Mathematik I:
Theoretische Grundlagen der Informatik

Prof. Dr.-Ing. Sebastian Schlesinger

8. Januar 2025

Warum Mathematik?

- Mathematik ist die Sprache der Informatik
- Informatik ist aus der Mathematik entstanden
- Abstraktion ist eine Schlüsselkompetenz der Informatik
- Grundlegende Datenstrukturen, Algorithmen und Konzepte sind mathematisch
- Mathematik ist wie Programmiersprachen eindeutig und präzise

Ziele

- Einführung in die mathematische Denkweise
- Fähigkeit, mathematische Beweise zu verstehen und selbst zu führen
- Einführung in die Sprache der Mathematik: Aussagen- und Prädikatenlogik

Ziele

- Einführung in die mathematische Denkweise
- Fähigkeit, mathematische Beweise zu verstehen und selbst zu führen
- Einführung in die Sprache der Mathematik: Aussagen- und Prädikatenlogik
- Grundlagen der diskreten Mathematik:
  - Mengenlehre
  - Relationen
  - Funktionen
  - Verbände

Ziele

- Einführung in die mathematische Denkweise
- Fähigkeit, mathematische Beweise zu verstehen und selbst zu führen
- Einführung in die Sprache der Mathematik: Aussagen- und Prädikatenlogik
- Grundlagen der diskreten Mathematik:
  - Mengenlehre
  - Relationen
  - Funktionen
  - Verbände

Out of scope: Theoretische Informatik (z.B. Berechenbarkeitstheorie, Komplexitätstheorie)

Agenda

1. Einführung
2. Aussagenlogik
3. Prädikatenlogik
4. Diskrete Mathematik
   - Mengenlehre
   - Relationen
   - Funktionen

Agenda

Aussagen

Unter einer **Aussage** versteht man einen sprachlichen Ausdruck, dem man eindeutig einen der beiden Wahrheitswerte w („wahr“) bzw. f („falsch“) zuordnen kann.
Aussagen werden mit Großbuchstaben bezeichnet,

$$A : Beschreibung$$

und können mit logischen Operationen verknüpft werden.
Grundlegende mathematische Aussagen, die nicht aus anderen Aussagen abgeleitet werden können, nennt man **Axiome**.

Beispiele von Aussagen

- Wahre Aussage A: Jede natürliche Zahl ist ein Produkt von Primzahlen.
- Falsche Aussage B: Jede Primzahl ist ungerade
- Unbewiesene Vermutung (wahr oder falsch, d.h. eine Aussage, bei der der Wahrheitswert noch nicht entschieden werden konnte) C: Es gibt unendlich viele Primzahlzwillinge.
- Keine Aussage (Feststellung ohne Wahrheitswert) D: Freitag der dreizehnte ist ein Unglückstag.

Logische Operationen

Logische Aussagen können durch die in der folgenden Tabelle angegebenen Operationen verknüpft werden.

Bezeichnung	Schreibweise	(Sprechweise)	wahr, gdw
Negation	$\neg A$	(nicht A)	A falsch ist
Konjunktion	$A \wedge B$	(A und B)	A und B wahr sind
Disjunktion	$A \vee B$	(A oder B)	A oder B wahr ist
Implikation	$A \Rightarrow B$	(wenn A dann B)	A falsch oder B wahr
Äquivalenz	$A \Leftrightarrow B$	(A äquivalent B)	A und B äquivalent

Bindungsstärke

Um in logischen Ausdrücken Klammern zu sparen, wird festgelegt, dass $\neg$ stärker bindet als $\wedge$ sowie $\vee$ und diese wiederum stärker als $\Rightarrow, \Leftrightarrow$.

Wahrheitstabelle

In der folgenden Tabelle sind die Wahrheitswerte der vorgestellten Verknüpfungen angegeben. Dabei steht w für wahr und f für falsch.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
w	w	f	w	w	w	w
w	f	f	f	w	f	f
f	w	w	f	w	w	f
f	f	w	f	f	w	w

Hinweis: Statt w für *wahr* und f für *falsch* werden auch die Symbole $\top$ und $\bot$ verwendet.

Gesetze für logische Operationen

Für logische Operationen gelten die folgenden Identitäten.

- Assoziativgesetze:

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

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

- Kommutativgesetze:

$$A \wedge B = B \wedge A$$

$$A \vee B = B \vee A$$

- Distributivgesetze:

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

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

Gesetze für logische Operationen

Für logische Operationen gelten die folgenden Identitäten.

- De Morgansche Regeln:

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

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

- Idempotenz:

$$\neg(\neg A) = A$$

$$A \vee A = A$$

$$A \wedge A = A$$

- Kürzungsregeln:

$$A \vee \bot = A$$

$$A \wedge \top = A$$

Agenda

Quantoren

Wir führen nun Quantoren ein. Neben den atomaren Aussagen der Aussagenlogik möchte man in der Lage sein, Aussagen zu formulieren, die praktisch von Parametern abhängen.

Definition (Quantoren)

Wir definieren folgende Notation:

- Mit $\forall x : A(x)$ definieren wir, dass eine Aussage A, die eine Variable x beinhaltet, für alle Werte von x gelten soll (üblicherweise wird dann auch eine Grundmenge, aus denen die x stammen sollen, angegeben).
- Mit $\exists x : A(x)$ drücken wir aus, dass es ein x geben soll, so dass $A(x)$ gilt.

Die Aussagen $A(x)$ können komplexe Aussagen mit Verknüpfungen sein und es lassen sich auch Quantoren kombinieren und man kürzt oft ab.

Beweismethoden

Wie führt man nun einen Beweis? Es gibt verschiedene Beweismethoden. Die wichtigsten sind:

- Direkter Beweis: Man beweist direkt $A \Rightarrow B$, also dass B aus der Annahme von A folgt.
- Man verwendet die Umkehrung von $A \Rightarrow B$, also $\neg B \Rightarrow \neg A$
- Indirekter Beweis: Man nimmt an, A gelte und folgert dann B, was aber im Widerspruch zu A ist. Praktisch folgert man also $A \wedge \neq A$, was falsch sein muss. Also muss die Annahme falsch gewesen sein und da sie das Gegenteil von dem ist was man beweisen möchte, ist der Beweis komplett.

Agenda

Mengendefinition

Definition (Naive Mengendefinition)

Eine Menge ist die Zusammenfassung von bestimmten unterschiedlichen Objekten (die Elemente der Menge) zu einem neuen Ganzen. Wir schreiben $x \in M$, falls das Objekt x zur Menge M gehört. Wir schreiben $x \notin M$, falls das Objekt x nicht zur Menge M gehört. Falls $x \in M$ und $y \in M$ gilt, schreiben wir auch $x, y \in M$. Eine Menge, welche nur aus endlich vielen Objekten besteht (eine endliche Menge), kann durch explizite Auflistung dieser Elemente spezifiziert werden.

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

$$\{2, 3, 5, 7\} = \{7, 5, 3, 2\}$$

Auch Mehrfachauflistungen spielen keine Rolle:

$$\{2, 3, 5, 7\} = \{2, 2, 2, 3, 3, 5, 7\}$$

Mengennotation

Mengen können definiert werden durch

- Aufzählung der Elemente
- Formulierung von Bedingungen in der Form $M := \{x|p(x)\}$, wobei p ein *Prädikat*, also eine Aussage ist, die x enthält, so dass man jeweils bei Einsetzen von x entscheiden kann, ob sie wahr (und damit das Element zur Menge gehört) oder falsch ist (und damit das Element x nicht zu M gehört).

Wir schreiben zur Abkürzung auch $M := \{x \in N|p(x)\}$ statt $M := \{x|x \in N \wedge p(x)\}$.

Besondere Mengen

Eine besonders wichtige Menge ist die leere Menge $\emptyset = \{\}$, die keinerlei Elemente enthält.
In der Mathematik hat man es häufig auch mit unendlichen Mengen zu tun (Mengen, die aus unendlich vielen Objekten bestehen). Solche Mengen können durch Angabe einer Eigenschaft, welche die Elemente der Menge auszeichnet, spezifiziert werden.
Beispiele:

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q} = \{\frac{p}{q} | p, q \in \mathbb{Z}, q \neq 0\}$

Warum naive Mengenlehre?

Die „Definition“der Menge ist anfällig für Widersprüche, z.B. die **Russelsche Antinomie**:
Man bilde die Menge aller Mengen, die sich nicht selbst als Element enthalten, in Formeln:

$$M := \{N | N \notin N\}$$

Frage: Gilt $M \in M$? Das führt auf einen Widerspruch.
Daher hat man die Mengenlehre mit dem **Zermelo-Fraenkelschen Axiomensystem** auf ein solides Fundament gehoben. Mehr dazu im optionalen Inhalt (ist zu kompliziert für eine erste Einführung).

Teilmengen

Definition (Teilmenge)

Seien A und B Mengen. $A \subseteq B$ bedeutet A ist *Teilmenge* von B, genau dann, wenn

$$\forall x : x \in A \Rightarrow x \in B$$

oder äquivalent dazu

$$\forall x \in A : x \in B$$

Lemma (Gleichheit von Mengen)

Seien A und B Mengen. Es ist $A = B$ genau dann, wenn $\forall x : x \in A \Leftrightarrow x \in B$, was wiederum äquivalent ist zu

$$A \subseteq B \land B \subseteq A$$

Um also die Gleichheit von zwei Mengen zu zeigen beweist man üblicherweise erst $A \subseteq B$ und dann $B \subseteq A$.

Mengenoperationen

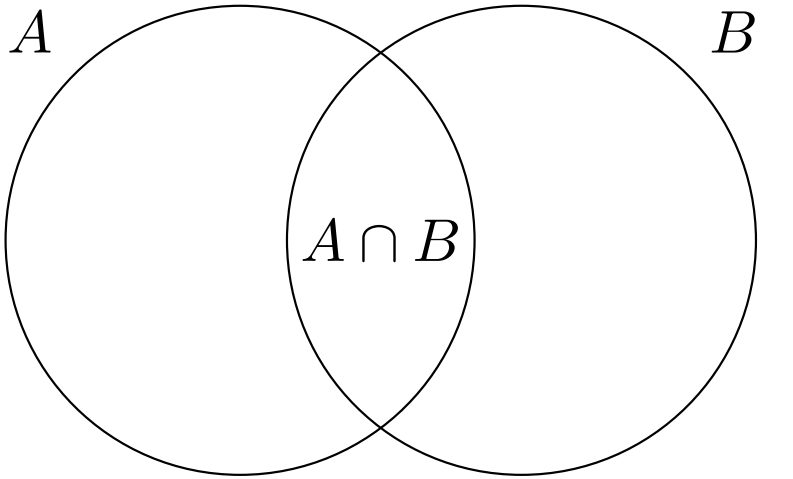
Definition (Mengenoperationen)

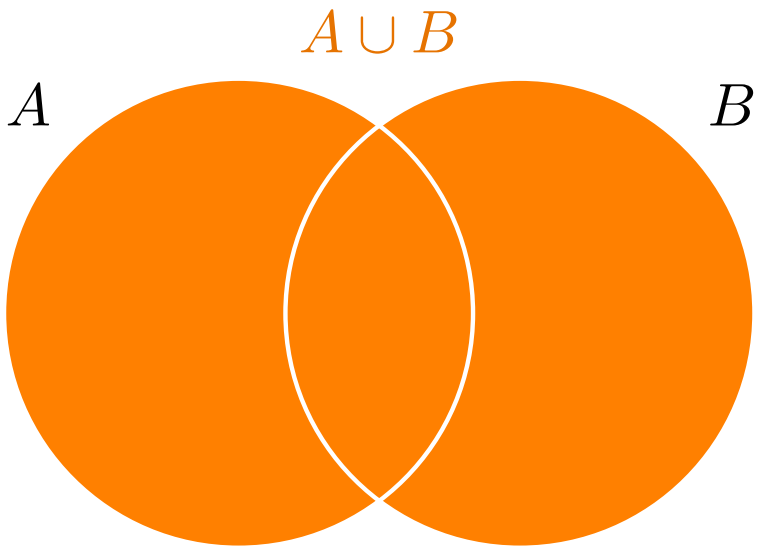
Seien A und B Mengen. Wir definieren:

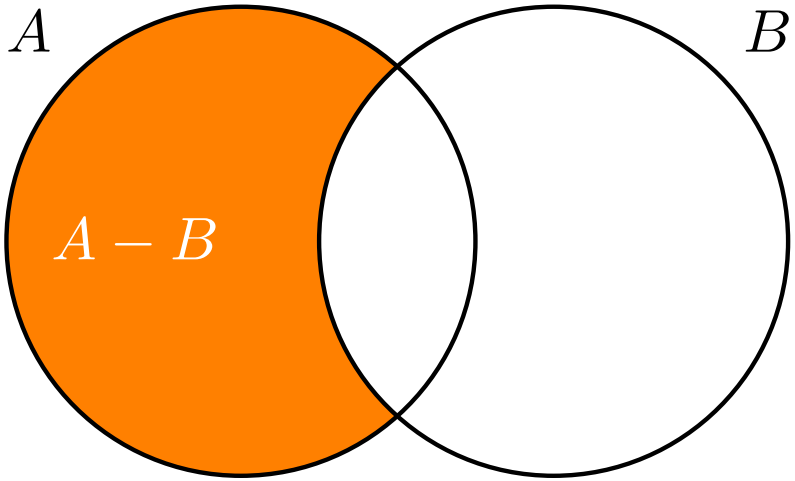
- $A \cap B := \{x | x \in A \land x \in B\}$, den *Schnitt* von A und B
- $A \cup B := \{x | x \in A \lor x \in B\}$, die *Vereinigung* von A und B
- $A \backslash B := \{x \in A | x \notin B\}$, die *Differenz* von A und B

Venn-Diagramme

Die Operationen lassen sich in **Venn-Diagrammen** visualisieren.







Weitere Mengen und Eigenschaften

Definition (Potenzmenge)

Mit

$$\mathscr{P}(A) := 2^A := \{B | B \subseteq A\}$$

bezeichnen wir die **Potenzmenge**, die Menge aller Teilmengen von A.

Definition (Disjunktheit)

Zwei Mengen A und B sind *disjunkt*, falls $A \cap B = \emptyset$ gilt.

Beispiele für Mengenaussagen

Es gilt:

- $\forall A : \emptyset \subseteq A$
- $\forall A : A \subseteq A$
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\{1, 2, 3\} \cap \{4, 5, 6\} = \emptyset$
- $\mathscr{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1.2\}\}$
- $\mathscr{P}(\emptyset) = \{\emptyset\}$
- $\forall A : A \cap \emptyset = \emptyset$
- $\forall A : A \cup \emptyset = A$
- $\forall A, B, C : A \cap (B \cup C) = (A \cap B) \cup (B \cap C)$
- $\forall A, B, C : A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $\forall A, B, C : A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$
- $\forall A, B, C : A \backslash (B \cap C) = (A \backslash B) \cap (A \backslash C)$

Agenda

Kartesisches Produkt

Zunächst führen wir Paare ein. Diese werden, im Gegensatz zu Mengen mit runden Klammern notiert, z.B. $(1, 2)$ das Paar, dessen erste Komponente die Zahl 1 und zweite Komponente 2 ist. Hier kommt es auf die Reihenfolge an, z.B. $(1, 2) \neq (2, 1)$, aber $\{1, 2\} = \{2, 1\}$, weil es bei Mengen nur auf die Elemente, nicht auf deren Reihenfolge ankommt.
Es gilt insbesondere

$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d$$

Definition (Kartesisches Produkt)

Seien M, N Mengen. Dann ist

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

das **kartesische Produkt** von M und N.

Relationen

Relationen sind intuitiv Strukturen, um Beziehungen zwischen Objekten auszudrücken.

Definition (Relationen)

Seien M und N Mengen. Eine Teilmenge R des kartesischen Produktes $M \times N$, also

$$R \subseteq M \times N$$

nennen wir **Relation** von M auf N.

Beispiele von Relationen

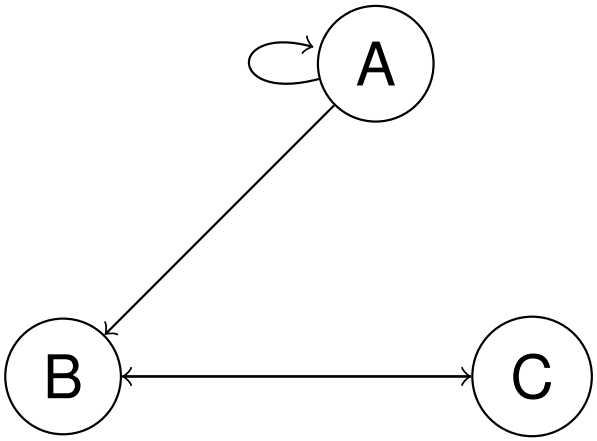
Ist M die Menge der Menschen, dann ist $R \subseteq M \times M$ die Eltern-Kind-Beziehung ein Beispiel für eine Relation. Also $(x, y) \in R \Leftrightarrow x$ ist Elternteil von y.
Ein anderes Beispiel ist die $\leq$ Relation auf $\mathbb{N}$, also $(x, y) \in R \subseteq \mathbb{Z} \times \mathbb{Z} \Leftrightarrow x \leq y$.
Generell kann man eine Relation zwischen zwei Elementen auf zwei Arten notieren: auf die herkömmliche Weise, also $(x, y) \in R$ oder mittels **Infixschreibweise** xRy.

Darstellung von Relationen

Eine Möglichkeit ist die Angabe als Menge, z.B.

$$R = \{(A, B), (A, A), (B, C), (C, B)\}$$

Eine Alternative ist ein Graph.



Darstellung von Relationen

Eine andere ist die einer Matrix.

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Hier kann man sich die Zeilen und Spalten der Matrix annotiert mit den Elementen der Grundmengen denken. Etwas formaler: Eine **Adjazenzmatrix** einer Relation $R \subseteq M \times N$ mit $M = \{x_1, ..., x_m\}$ und $N = \{y_1, ..., y_n\}$, also m Elementen in M und n Elementen in N, die man sich geordnet vorstellen kann (über die Indizierung) ist eine Matrix (a_{ij}) mit $1 \leq i \leq m, 1 \leq j \leq n$ und für die Einträge a_{ij} in Zeile i und Spalte j gilt:

$$a_{ij} = 1 \Leftrightarrow (x_i, y_j) \in R, a_{ij} = 0 \Leftrightarrow (x_i, y_j) \notin R$$

Eigenschaften von Relationen

Relationen sind in höchster Allgemeinheit definiert. Nun kann man bestimmte Eigenschaften untersuchen.

Definition

Sei $R \subseteq M \times M$ eine Relation über einer Menge M (Man beachte, dass die Elemente nur aus einer Menge M stammen). Dann ist R

1. **reflexiv**, wenn $\forall x \in M : (x, x) \in R$
2. **irreflexiv**, wenn $\forall x \in M : (x, x) \notin R$
3. **symmetrisch**, wenn $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \in R$
4. **antisymmetrisch**, wenn
   $\forall x, y \in M : (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$
5. **asymmetrisch**, wenn $\forall x, y \in M : (x, y) \in R \Rightarrow (y, x) \notin R$
6. **transitiv**, wenn $\forall x, y, z \in M : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Komposition von Relationen

Definition (Komposition von Relationen)

Seien $R \subseteq M \times N, S \subseteq N \times P$. Wir definieren

$$R \circ S = \{(x, z) \in M \times P | \exists y \in N : (x, y) \in R \wedge (y, z) \in S\}$$

als **Komposition** von R und S.

Die Komposition ist praktisch die „Hintereinanderschaltung“der Relationen R und S.

Algorithmische Berechnung der Komposition (Matrixmultiplikation)

Example

Seien R und S zwei Relationen auf den Mengen M und N mit den Adjazenzmatrizen:

$$R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \quad \text{und} \quad S = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Sei $R = (\alpha_{i,j})_{1 \leq i,j \leq n}$, $S = (\beta_{i,j})_{1 \leq i,j \leq n}$ Um das (i,j)-te Element von $R \circ S$, $\gamma_{i,j}$ zu berechnen, definieren wir $\gamma_{i,j} = \bigvee_{\nu=1}^{n} \alpha_{i,\nu} \wedge \beta_{\nu,j}$. Das bedeutet, dass wir das Element der Zielmatrix in Zeile i und Spalte j so erhalten, indem wir die $i-$te Zeile von R und die $j-$te Spalte von S durchgehen und suchen, ob 1 auf 1 trifft. Finden wir ein Paar, wird das Zielelement 1, sonst 0.

Ordnungen und Äquivalenzrelationen

Definition (Ordnung)

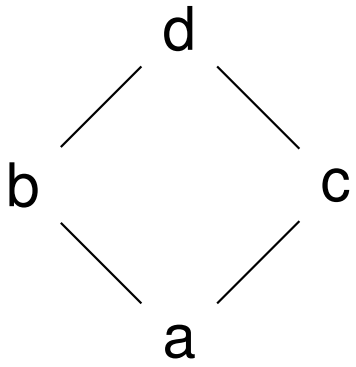
Eine Relation $R \subseteq M \times M$ heißt **Ordnung**, wenn sie reflexiv, antisymmetrisch und transitiv ist.

Definition (Äquivalenzrelation)

Eine Relation $R \subseteq M \times M$ heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

Hasse-Diagramme

Hasse-Diagramme sind eine spezielle Art von Graphen, die Ordnungen visualisieren. Sie sind besonders nützlich, um die Struktur von Ordnungen zu verdeutlichen.



In dem Beispiel ist die Ordnung $\{(a,a),(a,b),(a,c),(a,d),(b,b),(b,d),(c,c),(c,d),(d,d)\}$ dargestellt. Die Idee ist, die reflexiven und transitiven Beziehungen nicht darzustellen. Sie gelten implizit. Und gilt aRb in der Ordnung R, dann wird a unterhalb von b angeordnet und beide werden mit einer Linie verbunden.

Partitionen

Definition (Partition)

Eine Partition einer Menge M ist eine Menge von nicht-leeren Teilmengen $\{A_i\}_{i \in I}$, so dass

- $\bigcup_{i \in I} A_i = M$ (die Vereinigung aller Teilmengen ergibt die Menge M)
- $A_i \cap A_j = \emptyset$ für alle $i \neq j$ (die Teilmengen sind paarweise disjunkt)

Example

Sei $M = \{1, 2, 3, 4\}$. Eine mögliche Partition von M ist $\{\{1, 2\}, \{3, 4\}\}$.

Zusammenhang von Partitionen und Äquivalenzrelationen

- Jede Äquivalenzrelation auf einer Menge M definiert eine Partition von M.
- Umgekehrt definiert jede Partition einer Menge M eine Äquivalenzrelation auf M.

Example

Sei $M = \{1, 2, 3, 4\}$ und die Partition $\{\{1, 2\}, \{3, 4\}\}$. Die entsprechende Äquivalenzrelation ist:

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

Zusammenhang von Partitionen und Äquivalenzrelationen

Definition (Menge der Äquivalenzklassen)

Sei R eine Äquivalenzrelation auf einer Menge M. Die Menge der Äquivalenzklassen von M bzgl. R (auch bezeichnet als Quotienten- oder Faktormenge) ist definiert als:

$$M/R := \{[x]_R \mid x \in M\}$$

wobei $[x]_R := \{y \in M \mid (x, y) \in R\}$ die Äquivalenzklasse von x bzgl. R ist.

Es gilt, dass zu jeder Äquivalenzrelation $R \subseteq M \times M$ die Menge der Äquivalenzklassen M/R eine Partition bildet. Umgekehrt gibt es zu jeder Partition $P \subseteq \mathscr{P}(M)$ eine passende Äquivalenzrelation $R \subseteq M \times M$, so dass also $M/R = P$.

Reflexiv-transitive Hülle

Zu jeder Relation $R \subseteq M \times M$ lässt sich die reflexiv-transitive Hülle R^* bilden. Das ist die kleinste (im Sinne $\subseteq$) R enthaltende Relation, die reflexiv und transitiv ist.
Es gilt $R^* = \bigcup_{n=0}^{\infty} R^n$ mit $R^0 = Id$, $R^{n+1} = R^n \circ R$. Dabei ist $Id = \{(x, x) | x \in M\}$ die Relation, die jedes Element und nur diese mit sich selbst in Beziehung setzen.
Bei endlichen Mengen kann man R^* berechnen, indem man so lange R^n hinzufügt bis $\bigcup i = 0^n R^i$ stationär wird.

Agenda

1. Einführung
2. Aussagenlogik
3. Prädikatenlogik
4. Diskrete Mathematik
   - Mengenlehre
   - Relationen
   - Funktionen

Funktionen

Funktionen sind spezielle Relationen, die jedem Element im Urbildraum (der ersten Menge im kartesischen Produkt) genau ein ELement im Bildraum zuordnen.

Definition (Funktionen)

Eine Relation $f \subseteq M \times N$ heißt **Funktion**, wenn

$$\forall x \in M \exists y \in N : (x, y) \in f \wedge \forall y' \in N : (x, y') \in f \Rightarrow y = y'$$

Da somit das mit einem Element x in Relation stehende Element y eindeutig bestimmt ist, schreiben wir auch $y = f(x)$ und bezeichnen y als **das Bild** von x.

Wir notieren eine Relation $f \subseteq M \times N$, die eine Funktion ist auch mit $f : M \to N, x \mapsto f(x)$.

Ordnungen und Äquivalenzrelationen

Definition (Ordnungen)

Eine Relation $R \subseteq M \times M$ heißt **Ordnung**, wenn sie reflexiv, antisymmetrisch und transitiv ist.

Definition (Äquivalenzrelationen)

Eine Relation $R \subseteq M \times M$ heißt **Äquivalenzrelation**, wenn sie reflexiv, symmetrisch und transitiv ist.

Eigenschaften von Funktionen

Definition (Eigenschaften von Funktionen)

Eine Funktion $f : M \to N$ heißt

- **injektiv**, wenn $\forall x_1, x_2 \in M : f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- **surjektiv**, wenn $\forall y \in N \exists x \in M : y = f(x)$.
- **bijektiv**, wenn f injektiv und surjektiv ist.

Intuitiv bedeutet *injektiv*, dass ein Funktionswert höchstens einen Ursprungswert hat, oder anders: Jeder Wert im Zielraum wird höchstens einmal von f „getroffen“. *Surjektiv* bedeutet, dass jeder Wert von f „getroffen“wird.