Mathematische Grundlagen

Quid est veritas?

- Wissenschaft dient dem Erkenntnisgewinn.
- In jedem Fachgebiet kann man viele Aussagen treffen: manche stimmen, manche nicht.
  - Beispiele in der Informatik:
    - Mit einem Carry-Chain-Schaltkreis kann man zwei ganze Zahlen addieren. ✓
    - Man kann ein Computerprogramm schreiben, das testet, ob ein beliebiges anderes Computerprogramm ungewollt in eine Endlosschleife laufen könnte. ✗
    - Für das Rucksackproblem gibt es eine effiziente Lösung. ?
- Wie findet man den Wahrhaltsgehalt solcher Aussagen?

Sätze, Lemmas, Korollare

- Nicht alle interessanten Aussagen sind wahr.
- Nicht alle wahren Aussagen sind interessant.
- Eine wahre Aussage von besonderem Interesse nennt man je nach Wichtigkeit:
  - Satz
  - Lemma
  - Korollar
- Aufgabe der Wissenschaft: Aussagen von besonderem Interesse identifizieren und nachweisen, dass diese wahr sind.
- Dies erfordert u.a. eine klare, eindeutige Sprache, um alle involvierten Konzepte präzise abzugrenzen.

Der naive Mengenbegriff

Unter einer ‚Menge' verstehen wir jede Zusammenfassung M *von bestimmten wohlunterschiedenen Objecten* m *unserer Anschauung oder unseres Denkens (welche die ‚Elemente' von* M *genannt werden) zu einem Ganzen.*

Georg Cantor (1895)

- Beispiele
  - Die Menge M_{EU} der Mitgliedsstaaten der EU: *{ Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, die Niederlande, Österreich, Polen, Portugal, Rumänien, Schweden, die Slowakei, Slowenien, Spanien, die Tschechische Republik, Ungarn, Zypern }*
  - Die Menge M_{dS} aller deutschen Sätze: *{ „Es regnet", „Ich gehe gleich einkaufen", ... }*

Der naive Mengenbegriff (2)

1. Mengen sind somit selbst Objekte unseres Denkens, die voneinander unterscheidbar sind.
    1. Mengen können Elemente von Mengen sein.
    2. Beispiel: die Menge der Beispielmengen der vorherigen Folie: $\{M_{EU}, M_{dS}\}$
2. Mengen können sich selbst enthalten.
    - Beispiel
        - Sei $M_{>2}$ die Menge aller Mengen mit mehr als zwei Elementen:
          $$M_{>2} = \{\, M_{EU}, M_{dS}, \{\text{"positiv", "negativ", "neutral"}\}, \ldots\}$$
        - Offensichtlich gilt dann: $M_{>2}$ ist ein Element von $M_{>2}$.

Der naive Mengenbegriff (3)

3. Es gibt also Mengen, die sich selbst enthalten, und solche, die sich nicht selbst enthalten.
   Sei R die Menge aller Mengen, die sich <u>nicht</u> selbst enthalten.
4. Frage: enthält R sich selbst oder nicht?
5. Wir betrachten die zwei möglichen Fälle:
   a) Annahme: R enthält sich selbst
      Dann muss R laut Definition eine Menge sein, die sich nicht selbst enthält. $\lightning$
   b) Annahme: R enthält sich selbst nicht
      Dann muss R laut Definition in R enthalten sein. $\lightning$

Ist das das Ende der Mengenlehre?

- Um das obige Paradox zu vermeiden, erlauben wir vorerst nur Mengen, die sich nicht selbst enthalten.
- Das Beispiel zeigt, dass wir sehr sorgfältig wir mit unseren Begrifflichkeiten umgehen müssen.

Notation für Mengen

- Als Bezeichner für Mengen wählen wir typischerweise einzelne Großbuchstaben, z.B. M
  - Zur weiteren Unterscheidung oder zur besseren Übersichtlichkeit können Bezeichner durch weitere Informationen in Subskript oder Superskript ergänzt werden, z.B.:
    - $M_{1,} M_{2,} M_{3,}$ usw.,
    - M'
    - $\widehat{M}$
- Ist x ein Element einer Menge M, sagen wir auch „M enthält x" und schreiben: $x \in M$. Ist dies nicht der Fall, schreiben wir: $x \notin M$
- Wenn $P(x)$ eine Eigenschaft beschreibt, bezeichnen wir mit dem Ausdruck $\{\ x \mid P(x)\ \}$ die Menge all derjenigen Elemente, auf die diese Eigenschaft zutrifft.

Beispiele

- $M_1 = \{1,2,3\}$
- $M_2 = \{2,4,6\}$
- Quiz: Was ist M_3?
  - (Noch) nicht definiert.
- $M_i = \{i, 2i, 3i\}$ für $i = 1$, $i = 2$, $i = 3$ usw…
- $N = \{\text{Montag, Dienstag, Mittwoch, Donnerstag, Freitag}\}$
- $I = \{|, ||, |||, ||||, |||||, \dots\}$
- $S = \{\, s \mid s \text{ studiert Informatik an der UdS}\}$

Mengenoperationen

- **Definition.** Seien A und B Mengen.

  Wir definieren die Mengen-Operationen $\subseteq, =, \cap, \cup, \setminus$ wie folgt:

  - $A \subseteq B$ gilt genau dann, wenn für alle $x \in A$ gilt: $x \in B$ **(Teilmenge)**
  - $A = B$ gilt gdw. $A \subseteq B$ und $B \subseteq A$ gelten **(Gleichheit)**
  - $A \cup B = \{\, x \mid x \in A \text{ oder } x \in B \,\}$ **(Vereinigungsmenge)**
  - $A \cap B = \{\, x \mid x \in A \text{ und } x \in B \,\}$ **(Schnittmenge)**
  - $A \setminus B = \{\, x \mid x \in A \text{ und } x \notin B \,\}$ **(Komplement)**

Quiz

- Sei $A = \{1, 2, 3\}$, $B = \{2, 3, 4\}$ und $C = \{2, 3\}$.
- Welche dieser Mengen sind Teilmengen von welchen anderen dieser Mengen?
  - $C \subseteq A, C \subseteq B, A \subseteq A, B \subseteq B, C \subseteq C$
- $A \cup B = \{1, 2, 3, 4\}$
- $A \cap B = \{2, 3\}$
- $A \backslash \mathrm{B} = \{1\}$

Mengenkompositionen

- **Definition (Leere Menge).** $\{\}$ bezeichnet die Menge, die keine Elemente enthält.
- **Definition.** Zwei Mengen A und B sind *disjunkt*, wenn gilt: $A \cap B = \{\}$.
- **Definition (Kartesisches Produkt).** Seien $M_1, M_2, \dots, M_n$ nicht-leere Mengen. Dann gilt $M_1 \times M_2 \times \cdots \times M_n = \{\, (x_1, x_2, \dots, x_n) \mid x_i \in M_i \text{ für alle } i \in \{1, 2, \dots, n\}\}$.
  - Elemente der Form $(x_1, x_2, \dots, x_n)$ heißen n-Tupel oder kurz Tupel oder Paare, falls $n = 2$.
- **Definition (n-faches Kartesisches Produkt).** Sei M eine Menge und n eine natürliche Zahl. Dann bezeichnet $M^n = \underbrace{M \times \cdots \times M}_{n\text{-mal}}$. Zudem gilt $M^0 = \{\}$.
- **Definition (Potenzmenge).** Sei M eine Menge. Dann bezeichnet $2^M = \{m | m \subseteq M\}$ die Menge aller Teilmengen von M.

Quiz

- Gilt $\{\} \in \{\}$?
  - Nein: die Leere Menge enthält nichts.
- Gilt $\{\} \subseteq \{\}$?
  - Ja.
  - Definition des „Teilmengen"-Operators:
    $A \subseteq B$ gilt genau dann, wenn für alle $x \in A$ gilt: $x \in B$
  - Hier: $A = \{\}$ und $B = \{\}$. In die Definition eingesetzt ergibt dies:
    $\{\} \subseteq \{\}$ gilt genau dann, wenn für alle $x \in \{\}$ gilt: $x \in \{\}$
  - Wäre $\{\}$ keine Teilmenge von $\{\}$, müsste es also mindestens ein $x \in \{\}$ geben, für das gilt: $x \notin \{\}$.
- Mit demselben Argument zeigt man: für alle Mengen M gilt $M \subseteq M$.

Mengen von Zahlen

- Wir bezeichnen mit
  - $\mathbb{N}$ die Menge der natürlichen Zahlen: $\mathbb{N} = \{1, 2, 3, \dots\}$
  - $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$
  - $\mathbb{Z}$ die Menge der ganzen Zahlen: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
  - $\mathbb{Q}$ die Menge der rationalen Zahlen, also derjenigen Zahlen, die als Bruch $\frac{x}{y}$ zweier ganzen Zahlen x, y mit $y \neq 0$ dargestellt werden können.
  - $\mathbb{R}$ die Menge der reellen Zahlen.
- Mathe-Vorlesung: “Körperaxiome”
  - Rechenoperationen $+, \cdot$
  - Darauf aufbauend $-, \div$ sowie für $n \in \mathbb{N}$ die n-te Potenz einer Zahl.
  - Algebra über einem Körper (Assoziativ-, Kommutativ- und Distributivgesetze)

Relationen

- Seien $M_1, \dots, M_n$ Mengen.
  Eine n-stellige *Relation* R ist eine Teilmenge $\mathrm{R} \subseteq M_1 \times \cdots \times M_n$.
- Gilt $M_1 = \cdots = M_n = M$ dann nennen wir R eine *Relation über* M.
- Beispiel: Sei S die Menge aller Fußballspieler, V die Menge aller Fußballvereine, J die Menge aller Jahre.
  Die Relation *spieltFür* $\subseteq S \times V \times J$ enthält ein Tripel (s, v, j) genau dann, wenn der Spieler s im Jahre j für den Verein v spielt(e).

  spieltFür = { (Thomas Müller, 1. FC. Bayern München, 2022),
  (Dzsenifer Marozsán, 1. FC Saarbrücken, 2008), …}


adidas


adidas

Binäre Relationen

- 2-stellige Relationen heißen auch *binäre* Relationen.
- Seien A, B Mengen. Für manche binäre Relationen $R \subseteq A \times B$ sind folgende Schreibweisen gebräuchlich, um $(a, b) \in R$ auszudrücken:
  - Präfixnotation: $R(a, b)$, seltener $R\ a\ b$
  - Infixnotation: $a\ R\ b$
  - (Postfixnotation: $a\ b\ R$)

Eigenschaften binärer Relationen

- **Definitionen.** Sei R eine binäre Relation über einer Menge A. R heißt:
  - *reflexiv* gdw. für alle $a \in A$ gilt: $(a, a) \in R$
  - *symmetrisch* gdw. für alle $a, b \in A$ gilt: $(a, b) \in R \Leftrightarrow (b, a) \in R$
  - *antisymmetrisch* gdw. für alle $a, b \in A$ gilt: $(a, b) \in R$ und $(b, a) \in R \;\Rightarrow a = b$
  - *transitiv* gdw. für alle $a, b, c \in A$ gilt: $(a, b) \in R$ und $(b, c) \in R \Rightarrow (\mathrm{a}, \mathrm{c}) \in R$
- **Definitionen.** Seien A,B Mengen und $\mathrm{R} \subseteq A \times \mathrm{B}$ eine Relation. R heißt:
  - *linkseindeutig* gdw. für alle $a, b, c \in A$ gilt: $(a, c) \in R$ und $(b, c) \in R \Rightarrow a = b$
  - *rechtseindeutig* gdw. für alle $a, b, c \in A$ gilt: $(a, b) \in R$ und $(a, c) \in R \Rightarrow b = c$
  - *linkstotal* gdw. es für alle $a \in A$ ein $b \in A$ gibt, sodass gilt: $(a, b) \in R$
  - *rechtstotal* gdw. es für alle $b \in A$ ein $a \in A$ gibt, sodass gilt: $(a, b) \in R$

Abkürzungen 1

- Da die Formulierungen „für alle“ und „es existiert“ bzw. „es gibt“ sehr häufig vorkommen, führen wir dafür eigene Symbole ein:
  - $\forall$ sei die Abkürzung für „für alle“
  - $\exists$ sei die Abkürzung für „es existiert“ und $\nexists$ die Abkürzung für „es existiert nicht“
- Sprechweisen werden kontextabhängig an die deutsche Grammatik angepasst.
- Beispiele:
  - $\forall x \in X$ gilt:...
    (lies: „für alle x der Menge X gilt...“)
  - $\exists a, b \in \mathbb{N}$ mit $a < b$ und...
    (lies: „es existieren zwei natürliche Zahlen a und b, sodass a kleiner als b ist und...)
  - $\forall x \in X\ \exists y \in Y$...
    (lies: „für alle x in X gibt es ein y in Y...“)

Abkürzungen 2

- Für eine beliebige Aussage A bezeichne der Ausdruck $\neg A$ das Gegenteil von A.
  - $A = \text{Es regnet.}$
  - $\neg A = \text{Es regnet nicht.}$
- Equivalenz
  - $A \Leftrightarrow B$ sei die Abkürzung für „A gilt genau dann wenn B gilt.“.
- Implikation
  - $A \Rightarrow B$ sei die Abkürzung für „Aus A folgt B.“.
  - $A \Leftarrow B$ sei die Abkürzung für „Aus B folgt A.“.

(Partielle) Funktionen

- **Definition.** Eine *partielle Funktion* ist eine rechtseindeutige binäre Relation.
- **Definition.** Eine *Funktion* ist eine linkstotale, rechtseindeutige binäre Relation.
- Aufgrund dieser Eigenschaften nennt man Funktionen auch „Abbildungen“.
- Ist f eine (partielle) Funktion und $(x, y) \in f$, dann bezeichnen wir y als den Funktionswert $f(x)$.
- Notation: statt $f \subseteq X \times Y$ schreiben wir normalerweise $f: X \to Y$.
  - X heißt Definitionsmenge von f
  - Y heißt Zielmenge oder Wertebereich von f
- Üblicherweise wird eine (partielle) Funktion nicht durch Aufzählung ihrer Elemente definiert, sondern mittels einer Abbildungsvorschrift, die angibt, auf welchen Wert $f(x)$ jedes $x \in X$ abgebildet wird: $x \mapsto f(x)$

Beispiel 1

- Sei X die Menge aller Studenten der Universität des Saarlandes.
- Sei $Y = \{\text{Januar, Februar, März, April, Mai, Juni, Juli, August, September, Oktober, November, Dezember}\}$.
- Die Funktion $g\colon X \to Y$ sei wie folgt definiert:

$$x \mapsto \text{Geburtsmonat von } x.$$

- Wie man sieht, muss man nicht alle Funktionswerte explizit kennen, um die Funktion definieren zu können.

Beispiel 2

- **Definition.** Sei M eine Menge. Die Funktion $|\cdot|$ sei wie folgt definiert:
  - Enthält M n Elemente mit $n \in \mathbb{N}_0$, so ist $|M| = n$.
  - Enthält M unendlich viele Elemente, so ist $|M| = \infty$.
- Der Definitionsbereich von $|\cdot|$ ist die Menge aller Mengen.
- Der Wertebereich von $|\cdot|$ ist $\mathbb{N}_0 \cup \{\infty\}$.

- $|\{\mathrm{rot}, \mathrm{gelb}, \mathrm{blau}\}| = 3$
- $|\mathbb{Z}| = \infty$

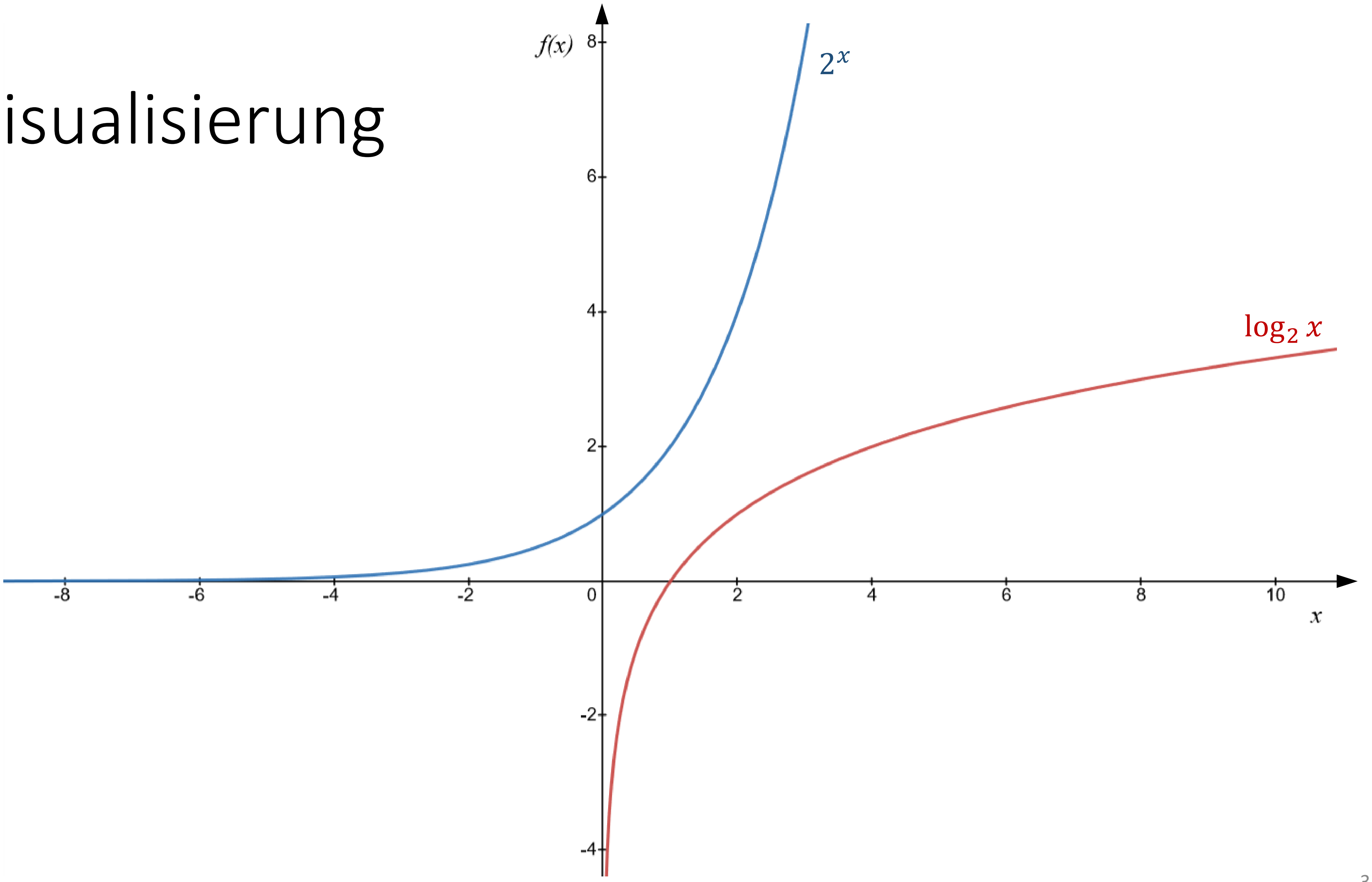
Injektiv, Surjektiv, Bijektiv - Umkehrfunktion

- Seien X, Y Mengen und $f\colon X \to Y$ eine Abbildung.
- **Definition.** f heißt *injektiv* oder *umkehrbar*, wenn es zu jedem $y \in Y$ höchstens ein $x \in X$ gibt mit $f(x) = y$.
- **Definition.** f heißt *surjektiv,* wenn es zu jedem $y \in Y$ mindestens ein $x \in X$ gibt mit $f(x) = y$.
- **Definition.** f heißt *bijektiv*, wenn f injektiv und surjektiv ist.
- **Definition.** Ist f injektiv, dann bezeichnen wir mit f^{-1}die partielle Funktion $\{(y, x) | f(x) = y\}$, genannt *Umkehrfunktion von* f. Ist f darüber hinaus auch surjektiv, dann ist f^{-1} eine Funktion.
  - Es gilt: $f\left(f^{-1}(x)\right) = f^{-1}\left(f(x)\right) = x$

Logarithmen und Potenzen

- Wir bezeichnen mit $\exp(x) = \mathrm{e}^{\mathrm{x}}$ die Exponentialfunktion und mit $\ln(x)$ den natürlichen Logarithmus (siehe Mathe-Vorlesung).
- **Definition.** Seien b, r reelle Zahlen mit $b > 0$. Wir definieren:
$$b^r = \exp(r \cdot \ln(b))$$
- **Definition.** Die Umkehrfunktion der Funktion $x \mapsto b^x$ heißt *Logarithmus zur Basis* b und wird geschrieben als $\log_b(x)$.
- **Notation**
  1. Solange dadurch keine Unklarheiten entstehen, lassen wir die Klammern um das Argument des Logarithmus weg, z.B.: $\log_{10} 5$, ln e
  2. Ist $b = 2$, lassen wir die Basis beim Logarithmus oft weg, z.B.: $\log 8$.

Visualisierung



Identitäten von Logarithmen und Potenzen

	Logarithmus	Potenz
0	$\log_b 0$ *nicht definiert*	$b^0 = 1$
1	$\log_b 1 = 0$	$b^1 = b$
b	$\log_b b = 1$	
Summe		$b^{x+y} = b^x \cdot b^y$
Differenz		$b^{x-y} = \frac{b^x}{b^y}$
Produkt	$\log_b xy = \log_b x + \log_b y$	$b^{xy} = (\mathrm{b}^x)^{\mathrm{y}}$
Quotient	$\log_b \frac{x}{y} = \log_b x - \log_b y$	$b^{\frac{x}{y}} = \sqrt[y]{b^x} = (\sqrt[y]{b})^x$
Potenzierung	$\log_b x^p = \mathrm{p} \cdot \log_b x$	

Axiome und Beweise

- Ein Beweis ist ein Argument dafür, dass eine gegebene Aussage (Satz, Lemma, Korrolar) wahr ist.
  - Genauer: dass die Aussage logisch aus zuvor getroffenen Annahmen folgt.
- Die initialen Annahmen nennt man Axiome.
  - Bereits bewiesene Aussagen können als Ausgangspunkt oder Hilfsmittel für die Beweise anderer Aussagen dienen.
- Spezifikation erlaubter Deduktionsschritte durch Formale Logik.

Beispiel Beweisargument

- **Lemma.** Für endliche, nicht-leere Mengen $M = \{\mathrm{m_1}, \dots, \mathrm{m_k}\}$ und $N = \{n_1, \dots n_l\}$ gilt: $|M \times N| = |M| \cdot |N| = k \cdot l$
- Beweis. Die Elemente von $M \times N$ lassen sich wie folgt in einem Rechteck anordnen:

$$M \times N = \left\{ \left.\underbrace{\begin{matrix} (m_1, n_1), & \dots, & (m_1, n_l), \\ \dots & & \dots \\ (m_k, n_1), & \dots, & (m_k, n_l) \end{matrix}}_{l \text{ Spalten}} \right\} \right\} k \text{ Zeilen}$$

qed.

Auswahl wichtiger Beweistechniken

- Equivalente Einsetzungen / Umformungen
- Fallunterscheidung
- Beidseitige Implikation
- Gegenbeispiel
- Beweis per Kontraposition
- Beweis per Widerspruch
- Vollständige Induktion

Equivalente Einsetzungen / Umformungen

- Aussagen, die auf einer transitiven Relation beruhen (z.B. mathematische Gleichheit, Equivalenz), können durch die Deduktion leicht nachvollziehbarer Zwischenschritte bewiesen werden.
- Beispiel: Zeige, dass gilt: $b^{xy} = (\mathrm{b}^{x})^{\mathrm{y}}$ für positive Basen b und $x, y \in \mathbb{R}$.
- Beweis: $b^{xy} = \exp(xy \cdot \ln(b))$; Definition b^r

$$= \exp(y \cdot (x \cdot \ln(b)))$$; Assoziativität/Kommutativität

$$= \exp(y \cdot \ln(\exp(x \cdot \ln(b))))$$; Umkehrfunktion $\ln/\exp$

$$= \exp(\mathrm{y} \cdot \ln(b^{x}))$$; Definition b^r

$$= (\mathrm{b}^{\mathrm{x}})^{\mathrm{y}}$$; Definition b^r

■

Fallunterscheidung

- Lässt sich eine Aussage A in eine Reihe von Teilaussagen aufteilen, die zusammen genommen A implizieren, genügt der Beweis der Teilaussagen.
- Beispiel: Ist n eine natürliche Zahl, dann ist $n^2 + n$ gerade.
- Beweis: Fall 1: n ist gerade. Dann gibt es eine natürliche Zahl k, sodass gilt: $n = 2k$. Somit gilt: $n^2 + n = (2k)^2 + 2k = 4k^2 + 2k = 2(2k^2 + k)$, d.h. $n^2 + n$ ist durch 2 teilbar. ■

  Fall 2: n ist ungerade. Dann gibt es eine natürliche Zahl k, sodass gilt: $n = 2k - 1$. Somit gilt: $n^2 + n = (2k - 1)^2 + 2k - 1$ $= 4k^2 - 4k + 1 + 2k - 1 = 4k^2 - 2k = 2(2k^2 - k)$. ■ *qed.*

Implikation in beide Richtungen

- Um die Aussage $A \Leftrightarrow B$ zu beweisen, kann man separat $A \Rightarrow B$ und $B \Rightarrow A$ zeigen.
- Beispiel. Sei x eine Zahl. Wir bezeichnen mit $\lfloor x \rfloor$ die größte ganze Zahl, die kleiner als oder gleich x ist, und mit $\lceil x \rceil$ die kleinste ganze Zahl, die größer als oder gleich x ist. Zeige, dass $\lfloor x \rfloor = \lceil x \rceil$ genau dann gilt, wenn x eine ganze Zahl ist.

Beweis

- "⇒": Sei $\lfloor x \rfloor = \lceil x \rceil$. Dann ist x eine ganze Zahl.
  Beweis: Gemäß Definition gilt bereits $\lfloor x \rfloor \leq x \leq \lceil x \rceil$. Wenn $\lfloor x \rfloor$ und $\lceil x \rceil$ nun aber gleich sind, muss auch $\lfloor x \rfloor = x = \lceil x \rceil$ gelten (Einschnürungssatz, siehe Mathe-Vorlesung). $\blacksquare$
- "⇐": Sei x eine ganze Zahl. Dann gilt $\lfloor x \rfloor = \lceil x \rceil$.
  Beweis: Gemäß Definition gilt $\lfloor x \rfloor = x$ und $\lceil x \rceil = x$ und somit auch $\lfloor x \rfloor = \lceil x \rceil$. $\blacksquare$

qed.

Gegenbeispiele

- Leider nicht möglich: „Beweis per Beispiel“
  - Beispiel: Behauptung: Männer können schneller laufen als Frauen.
  - “Beweis”: Den Weltrekord im 100m-Sprint hält Usain Bolt, der ein Mann ist. ■
- Jedoch zulässig: Widerlegung einer Behauptung durch ein Gegenbeispiel.
  - Beispiel Eulersche Vermutung: Die Gleichung $x_1^n + \cdots + x_{n-1}^n = \mathrm{x}_\mathrm{n}^\mathrm{n}$ hat keine ganzzahlige Lösung für $n > 3$.
  - Gegenbeispiel: $95800^4 + 217519^4 + 414560^4 = 422481^4$
- Ebenfalls zulässig: kann eine Behauptung für ein Element einer Menge gezeigt werden, ohne spezielle Annahmen zu diesem Element zu machen, folgt die Behauptung dadurch für alle Elemente der Menge.

Beweis per Kontraposition

- Eine Aussage der Form „Wenn A, dann B“ kann bewiesen werden, indem man die equivalente Umformung „Wenn $\neg B$, dann $\neg A$“ beweist.
- Beispiel: Zu zeigen: alle Primzahlen $p > 2$ sind ungerade.
- Beweis. Kontraposition: Ist $p > 2$ gerade, dann ist p keine Primzahl. Dies ist sofort ersichtlich, da 2 dann Teiler von p ist. $\blacksquare$

Beweis per Widerspruch

- Um eine Aussage A zu beweisen, nimmt man $\neg A$ an und zeigt, dass sich daraus ein Widerspruch ergibt.
- Beispiel: Es gilt: $\{\} \subseteq \{\}$
- Beweis s.o.

Beweis per vollständiger Induktion

- Eine Aussage $A(n)$ über alle natürlichen Zahlen n kann man beweisen, indem man sowohl $A(1)$ (*Induktionsanfang*) als auch die Implikation $A(n) \to A(n+1)$ (*Induktionsschritt*) für $n \geq 1$ beweist.

Beispiel

- Zeige: Es gilt: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$
- Beweis.

  Induktionsanfang ($n = 1$):

  $$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2} \quad \blacksquare$$

- Induktionsschritt ($n \to n+1$):

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

  qed.

Zahlendarstellungen

- Was ist eine Zahl überhaupt?
- Unterscheidung zwischen einer Zahl und ihrer Darstellung.
  - Beispiel: 7 und XII bezeichnen dieselbe Zahl, aber in unterschiedlichen Zahlschriften
  - Beispiel: $\frac{1}{2}$ und 0.5
- ∞ bezeichnet das Konzept “unendlich viele”, ist aber keine Zahl.

Darstellung natürlicher Zahlen

- Übliche Darstellung mittels der Ziffern $0, \dots, 9$, also zur Basis 10.
- Allgemein: seien $B \in \mathbb{N} \setminus \{1\}$ und $z = z_0, \dots, z_{B-1}$ eine Folge paarweise verschiedener Symbole. Eine n-stellige Zahldarstellung ($n \in \mathbb{N}$) zur Basis B ist eine Folge $a_{n-1} \dots a_0$, wobei für alle $0 \leq i < n$ gilt: $a_i \in \{z_0, \dots, z_{B-1}\}$.

  Die durch die Zahldarstellung $a = a_{n-1} \dots a_0$ dargestellte Zahl $\langle a \rangle_{B,z}$ ist

$$\langle a \rangle_{B,z} = \begin{cases} k\,, & \text{falls } n = 1 \text{ und } a_0 = z_k \\ k \cdot B^{n-1} + \langle a_{n-2} \dots a_0 \rangle_{B,z}, & \text{falls } n > 1 \text{ und } a_{n-1} = z_k \end{cases}$$

- Konkrete Wahl der Symbole $z_0, \dots, z_{B-1}$ spielt keine Rolle, daher kurz: $\langle a \rangle_B$
- Vorlesung: $B \leq 16$, $z = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, G, H$

Beispiele

- Die Zahldarstellung 123 stellt je nach Basis B folgenden Zahlen dar:
  - $B = 16$: $\langle 123 \rangle_{16} = 1 \cdot 16^2 + 2 \cdot 16^1 + 3 \cdot 16^0 = 1 \cdot 256 + 2 \cdot 16 + 3 \cdot 1 = 291$
  - $B = 10$: $\langle 123 \rangle_{10} = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 = 1 \cdot 100 + 2 \cdot 10 + 3 \cdot 1 = 123$
  - $B = 2$: $\langle 123 \rangle_2 = ?$ → nicht definiert, da 2 und 3 bei $B = 2$ nicht in z vorkommen.
- Je nach Basis werden für Zahldarstellung folgende Namen verwendet:
  - $B = 2$: Binärzahlen
  - $B = 8$: Oktalzahlen
  - $B = 10$: Dezimalzahlen
  - $B = 16$: Hexadezimalzahlen
- Die Verwendung von Dezimalzahlen mit führenden Nullen ist unüblich.
- Die Ziffern von Binärzahlen heißen Bits, Gruppen von 8 Bits heißen Bytes.

Anzahl aller n-stelligen Zahlendarstellungen

- **Satz.** Seien $B \in \mathbb{N} \backslash \{1\}$ und $n \in \mathbb{N}$. Für jede Symbolfolge $z = z_0, \ldots z_{B-1}$ gibt es genau B^n verschiedene n-stellige Zahlendarstellungen a zur Basis B.
- Beweis: per vollständiger Induktion über n.

  Induktionsanfang. Sei $n = 1$. Dann ist $a = a_0$ mit $a_0 \in \{z_0, \ldots, z_{B-1}\}$. ■

  Induktionsschritt ($n \to n + 1$). Sei $n \geq 1$ und $a = a_n \ldots a_0$ mit $a_i \in \{z_0, \ldots, z_{B-1}\}$ für alle $0 \leq i < n$.
  Wenn wir mit $|a|$ die Anzahl der möglichen Zahlendarstellungen a bezeichnen, gilt wegen $a_n \in \{z_0, \ldots, z_{B-1}\}$:

$$\begin{aligned}|a_n \ldots a_0| &= B \cdot |a_{n-1} \ldots a_0| \\ &= B \cdot B^{n-1} \\ &= B^n\end{aligned}$$

qed.

Ein Hilfslemma

- **Lemma.** Sei $n \in \mathbb{N}$. Dann existiert für jedes $m \in \mathbb{N}_0$ ein $i \in \mathbb{N}_0$, sodass gilt: $i \cdot n \leq m < (i+1) \cdot n$.
- Beweis. Sei $M = \{j \in N_0 \mid j \cdot n \leq m\}$. Diese Menge ist nicht leer, da sie mindestens das Element 0 enthält.
  Da alle endlichen, nicht-leeren Mengen reeller Zahlen ein maximales Element enthalten, können wir $i = \max(M)$ setzen. Da $i \in M$ ist, gilt per Definition: $i \cdot n \leq m$.
  Weiterhin kann $(i+1) \cdot n$ nicht kleiner oder gleich m sein, denn sonst wäre $i + 1 \in M$, und wegen $i < i + 1$ wäre i somit nicht das Maximum von M. Das widerspricht jedoch unserer Wahl von i, und daher muss gelten: $(i+1) \cdot n > m$. ■

Darstellungsvermögen

- **Satz.** Sei $B \in \mathbb{N} \backslash \{1\}$ eine Basis, $z_0, \dots, z_{B-1}$ eine Folge paarweise disjunkter Symbole und $n \in \mathbb{N}$. Dann gibt es für jede Zahl $m \in \{0, \dots, B^n - 1\}$ eine n-stellige Zahlendarstellung $a = a_{n-1} \dots a_0$ zur Basis B, sodass gilt: $\langle a \rangle_{B,z} = m$.

  Beweis. Induktionsanfang. Sei $n = 1$. Dann gilt per Definition: $\langle z_m \rangle_{B,z} = m$. ■

  Induktionsschritt. Sei $n > 1$. Setze $i \in \mathbb{N}_0$ so, dass $i \cdot B^{n-1} \leq m < (i+1) \cdot B^{n-1}$ und setze $l = m - i \cdot B^{n-1}$.

$$
\begin{array}{lrcl}
 & i \cdot B^{n-1} & \leq \quad m & < (i+1) \cdot B^{n-1} \\
\Leftrightarrow & i \cdot B^{n-1} - i \cdot B^{n-1} & \leq m - i \cdot B^{n-1} & < (i+1) \cdot B^{n-1} - i \cdot B^{n-1} \\
\Leftrightarrow & 0 & \leq \quad l & < B^{n-1}
\end{array}
$$

  Nach Induktionsannahme gibt dann es eine $n-1$-stellige Zahlendarstellung $a_{n-2} \dots a_0$ der Zahl l. Da $m < B^n$, gilt auch $i \cdot B^{n-1} < B^n$ und daher $i < B$. Setzen wir $a_{n-1} = z_i$, erhalten wir:

$$
\begin{aligned}
\langle a_{n-1} \dots a_0 \rangle_{B,z} &= i \cdot B^{n-1} + \langle a_{n-2} \dots a_0 \rangle_{B,z} \\
&= i \cdot B^{n-1} + l \\
&= m
\end{aligned}
$$

qed.

Darstellung ganzer Zahlen

- Zur Darstellung negativer ganzer Zahlen verwendet man bei Dezimalzahlen ein gesondertes Zeichen (-) vor der Zahl.
- Bei Binärzahlen kann man zu demselben Zweck ein weiteres Bit s verwenden:

$$\left\langle\langle s a_{n-1} \dots a_0 \rangle\right\rangle_2 = \begin{cases} \langle a_{n-1} \dots a_0 \rangle_2, & \text{falls } s = 0 \\ -\langle a_{n-1} \dots a_0 \rangle_2, & \text{falls } s = 1 \end{cases}$$

- Diese Kodierung hat aber ein paar Nachteile, z.B. zwei Darstellungen der Null.

Zweierkomplement

- Alternative Darstellung von negativen Binärzahlen:

$$\left\langle\langle s a_{n-2} \dots a_0 \rangle\right\rangle_2 = \begin{cases} \langle a_{n-2} \dots a_0 \rangle_2, & \text{falls } s = 0 \\ \langle a_{n-2} \dots a_0 \rangle_2 - 2^{n-1}, & \text{falls } s = 1 \end{cases}$$

- Beispiele
  - $\left\langle\langle 0010 \rangle\right\rangle_2 = 2$
  - $\left\langle\langle 1111 \rangle\right\rangle_2 = -1$
  - $\left\langle\langle 1000 \rangle\right\rangle_2 = -8$

Zweierkomplement

- **Satz:** Mit einer n-stelligen Zweierkomplementzahl lassen sich genau die Zahlen im Bereich $\{-2^{n-1}, \dots, 2^{n-1} - 1\}$ darstellen.

  Beweis: Aus den Sätzen auf den Folien 49 und 51 folgt, dass $\left\langle\langle s a_{n-2} \dots a_0 \rangle\right\rangle_2$ für den Fall $s = 0$ alle Zahlen im Bereich $\{0, \dots, 2^{n-1} - 1\}$ darstellen kann.
  Subtrahiert man von diesen Zahlen 2^{n-1}, erhält man alle Zahlen, die für den Fall $s = 1$ dargestellt werden können, nämlich $\{-2^{n-1}, \dots, -1\}$. Zusammen folgt die Behauptung. *qed.*

Zusammenfassung

- Mengen (Notation, Operationen, Leere Menge, Mengen von Zahlen)
- Relationen, Funktionen (log, exp)
- Sätze, Lemmas, Korrolare
- Axiome und Beweise
  - 7 Beweistechniken
- Zahlendarstellungen
  - Zweierkomplement