $\text{Abb}(M, \{0,1\})$ sind gleichmächtig.

Beweis.
(a): Übungsaufgabe.
(b): Dies folgt direkt aus Satz 2.38(a). $\square$

Folie 107

Bemerkung 2.65. In einem späteren Kapitel (Kapitel 3) werden wir beweisen, dass Folgendes für alle Mengen A und B gilt:

> Wenn es eine injektive Funktion von A nach B und eine injektive Funktion von B nach A gibt, dann gibt es auch eine bijektive Funktion von A nach B.

Daraus folgt dann:

> Zwei Mengen A und B sind genau dann gleichmächtig, wenn gilt: A ist höchstens so mächtig wie B und B ist höchstens so mächtig wie A.

Folie 108

Definition 2.66.

(a) Eine Menge A heißt *abzählbar*, wenn es eine injektive Abbildung $f : A \to \mathbb{N}$ gibt (d.h. wenn A höchstens so mächtig ist wie $\mathbb{N}$).

(D.h. die Elemente in A können mit natürlichen Zahlen so "durchnummeriert" werden, dass jedes Element in A eine andere "Nummer" bekommt.)

(b) Eine Menge heißt *abzählbar unendlich*, wenn sie abzählbar und unendlich ist.

(c) Eine Menge heißt *überabzählbar*, wenn sie nicht abzählbar ist.

Bemerkung. In vielen Teilen der Fachliteratur werden die Begriffe "abzählbar" und "abzählbar unendlich" genau so verwendet, wie wir sie hier definiert haben. Aber in manchen Teilen der Literatur wird der Begriff "abzählbar" verwendet um das zu bezeichnen, das wir hier "abzählbar unendlich" nennen; das, was wir hier "abzählbar" nennen, wird dort dann "höchstens abzählbar" genannt.

Satz 2.67. $\mathcal{P}(\mathbb{N})$ *ist überabzählbar.*
Beweis: Durch Widerspruch.
Angenommen, $\mathcal{P}(\mathbb{N})$ wäre abzählbar. Dann gibt es eine injektive Funktion $g : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$. Sei dann die Funktion $f : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ für alle $n \in \mathbb{N}$ wie folgt definiert: Falls es ein $X \in \mathcal{P}(\mathbb{N})$ mit $g(X) = n$ gibt, so setze $f(n) := X$ (dies ist wohldefiniert, da g injektiv ist — daher gibt es kein weiteres $X' \in \mathcal{P}(\mathbb{N})$ mit $X' \neq X$, für das $g(X') = n$ gilt). Ansonsten setze $f(n) := \emptyset$.

Behauptung: Die Funktion f ist surjektiv.
Beweis: Für jedes beliebige $X \in \mathcal{P}(\mathbb{N})$ gilt: $f(n) = X$ für $n := g(X)$.

$\square_{\text{Beh.}}$

Aber diese Behauptung widerspricht Satz 2.48. $\square$

Folie 109

Beispiel 2.68. Jede der folgenden Mengen ist abzählbar:
$\mathbb{N}$, jedes $M \subseteq \mathbb{N}$, $\mathbb{Z}$.

Beweis: Die Abzählbarkeit der Menge $\mathbb{N}$ wird durch die Identitätsfunktion $\mathrm{id}_{\mathbb{N}}$ belegt; diese Funktion ist injektiv.

Sei $M \subseteq M$. Die Abzählbarkeit der Menge M wird durch die Funktion $f : M \to \mathbb{N}$ mit $f(x) := x$ f.a. $x \in M$ belegt; diese Funktion ist injektiv.

Die Abzählbarkeit der Menge $\mathbb{Z}$ wird durch die Funktion $g : \mathbb{Z} \to \mathbb{N}$ belegt, die f.a. $z \in \mathbb{Z}$ wie folgt definiert ist:

$$g(z) \;:=\; \begin{cases} 2z & \text{falls } z \geqslant 0 \\ 2|z| - 1 & \text{falls } z < 0 \end{cases}$$

Offensichtlicherweise bildet diese Funktion g die nicht-negativen ganzen Zahlen auf die geraden natürlichen Zahlen ab; und sie bildet die negativen ganzen Zahlen auf die ungeraden natürlichen Zahlen ab. Man sieht leicht, dass die Funktion g injektiv ist. $\square$

Folie 110

Satz 2.69 ("pairing function")**.** *Die Abbildung* $\pi : \mathbb{N}^2 \to \mathbb{N}$ *mit*[2]

$$\pi(x,y) \ := \ y + \sum_{i=0}^{x+y} i \ , \qquad \text{f.a.} \ (x,y) \in \mathbb{N}^2$$

ist bijektiv.

Beachte: Gemäß der Gaußschen Summenformel ist

$$\pi(x,y) \ = \ y \ + \ \tfrac{1}{2}(x{+}y)(x{+}y{+}1) \ .$$

Beweis. Wir zeigen zunächst, dass π *surjektiv* ist:
Betrachte ein beliebiges $n \in \mathbb{N}$. Unser Ziel ist, $(x,y) \in \mathbb{N}^2$ zu finden, so dass gilt: $\pi(x,y) = n$.
Dazu wählen wir die größte Zahl $d \in \mathbb{N}$, für die gilt: $\sum_{i=0}^{d} i \leqslant n$. Es gilt:

$$\sum_{i=0}^{d} i \ \leqslant \ n \ < \ \sum_{i=0}^{d} i \ + \ d{+}1 \ .$$

Wähle

$$y \ := \ n \ - \ \sum_{i=0}^{d} i \qquad \text{und} \qquad x \ := \ d - y \ .$$

Klar: $y \in \{j \in \mathbb{N} \ : \ 0 \leqslant j \leqslant d\}$ und $x \in \{j \in \mathbb{N} \ : \ 0 \leqslant j \leqslant d\}$.
Insbesondere ist also $(x,y) \in \mathbb{N}^2$. Außerdem gilt: $x + y = d$ und

$$\pi(x,y) \ = \ y \ + \ \sum_{i=0}^{x+y} i \ = \ n \ - \ \sum_{i=0}^{d} i \ + \ \sum_{i=0}^{d} i \ = \ n \ .$$

Somit ist π also surjektiv.

Wir zeigen nun noch, dass π *injektiv* ist:
Seien $(x,y) \in \mathbb{N}^2$ und $(x',y') \in \mathbb{N}^2$ mit $\pi(x,y) = \pi(x',y')$. Unser Ziel ist zu zeigen, dass $(x,y) = (x',y')$.

[2] Statt $\pi(x,y)$ müssten wir, um formal korrekt zu sein, eigentlich $\pi((x,y))$ schreiben. Der besseren Lesbarkeit halber nutzt man i.d.R. aber meistens die "Kurzschreibweise" bei der man die äußeren Klammern eines Tupels, auf das die Funktion angewendet wird, weglässt.

Fall 1: $x{+}y = x'{+}y'$. Gemäß Voraussetzung gilt dann:

$$0 \;=\; \pi(x',y') - \pi(x,y) \;=\; y' - y \;+\; \sum_{i=0}^{x'+y'} i \;-\; \sum_{i=0}^{x+y} i \;=\; y' - y.$$

Also ist $y = y'$. Und wegen $x + y = x' + y'$ folgt dann auch, dass $x = x'$ ist. Somit ist $(x,y) = (x',y')$.

Fall 2: $x{+}y < x'{+}y'$. Sei $I := \{i \in \mathbb{N} \;:\; x{+}y < i \leqslant x'{+}y'\}$. Insbesondere ist $x{+}y{+}1 \in I$. Gemäß Voraussetzung gilt:

$$\begin{aligned}
0 \;=\; \pi(x',y') - \pi(x,y) \;&=\; y' - y \;+\; \sum_{i=0}^{x'+y'} i \;-\; \sum_{i=0}^{x+y} i \\
&=\; y' - y \;+\; \sum_{i \in I} i \\
&\geqslant\; y' - y \;+\; x{+}y{+}1 \\
&=\; y' + x + 1
\end{aligned}$$

Da $y' \in \mathbb{N}$ und $x \in \mathbb{N}$, ist $y'{+}x{+}1 \geqslant 1$. Insgesamt ergibt dies, dass $0 \geqslant 1$ ist. Dies ist ein Widerspruch. Somit kann Fall 2 nicht eintreten.

Fall 3: $x{+}y > x'{+}y'$. Analog zu Fall 2 (wobei die Rollen von (x,y) und (x',y') vertauscht werden).

Insgesamt haben wir somit gezeigt, dass π injektiv ist. □

Folie 111

Cantors erstes Diagonalargument

Bemerkung 2.70. Die bijektive Funktion $\pi : \mathbb{N}^2 \to \mathbb{N}$ aus Satz 2.69 wird auch *pairing function* genannt. Die Grundidee der Wahl dieser Funktion ist unter dem Namen *Cantors erstes Diagonalargument* bekannt und lässt sich folgendermaßen veranschaulichen (siehe Abbildung 2.1):

Die Menge $\mathbb{N}^2$ wird eingeteilt in "Diagonalen": Für jede Zahl $i \in \mathbb{N}$ ist die *i-te Diagonale* definiert als die Menge

$$D_i \;:=\; \{\, (x,y) \in \mathbb{N}^2 \;:\; x{+}y = i \,\}$$

Insbes. ist $D_0 = \{(0,0)\}$, $D_1 = \{(1,0),(0,1)\}$, $D_2 = \{(2,0),(1,1),(0,2)\}$. Um die Menge $\mathbb{N}^2$ "abzuzählen" nummerieren wir die Elemente in $\mathbb{N}^2$ wie

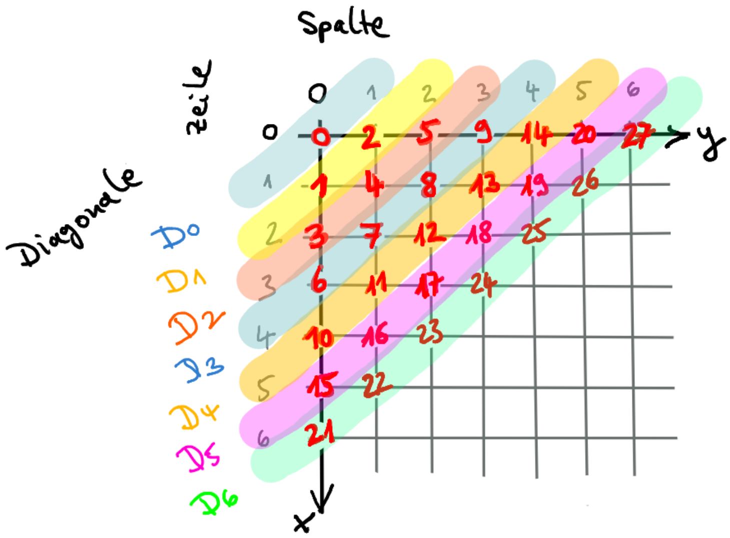


Abbildung 2.1: Veranschaulichung der Funktion π. Der Wert $\pi(x, y)$ ist in Zeile x und Spalte y eingetragen (rote Zahlen). Die "i-te Diagonale" D_i besteht aus allen Punkten (x, y), für die gilt: $x+y = i$.

folgt durch: Zunächst betrachten wir D_0 und geben dem einzigen Element darin die Nummer 0. Dann betrachten wir D_1 und geben dem Tupel $(1, 0)$ die Nummer 1 und dem Tupel $(0, 1)$ die Nummer 2. Danach betrachten wir D_2 und geben den Tupeln $(2, 0)$, $(1, 1)$ und $(0, 2)$ die Nummern 3, 4 und 5. Insgesamt betrachten wir nacheinander alle Diagonalen D_i (für $i = 0, 1, 2, 3, \ldots$), betrachten die Elemente in D_i in der Reihenfolge gemäß aufsteigendem y-Wert und verteilen fortlaufende Nummern. Die Funktion π aus Satz 2.69 ist so gewählt, dass die Nummer, die das Tupel $(x, y) \in \mathbb{N}^2$ bekommt genau die Zahl $\pi(x, y)$ ist.

Folie 112

Lemma 2.71. *Seien Mengen A, B und B_i für alle $i \in \mathbb{N}$ gegeben. Es gilt:*

(a) Falls A und B abzählbar sind ist, so ist auch $A \times B$ abzählbar.

(b) Falls B abzählbar ist, so ist auch B^k abzählbar für jedes $k \in \mathbb{N}$.

(c) Falls für jedes $i \in \mathbb{N}$ die Menge B_i abzählbar ist, so ist auch die Menge $\bigcup_{i \in \mathbb{N}} B_i$ abzählbar.

Beweis. Wir nutzen die bijektive Funktion $\pi : \mathbb{N}^2 \to \mathbb{N}$ aus Satz 2.69.

(a)*:* Gemäß Voraussetzung sind A und B abzählbar, d.h. es gibt injektive Funktionen $f : A \to \mathbb{N}$ und $g : B \to \mathbb{N}$. Wir wollen zeigen, dass es eine injektive Funktion $h : A \times B \to \mathbb{N}$ gibt. Wir wählen h wie folgt: Für alle $(a, b) \in A \times B$ setzen wir

$$h(a,b) \quad := \quad \pi\big(f(a), g(b)\big) \;.$$

Klar: $h(a, b) \in \mathbb{N}$. Somit ist h eine Funktion von $A \times B$ nach $\mathbb{N}$.

Diese Funktion h ist injektiv, denn: Seien (a, b) und (a', b') Elemente in $A \times B$ mit $h(a, b) = h(a', b')$. Wir müssen zeigen, dass $(a, b) = (a', b')$ ist.
Wegen $h(a, b) = h(a', b')$ gilt: $\pi\big(f(a), g(b)\big) = \pi\big(f(a'), g(b')\big)$.
Da π injektiv ist gilt: $\big(f(a), g(b)\big) = \big(f(a'), g(b')\big)$.
Somit ist $f(a) = f(a')$ und $g(b) = g(b')$.
Da f und g injektiv sind gilt $a = a'$ und $b = b'$. Somit ist $(a, b) = (a', b')$.
Dies beendet den Beweis von (a).

(b)*:* Wir führen den Beweis per Induktion nach k. Im Induktionsschritt benutzen wir Aussage (a). Gemäß Voraussetzung ist B abzählbar, d.h. es gibt eine injektive Funktion $g : B \to \mathbb{N}$.

INDUKTIONSANFANG: Betrachte $k = 0$ und $k = 1$.
Behauptung: B^0 und B^1 sind abzählbar.
Beweis:
$B^0 = \{()\}$ ist abzählbar; dies wird belegt durch die injektive Funktion $f_0 : B^0 \to \mathbb{N}$ mit $f_0(()) := 0$.

$B^1 = \{(b) \;:\; b \in B\}$ ist abzählbar; dies wird belegt durch die injektive Funktion $f_1 : B^1 \to \mathbb{N}$ mit $f_1((b)) := g(b)$ für jedes $b \in B$.

INDUKTIONSSCHRITT: $k \to k+1$
Sei $k \in \mathbb{N}$ beliebig mit $k \geqslant 1$.
Induktionsannahme: B^k ist abzählbar.
Behauptung: B^{k+1} ist abzählbar.
Beweis: Gemäß Induktionsannahme ist B^k abzählbar. Gemäß Voraussetzung ist B abzählbar. Aussage (a) (für $A := B^k$) liefert, dass $B^k \times B$ abzählbar ist. Somit gibt es eine injektive Funktion $g : B^k \times B \to \mathbb{N}$.
Wir wollen zeigen, dass es eine injektive Funktion $h : B^{k+1} \to \mathbb{N}$ gibt. Dazu wählen wir h wie folgt: Für alle $(b_1, \ldots, b_k, b_{k+1}) \in B^{k+1}$ setze[3]

$$h\big((b_1, \ldots, b_k, b_{k+1})\big) \quad := \quad g\big(((b_1, \ldots, b_k), b_{k+1})\big) \;.$$

[3]Dies ist die formal korrekte Schreibweise, die alle nötigen Klammern enthält. Gemäß der in der vorherigen Fußnote vereinbarten Kurzschreibweise können wir stattdessen auch schreiben: $h\big(b_1, \ldots, b_k, b_{k+1}\big) := g\big((b_1, \ldots, b_k), b_{k+1}\big)$

Offensichtlicherweise ist h injektiv (da g injektiv ist).
Dies beendet den Beweis von (b).

(c)*:* Wir benutzen Aussage (b) und die Funktion π.
Gemäß Voraussetzung gilt für jedes $i \in \mathbb{N}$: Die Menge B_i ist abzählbar — d.h. es gibt eine injektive Funktion $f_i : B_i \to \mathbb{N}$. Sei

$$M \quad := \quad \bigcup_{i \in \mathbb{N}} B_i \ .$$

Wir wollen zeigen, dass es eine injektive Funktion $h : M \to \mathbb{N}$ gibt. Wir wählen h wie folgt: Für jedes $x \in M$ sei i_x die kleinste natürliche Zahl i, für die gilt: $x \in B_i$. Für jedes $x \in M$ setzen wir

$$h(x) \quad := \quad \pi\big(f_{i_x}(x), i_x\big) \ .$$

Klar: $h(x) \in \mathbb{N}$. Somit ist h eine Funktion von M nach $\mathbb{N}$.
Diese Funktion ist injektiv, denn: Seien x und y Elemente in M mit $h(x) = h(y)$. Wir müssen zeigen, dass $x = y$ ist.
Wegen $h(x) = h(y)$ ist $\pi\big(f_{i_x}(x), i_x\big) = \pi\big(f_{i_y}(y), i_y\big)$.
Da π injektiv ist, gilt: $\big(f_{i_x}(x), i_x\big) = \big(f_{i_y}(y), i_y\big)$. Somit ist $i_x = i_y$ und $f_{i_x}(x) = f_{i_y}(y)$.
Sei $i := i_x$. Gemäß unserer Wahl von i_x und i_y und da $i = i_x = i_y$ ist, gilt: $x \in B_i$ und $y \in B_i$. Da f_i injektiv ist und $f_i(x) = f_i(y)$ gilt, erhalten wir, dass $x = y$ ist.
Dies beendet den Beweis von (c). □

Folie 113

Satz 2.72. *Für jede Menge A gilt:*
Falls A abzählbar ist, so ist auch A^* abzählbar.

Beweis. Dies folgt leicht aus Lemma 2.71:
Für jedes $i \in \mathbb{N}$ sei $B_i := A^i$. Es gilt:

$$A^* \quad = \quad \bigcup_{i \in \mathbb{N}} A^i \quad = \quad \bigcup_{i \in \mathbb{N}} B_i \ .$$

Lemma 2.71(b) liefert für jedes $i \in \mathbb{N}$, dass B_i abzählbar ist.
Lemma 2.71(c) liefert, dass $\bigcup_{i \in \mathbb{N}} B_i$ abzählbar ist.
Dies beendet den Beweis. □

Folie 114

Existenz nicht-berechenbarer Funktionen

Folgerung 2.73.
Es gibt Funktionen $f : \mathbb{N} \to \{0,1\}$, die nicht berechenbar sind.

Begründung:
Aus Satz 2.67 und Satz 2.64(b) folgt, dass die Menge $\mathrm{Abb}(\mathbb{N}, \{0,1\})$ überabzählbar ist. Somit gibt es überabzählbar viele verschiedene Funktionen $f : \mathbb{N} \to \{0,1\}$.

Eine Funktion $f : \mathbb{N} \to \{0,1\}$ nennen wir *berechenbar*, wenn es ein JAVA-Programm P gibt, so dass für jedes $n \in \mathbb{N}$ gilt: Bei Eingabe von n hält das Programm P nach endlich vielen Schritten an und gibt den Wert $f(n)$ aus — wir sagen dann: *Das Programm P berechnet die Funktion f.*

Jedes JAVA-Programm ist ein Text, dessen Buchstaben Elemente des ASCII-Alphabets sind. Somit ist jedes JAVA-Programm P ein Element in A^*, wobei A das ASCII-Alphabet ist.

Klar: A besteht aus nur endlich vielen verschiedenen Symbolen. Insbesondere ist A abzählbar. Gemäß Satz 2.72 ist A^* abzählbar. Somit gibt es nur abzählbar viele verschiedene JAVA-Programme.

Aber es gibt überabzählbar viele verschiedene Funktionen $f : \mathbb{N} \to \{0,1\}$. Daher muss es Funktionen $f : \mathbb{N} \to \{0,1\}$ geben, die nicht berechenbar sind.

Formaler Beweis:
Durch Widerspruch. Wir nehmen an, dass es für jedes $f : \mathbb{N} \to \{0,1\}$ ein JAVA-Programm P_f gibt, das die Funktion f berechnet.
Klar: $P_f \in A^*$, wobei A das ASCII-Alphabet ist.
Da A abzählbar ist, ist gemäß Satz 2.72 auch A^* abzählbar. D.h. es gibt eine injektive Funktion $g : A^* \to \mathbb{N}$. Wir definieren die Funktion

$$h \;:\; \mathrm{Abb}(\mathbb{N}, \{0,1\}) \to \mathbb{N}$$

wie folgt: Für jedes $f \in \mathrm{Abb}(\mathbb{N}, \{0,1\})$ setzen wir

$$h(f) \quad := \quad g(P_f)\ .$$

Diese Funktion h ist injektiv, denn:
Seien $f_1, f_2 \in \mathrm{Abb}(\mathbb{N}, \{0,1\})$ mit $h(f_1) = h(f_2)$. *Zu zeigen:* $f_1 = f_2$.
Wegen $h(f_1) = h(f_2)$ gilt: $g(P_{f_1}) = g(P_{f_2})$. Da g injektiv ist, gilt $P_{f_1} = P_{f_2}$.
Das heißt: f_1 und f_2 werden durch genau dasselbe JAVA-Programm berechnet. Somit gilt für alle Eingaben $n \in \mathbb{N}$, die dieses JAVA-Programm erhält, dass dessen Ausgabe der Wert $f_1(n) = f_2(n)$ ist. Daher ist $f_1 = f_2$.

Wir haben also gezeigt, dass die Funktion h injektiv ist.

Gemäß Satz 2.64(b) sind die Mengen $\mathcal{P}(\mathbb{N})$ und $\text{Abb}(\mathbb{N}, \{0,1\})$ gleichmächtig. D.h. es gibt eine bijektive Funktion $\beta : \mathcal{P}(\mathbb{N}) \to \text{Abb}(\mathbb{N}, \{0,1\})$. Da β und h injektiv sind, ist auch die wie folgt definierte Funktion $\gamma : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ injektiv: F.a. $M \in \mathcal{P}(\mathbb{N})$ setze

$$\gamma(M) \quad := \quad h\big(\beta(M)\big) \ .$$

Somit ist also $\mathcal{P}(\mathbb{N})$ abzählbar. Dies ist ein Widerspruch zu Satz 2.67.

$\square_{\text{Folg.2.73}}$

Folie 115

Abzählbarkeit der rationalen Zahlen und Überabzählbarkeit der reellen Zahlen

Satz 2.74.

(a) $\mathbb{Q}$ ist abzählbar.

(b) $\mathbb{R}$ ist überabzählbar.

Beweis.
(a): Gemäß Beispiel 2.68 ist $\mathbb{Z}$ abzählbar, d.h. es gibt eine injektive Funktion $f : \mathbb{Z} \to \mathbb{N}$.
Außerdem sei $\pi : \mathbb{N}^2 \to \mathbb{N}$ die bijektive Funktion aus Satz 2.69, d.h. f.a. $(x,y) \in \mathbb{N}^2$ ist $\pi(x,y) = y + \sum_{i=0}^{x+y} i$. Insbesondere gilt f.a. $(x,y) \in \mathbb{N}^2$:

$$\pi(x,y) = 0 \qquad \Longleftrightarrow \qquad (x,y) = 0 \ . \tag{2.2}$$

Gesucht ist eine injektive Funktion $g : \mathbb{Q} \to \mathbb{N}$. Wir gehen wie folgt vor: Jede rationale Zahl $\neq 0$ lässt sich eindeutig darstellen als "gekürzten Bruch", bei dem der Zähler eine ganze Zahl $\neq 0$ und der Nenner eine natürliche Zahl $\neq 0$ ist.
Wir wählen

$$g(0) \quad := \quad 0 \ ;$$

und für jeden gekürzten Bruch $\frac{z}{y}$ mit $z \in \mathbb{Z} \setminus \{0\}$ und $y \in \mathbb{N}_{\geqslant 1}$ wählen wir

$$g\big(\tfrac{z}{y}\big) \quad := \quad \pi\big(f(z), y\big) \ .$$

Beachte: Wegen $y \geqslant 1$ und (2.2) ist

$$g\big(\tfrac{z}{y}\big) \quad \neq \quad 0 \ . \tag{2.3}$$

Klar: g ist eine Funktion von $\mathbb{Q}$ nach $\mathbb{N}$.
Wir zeigen nun, dass g injektiv ist. Seien dazu $q, q' \in \mathbb{Q}$ mit $g(q) = g(q')$.
Unser Ziel ist zu zeigen, dass $q = q'$ ist.

Fall 1: $g(q) = 0$.
Gemäß (2.3) und unserer Wahl von g ist dann $q = q' = 0$; insbes. ist $q = q'$.

Fall 2: $g(q) \neq 0$.
Gemäß unserer Wahl von g gilt dann: $q \neq 0$ und $q' \neq 0$. Wir stellen q und q' als gekürzte Brüche $\frac{z}{y}$ und $\frac{z'}{y'}$ mit Zählern $z, z' \in \mathbb{Z} \setminus \{0\}$ und Nennern $y, y' \in \mathbb{N}_{\geqslant 1}$ dar. Gemäß unserer Wahl von g gilt:

$$\pi\big(f(z), y\big) \quad = \quad g\big(\tfrac{z}{y}\big) \quad = \quad g\big(\tfrac{z'}{y'}\big) \quad = \quad \pi\big(f(z'), y'\big) \ .$$

Da π injektiv ist gilt $\big(f(z), y\big) = \big(f(z'), y'\big)$. Also ist $f(z) = f(z')$ und $y = y'$. Da f injektiv ist gilt $z = z'$. Also ist $z = z'$ und $y = y'$. Somit gilt auch: $\frac{z}{y} = \frac{z'}{y'}$, also $q = q'$.
Insgesamt haben wir gezeigt, dass die Funktion $g : \mathbb{Q} \to \mathbb{N}$ injektiv ist.
Somit ist $\mathbb{Q}$ abzählbar.

(b)*:* Wir führen einen Beweis durch Widerspruch. Angenommen, $\mathbb{R}$ wäre abzählbar. Dann gibt es eine injektive Funktion $f : \mathbb{R} \to \mathbb{N}$.
Wir zeigen, dass es dann auch eine injektive Funktion $g : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ gibt; dies steht dann im Widerspruch zu Satz 2.67.
Zur Definition der Funktion g gehen wir wie folgt vor.
Für jedes $M \subseteq \mathbb{N}$ und jedes $i \in \mathbb{N}$ sei

$$a_{M,i} \quad := \quad \begin{cases} 1 & \text{falls } i \in M \\ 0 & \text{sonst.} \end{cases}$$

Wir repräsentieren $M \subseteq \mathbb{N}$ durch die reelle Zahl r_M mit $0 \leqslant r_M < 1$, deren i-te Nachkommastelle die Ziffer $a_{M,i-1}$ ist (f.a. $i \in \mathbb{N}_{\geqslant 1}$). D.h.:

$$r_M \quad = \quad 0\ ,\ a_{M,0}\ a_{M,1}\ a_{M,2}\ a_{M,3} \cdots$$

Beispiele:

- $r_\emptyset \ = \ 0,000000\cdots \ = \ 0$
- $r_{\{0,1\}} \ = \ 0,1100000\cdots \ = \ 0,11$
- $r_{\{0,1,4\}} \ = \ 0,11001000000\cdots \ = \ 0,11001$
- $r_{\{i \in \mathbb{N} \,:\, i \text{ gerade}\}} \ = \ 0,10101010\cdots \ = \ 0,\overline{10}.$

Für jedes $M \subseteq \mathbb{N}$ setzen wir $g(M) := f(r_M)$.
Klar: g ist eine Funktion von $\mathcal{P}(\mathbb{N})$ nach $\mathbb{N}$.
Wir zeigen nun, dass g injektiv ist.
Seien dazu $M, M' \subseteq \mathbb{N}$ mit $g(M) = g(M')$. Unser Ziel ist zu zeigen, dass $M = M'$ ist.

Gemäß unserer Definition der Funktion g ist $f(r_M) = f(r_{M'})$.
Gemäß unserer Annahme ist f injektiv. Daher ist $r_M = r_{M'}$. Um den Beweis zu beenden, müssen wir hieraus noch folgern, dass $M = M'$ ist. Das hierfür nötige formale Argument liefern wir im nächsten Abschnitt nach (siehe Bemerkung 2.77). □

2.7 Darstellung von Zahlen

Folie 116

Vorsicht mit der Darstellung reeller Zahlen

Beobachtung 2.75. *Es gilt:* $0,\overline{9} \;=\; 1.$

Beweis. Sei

$$x \;:=\; 0,\overline{9} \;=\; 0,999999999\cdots$$

Dann gilt: $10 \cdot x \;=\; 9,\overline{9}$.
Und es gilt: $9 \cdot x \;=\; 10 \cdot x - x \;=\; 9,\overline{9} - 0,\overline{9} \;=\; 9$.
Teilen durch 9 liefert: $x = 1$. □

Im Folgenden schauen wir uns etwas genauer an, was hier passiert ist und wie wir korrekt mit der Darstellung reeller Zahlen umgehen können.

Folie 117

Ein Lemma, das man sich merken sollte

Lemma 2.76 (*Geometrische Summenformel*)**.**
Für alle $x \in \mathbb{R} \setminus \{1\}$ *und alle* $\ell \in \mathbb{N}$ *gilt:*

$$\sum_{i=0}^{\ell} x^i \;=\; \frac{x^{\ell+1} - 1}{x - 1}\,.$$

Beweis. Es gilt:

$$(x-1) \cdot \sum_{i=0}^{\ell} x^i \;=\; \sum_{i=1}^{\ell+1} x^i \;-\; \sum_{i=0}^{\ell} x^i \tag{2.4}$$

$$=\; x^{\ell+1} \;+\; \sum_{i=1}^{\ell} x^i \;-\; \sum_{i=1}^{\ell} x^i \;-\; x^0 \tag{2.5}$$

$$=\; x^{\ell+1} \;-\; 1\;. \tag{2.6}$$

Gemäß Voraussetzung ist $x - 1 \neq 0$. Somit liefert Teilen durch $(x-1)$, dass

$$\sum_{i=0}^{\ell} x^i \;=\; \frac{x^{\ell+1}-1}{x-1}\;.$$

$\square$

Bemerkung. Die in (2.4) bzw. (2.5) stehende Summe (sowie ähnliche Summen, bei denen sich die meisten Summanden gegenseitig wegheben), nennt man *Teleskopsumme*.

Folie 118

Details zur Darstellung reeller Zahlen

Bemerkung 2.77. Eine nicht-negative reelle Zahl stellen wir in der Form

$$n_0\;,\;n_1\;n_2\;n_3\;n_4\;\cdots$$

dar, wobei gilt: $n_0 \in \mathbb{N}$ und $n_i \in \{0,1,\ldots,9\}$ für jedes $i \in \mathbb{N}_{\geqslant 1}$. Dies ist genau die Zahl r, die man durch Ausrechnen des folgenden Ausdrucks erhält:

$$n_0 \;+\; \sum_{i=1}^{\infty} n_i \cdot \left(\tfrac{1}{10}\right)^i\;.$$

Um einzusehen, dass die "unendliche Summe" sinnvoll ist, kann man Lemma 2.76 für $x := \frac{1}{10}$ nutzen.

Daraus ergibt sich:

$$\sum_{i=0}^{\infty} \left(\tfrac{1}{10}\right)^i \;=\; \sum_{i=0}^{\infty} x^i \;=\; \lim_{\ell\to\infty} \sum_{i=0}^{\ell} x^i \;=\; \lim_{\ell\to\infty} \tfrac{x^{\ell+1}-1}{x-1}$$

$$=\; \lim_{\ell\to\infty} \tfrac{1-(\frac{1}{10})^{\ell+1}}{1-\frac{1}{10}} \;=\; \tfrac{1}{1-\frac{1}{10}} \;=\; \tfrac{1}{\frac{9}{10}} \;=\; \tfrac{10}{9}\;.$$

Somit ist

$$\sum_{i=1}^{\infty} \left(\tfrac{1}{10}\right)^i \;=\; \sum_{i=0}^{\infty} x^i \;-\; x^0 \;=\; \tfrac{10}{9} - 1 \;=\; \tfrac{1}{9}\,.$$

Daraus folgt:

$$\sum_{i=1}^{\infty} 9\cdot\left(\tfrac{1}{10}\right)^i \;=\; 9\cdot\sum_{i=1}^{\infty} \left(\tfrac{1}{10}\right)^i \;=\; 9\cdot\tfrac{1}{9} \;=\; 1\,,$$

d.h.: $0,999999\cdots = 1$ (was wir ja auch bereits in Beobachtung 2.75 festgestellt haben).

Folie 119

Auf ähnliche Art kann man sich davon überzeugen (Details: Übungsaufgabe), dass für jede Wahl von $n_0, \tilde{n}_0 \in \mathbb{N}$ und alle $n_i, \tilde{n}_i \in \{0,1,\ldots,9\}$ (f.a. $i \in \mathbb{N}_{\geqslant 1}$) die beiden Ausdrücke

$$n_0\,,\, n_1\; n_2\; n_3 \cdots \qquad \text{und} \qquad \tilde{n}_0\,,\, \tilde{n}_1\; \tilde{n}_2\; \tilde{n}_3 \cdots$$

genau dann *dieselbe* reelle Zahl beschreiben, wenn gilt:

- $n_i = \tilde{n}_i$ für alle $i \in \mathbb{N}$, oder
- es gibt ein $j \in \mathbb{N}$ s.d. gilt:
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $\tilde{n}_j = n_j{+}1$ und
    f.a. $i > j$ ist $n_i = 9$ und $\tilde{n}_i = 0$, oder
  - f.a. $i < j$ ist $n_i = \tilde{n}_i$ und
    $n_j = \tilde{n}_j{+}1$ und
    f.a. $i > j$ ist $\tilde{n}_i = 9$ und $n_i = 0$.

Am Ende des Beweises von Satz 2.74(b) benutzen wir, dass für alle Mengen $M, M' \subseteq \mathbb{N}$ mit $M \neq M'$ gilt: die im Beweis von Satz 2.74(b) betrachteten Darstellungen der reellen Zahlen r_M und $r_{M'}$ beschreiben *verschiedene* Zahlen (dies sieht man anhand der obigen Charakterisierung und der Tatsache, dass keine der beiden Darstellungen die Ziffer 9 enthält).

Folie 120

Darstellung natürlicher Zahlen zur Basis n

Wir sind es gewohnt, Zahlen im *Dezimalsystem* darzustellen. Zum Beispiel steht

$$1024 \qquad \text{für die Zahl} \qquad 4{\cdot}10^0 + 2{\cdot}10^1 + 0{\cdot}10^2 + 1{\cdot}10^3\ .$$

Das ist genau die Zahl 2^{10}, die sich im *Binärsystem* darstellen lässt als

$$10000000000 \quad \text{— dies steht für die Zahl} \quad \sum_{i=0}^{9} 0{\cdot}2^i \ + \ 1{\cdot}2^{10}.$$

An Stelle der Basis 10 (im Dezimalsystem) und der Basis 2 (im Binärsystem) kann man allgemein auch jede beliebige natürliche Zahl $n \geqslant 2$ als Basis benutzen. Zahlen werden dann unter Verwendung der Ziffern $0, 1, \ldots, n{-}1$ dargestellt. Für $\ell \in \mathbb{N}$ und $a_i \in \{0, 1, \ldots, n{-}1\}$ (f.a. $i \leqslant \ell$) steht dann

$$a_\ell \cdots a_1 a_0 \qquad \text{für die Zahl} \qquad \sum_{i=0}^{\ell} a_i{\cdot}n^i.$$

Zumeist vermeidet man "führende Nullen", d.h. man fordert, dass $a_\ell \neq 0$ ist.

Beispiel: Die zur Basis $n := 8$ (d.h. im *Oktalsystem*) geschriebene Darstellung

$$2000 \qquad \text{steht für die Zahl} \qquad 0{\cdot}8^0 + 0{\cdot}8^1 + 0{\cdot}8^2 + 2{\cdot}8^3 \ \ (\text{also } 2^{10}).$$

Folie 121

Eindeutigkeit der Darstellung natürlicher Zahlen zur Basis n

Der folgende Satz besagt, dass die Darstellung einer natürlichen Zahl zur Basis n eindeutig ist (d.h. jede natürliche Zahl hat genau *eine* Darstellung zur Basis n).

Satz 2.78. *Sei $n \in \mathbb{N}$ mit $n \geqslant 2$. Seien $\ell, m \in \mathbb{N}$ und seien $a_0, \ldots, a_\ell, b_0, \ldots, b_m \in \{0, 1, \ldots, n{-}1\}$ mit $a_\ell \neq 0$ und $b_m \neq 0$. Dann gilt:*

$$\sum_{i=0}^{\ell} a_i{\cdot}n^i \ = \ \sum_{j=0}^{m} b_j{\cdot}n^j \quad \Longleftrightarrow \quad \ell = m \ \ \textit{und} \ \ a_i = b_i \ \textit{f.a.} \ \ i \leqslant \ell.$$

Beweis. Die Richtung "$\Longleftarrow$" ist offensichtlich.
Zum Beweis der Richtung "$\Longrightarrow$" nutzen wir Lemma 2.76 (für $x := n$). Wir betrachten[4] o.B.d.A. den Fall, dass $\ell \geqslant m$ ist.[5] Gemäß Voraussetzung gilt $\sum_{i=0}^{\ell} a_i \cdot n^i = \sum_{j=0}^{m} b_j \cdot n^j$. Wir führen einen Beweis durch Widerspruch. Dazu nehmen wir an, dass $\ell \neq m$ ist oder dass es ein $i \leqslant \ell$ mit $a_i \neq b_i$ gibt.

Für alle $k \in \mathbb{N}$ mit $m < k \leqslant \ell$ setzen wir $b_k := 0$ und erhalten:

$$\sum_{i=0}^{\ell} b_i \cdot n^i \quad = \quad \sum_{j=0}^{m} b_j \cdot n^j \quad = \quad \sum_{i=0}^{\ell} a_i \cdot n^i \,. \tag{2.7}$$

Wir wählen nun die *größte* natürliche Zahl $k \leqslant \ell$ so dass $a_k \neq b_k$.[6]
Für jede natürliche Zahl $j \in G := \{i \in \mathbb{N} \;:\; k < i \leqslant \ell\}$ gilt dann $a_j = b_j$.

Falls $k = 0$ ist, so ist $a_i = b_i$ f.a. $i \in \{1, \ldots, \ell\}$, und daher

$$0 \quad = \quad \sum_{i=0}^{\ell} a_i \cdot n^i \; - \; \sum_{i=0}^{\ell} b_i \cdot n^i \quad = \quad a_0 - b_0 \,.$$

Dies ist ein Widerspruch zu $a_k \neq b_k$.
Somit gilt: $k \geqslant 1$.

Fall 1: $a_k > b_k$, d.h. $a_k \geqslant b_k{+}1$.
Dann ist

$$\sum_{i=0}^{\ell} b_i \cdot n^i \quad = \quad \sum_{i \in G} a_i \cdot n^i \; + \; b_k \cdot n^k \; + \; \sum_{i=0}^{k-1} b_i \cdot n^i \,. \tag{2.8}$$

Es gilt:

$$\begin{aligned} \sum_{i=0}^{k-1} b_i \cdot n^i \;\leqslant\; \sum_{i=0}^{k-1} (n{-}1) \cdot n^i \quad &= \quad (n{-}1) \cdot \sum_{i=0}^{k-1} n^i \\ &\overset{\text{Lem.2.76}}{=} \quad (n{-}1) \cdot \tfrac{n^k - 1}{n-1} \quad = \quad n^k - 1 \,. \end{aligned}$$

[4]"*o.B.d.A.*" steht für "ohne Beschränkung der Allgemeinheit"
[5]Diese Annahme ist tatsächlich "o.B.d.A.", weil der Fall $\ell < m$ durch Vertauschen der Rollen von ℓ und m genauso behandelt werden kann.
[6]Falls $\ell > m$ ist, so ist $k = \ell$. Aber falls $\ell = m$ ist, so könnte k auch $\leqslant \ell$ sein.

Gemeinsam mit (2.8) erhalten wir:

$$
\begin{aligned}
\sum_{i=0}^{\ell} b_i{\cdot}n^i \quad &\leqslant \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; b_k{\cdot}n^k \;+\; n^k - 1 \\
&< \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; (b_k{+}1){\cdot}n^k \\
&\leqslant \quad \sum_{i\in G} a_i{\cdot}n^i \;+\; a_k{\cdot}n^k \\
&\leqslant \quad \sum_{i=0}^{\ell} a_i{\cdot}n^i
\end{aligned}
$$

Somit ist also $\displaystyle\sum_{i=0}^{\ell} b_i{\cdot}n^i < \sum_{i=0}^{\ell} a_i{\cdot}n^i$. Dies ist ein Widerspruch zu (2.7).

Fall 2: $a_k \not< b_k$. Wegen $a_k \neq b_k$ gilt dann: $b_k > a_k$, d.h. $b_k \geqslant a_k{+}1$.
Dieser Fall kann analog zu Fall 1 behandelt werden, indem man die Rollen von $\sum_{i=0}^{\ell} a_i{\cdot}n^i$ und $\sum_{i=0}^{\ell} b_i{\cdot}n^i$ vertauscht (Details: Übungsaufgabe). □

Folie 122

"Plus 1"-Rechnen bei Darstellungen von Zahlen zur Basis n

Beispiel:
Wenn wir die im Dezimalsystem dargestellte Zahl 12999 um 1 erhöhen, erhalten wir die Zahl 13000.

Allgemein funktioniert "+1"-Rechnen im Dezimalsystem wie folgt:
Suche von rechts nach links die erste Ziffer $\neq 9$; erhöhe diese um 1 und ersetze bei jeder Ziffer rechts davon die 9 durch eine 0.
Spezialfall: Wenn *jede* Ziffer der Zahl eine 9 ist, dann häng ganz links eine neue Ziffer 0 an und gehe wie oben beschrieben vor.

Das gleiche Vorgehen funktioniert auch bei der Darstellung von Zahlen zur Basis n für jedes beliebige $n \in \mathbb{N}$ mit $n \geqslant 2$. Hierbei spielt dann die Ziffer $n{-}1$ die Rolle der Ziffer 9 im Dezimalsystem.

"+1"-Rechnen bei Darstellung einer Zahl zur Basis n:
Suche von rechts nach links die erste Ziffer $\neq n{-}1$; erhöhe diese um 1 und ersetze bei jeder Ziffer rechts davon die $n{-}1$ durch eine 0.
Spezialfall: Wenn *jede* Ziffer der Zahl eine $n{-}1$ ist, dann häng ganz links eine neue Ziffer 0 an und gehe wie oben beschrieben vor.

Folie 123

Beispiel 2.79. Im *Binärsystem* werden Zahlen dargestellt zur Basis $n := 2$.

Dezimalzahl	Binärzahl
0	0
1	1
2	10
3	11
4	100
5	101
6	110
7	111
8	1000
9	1001
10	1010

Antwort auf die Frage aus Beispiel 2.55:

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

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

Insbesondere gilt also zwar, dass $a_2 \in M''$, aber es gilt nicht, dass $a_2 \in M'$.

2.8 Literaturhinweise

Als vertiefende Lektüre seien die Kapitel 3, 6 und 7 in [MM00] empfohlen. Wertvolle Tipps und Tricks zur Formulierung mathematischer Gedanken und Beweise finden sich in [Beu02] und [Wol17]. Einen Crashkurs in die diskrete Mathematik für Informatiker*innen gibt das Buch [Juk08]. Eine umfassende Einführung in die Mengenlehre gibt das Lehrbuch [Ebb03].

Quellennachweis: Kapitel 2.1–2.5 sind dem Vorlesungsskript [Sch13] entnommen. Teile der Abschnitte 2.1–2.3 sowie 2.5 orientieren sich an [Gro07]. Teile von Abschnitt 2.4 orientieren sich an [MM00].