2 Grundbegriffe der Mengenlehre

2.1 Mengen und Operationen auf Mengen

Moderne Mengentheorie wird in Form eines axiomatischen Kalküls betrieben. Dieser Ansatz hat aber den Nachteil, daß einfache inhaltliche Fragen oft durch einen technisch komplizierten Apparat verdeckt werden. Wir werden uns deshalb auf die Entwicklung einer "naiven" Mengenlehre beschränken, die als sprachliches Werkzeug für die nachfolgenden Teile der Vorlesung völlig ausreichend ist.
Nach G. Cantor ist eine *Menge* "eine Zusammenfassung von bestimmten wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens (welche die Elemente der Menge genannt werden) zu einem Ganzen".
Der Sachverhalt, daß ein Objekt a Element einer Menge A ist, wird durch $a \in A$ dargestellt, anderenfalls schreibt man $a \notin A$. Zwei Mengen A und B sind *gleich*, wenn sie die gleichen Elemente besitzen, d.h. wenn für alle a gilt: $a \in A$ dann und nur dann, wenn $a \in B$.

Darstellungen von Mengen

a) Mengen können durch *Auflistung ihrer Elemente* in geschweiften Klammern dargestellt werden. Das betrifft insbesondere endliche Mengen, wie z.B. $A = \{2, 3, 5, 7\}$ oder $B = \{rot, gelb, blau\}$. Dabei ist die Reihenfolge der Elemente in der Auflistung ohne Bedeutung. Auch die Mehrfachnennung von Elementen ist erlaubt, sie hat aber nur Einfluß auf die Darstellung der Menge und nicht auf die Menge selbst, z.B. $\{2, 3, 5, 7\} = \{5, 7, 3, 2, 2, 5, 2\}$.
Wir vereinbaren, daß auch unendliche Mengen durch Auflistung dargestellt werden können, sofern dies unmißverständlich ist, wie z.B. $\{0, 1, 2, 3, \ldots\}$ für die natürlichen Zahlen oder $\{2, 4, 6, 8, \ldots\}$ für die positiven, geraden Zahlen.

b) Die in der Mathematik gebräuchlichste Darstellungsform von Mengen beruht auf dem sogenannten *Abstraktionsprinzip*, nach dem man Mengen – im Sinne der Cantorschen Definition – durch wohlbestimmte Eigenschaften definieren kann. Dazu werden Prädikate $P(x)$ über einem festgelegten Individuenbereich für x benutzt. Dann wird mit $\{x \mid P(x)\}$ oder (wenn der Bereich B explizit genannt werden soll) mit $\{x \in B \mid P(x)\}$ die Menge bezeichnet, die sich aus allen Individuen aus dem Bereich zusammensetzt, für die $P(x)$ wahr ist.

c) Zur Veranschaulichung können Mengen durch sogenannte *Venn–Diagramme* als Kreisscheiben oder andere Flächen in der Ebene dargestellt werden.

Definition: Eine Menge A ist *Teilmenge* (oder *Untermenge*) einer Menge B (Schreibweise $A \subseteq B$), wenn aus $a \in A$ auch $a \in B$ folgt.

Es gilt $A = B$ genau dann, wenn $A \subseteq B$ und $B \subseteq A$. Außerdem folgt aus $A \subseteq B$ und $B \subseteq C$ auch $A \subseteq C$.

Definition: Zwei Mengen A und B sind *disjunkt*, wenn sie keine gemeinsamen Elemente besitzen, d.h wenn aus $a \in A$ folgt $a \notin B$.

Definition: Die *Vereinigung* $A \cup B$ der Mengen A und B besteht aus allen Mengen,

die Elemente von A oder von B sind, dh. $A \cup B = \{x \mid x \in A \ \vee \ x \in B\}$.
Definition: Der *Durchschnitt* $A \cap B$ der Mengen A und B besteht aus allen Mengen, die Elemente von A und von B sind, dh. $A \cap B = \{x \mid x \in A \ \wedge \ x \in B\}$.
Definition: Die *Differenz* $A \setminus B$ der Mengen A und B besteht aus allen Mengen, die Elemente von A aber nicht von B sind, dh. $A \setminus B = \{x \mid x \in A \ \wedge \ x \notin B\}$
Definition: Die Menge, die kein Element enthält wird *leere Menge* genannt und mit $\emptyset$ bezeichnet.
Oft ist es sinnvoll, den zu betrachtenden Individuenbereich generell festzulegen, z.B. wenn man nur Mengen von natürlichen Zahlen betrachten will. Ein solcher Bereich wird *Universum* genannt und allgemein mit U bezeichnet. Es ist klar, daß Aussageformen über U immer Teilmengen von U definieren.

Definition: Ist A Teilmenge eines festgelegten Universums U, dann ist das *Komplement* von A definiert als $U \setminus A$. Es wird mit $\overline{A}$ bezeichnet.

Satz: Folgende Identitäten gelten für alle Untermengen A, B, C eines Universums U:

Kommutativität:	$A \cup B$	$= B \cup A$
	$A \cap B$	$= B \cap A$
Assoziativität:	$A \cup (B \cup C)$	$= (A \cup B) \cup C$
	$A \cap (B \cap C)$	$= (A \cap B) \cap C$
Distributivität:	$A \cap (B \cup C)$	$= (A \cap B) \cup (A \cap C)$
	$A \cup (B \cap C)$	$= (A \cup B) \cap (A \cup C)$
Idempotenz:	$A \cup A$	$= A$
	$A \cap A$	$= A$
Dominanz:	$A \cup U$	$= U$
	$A \cap \emptyset$	$= \emptyset$
Identität:	$A \cup \emptyset$	$= A$
	$A \cap U$	$= A$
Absorbtion:	$A \cup (A \cap B)$	$= A$
	$A \cap (A \cup B)$	$= A$
De Morgan'sche Regel:	$\overline{A \cup B}$	$= \overline{A} \cap \overline{B}$
	$\overline{A \cap B}$	$= \bar{A} \cup \bar{B}$
Komplementierung:	$A \cup \overline{A}$	$= U$
	$A \cap \overline{A}$	$= \emptyset$
	$\overline{(\overline{A})}$	$= A$
	$A \setminus B$	$= A \cap \overline{B}$

Auf Grund der Assoziativität ist kann man bei der Vereinigung (bzw. beim Durchschnitt) von n Mengen $A_1, A_2, \ldots, A_n$ auf Klammerungen verzichten und die folgende Schreibweise nutzen:

$$A_1 \cup A_2 \cup \ldots \cup A_n = \bigcup_{i=1}^{n} A_i$$
$$A_1 \cap A_2 \cap \ldots \cap A_n = \bigcap_{i=1}^{n} A_i$$

Definition: Ist I eine beliebige Menge und ist für jedes $i \in I$ eine Menge A_i gegeben, dann nennen wir die Menge dieser Mengen eine *Mengenfamilie* und bezeichnen sie durch $\{A_i \mid i \in I\}$. Die Vereinigung (bzw. der Durchschnitt) dieser Mengenfamilie ist definiert durch

$$\bigcup_{i\in I} A_i = \{x \mid \text{es gibt ein } i \in I, \text{ so daß } x \in A_i\}$$

$$\bigcap_{i\in I} A_i = \{x \mid \text{für alle } i \in I, \text{ gilt } x \in A_i\}$$

Definition: Eine Familie $\{A_i \mid i \in I\}$ von nichtleeren Mengen wird *Partition* oder *Zerlegung* einer Menge A genannt, falls
1) $A = \bigcup_{i\in I} A_i$ und
2) Für beliebige, voneinander verschiedene $i, j \in I$ gilt $A_i \cap A_j = \emptyset$.

Definition: Ist A eine Menge, dann wird die Menge aller Untermengen von A die Potenzmenge von A genannt und mit $\mathcal{P}(A)$ bezeichnet.

Satz: Ist A eine endliche, n-elementige Menge, dann hat die Potenzmenge $\mathcal{P}(A)$ genau 2^n Elemente.

2.2 Das Kartesische Produkt und Relationen

Definition: Ein *geordnetes Paar* (a, b) ist eine (den Objekten a und b zugeordnetes) Konstrukt mit der folgenden Eigenschaft: $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$.

Definition: Das *kartesische Produkt* $A \times B$ von zwei Mengen A und B ist definiert als die Menge aller geordneten Paare (a, b) mit $a \in A$ und $b \in B$, als Formel:

$$A \times B = \{\, (a, b) \mid a \in A \wedge b \in B \,\}$$

Definition: Eine Untermenge R eines kartesischen Produkts $A \times B$ wird *binäre Relation* oder kurz *Relation* zwischen A und B genannt. Für $(a, b) \in R$ kann auch $a\,R\,b$ geschrieben werden. In diesem Fall sagt man, dass a in Relation zu b steht.
Eine Untermenge R eines kartesischen Produkts der Form $A \times A$ wird (binäre) Relation über A genannt.

Die ersten drei Relationen in den folgenden Beispielen sind generisch, d.h. man kann sie über beliebigen Grundmengen betrachten:

- $\emptyset \subseteq A \times B$ wird *leere Relation* genannt.
- $A \times B$ wird *Allrelation* zwischen A und B genannt.
- Die Menge $\{(a, a) \mid a \in A\}$ wird die *identische Relation* über A genannt und kurz mit Id_A bezeichnet.
- Die Teilbarkeitsrelation $\mid$ kann man als Relation über den natürlichen Zahlen (aber auch über den ganzen Zahlen) betrachten. Wie bereits besprochen, kann man diese Relation wie folgt definieren:

$$\forall\, a, b \in \mathbb{N} \quad (\, a \,|\, b \Longleftrightarrow \exists c \in \mathbb{N} \qquad b = a \cdot c)$$

- Über den natürlichen Zahlen $\mathbb{N}$, den ganzen Zahlen $\mathbb{Z}$, den rationalen Zahlen $\mathbb{Q}$ und den reellen Zahlen $\mathbb{R}$ kennen wir eine Reihe von Vergleichsrelationen, nämlich $<, \leq, \geq, >$.
- Ist A die Menge aller Informatikstudenten an der FU Berlin und B die Menge aller Pflichtmodule im Informatikstudium, dann ist $R = \{(a, b) \in A \times B \mid \text{Student } a \text{ hat das Modul } b \text{ abgeschlossen }\}$ eine binäre Relation.
- Jede Abbildung $f : A \longrightarrow B$ kann auch als binäre Relation $f = \{(a, b) \in A \times B \mid a \in A \wedge b = f(a)\}$ gesehen werden.

Zur Darstellung von Relationen sind verschiedene Methoden gebräuchlich:

- Darstellungen in Tabellenform bei denen für jedes $a \in A$ eine Spalte und für jedes $b \in B$ eine Zeile angelegt wird. Die Zelle in der Spalte von a und der Zeile von b wird mit einer 1 gefüllt, wenn $a\,R\,b$ gilt, und sonst mit einer 0. (Verwendung in relationalen Datenbanken);
- Anschauliche Darstellungen durch Diagramme in einem Rechteck;
- Graphen bei denen die Elemente aus A und B als Knoten gezeichnet werden, wobei zwei Elemente, die zueinander in Relation stehen, durch eine Kante (Verbindungsstrecke) verbunden werden.

Relationsoperationen

1. Sind R und R' Relationen zwischen A und B, dann sind auch die Vereinigung $R \cup R'$, der Durchschnitt $R \cap R'$ sowie das Komplement $\overline{R} = (A \times B) \setminus R$ Relationen zwischen A und B.
2. Die zu einer Relation $R \subseteq A \times B$ *inverse Relation* $R^{-1} \subseteq B \times A$ ist definiert durch $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$.
3. Die *Verkettung* oder *Komposition* $R \circ S$ von zwei Relationen $R \subseteq A \times B$ und $S \subseteq B \times C$ ist definiert durch

$$\{(a, c) \in A \times C \mid \text{es gibt ein } b \in B \text{ mit } (a, b) \in R \text{ und } (b, c) \in S\}$$

Beispiele:

1) Wir betrachten die Vergleichsrelationen $<$, $\leq$, $\geq$ und $=$ über den natürlichen Zahlen $\mathbb{N}$. Offensichtlich ist die Vereinigung der Relationen $<$ und $=$ die Relation $\leq$. Das Komplement der Relation $<$ ist die Relation $\geq$. Der Durchschnitt der Relationen $\leq$ und $\geq$ ist die identische Relation $Id_{\mathbb{N}}$. Die zu $\leq$ inverse Relation ist $\geq$, die identische Relation ist zu sich selbst invers.

2) Sei M die Menge aller Menschen und $R \subseteq M \times M$ "Elternrelation", also $a\,R\,b$, falls a Vater oder Mutter von b ist. Dann kann man die inverse Relation R^{-1} sowie die Verkettungen $R \circ R$, $R \circ R^{-1}$ und $R^{-1} \circ R$ wie folgt charakterisieren:

- $a\,R^{-1}\,b$, falls a Kind von b ist,
- $a\,R \circ R\,b$, falls a Großvater oder Großmutter von b ist,
- $a\,R \circ R^{-1}\,b$, falls a und b ein gemeinsames Kind haben oder falls $a = b$ und a hat ein Kind ,
- $a\,R^{-1} \circ R\,b$, falls $a = b$ oder a und b Geschwister oder Halbgeschwister sind.

Eigenschaften von Relationen über Mengen

Definition: Sei R eine Relation über A.

- R ist *reflexiv*, falls für jedes $a \in A$ gilt, daß $a\,R\,a$, d.h. $Id_A \subseteq R$.
- R ist *symmetrisch*, falls aus $a\,R\,b$ folgt, daß $b\,R\,a$, d.h. $R^{-1} \subseteq R$.
- R ist *trasitiv*, falls aus $a\,R\,b$ und $b\,R\,c$ folgt, daß $a\,R\,c$, d.h. $R \circ R \subseteq R$.
- R ist *antisymmetrisch*, falls aus $a\,R\,b$ und $b\,R\,a$ die Gleichheit von a und b folgt, d.h. $R \cap R^{-1} \subseteq Id_A$.
- R ist *asymmetrisch*, falls aus $a\,R\,b$ folgt, daß $(b, a) \notin R$, d.h. $R \cap R^{-1} = \emptyset$.

Beispiele:
1) Die Vergleichsrelationen $\leq$ und $\geq$ sind über $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ reflexiv, transitv und antisymmetrisch. Die Relationen $<$ und $>$ sind nicht reflexiv, aber transiv, antisymmetrisch und asymmetrisch.
2) Die oben definierte Teilbarkeitsrelation ist reflexiv und transitiv über $\mathbb{N}$ und über $\mathbb{Z}$. Sie ist antisymmetrisch über $\mathbb{N}$, aber als Relaion über $\mathbb{Z}$ ist sie nicht antisymmetrisch, denn $1| - 1$ und $-1|1$, aber $1 \neq -1$.

2.3 Äquivalenzrelationen

Definition: Eine Relation über einer Menge A wird *Äquivalenzrelation* genannt, wenn sie reflexiv, symmetrisch und transitiv ist.

Beispiel: Sei $\mathbb{N}$ die Menge der natürlichen Zahlen und R definiert durch $a\,R\,b$, genau dann wenn a und b beim Teilen durch 5 den gleichen Rest haben. Dann ist R eine Äquivalenzrelationin $\mathbb{N}$.

Definition: Ist $R \subseteq A \times A$ eine Äquivalenzrelation und ist $a \in A$, dann nennt man die Menge $\{x \in A \mid xRa\}$ die *Äquivalenzklasse* von a (bezüglich R). Sie wird mit $[a]_R$ oder auch mit $a/_R$ bezeichnet. Ein Element einer Äquivalenzklasse wird *Repräsentant* dieser Klasse genannt.

Lemma: Sei R eine Äquivalenzrelation, dann sind zwei Äquivalenzklassen $[a]_R$ und $[b]_R$ entweder gleich oder disjunkt. Sie sind genau dann gleich, wenn $a\,R\,b$ gilt.

Beweis: Wir verifizieren dazu die folgende Schlusskette:

$$[a]_R \cap [b]_R \neq \emptyset \qquad \stackrel{(1)}{\Longrightarrow} \qquad a\,R\,b \qquad \stackrel{(2)}{\Longrightarrow} \qquad [a]_R = [b]_R$$

(1) Sei $c \in [a]_R \cap [b]_R$, dann gilt cRa und cRb, wegen der Symmetrie auch aRc und wegen der Transitivität auch aRb.
(2) Sei d ein beliebiges Element aus $[a]_R$ und gelte aRb. Dann gilt dRa und wegen der Transitivität auch dRb. Damit liegt d in der Äquivalenzklasse$[b]_R$ und folglich ist $[a]_R \subseteq [b]_R$. Wegen der Symmetrie kann man aber auch die Rollen von a und b vertauschen und somit $[b]_R \subseteq [a]_R$ ableiten, woraus letztlich die Gleichheit der beiden Äquivalenzklassen folgt. □

Die erste Aussage des folgenden Satzes kann als einfache Schlussfolgerung aus dem Lemma abgeleitet werden.

Satz: Ist $R \subseteq A \times A$ eine Äquivalenzrelation, dann bildet die Menge aller Äquivalenzklassen eine Partition von A. Umgekehrt, ist eine Partition $\{A_i \mid i \in I\}$ von A gegeben, dann ist die durch

$$a\,R\,b \iff \exists i \in I \qquad a \in A_i \;\wedge\; b \in A_i$$

definierte Relation R eine Äquivalenzrelation.

Definition: Sei $R \subseteq A \times A$ eine Äquivalenzrelation. Eine Untermenge von A wird Repräsentantensystem für R genannt, wenn sie aus jeder Äquivalenzklasse genau ein Element enthält.

Beispiel: Wir betrachten noch einmal die Relation R in $\mathbb{N}$ die zwei Zahlen a und b genau dann in Beziehung setzt, wenn sie beim Teilen durch 5 den gleichen Rest haben. Dann werden die einzelnen Äquivalenzklassenjeweils durch die Zahlen mit gleichen Rest gebildet, was zu der folgenden Partition von $\mathbb{N}$ führt:

$$\{\{0, 5, 10 \ldots\}, \{1, 6, 11, \ldots\}, \{2, 7, 12, \ldots\}, \{3, 8, 13, \ldots\}, \{4, 9, 14, \ldots\}\}$$

Offensichtlich bilden die Reste {0,1,2,3,4} ein Repräsentatensystem (das sogenannte Standard–Repräsentatensystem), aber auch die Menge $\{3, 10, 7, 21, 9\}$ ist ein Repräsentatensystem.

Natürlich hätten wir an Stelle der 5 auch jede andere Zahl $n \in \mathbb{N}^+$ als Teiler wählen können. Man bezeichnet die dadurch entstehenden Relationen als Kongruenzen modulo n und schreibt für zwei Zahlen a, b, die beim Teilen durch n den gleichen Rest haben auch $a \equiv b \;(\boldsymbol{mod}\; n)$. In diesem Fall bilden die möglichen Reste $\{0, 1, \ldots, n-1\}$ das Standard–Repräsentatensystem.

Satz: Die identische Relation Id_A und die Allrelation $A \times A$ sind Äquivalenzrelationen. Sind R und R' Äquivalenzrelationen in A, dann ist auch $R \cap R'$ eine Äquivalenzrelation in A.

Achtung: Die letzte Aussage gilt im Allgemeinen nicht für Vereinigungen. Als Gegenbeispiel kann man die Kongruenzrelationen modulo 2 und modulo 3 betrachten.

Offensichtlich ist das Paar $(1,6)$ nicht in der Vereinigung, denn 1 und 6 haben sowohl beim Teilen durch 2 als auch beim Teilen durch 3 verschiedene Reste. Andererseits sind die Paare $(1,4)$ - gleicher Rest beim Teilen durch 3 - und $(4,6)$ - gleicher Rest beim Teilen durch 2 - in der Relationsvereinigung. Folglich ist diese Vereinigung nicht transitiv.

Allgemein kann jede Relation $R \subseteq A \times A$ durch die folgenden 3 Schritte zu einer Äquivalenzrelation erweitert werden:

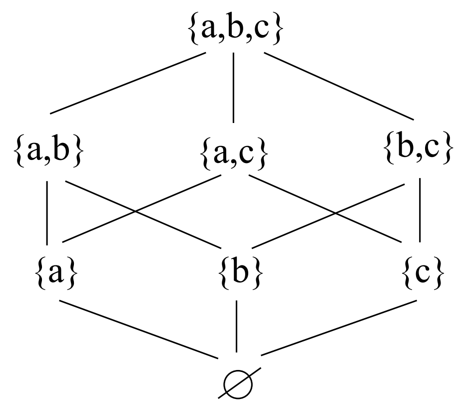
1) reflexiver Abschluss: $R_r = R \cup Id_A$
2) symmetr. Abschluss: $R_{rs} = R_r \cup R_r^{-1} = R \cup R^{-1} \cup Id_A$
3) transitiver Abschluss: $R_{rst} = R_{rs} \cup R_{rs} \circ R_{rs} \cup R_{rs} \circ R_{rs} \circ R_{rs} \cup \ldots = \bigcup_{i=1}^{\infty} R_{rs}^i$

wobei R_{rs}^i die i-fache Verkettung von R_{rs} ist.

2.4 Ordnungsrelationen

Definition: Eine Relation R über einer Menge A, die reflexiv, transitiv und antisymmetrisch ist, wird *Halbordnungsrelation* oder auch *partielle Ordnungsrelation* genannt. Das Paar (A, R) nennt man eine *halb– (partiell) geordnete Menge* oder kurz *poset* als Abkürzung für partially ordered set.

Endliche, halbgeordnete Mengen werden oft durch sogenannte *Hasse–Diagramme* dargestellt. Dabei werden die Elemente der Menge als Punkte in der Ebene gezeichnet, wobei direkte Nachfolger jeweils höher als ihre Vorgänger liegen und mit ihnen durch ein Liniensegment verbunden sind. Formal betrachtet beschreibt das Hasse–Diagramm eines Posets (A, R) die kleinste Unterrelation von R, deren reflexiver und transitiver Abschluss R ergibt. Die folgende Abbilddung zeigt das Hasse–Diagramm der Potenzmenge einer 3–elementigen Menge $M = \{a, b, c\}$:



Beispiele:
1) Für jede beliebige Menge M ist $(\mathcal{P}(M), \subseteq)$ eine halbgeordnete Menge.
2) Die Teilbarkeitsrelation $|$ ist eine Halbordnungsrelation in der Menge der positiven ganzen Zahlen $\mathbb{Z}^+$.

3) In der Menge der reellen Zahlen $\mathbb{R}$ ist die Relation $\leq$ eine Halbordnungsrelation.
4) Die Menge der Wörter einer Sprache wird durch die "lexikographische Ordnung" geordnet.

Zwei Begriffe sind eng verwandt mit partiellen Ordnungsrelationen: totale Ordnungsrelationen und strikte (oder strenge) Ordnungsrelationen. Diese Begriffe werden durch die folgenden Definitionen genauer erläutert.

Definition: Zwei Elemente a und b einer halbgeordneten Menge (A, R) nennt man vergleichbar, falls $a\,R\,b$ oder $b\,R\,a$ gilt. Anderenfalls nennt man sie unvergleichbar. Eine Halbordnungsrelation R in einer Menge A wird *totale* (oder auch *lineare*) *Ordnungsrelation* genannt, wenn jedes Paar von Elementen vergleichbar ist.

Beispiele: In den obigen Beispielen sind die Relationen aus 1) und 2) keine totalen Ordnungsrelationen. So sind für $M = \{a, b, c\}$ die Untermengen $\{a\}$ und $\{c\}$ unvergleichbar bezüglich der Teilmengenrelation. Die Zahlen 6 und 20 sind unvergleichbar bezüglich der Teilbarkeitsrelation. Dagegen ist $\leq$ eine totale Ordnungsrelation für die reellen Zahlen. Die lexikographische Ordnung ist eine totale Ordnungsrelation.

Bemerkung: Taucht in der Literatur der Begriff "Ordnungsrelation" auf, so ist darunter in der Regel eine "Halbordnungsrelation" zu verstehen.

Definition: Eine Relation R über einer Menge A wird *strikte* oder *strenge Ordnungsrelation* genannt, wenn Sie transitiv und asymmetrisch ist.

Typische Beispiele für strikte Orddnungsrelationen sind die "echt–kleiner"–Relation $<$ oder die Relation ein echter Teiler zu sein. Generell, kann man aus jeder Halbordnungsrelation R über einer Menge A eine strikte Ordnungsrelation $R' = R \setminus Id_A$ ableiten und umgekehrt kann aus jeder strikten Ordnungsrelation durch Vereinigung mit Id_A eine Halbordnungsrelation gemacht werden.

Weitere Begriffe, die wie das Maximum und Minimum aus der Schulmathematik bekannt sind, müssen im Kontext mit Halbordnungsrelationen noch einmal neu definiert werden.

Definition: Sei $(A, \prec)$ ein Poset, $B \neq \emptyset$ eine Teilmenge von A und $a \in A$.

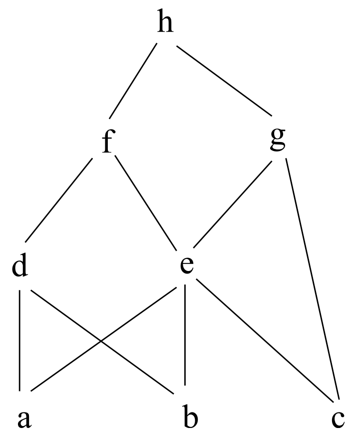
- a ist eine obere (bzw. untere) Schranke von B wenn $b \prec a$ (bzw. $a \prec b$) für alle $b \in B$ gilt.
- a wird das *Maximum* oder *größtes Element* von B (bzw. *Minimum* oder *kleinstes Element* von B) genannt, wenn a ein Element von B und eine obere (bzw. untere) Schranke von B ist.
- a wird *Supremum* oder *obere Grenze* von B (bzw. *Infimum* oder *untere Grenze* von B) genannt, wenn die Menge $O(B)$ der oberen Schranken von B (bzw. die Menge $U(B)$ der unteren Schranken von B) nicht leer ist und a das Minimum von $O(B)$ (bzw. das Maximum von $U(B)$) ist.

Achtung: Nicht in jedem Fall existiert ein Maximum, Minimum, Supremum oder Infimum einer Teilmenge B, aber wenn ein Element a existiert, das für einen dieser Begriffe, die in der Definition geforderten Eigenschaften hat, dann ist es auch eindeutig. Man kann deshalb die Bezeichnungen $max(B), min(B), sup(B), inf(B)$ einführen, die entweder für ein eindeutig existierendes Element oder für nicht existierend stehen.

Beobachtung: Wenn für eine Teilmenge B einer Halbordnung $(A, \prec)$ das Maximum (bzw. Minumum) existiert, dann existiert auch das Supremum (bzw. das Infimum) und es gilt $sup(B) = max(B)$ (bzw. $inf(B) = min(B)$).

Beispiel: In der durch das nachfolgende Hasse-Diagramm dargestellten Halbordnung gilt für die Teilmengen $B = \{d, e\}$ und $C = \{f, g, h\}$:

- B hat zwei obere Schranken, nämlich f und h und zwei untere Schranken, nämlich a und b.
- C hat eine obere Schranke, nämlich h und vier untere Schranken, nämlich a, b, c und e
- B hat weder ein Maximum noch ein Minimum noch ein Infimum, aber ein Supremum $sup(B) = f$
- C hat kein Minimum, aber $inf(C) = e$ und $sup(C) = max(C) = h$



2.5 Funktionen

Definition: Unter einer *Funktion* (oder *Abbildung*) f von einer Menge A in eine Menge B versteht man eine Zuordnung, bei der jedem Element aus A ein eindeutig bestimmtes Element aus B entspricht. Formal kann f als eine Relation zwischen A und B charakterisiert werden, so daß für jedes $a \in A$ genau ein $b \in B$ existiert mit $a\, f\, b$. Als übliche Schreibweise verwenden wir $f : A \longrightarrow B$ um auszudrücken, dass f eine Funktion von A nach B ist, und $f(a) = b$ um auszudrücken, dass dem Element a durch die Funktion f der Wert b zugeordnet wird. Die Menge A wird

Definitionsbereich von f und die Menge B wird *Wertebereich* oder *Wertevorrrat* von f genannt.

Definition: Ist $f : A \longrightarrow B$ eine Funktion, $M \subseteq A$ und $N \subseteq B$, dann nennt man die Menge

$f(M) = \{y \in B \mid \text{es gibt ein } x \in M \text{ mit } f(x) = y\}$ das *Bild* von M unter f

und die Menge

$f^{-1}(N) = \{x \in A \mid f(x) \in N\}$ das *vollständige Urbild* von N unter f.

Definition:

- Eine Funktion $f : A \longrightarrow B$ heißt *surjektiv*, falls jedes Element von B im Bild von A auftritt, d.h. $f(A) = B$.
- Eine Funktion $f : A \longrightarrow B$ heißt *injektiv* oder *eineindeutig*, falls je zwei verschiedene Elemente aus A auch verschiedene Bilder haben, d.h. wenn aus $f(a) = f(a')$ die Gleichheit von a und a' folgt.
- Eine Funktion wird *bijektiv* genannt, wenn sie injektiv und surjektiv ist.

Beispiel: Wir betrachten die bekannte Sinusfunktion. Als Funktion von den reellen Zahlen in die reellen Zahlen ist $sin : \mathbb{R} \longrightarrow \mathbb{R}$ weder injektiv noch surjektiv.
Durch Einschränkungen von Definitions– und/oder Wertebereich kann man diese Eigenschaften erzwingen:

- $sin : \mathbb{R} \longrightarrow [-1, 1]$ ist surjektiv, aber nicht injektiv
- $sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow \mathbb{R}$ ist injektiv, aber nicht surjektiv
- $sin : [-\frac{\pi}{2}, \frac{\pi}{2}] \longrightarrow [-1, 1]$ ist bijektiv.

Betrachtet man eine Funktion $f : A \longrightarrow B$ als Relation, dann ist die zu f inverse Relation f^{-1} genau dann eine Funktion, wenn f bijektiv ist. In diesem Fall wird f^{-1} die zu f *inverse Funktion* genannt.

Definition: Sind $f : A \longrightarrow B$ und $g : B \longrightarrow C$ Funktionen, dann ist die Relationsverkettung $f \circ g$ eine Funktion von A in C. Sie wird *Verknüpfung* oder *Komposition* von f und g genannt und durch $gf : A \longrightarrow C$ bezeichnet, wobei $gf(a) = g(f(a))$ gilt. Man beachte, daß Relationsverkettungen von links nach rechts und Funktionsverknüpfungen von rechts nach links geschrieben werden.

Satz: Die folgenden Fakten ergeben sich als einfache Schlußfolgerungen aus den Definitionen. Seien $f : A \longrightarrow B$ und $g : B \longrightarrow C$ zwei Funktionen, dann gilt:

- Ist f bijektiv, dann ist $f^{-1}f = Id_A$ und $ff^{-1} = Id_B$
- f ist genau dann injektiv, wenn eine Funktion $h : B \longrightarrow A$ existiert mit $hf = Id_A$.

- f ist genau dann surjektiv, wenn eine Funktion $h : B \longrightarrow A$ existiert mit $fh = Id_B$.
- Sind f und g injektiv, dann ist auch gf injektiv.
- Sind f und g surjektiv, dann ist auch gf surjektiv.
- Sind f und g bijektiv, dann ist auch gf bijektiv und es gilt $(gf)^{-1} = f^{-1}g^{-1}$.

Satz: Jede Funktion $f : A \longrightarrow B$ induziert eine Äquivalenzrelation $\sim_f$ durch
$a \sim_f b$ genau dann, wenn $f(a) = f(b)$.
Diese Äquivalenzrelation wird auch *Faserung* von A durch f genannt.

2.6 Natürliche Zahlen und vollständige Induktion

Alle aus der Schulmathematik bekannten Aussagen über natürliche Zahlen können aus einigen wenigen Grundannahmen abgeleitet werden. Diese grundlegenden Voraussetzungen für die Existenz der natürlichen Zahlen (und letzlich Grundlagen der gesamten Zahlentheorie) gehen auf Richard Dedekind und Giuseppe Peano zurück und sind als die Peano'schen Axiome bekannt:

1. 0 ist eine natürliche Zahl.
2. Jede natürliche Zahl n hat eine eindeutigen Nachfolger $S(n)$, der auch eine natürliche Zahl ist.
3. Aus $S(n) = S(m)$ folgt $n = m$.
4. 0 ist kein Nachfolger einer natürlichen Zahl.
5. Jede Menge X, die 0 enthält und für die gilt, dass aus $n \in X$ auch $S(n) \in X$ folgt, enthält alle natürlichen Zahlen.

Achtung: Wir schreiben für den Nachfolger $S(n)$ auch $n + 1$, aber das ist als symbolische Schreibweise und nicht als Anwendung der Operation Addition zu verstehen. Im Gegenteil, wie die folgenden Betrachtungen zeigen, kann die Addition durch Anwendung der Nachfolgerfunktion rekursiv definiert werden.
Konsequenz 1: Man kann Funktionen $f : \mathbb{N} \longrightarrow A$ definieren, indem man $f(0)$ festlegt und $f(S(n))$ auf $f(n)$ zurückführt. Dieses Prinzip der Definition von Funktionen nennt man *Rekursion*.
Beispiel: Um die Addition von natürlichen Zahlen zu einzuführen, definieren wir für jede fest gewählte Zahl m die Funktion $m+ : \mathbb{N} \longrightarrow \mathbb{N}$, die jedem n aus dem Definitionsbereich die Summe $m + n$ zuordnen soll. Diese Funktion hat die folgende rekursive Definition: $m + (0) := m$ und $m + (S(n)) := S(m + n)$. Das entspricht den Regeln $m + 0 := m$ und $m + (n + 1) := (m + n) + 1$.

Analog kann man die Multiplikation durch $m\cdot : \mathbb{N} \longrightarrow \mathbb{N}$ mit $m \cdot (0) := 0$ und $m \cdot (S(n)) := (m \cdot (n)) + m$ definieren, was den Regeln $m \cdot 0 := 0$ und $m \cdot (n+1) := (m \cdot n) + m$ entspricht.

Konsequenz 2: Man kann allgemeine Aussagen über natürliche Zahlen nach dem folgenden Schema beweisen. Eine Aussageform $P(x)$ über dem Bereich der natürlichen Zahlen ist wahr für alle natürlichen Zahlen, wenn sie die folgenden zwei Bedingungen erfüllt:
1) $P(0)$ ist wahr.
2) Für beliebige $n \in \mathbb{N}$ gilt: Ist $P(n)$ wahr, dann ist auch $P(n+1)$ wahr.
Dieses Beweisprinzip nennt man *vollständige Induktion.* Die erste Bedingung wird *Induktionsanfang* oder *Induktionsbasis*, die zweite Bedingung *Induktionsschluss* genannt. Dabei heißt $P(n)$ *Induktionsvoraussetzung* oder *Induktionsannahme* und $P(n+1)$ *Induktionsbehauptung.*

Beispiele für Aussagen, die man mit Induktion beweisen kann:

- Für jede natürliche Zahl $n > 0$ ist die Summe der ungeraden Zahlen von 1 bis $2n-1$ gleich n^2.
- Für beliebige reelle Zahlen a und $r \neq 1$ und für jede natürliche Zahl n gilt
$$\sum_{i=0}^{n} ar^i = \frac{ar^{n+1} - a}{r-1}.$$

. Zwei Varianten des Induktionsprinzips werden häufig verwendet:

1) Wird die Induktionsbasis nicht für $n = 0$ sondern für einen anderen festen Anfangswert $k > 0$ bewiesen, so gilt die Aussage für alle natürlichen Zahlen $n \geq k$.

2) Beim Induktionsschritt ist es erlaubt, nicht nur auf $P(n)$, sondern auf beliebige kleinere Zahlen zurückzugreifen, d.h. an Stelle von $P(n) \longrightarrow P(n+1)$ zeigt man $P(k) \wedge P(k+1) \wedge \ldots \wedge P(n) \longrightarrow P(n+1)$, wobei k der Anfangswert aus der Induktionsbasis ist. Dieses Prinzip wird *verallgemeinerte vollständige Induktion* genannt.

Der folgende Satz gibt ein typisches Beispiel für eine Aussage, die man mit verallgemeinerter Induktion bewiesen kann.

Satz: Jede natürliche Zahl $n \geq 2$ kann man als Produkt von Primzahlen darstellen.

2.7 Endliche Mengen und Kardinalzahlen

Definition: Zwei Mengen A und B werden *gleichmächtig* genannt, wenn eine bijektive Funktion $f : A \longrightarrow B$ existiert.
In diesem Sinne bedeutet eine Abzählung einer endlichen (n-elementigen) Menge M, dass eine Bijektion zwischen der Menge $\{1, 2, \ldots, n\}$ und M (oder zwischen $\{0, 1, \ldots, n-1\}$ und M) konstruiert wird. Problematisch ist dabei, dass die Beschreibung von $\{1, 2, \ldots, n\}$ (oder $\{0, 1, \ldots, n-1\}$) genau gesehen eine rekursive Definition

ist. John von Neumann löste dieses Problem durch eine spezielle Konstruktion der natürlichen Zahlen.

Definition: Die natürlichen Zahlen in Sinne von *von Neumann* bilden die kleinste Menge mit den folgenden zwei Eigenschaften:

1) $0 = \emptyset \in \mathbb{N}$

2) Ist $n \in \mathbb{N}$, dann ist auch der Nachfolger $S(n) := n \cup \{n\}$ in $\mathbb{N}$.

Damit erhalten wir die folgende Darstellung der natürlichen Zahlen:

$0 = \emptyset$,
$1 = \{\emptyset\} = \{0\}$,
$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$,
$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$
$\ldots\ldots$

Jede natürliche Zahl ist nach dieser Konstruktion durch die Anzahl ihrer Elemente bestimmt.

Definition: Eine Menge A wird *endlich* genannt, wenn es eine von Neumannsche natürliche Zahl n gibt, so daß A und n gleichmächtig sind. In diesem Fall wird n die *Kardinalzahl* von A genannt (Schreibweise $|A| = n$). Zwei endliche Mengen sind also gleichmächtig, wenn die Anzahlen ihrer Elemente gleich sind.

Satz: Sind A, B und M endliche Mengen, dann gelten die folgenden Aussagen über ihre Mächtigkeiten:

1. $|A \setminus B| = |A| - |A \cap B|$
2. $|A \cup B| = |A| + |B| - |A \cap B|$
3. $|A \times B| = |A| \cdot |B|$
4. $|\mathcal{P}(M)| = 2^{|M|}$

Anmerkungen zu diesen Punkten 1) Die Summenregel ist eine Grundregel der Kombinatorik, die besagt, dass die Größe der Vereinigung von zwei disjunkten endlichen Mengen A und B sich als Summe aus $|A|$ und $|B|$ ergibt. Diese Regel ist als Spezialfall in der ersten und zweiten Aussage enthalten.

2) Die Verallgemeinerung der zweiten Aussage für drei und mehr Mengen führt zum sogenannten *Prinzip der Inklusion–Exklusion*:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

$$\begin{aligned} |\bigcup_{i=1}^{k} A_i| = & \sum_{1 \le i \le k} |A_i| - (\sum_{1 \le i_1 < i_2 \le k} |A_{i_1} \cap A_{i_2}|) + (\sum_{1 \le i_1 < i_2 < i_3 \le k} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|) - \ldots \\ & + \ldots\ldots + (-1)^{k+1} |\bigcap_{i=1}^{k} A_i| \end{aligned}$$

3) Die dritte Aussage ist auch eine Grundregel der Kombinatorik und wird Produktregel genannt.

4) Wie man leicht sieht, gibt es eine bijektive Abbildung von $\mathcal{P}(M)$ auf die Menge der Funktionen von M nach $\{0,1\}$. Dabei wird jedem $A \in \mathcal{P}(M)$ die charakteristische Funktion $\chi_A : M \longrightarrow \{0,1\}$ zugeordnet, welche jedes $x \in A$ auf 1 abbildet und für alle $x \notin A$ den Wert 0 hat. Bezeichnet man für zwei Mengen N und M mit N^M die Menge aller Funktionen von M nach N, dann kann die oben beschriebene Bijektion auch wie folgt gelesen werden:
$\mathcal{P}(M)$ ist gleichmächtig mit $\{0,1\}^M$ (also mit 2^M, da $2 = \{0,1\}$ im Sinne der von Neumannschen natürlichen Zahlen).

Aus dieser Sicht kann man die vierte Aussage wie folgt verallgemeinern: Sind N und M zwei beliebige endliche Mengen, dann ist die Anzahl der Funktionen von M in N gleich $|N|^{|M|}$, also $|N^M| = |N|^{|M|}$.

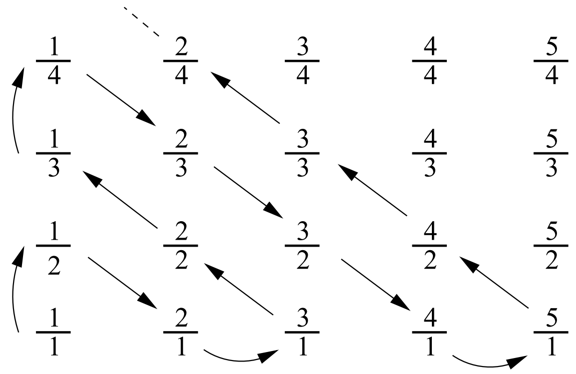
Definition: Eine Menge A, die nicht endlich ist, wird *unendlich* genannt (Schreibweise $|A| = \infty$).
Eine Menge A wird *abzählbar* genannt, wen sie endlich ist oder wenn sie mit der Menge der natürlichen Zahlen $\mathbb{N}$ gleichmächtig ist.

Satz: Die Menge $\mathbb{Z}$ der ganzen Zahlen und die Menge $\mathbb{Q}$ der rationalen Zahlen sind abzählbar.

Beweisidee: Für $\mathbb{Z}$ reicht es aus, eine unendliche Folge $z_0, z_1, z_2, \ldots$ zu bilden in der jede ganze Zahl genau einmal auftritt, denn dann wird durch $f(n) := z_n$ eine Bijektion zwischen $\mathbb{N}$ und $\mathbb{Z}$ definiert. Eine solche Folge ist z.B. $0, 1, -1, 2, -2.3, -3, \ldots$. In diesem Fall ist es auch leicht, eine geschlossene Formel für die Bijektion $f : \mathbb{N} \longrightarrow \mathbb{Z}$ anzugeben:

$$f(n) = (-1)^{n+1} \cdot \left\lceil \frac{n}{2} \right\rceil = \begin{cases} -\frac{n}{2} & \text{falls } n \text{ gerade} \\ \frac{n+1}{2} & \text{falls } n \text{ ungerade} \end{cases}$$

Für $\mathbb{Q}$ kombiniert man diesen Trick der alternierenden Aufzählung mit einem Schema zur Aufzählung aller positiven rationalen Zahlen. Dazu schreibt man alle Brüche mit positiven Zählern und Nennern in eine Tabelle und läuft die Zellen systematisch nach folgendem Schema ab. Daraus ergibt sich ein surjektive Abbildung $g : \mathbb{N} \longrightarrow \mathbb{Q}^+$.



Um nicht nur eine surjektive Abbildung sondern eine Bijektion zu erhalten, muss man letzlich noch dafür sorgen, dass alle Brüche übersprungen werden, deren rationaler

Wert schon vorher erreicht wurde (das sind alle Brüche, die sich kürzen lassen). Im abgebildeten Schema ist der Bruch $\frac{2}{2}$ der erste, den man überspringen muss, danach die Brüche $\frac{4}{2}, \frac{3}{3}$ und $\frac{2}{4}$. Da es in diesem Fall wesentlich schwerer ist, eine geschlossene Formel fr g anzugeben, begnügen wir uns hier mit der verbalen Konstruktionsbeschreibung einer solchen Bijektion.

Satz: Die Menge der reellen Zahlen ist nicht abzählbar.

Beweis: Wir führen einen Widerspruchsbeweis, um zu zeigen, dass schon die reellen Zahlen aus dem Intervall $[0, 1]$ nicht abzählbar sind. Dazu nehmen wir an, dass es eine bijektive Abbildung $f : \mathbb{N} \longrightarrow [0, 1]$ gibt und schreiben die Bilder $f(0), f(1), f(2), \ldots$ als Dezimalbrüche

$$\begin{array}{lcl} f(0) & = & 0, a_{0,0}, a_{0,1}a_{0,2}a_{0,3}\ldots \\ f(1) & = & 0, a_{1,0}, a_{1,1}a_{1,2}a_{1,3}\ldots \\ f(2) & = & 0, a_{2,0}, a_{2,1}a_{2,2}a_{2,3}\ldots \\ \vdots & \vdots & \vdots \end{array} \qquad\qquad a_{i,j} \in \{0, 1, 2, \ldots, 9\}$$

Es ist bekannt, dass Dezimalbruch–Darstellungen von reellen Zahlen immer dann eindeutig sind, wenn sie nicht mit $\overline{9}$ (d.h. 9–Periode) enden und auch nicht abbrechen (d.h. 0–Periode).
Jetzt ist es leicht, eine Zahl $r \in [0, 1]$ mit der Darstellung $0, b_0b_1b_2\ldots$ zu konstruieren, die nicht im Bild von f liegt, indem man die einzelnen Dezimalstellen wie folgt festlegt

$$b_i = \begin{cases} 1 & \text{falls } a_{i,i} \neq 1 \\ 2 & \text{falls } a_{i,i} = 1 \end{cases}$$

Offensichtlich hat die Zahl r eine eindeutige Darstellung und liegt nicht im Bild von f, weil sie sich von jedem $f(n)$ aus dem Bild an der n–ten Stelle unterscheidet. Folglich ist die Abbildung f nicht surjektiv, ein Widerspruch zur Annahme, dass f eine Bijektion ist.

Die hier verwendete Beweistechnik bezeichnet man als Diagonalisierung. In der theoretischen Informatik wird sie in abgewandelter Form für Unmöglichkeitsbeweise eingesetzt (z.B. um zu zeigen, daß bestimmte Funktionen nicht berechenbar sind). Der folgende Satz beinhaltet eine weitere Anwendung dieser Technik.

Satz: Es gibt keine surjektive Abbildung von einer Menge M auf ihre Potenzmenge.

Beweis durch Widerspruch: Angenommen M wäre eine Menge mit einer surjektiven Abbildung $f : M \longrightarrow \mathcal{P}(M)$. Wir bilden die Menge $A = \{x \in M \mid x \notin f(x)\}$.
Da A Untermenge von M, also Element von $\mathcal{P}(M)$ ist, muß es ein $a \in M$ mit $f(a) = A$ geben, anderenfalls wäre f nicht surjektiv. Der Widerspruch besteht darin, daß aus der Definition von A die logische Äquivalenz der Aussagen $a \in A$ und $a \notin A$ folgt.