Definitionen

Aussage: Eine Aussage ist ein Satz, der entweder wahr (w) oder falsch (f) ist, also nie beides zugleich.

Konjunktion: Seien A und B Aussagen. Dann ist auch A **und** B eine Aussage - die sogenannte **(logische) Konjunktion**. Kurz: $(A \wedge B)$.
$(A \wedge B)$ ist genau dann wahr, wenn sowohl A als auch B wahr ist.

Disjunktion: Seien A und B Aussagen. Dann ist auch A **oder** B eine Aussage - die sogenannte **(logische) Disjunktion**. Kurz: $(A \vee B)$.
$(A \vee B)$ ist genau dann wahr, wenn A oder B wahr ist — oder beide.

Negation: Sei A eine Aussage. Dann ist auch **nicht** A eine Aussage - die **(logische) Negation**. Kurz: $(\neg A)$.
Die Aussage $(\neg A)$ ist genau dann wahr, wenn A falsch ist.

Implikation: Seien A und B Aussagen. Dann ist auch **wenn** A, **dann** B eine Aussage, die **(logische) Implikation**. Kurz: $(A \Rightarrow B)$.
Die Aussage $(A \Rightarrow B)$ ist genau dann falsch, wenn A wahr und B falsch ist.

Bi-Implikation: Seien A und B Aussagen. Dann ist auch A **genau dann, wenn** B eine Aussage, die **Bi-Implikation**. Kurz: (A $\iff$ B). Die Aussage (A $\iff$ B) ist genau dann wahr, wenn A und B beide den gleichen Wahrheitswert haben.

Formel: Eine aussagenlogische Verknüpfungvon Aussagenvariablen (durch endlich viele Junktoren) heißt **(aussagenlogische) Formel**. Aussagenvariablen werden auch als **atomare Formeln** bezeichnet.

Auswertung $A_B(x)$: Sei $B : Var \rightarrow \{w, f\}$ eine Belegung. Die Auswertung $A_B(F)$ ergibt sich **rekursiv**; das Rekursionsende sind die Variablen:

Tautologie: Eine **Tautologie** ist eine Formel, die stets wahr is, in deren Wahrheitswerteverlauf also ausschließlich den Wahrheitswert w vorkommt.

Kontradiktion: Eine **Kontradiktion** ist eine Formel, die stets falsch ist, in deren Wahrheitswerteverlauf also ausschließlich der Wahrheitswert f vorkommt.

Erfüllbarkeit: Eine Formel F heißt **erfüllbar**, wenn es mindestens eine Belegung der Aussagenvariablen gibt, die F wahr macht.

Äquivalenz: Zwei Formeln F und G heißen **(logisch) äquivalent** genau dann, wenn die Formel $(F \iff G)$ eine Tautologie ist. Dies wird durch $F \equiv G$ dargestellt.

Folgerungsbeziehung: Die Formel F **imliziert die Formel** G genau dann, wenn $(F \Rightarrow G)$ eine Tautologie ist.
Dies wird durch $F| = G$ dargestellt. (Aus F folgt G)

Aussageform: Eine **Aussageform** Über den Universen $U_1, \ldots, U_n$ ist ein Satz mit den freien Variablen $x_1, \ldots, x_n$.

Quantoren: Sei $p(x)$ eine Aussageform über dem Universum U. $\exists x : p(x)$ ist wahr genau dann, wenn ein u in U existiert, so dass $p(u)$ wahr ist.
$\forall : p(x)$ ist wahr genau dann, wenn $p(u)$ für jedes u aus U wahr ist.

gebundene Variablen: Eine Variable x wird in einer Formel $F = \forall x : G$ durch den Allquantor **gebunden**.
Analog wird x in $F = \exists x : G$ durch den Existenzquantor **gebunden**.

Normalisierte Darstellung: Eine Formel ist in normalisierter Variablenschreibweise, wenn gilt:

1. keine Variable kommt sowohl frei, als auch gebunden vor
2. keine Variable ist mehrfach gebunden

Wahrheitstabellen

A	B	(A ∧ B)
w	w	w
w	f	f
f	w	f
f	f	f

A	B	(A ∨ B)
w	w	w
w	f	w
f	w	w
f	f	f

A	¬A
w	f
f	w

A	B	(A ⇒ B)
w	w	w
w	f	f
f	w	w
f	f	w

A	B	(A ⟺ B)
w	w	w
w	f	f
f	w	f
f	f	w

Umformungsregeln	
Kommutativgesetz:	$(p \wedge q) \equiv (q \wedge p)$ $(p \vee q) \equiv (q \vee p)$
Assoziativgesetz:	$(p \wedge (q \wedge r)) \equiv ((p \wedge q) \wedge r)$ $(p \vee (q \vee r)) \equiv ((p \vee q) \vee r)$
Distributivgesetz:	$(p \wedge (q \vee r)) \equiv ((p \wedge q) \vee (p \wedge r))$ $(p \vee (q \wedge r)) \equiv ((p \vee q) \wedge (p \vee r))$
Idempotenzgesetz:	$(p \wedge p) \equiv p$ $(p \vee p) \equiv p$
Doppelnegation:	$\neg(\neg p) \equiv p$
de Morgan Gesetz:	$\neg(p \wedge q) \equiv ((\neg p) \vee (\neg q))$ $\neg(p \vee q) \equiv ((\neg p) \wedge (\neg q))$
Tautologieregeln:	$(p \wedge q) \equiv p$ $(p \vee q) \equiv q$ wobei: (q = Tautologie)
Kontradiktionsregeln:	$(p \wedge q) \equiv q$ $(p \vee q) \equiv p$ wobei: (q = Kontradiktion)

Umformungsregeln für Quantoren	
Negations-regeln:	$\neg \forall x : p(x) \equiv \exists x : (\neg p(x))$ $\neg \exists x : p(x) \equiv \forall x : (\neg p(x))$
Ausklammer-regeln:	$(\forall x : p(x) \wedge \forall y : q(y)) \equiv \forall z : (p(z) \wedge q(z))$ $(\exists x : p(x) \vee \exists y : q(y)) \equiv \exists z : (p(z) \vee q(z))$
Vertauschungs-regeln:	$\forall x \forall y : p(x,y) \equiv \forall y \forall x : p(x,y)$ $\exists x \exists y : p(x,y) \equiv \exists y \exists x : p(x,y)$

Definitionen

Menge Eine **Menge** ist eine Zusammenfassung **wohlunterschiedenen Objekten** zu einem Ganzen.
Es muss zudem einwandfrei entscheidbar sein, ob ein Objekt der Gesamtheit angehört oder nicht.
Die Objekte der Menge heißen **Elemente** der Menge.

gleichheit von Mengen: Zwei Mengen A und B heißen **gleich** ($A = B$) genau dann, wenn jedes Element aus A auch ein Element aus B ist – und umgekehrt.
für alle $x \in A$ gilt auch $x \in B$ und für alle $y \in B$ gilt auch $y \in A$
Sind die Mengen A und B nicht gleich, notiert man $A \neq B$.

Komplementärmenge: Sei $E(x)$ eine Aussageform über der Menge U.
Dann heißen die Mengen $M = \{x \in U | E(x)\}$ und $\bar{M} = \{x \in U | \neg E(x)\}$ in U komplemetär.
$\bar{M}$ heißt **Komplementärmenge** oder **Komplement** von M in U.

Leere Menge: Die Menge, die kein Element enthält, heißt **leere Menge** und wird mit $\emptyset$ bezeichnet.

Teilmenge: Eine Menge B heißt **Teilmenge** einer Menge A genau dann, wenn jedes Element von B auch ein Element von A ist. ($B \subseteq A$ gilt gdw. $\forall x : x \in B \rightarrow x \in A$) .
A heißt dann **Obermenge** von B. B heißt echte Teilmenge von A.

Potenzmenge: Sei M eine Menge. Die Menge aller Teilmengen von M heißt **Potenzmenge** von M und wird $\mathscr{P}(M)$ notiert:
$\mathscr{P}(M) := \{X | X \subseteq M\}$

Vereinigung: Seien M und N Mengen. Die Vereinigungsmenge ist Definiert durch: $M \cup N := \{x | x \in M \ oder \ x \in N\}$

Schnitt: Seien M und N Mengen. Der Schnitt ist Definiert als $M \cap N := \{x | x \in M \ und \ x \in N\}$

Differenz: Seien M und N Mengen. Die Differenz ist definiert durch $M | N := \{x | x \in M \ und \ x \notin N\}$

Mengenfamilie: Die Mengenfamilie $\mathscr{F}$ sei definiert als $\mathscr{F} \subseteq \mathscr{P}(M)$
Dann ist die Vereinigung aller Mengen aus $\mathscr{F}$:
$\bigcup \mathscr{F} = \{x | \exists N \in \mathscr{P}(M) : (N \in \mathscr{F} \wedge x \in N)\}$
Der Durchschnitt aller Mengen aus $\mathscr{F}$:
$\bigcap \mathscr{F} = \{x | \forall N \in \mathscr{P}(M) : (N \in \mathscr{F} \rightarrow x \in N)\} \cap \bigcup \mathscr{F}$

kartesisches Produkt: Seien A und B Mengen.
Das **kartesische Produkt** (auch Kreuzprodukt) von A und B ist definiert durch
$A \times B := \{(a, b) | a \in A und b \in B\}$

Isomorphie: Zwei Mengen X und Y sind **isomorph**, wenn dich ihre Elemente eins zu eins zuordnen lassen. ($X \cong Y$)

Disjunkte Vereinigung: Die **disjunkte Vereinigung** von A und B ist definiert durch:
$A \uplus B := (A \times 0) \cup (B \times 1)$

Rechengesetze

Assoziativgesetz:	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
Kommutativgesetz:	$A \cup B = B \cup A$ $A \cap B = B \cap A$
Distributivgesetz:	$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$
De-Morgan:	$A \| (B \cup C) = (A \| B) \cap (A \| C)$ $A \| (B \cap C) = (A \| B) \cup (A \| C)$
Absorption:	$A \cap (A \cup B) = A$ $A \cup (A \cap B) = A$
Idempotenz:	$A \cap A = A$ $A \cup A = A$
Komplement:	$A \cap \bar{A} = \emptyset$ $A \cup \bar{A} = G$

Zahlenmengen

natürliche Zahlen:	$\mathbb{N} = 0, 1, 2, \ldots$
ganze Zahlen:	$\mathbb{Z} = \{0, -1, 1, -2, 2, \ldots\}$
rationale Zahlen:	$\mathbb{Q} = \{\frac{m}{n} \| m \in \mathbb{Z}, n \in \mathbb{N}, n \neq 0\}$
reelle Zahlen:	$\mathbb{R}$
irrationale Zahlen:	$\mathbb{R} \backslash \mathbb{Q}$
komplexe Zahlen:	$\mathbb{C}$
Dabei gilt:	$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

Schreibweisen Mengen

explizit: $M = \{1, 2, 3, 4\}$

verbal: "Die Menge aller nicht-negativen, geraden Ganzzahlen"

unendliche Mengen: $M := \{0, 2, 4, 6, 8, \ldots\}$

implizit: $M := \{x \in \mathbb{N} | x ist gerade\}$

Potenzmenge:

Jede mögliche Teilmenge einer Menge. Bsp: $M := \{1,2,3\}$ dann ist $\mathscr{P}(M) := \{\emptyset\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}$.

disjunkten Vereinigung:

Bei der disjunkten Vereinigung zweier Mengen kreuzt man die jeweiligen Elemente mit einer Menge aus einem Index ($A \times 1$, $B \times 2$ usw.) und vereinigt die daraus resultierenden Kreuzprodukte. Dadurch ist jedem Element aus $A \uplus B$ anzusehen, ob es aus A oder B stammt.

Definitionen

Relation: Eine **Relation** zwischen A und B ist eine Teilmenge von $A \times B$. Man schreibt aRb.
$aRb \leftrightarrow (a,b) \in R$

Inverse Relation: Sei $R \subseteq A \times B$ eine Relation zwischen A und B. Die **Inverse Relation** zu R wird R^{-1} notiert.
$R^{-1} = \{(y,x) \in B \times A | (x,y) \in R\}$

Komposition: Seien $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$ zweistellige Relationen.
Die Verknüpfung $(R \circ S) \subseteq (M_1 \times M_3)$ heißt **Komposition** der Relationen R und S:
$R \circ S := \{(x,z) | \exists y \in M_2 : (x,y) \in R \wedge (y,z) \in S\}$

Reflexivität: Eine Relation $R \subseteq A^2$ über einer Menge A heißt **reflexiv**, wenn jedes Element in Relation zu sich selbst steht:
$\forall a \in A : (a,a) \in R$

Symmetrie: Eine Relation $R \subseteq A^2$ über einer Menge A heißt **symmetrisch**, wenn die Reihenfolge der Elemente keine Rolle spielt:
$(a,b) \in R \to (b,a) \in R$

Antisymmetrie: Das Gegenteil von Symmetrie:
$(a,b) \in R \to \neg(b,a) \in R$

Antisymmetrie: Eine Relation R $\subseteq A^2$ über einer Menge A heißt **antisymmetrisch**, wenn aus der Symmetrie die Identität folgt:
$((a,b) \in R \wedge (b,a) \in R) \to a = b$

Transitivität: Eine Relation $R \subseteq A^2$ über einer Menge A heißt **transitiv**, wenn aus einer Kette das mittlere Element entfernt werden kann:
$((a,b) \in R \wedge (b,c) \in R) \to (a,c) \in R$

Totalität Eine Relation $R \subseteq A^2$ über einer Menge A heißt **total** (auch: linear), wenn je zwei Elemente in mindestens einer Richtung in Relation stehen:
$\forall (a,b) \in A : (a,b) \in R \vee (b,a) \in R$

Teilbarkeitsrelation: Sei $a \in \mathbb{N}^+, b \in \mathbb{Z}$.
Wir schreiben $a|b$, wenn "a ein Teiler von b" ist, d.h. wenn gilt:
$\exists k \in \mathbb{Z} : b = k \cdot a$

Rechtseindeutigkeit: Eine Relation $R \subseteq A \times B$ heißt **rechtseindeutig** (nacheindeutig) wenn Für alle $a \in A$ gilt:
$((a,b) \in R \wedge (a,c) \in R) \to b = c$

Linkseindeutigkeit: Eine Relation $R \subseteq A \times B$ heißt **linkseindeutig** wenn für alle $a \in B$ gilt:
$((b,a) \in R \wedge (c,a) \in R) \to b = c$

Eindeutigkeit: Eine Relation $R \subseteq A \times B$ heißt **eindeutig** wenn:
R rechtseindeutig und R linkseindeutig.

Linkstotal: Eine Relation $R \subseteq A \times B$ heißt **linkstotal** wenn:
$\forall a \in A \exists b \in B : (a,b) \in R$

Rechtstotal: Eine Relation $R \subseteq A \times B$ heißt **rechtstotal**:
$\forall b \in B \exists a \in A : (a,b) \in R$

Irreflexiv: Eine Relation $R \subseteq A^2$ über einer Menge A heißt **irreflexiv** wenn:
$\forall a \in A : (a,a) \notin R$

Alternativ: Eine Relation $R \subseteq A^2$ über einer Menge A heißt **alternativ** wenn:
$\forall a,b \in R : (a,b) \in R xor (b,a) \in R$

Äquivalenzrelation: Ist eine Relation ~ reflexiv, symmetrisch und transitiv, so wird sie **Äquivalenzrelation** genannt.

Äquivalenzklasse: Gegeben sei eine Äquivalenzrelation R über der Menge A. Dann ist Für $a \in A : [a]_R = \{x | (a,x) \in R\}$ die **Äquivalenzklasse** von a.

Zerlegung: Sei A eine nichtleere Menge. Eine **Zerlegung** (oder **Partition**) von A ist eine Mengenfamilie $\mathcal{Z} \subseteq \mathcal{P}(A)$ mit:

1. Überdeckung: $A \subseteq \bigcup \mathcal{Z}$
2. $\emptyset \notin \mathcal{Z}$
3. Disjunktivität: $\forall M_1, M_2 \in \mathbb{Z}$ gilt entweder $M_1 = M_2 \vee M_1 \cap M_2 = \emptyset$

Eine Zerlegung ist also eine Einteilung von A in nicht leere, paarweise elementfremde Teilmengen, deren Vereinigung mit A übereinstimmt.

Abschluss: Sei R eine Relation über A und sei ϕ (reflexiv, usw.) eine Eigenschaft von Relationen.
Die Relation R^* heißt **Abschluss** von R bezüglich ϕ, wenn gilt:

1. $R*$ besitzt die Eigenschaft ϕ
2. $R \subseteq R*$
3. Für alle Relationen D, die R umfassen und ebenfalls die Eigenschaft ϕ besitzen, gilt $R* \subseteq S$

Mit anderen Worten: $R*$ ist die kleinste Relation, die R umfasst und die Eigenschaft ϕ besitzt.
Besitzt R bereits die Eigenschaft, so fügt der Abschluss nichts hinzu: $R* = R$

Ordnung: Ist eine Relation $\leq$ reflexiv, antisymmetrisch und transitiv, so ist sie eine **Halbordnung** (partielle Ordnung)
a und b heißen **vergleichbar** bzgl. $\leq$, falls $a \leq b \vee b \leq a$ gilt (sonst unvergleichbar).
Ist eine Halbordnung zusätzlich total, heißt die **(totale) Ordnung** und A heißt durch $\leq$ geordnet.

minimal/maximal: Sei $\leq$ eine Halbordnungsrelation auf A. Sei M eine nichtleere Teilmenge von A.
Ein Element $m \in M$ heißt **maximal** Element in M, wenn:
$\forall m' \in M : m \leq m' \Rightarrow m = m'$
m heißt **minimales** Element, wenn:
$\forall m' \in M : m' \leq m \Rightarrow m = m'$

Spezielle Relationen

Es gibt spezielle Relationen, die im weiteren auch noch genutzt werden:

Leere Relation:	$R = \emptyset$
All-Relation:	$R = A \times B$
Identität (über M):	$R = Id_M = \triangle_M := \{(x,x) \mid x \in M\}$

Definitionen

Term: Ein Term setzt sich zusammen aus:

- Konstanten: $e, \pi, \ldots$
- Variablen: $x, y, \ldots$
- Operatoren: $+, -, \times, \surd, \ldots$
- Funktionen: $f(x), sin(x), \ldots$

Gleichung: Eine Gleichung $t_1 = t_2$ setzt zwei Terme in Beziehung.

Grad (von Fkt.): Ein reellwertiges Polynom ist ein Ausdruck der Form ($x \in \mathbb{R}$):
$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_n x^n + a_1 x^1 + a_0$
Falls $a_n \neq 0$, dann ist n der Grad des Polynoms.

Logarithmus: $log_a(c) = x$ für $a^x = c$

Brüche	
Addition bei gleichem Nenner:	$\frac{a}{d} + \frac{b}{d} = \frac{a+b}{d}$
Multiplikation:	$\frac{a}{c} + \frac{b}{d} = \frac{ab}{cd}$
Kürzen eines gleichen Faktors:	$\frac{a \cdot c}{d \cdot c} = \frac{a}{d} \cdot \frac{c}{c} = \frac{a}{d} \cdot 1 = \frac{a}{d}$
Erweitern um c:	$\frac{a}{d} = \frac{a}{d} \cdot 1 = \frac{a}{d} \cdot \frac{c}{c} = \frac{a \cdot c}{d \cdot c}$
Addieren mit verschiedenen Nennern (durch erweitern):	$\frac{a}{c} + \frac{b}{d} = (\frac{a}{c} \cdot \frac{d}{d}) + (\frac{b}{d} \cdot \frac{c}{c}) = \frac{ad+bc}{cd}$

Summen-/Produktnotation

Summennotation: $\sum_{i=1}^{n} a_i := a_1 + a_2 + \cdots + a_n$ ist äquivalent zu $\sum_{1 \leq i \leq n} a_i$

Produktnotation: $\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \cdots \cdot a_n$

Exponential-Gesetze

Sei $m, n \in \mathbb{N}$:

- $b^{-n} = \frac{1}{b^n}$
- $b^m \cdot b^n = b^{m+n}$
- $\frac{b^m}{b^n} = b^{m-n}$
- $(b^m)^n = b^{m \cdot n}$
- $b^m \cdot c^m = (b \cdot c)^m$
- $\frac{b^m}{c^m} = (\frac{b}{c})^m$
- $\sqrt[n]{x^m} = x^{\frac{m}{n}}$
- $x^{-\frac{m}{n}} = \frac{1}{\sqrt[n]{x^m}}$

Binomische Formeln

- $(a+b)^2 = a^2 + 2ab + b^2$
- $(a-b)^2 = a^2 - 2ab + b^2$
- $(a-b) \cdot (a+b) = a^2 - b^2$

Logarithmen	
Umkehrung:	$log_b(b^q) = q \Leftrightarrow b^{log_b(q)} = q$
Mul/Additivität:	$log_b(xy) = log_b(x) + log_b(y)$ $log_b(a^q) = q log_b(a)$
Basiswechsel:	$log_b(a) = \frac{log_d(a)}{log_d(b)}$

Trigonometrische Funktionen	
Tangensfunktion:	$tan(x) := \frac{sin(x)}{cos(x)}$
Co-Tangensfunktion:	$cot(x) := \frac{cos(x)}{sin(x)}$

Zusammenfassung

- Ein Term ist ein Ausdruck, der für einen Zahlenwert steht. Ein Beispiel für einen Term ist z.B: $sin(x)^2 + cos(x^2)$ Wobei $x^2 - 3 = 0$ kein Term ist, sondern eine Gleichung.
- für die Summen-/Produktnotation gibt man unten die untere Grenze und oben die obere Grenze die Summierung/Produktbildung an. Bsp:
  $\sum_{i=1}^{5} a_i := 1+2+3+4+5$
  $\prod_{0 \leq i \leq 5, i\%2=1} (i+1) := (1+1) \cdot (3+1) \cdot (5+1)$
- Hyperbeln können nach ähnlichem Schema umgeformt werden. Dabei wird ein Term $\frac{1}{x}$ zu x^{-1}. Wenn der Nenner einen Exponenten besitzt kann dieser auch wieder umgeformt werden, damit die Rechengesetze gelten. $\frac{1}{x^m} = x^{-m}$
- Wurzelfunktionen können umgeformt werden. Wenn man z.B einen Term $\sqrt[2]{x}$ hat, kann dieser zu $x^{\frac{1}{2}}$ umgeformt werden. Dadurch gelten auch für Wurzeln, die Exponentialgesetze.
- Logarithmen können genutzt werden, wenn bei einer Exponentialfkt. der Exponent unbekannt, aber das Ergebnis bekannt ist. Dabei gibt es den Spezialfall des natürlichen Logarithmus. Dieser ist definiert als:
  $ln(x) := log_e(x)$

Definitionen

Abbildung: Unter einer Abbildung f von einer Menge A in einer Menge B versteht man eine Vorschrift, die jedem $a \in A$ eindeutig ein bestimmtes $b = f(a) \in B$ zuordnet.

- Schreibweise: $f : A \to B$.
- für die Elementzuordnung verwendet man die Schreibweise $a \rightarrowtail b = f(a)$
- Man bezeichnet b als das Bild von a.
- a ist ein Urbild von b

Abbildung: Sei $F \subseteq A \times B$ eine linksvollständige und rechtseindeutige Relation.

1. F ist linksvollständig: für alle $a \in A$ gilt: Es existiert ein $b \in B$, so dass $(a, b) \in R$
2. F ist rechtseindeutig: für alle $a \in A$ und alle $b_1, b_2 \in B$ gilt: $(a, b_1) \in R$ und $(a, b_2) \in R$, dann $b_1 = b_2$

Das Tripel $f = (A, B, F)$ heißt Abbildung von A nach B.

- F heißt Graph der Abbildung
- A ist der Definitionsbereich
- B ist der Bildbereich

Zu jedem $a \in A$ wird das eindeutig bestimmte $b \in B$ mit aFb als Bild von f bei a bezeichnet. Notation: $f(a)$

Bild: Sei $f : A \to B$ und $M \subseteq A$

- Das Bild von M unter f ist die Menge: $f(M) := \{f(x) | x \in M\}$
- Insbesondere heißt $Bild(f) := f(A)$ das (volle) Bild von f (auch Wertebereich).
- Das Urbild einer Teilmenge $N \subseteq B$ ist definiert durch: $f^{-1}(N) := \{a \in A | f(a) \in N\}$

Einschränkung: Sei $f = (A, B, F)$ eine Abbildung und $M \subseteq A$.
Die Abbildung $f|_m = (M, B, F \cap (M \times B))$ heißt Einschränkung von f auf M.

Komposition: Kompositionen von Funktionen ist hier definiert als: $a \rightarrowtail (g \circ f)(a) = g(f(a)), a \in A$

Injektiv: Wenn für alle $a, a' \in A$ mit $a \neq a'$ gilt $f(a) \neq f(a')$.

surjektiv: Falls es für jedes $b \in B$ ein $a \in A$ gibt mit $f(a) = b$.

bijektiv: Falls f sowohl injektiv als auch surjektiv ist.

Inverse Abbildung: Sei $f : A \to B$ eine bijektive Abbildung. Da existiert zu f stets eine Abbildung g mit $g \circ f = id_A$ und $f \circ g = id_B$. g heißt die zu f inverse Abbildung oder Umkehrabbildung. Notation: f^{-1}.

Gleichmächtig: Seien M und N zwei Mengen. M und N heißen gleichmächtig (oder umfangsgleich) genau dann, wenn es eine bijektive Abbildung $f : M \to N$ gibt. Notation $M \cong N$. ($|M| = |N|$)

endlich: Eine Menge M heißt endlich genau dann, wenn $M = \emptyset$ oder es für ein $n \in \mathbb{N}$ eine bijektive Abbildung $b : M \to \mathbb{N}_n$ gibt.

unendlich: Eine Menge M heißt unendlich genau dann, wenn M nicht endlich ist.

abzählbar: Eine Menge M heißt abzählbar genau dann, wenn M endlich ist oder es eine bijektive Abbildung $b : M \to \mathbb{N}$ gibt.

abzählbar unendlich: Eine Menge M heißt abzählbar unendlich genau dann, wenn M abzählbar und unendlich ist.

überabzählbar: Eine Menge heißt überabzählbar genau dann, wenn M nicht abzählbar ist.

Folge: Eine Folge Reeller Zahlen ist eine Funktion $f : \mathbb{N} \to \mathbb{R}$.

konvergenz: Eine Folge (a_n) konvergiert gegen $a \in \mathbb{R}$, wenn gilt: Zu jedem $\epsilon > 0$ existiert ein $N \in \mathbb{R}$, so dass gilt:
$|a_n - a| < \epsilon$ für alle $n > N$
Die Zahl a heißt Grenzwert (Limes) der Folge (a_n). Eine Folge (a_n) mit Grenzwert heißt konvergent. Man schreibt: $lim_{n\to\infty} a_n = a$ oder auch $a_n \to a$ für $n \to \infty$.
Eine Folge, die gegen $a = 0$ konvergiert, heißt Nullfolge.

Reihe: Sei (a_n) eine Folge. Die Reihe (s_n) ergibt sich aus (a_n) durch Summation: $s_n := \sum_{k=0}^{n} a_n$

beschränkt(e Folge): Eine Folge (a_n)heißt beschränkt, wenn es eine Zahl s gibt, so dass $|a_n| \leq s$ für alle n gilt.

monoton wachsend: Eine Folge (a_n) heißt monoton wachsend, wenn $a_n \leq a_{n+1}$ für alle n gilt.

monoton fallend: Eine Folge (a_n) heißt monoton fallend, wenn $a_n \geq a_{n+1}$ für alle n gilt.

supremum: Eine Zahl s heißt Suprmum einer Menge $M \subseteq \mathbb{R}$, wenn s die kleinste obere Schranke von M ist, d.h:

- s ist obere Schranke von M ($\forall m \in M : m \leq s$)
- jede Zahl $x < s$ ist keine obere Schranke von M

infimum: Eine Zahl i heißt Infimum einer Menge $M \subseteq \mathbb{R}$, wenn i die größte untere Schranke von M ist.

Häufungspunkt: h heißt Häufungspunkt einer Folge (a_n), wenn jede Umgebung $K_\epsilon(h)$ von h undendlich viele Folgeglieder enthält. Also:
$|h - a_n| < \epsilon$ für unendlich viele n

Cauchy-Folge: Eine Folge (a_n) heißt Cauchy-Folge, wenn es zu jedem $\epsilon > 0$ ein n gibt so dass gilt: $|a_n - a_m| < \epsilon$, falls n und m > N sind.

Asymptotisch: Zwei Folgen (a_n) und (b_n) mit $b_n \neq 0$ heißen asymptotisch gleich, falls die Folge $(\frac{a_n}{b_n})$ gegen 1 konvergiert. Notation: $a_n \tilde{=} b_n$.

O-Notation: Sei $g : \mathbb{N} \to \mathbb{R}$. Eine Funktion $f : \mathbb{N} \to \mathbb{R}$ gehört zu der Menge $O(g)$, wenn es eine Konstante $c \in \mathbb{R}^+ gibt, sodass |f(n)| \leq c \circ |g(n)|$ für fast alle n gilt.

Rechenregeln Folgen
• $lim_{n\to\infty} \frac{1}{n^s} = 0$ für jedes positive $s \in \mathbb{Q}$. • $lim_{n\to\infty} \sqrt[n]{a} = 1$ für jedes reelle $a > 0$. • $lim_{n\to\infty} \sqrt[n]{n} = 1$. • $lim_{n\to\infty} q^n = 0$ für jedes reelle q mit $|q| < 1$.

Direkter Beweis

Wird bei wenn-dann-Aussagen genutzt. Modus ponens: Aus p und $(p \Rightarrow q)$ ergibt sich s. Vorgehen dabei ist:

1. Satz genau studieren–Welche Parameter werden gestellt?
2. Bei der Hypothese beginnen. Diese muss wahr sein, denn $(p \Rightarrow q)$.
3. ggf. die Hypothese mathematisch darstellen Bsp:
   gerade Zahl $n = 2k$
   ungerade Zahl $n = 2k + 1$
4. Dann durch (beliebig viele) Folgeaussagen von der Hypothese zur Schlussfolgerung kommen.
   $p \Rightarrow s_1, s_1 \Rightarrow s_2, s_2 \Rightarrow q$ wobei $s_1 - s_n$ wieder wahre Aussagen sind.
5. Praktisch dabei: Es muss nicht jeder Schritt aufgeschrieben werden–nur solche, die wichtig für die Beweisführung des Lemma sind.

Beispiel:

Satz: "Die Summe von drei aufeinander folgenden natürlichen Zahlen ist durch drei teilbar."
Gegebene Informationen: $n \in \mathbb{N}$ **und**
$p = n + (n+1) + (n+2)$ **ist durch 3 teilbar**

1. $n \in \mathbb{N} \Rightarrow (n+1) \in \mathbb{N}$
2. $\Rightarrow n + (n+1) + (n+2) = (3n+3)$
3. $\Rightarrow (3n+3) = 3(n+1)$

Damit ist der Satz bewiesen. □

Kontraposition

Ist dem Direkten Beweis sehr ähnlich. Nur dass hier die Behauptung negiert und umgekehrt wird um zu der äquivalenten Kontraposition zu gelangen. Aus $(p \Rightarrow q)$ wird also $(\neg q \Rightarrow \neg p)$. Man beweist also quasi rückwärts.

Beispiel:

Satz: "Wenn a^2 eine ungerade Zahl ist, dann ist a ungerade". Die äquivalente Kontraposition dazu ist: "Wenn a gerade, dann ist a^2 gerade".

1. $\neg q =$ „a ist gerade“
2. $a = 2 \cdot k$ (Def. gerade Zahl)
3. $a \cdot a = (2 \cdot k) \cdot a$ (mul. mit a)
4. $a^2 = 2 \cdot (k \cdot a)$ (Assoziativgesetz)
5. $a^2 = 2 \cdot k'$ (wobei $k' = a \cdot k$)
6. $\neg p = a^2$ ist gerade (durch $2 \cdot k'$)

Damit ist der Satz bewiesen. □

Wiederspruch

Basiert wieder auf der Implikation $(p \Rightarrow q)$. Hier wird aber ein Wiederspruch erzeugt sodass $(p \wedge \neg q)$

Beispiel:

Satz: "Wenn a und b gerade natürliche Zahlen sind, dann ist auch $a \cdot b$ gerade".

1. Annahme: $a \cdot b$ ist ungerade.
2. $a \cdot b = 2 \cdot (a \cdot k)$ (denn: $b = 2 \cdot k$)
3. $a \cdot k$ ist gerade. Also muss $a \cdot b$ gerade sein.

Damit ist der Satz bewiesen. □

Äquivalenzbeweis

Bei dieser Beweistechnik unterteilt man die Aussage in zwei direkte Beweise. Aus $(p \Leftrightarrow q)$ wir dann $(p \Rightarrow q)$ und $(q \Rightarrow p)$.

Beispiel:

Satz: "a ist gerade genau dann, wenn a^2 gerade ist".
Dabei ist $p =$"a ist gerade" und $q =$ "a^2 ist gerade"
In diesem Fall ist $(p \Rightarrow q)$ schon bewiesen. (siehe Bsp. Kontraposition)
$(q \Rightarrow p)$ wird durch Kontraposition bewiesen:

1. $\neg p$: „a ist ungerade“
2. $a - 1 = 2 \cdot k$ (def. ungerade Zahl umgestellt)
3. $a = 2 \cdot k + 1$
4. $a^2 = (2 \cdot k)^2 + 2 \cdot (2 \cdot k) + 1$ (quadrat schon ausmul.)
5. $a^2 = 2 \cdot (2 \cdot k \cdot k + 2 \cdot k) + 1$
6. a^2 ist ungerade

Da nun sowohl $(p \Rightarrow q)$ als auch $(q \Rightarrow p)$ bewiesen ist, ist der Äquivalenzbeweis erbracht. □

Fallunterscheidung

Jede Aussage p ist logisch äquivalent zu $(q \Rightarrow p) \wedge (\neg q \Rightarrow p)$. Dann Beweist man einfach beide Fälle.

Beispiel:

Satz: "Jede natürliche Zahl n^2 geteilt durch 4 lässt entweder den Rest 1 oder 0".

n ist gerade:

- $n = 2m$ für $m \in \mathbb{M}$
- $n^2 = 4m^2$
- n^2 ist durch 4 teilbar
- Rest ist 0
- Rest ist 1 oder 0

n ist ungerade:

- $n = 2m + 1$ für $m \in \mathbb{M}$
- $n^2 = 4m^2 + 4m + 1 = 4(m^2 + m) + 1$
- n^2 ist durch 4 teilbar mit Rest 1
- Rest ist 1
- Rest ist 1 oder 0

Damit sind alle Fälle betrachtet und die Aussage bewiesen. $\square$

Beweis mit Quantoren

Bei universellen Aussagen ($\forall x$) muss man unabhängig von konkreten Werten für die Quantifizierten Variablen Beweisen. Deswegen beginnt und beendet man den Beweis etwas anders:
Bei der Aussage $\forall x : (p(x) \Rightarrow q(x))$ würde man so vorgehen:

1. Sei a ein beliebiger, aber fester Wert aus dem Universum (also der Menge).
2. <Beweis>
3. Da a beliebig gewählt werden kann, folgt: $\forall x : (p(x) \Rightarrow q(x))$.

Damit ist die Aussage Bewiesen □

Bei existenziellen Aussagen $\exists x : (p(x) \Rightarrow q(x))$ geht man so vor:

1. Sei $a =$ <Ein geeignetes Element aus dem Universum>.
2. <Beweis>
3. Damit ist die Existenz eines a mit der Eigenschaft $(p(x) \Rightarrow q(x))$ bewiesen.
4. Damit ist die Gültigkeit der Aussage $\exists x : (p(x) \Rightarrow q(x))$ bewiesen.

Definitionen

Induktion: Ist $A(n)$ eine von $n \in \mathbb{N}$ abhängige Aussage, so sind dazu die folgenden beiden Beweisschritte 1 und 3 durchzuführen:

1. Induktionsanfang (IA): Man zeigt, dass $A(0)$ richtig ist.
2. Induktionsbehauptung (IB): Annahme, dass $A(k)$ für ein festes k richtig ist.
3. Induktionsschluss (IS): Man zeigt: Aus der Annahme, dass $A(k)$ richtig ist (Induktionsanker), folgt, dass auch $A(k+1)$ richtig ist:
   $A(k) \Rightarrow A(k+1)$

Dann ist gewährleistet, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt.
Wichtig: Wird der Induktionsanfang nicht für $n_0 = 0$, sondern für ein $n_0 > 0$ durchgeführt, so gilt die Aussage nur für alle $n \geq n_0$.

Induktiv erzeugte Menge: Die Menge M wird wie folgt induktiv definiert:

- Basismenge: jedes x mit˜gehört zu M.
- Erzeugungsregel: Sind m_1 und m_2 Elemente aus M, dann auch das Element $m = randoomFunction(m_1, m_2)$.
- Nur Elemente, die so gebildet werden können, gehören zu M.

Wörter/Zeichenketten: Sei $\sum$ ein Alphabet. Die Menge $\sum^*$ aller Wörter über $\sum$ ist induktiv definiert:

- Basismenge: Das leere Wort ϵ gehört zu $\sum^*$; das heißt: $\epsilon \in \sum^*$
- Erzeugungsregel: Ist w ein Wort in $\sum^*$ und a ein Element von $\sum$, dann gehört die Konkatenation wa zu $\sum^*$

Länge eines Wortes: Sei $\sum$ ein Alphabet. Die Länge eines Wortes $w \in \sum^*$ ist induktiv definiert durch:

- Die Länge des leeren Wortes ϵ ist 0, $|\epsilon| = 0$
- Sei $w \in \sum^*$ und $a \in \sum$. Dann ist $|wa| = |w| + 1$.

Aussagenlogische Formeln: Sei X die Menge der aussagenlogischen Variablen. Die Menge der aussagenlogischen Formeln wird wie folgt definiert:

- Basismenge: Die Konstanten w und f sind aussagenlogische Formeln.
- Basismenge: Jede Aussagenlogische Variable $x \in X$ ist eine aussagenlogische Formel.
- Erzeugungsregel: Sind α und β aussagenlogische Formeln, so sind auch $(\neg\alpha), (\alpha \wedge \beta), (\alpha \vee \beta), (\alpha \Rightarrow \beta) und (\alpha \Leftrightarrow \beta)$ aussagenlogische Formeln.

Beispiel Induktion

Satz: Für alle natürlichen Zahlen n gilt $\sum_{i=0}^{n} i = \frac{1}{2}n(n+1)$.

- Induktionsanfang (IA): Die Eigenschaft gilt für $n = 0$, denn $\sum_{i=1}^{n} i = 0$ und $\frac{1}{2}n(n+1) = 0$.
- Induktionsbehauptung (IB): Wir nehmen an, dass die Summenformel für ein beliebiges, aber festes k gilt: $\sum_{i=0}^{k} i = \frac{1}{2}k(k+1)$.
- Induktionsschluss (IS): Unter der Vorraussetzung, dass die IB gilt, wollen wir die Summenformel für $k+1$ zeigen: $\sum_{i=1}^{k+1} i = \frac{1}{2}k(k+1)(+2)$ Dies können wir durch folgende Umformung zeigen:
  $\sum_{i=1}^{k+1} i = (\sum_{i=0}^{k}) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+(2k+2)}{2} = \frac{k^2+3k+2}{2} = \frac{(k+1)(k+2)}{2}$

Nach dem Induktionsprinzip gilt die Aussage also für alle natürlichen Zahlen.

Verallgemeinerte vollständige Induktion

Diese wird genutzt, wenn die Induktionsannahme $A(n)$ nicht genug ist, um den Induktionsschluss $A(n+1)$ beweisen zu können. Die Aussage $A(n)$ gilt für alle natürlichen Zahlen, wenn sowohl der Induktionsanfang $A(0)$ als auch der Induktionsschritt gilt:

$$\forall n \in \mathbb{N} : (A(0) \wedge \cdots \wedge A(n)) \Rightarrow A(n+1)$$

Beispiel:

Sei n eine natürliche Zahl und $n \geq 2$. Dann ist n das Produkt von Primzahlen.

- **IA:** Die Eigenschaft gilt für $n = 2$, denn 2 ist das Produkt von sich selbst, also einer Primzahl.
- **Starke Induktionsbehauptung (IB):** für festes n nehmen wir an, dass sich alle Zahlen $2, 3, \dots, n$ als Produkt von Primzahlen schreiben lassen.
- **Induktionsschluss (IS):** Z.z.: $n+1$ ist ein Produkt von Primzahlen.
  Fall 1: $n+1$ ist eine Primzahl, dann auch ein Produkt von Primzahlen (sich selbst).
  Fall 2: $n+1$ ist keine Primzahl, dann gibt es mindestens zwei echte Teiler b und c:
  Da b und c beide echt kleiner als $n+1$ sind, gilt die IB für sie:
  $$b = p_1 \dots p_k c = q_1 \dots q_l$$
  Damit gilt: $n+1 = b \cdot c = (p_1 \dots p_k) \cdot (q_1 \dots q_l)$
  $n+1$ ist also ein Produkt von Primzahlen.

Nach dem verallgemeinerten Induktionsprinzip gilt die Aussage also für alle natürlichen Zahlen $n \geq 2$.

"Induktionsschablone"

1. **(IA):** Die Eigenschaft gilt für $n = 0$, denn ...
2. **(IB):** Wir nehmen an, dass die Summenformel für ein beliebiges, aber festes k gilt: $\sum_{i=0}^{k} \cdots$
3. **(IS):** Unter der Voraussetzung, dass die IB gilt, wollen wir die Summenformel für $k+1$ zeigen: $\sum_{i=0}^{k+1} \dots$

Nach dem Induktionsprinzip gilt die Aussage also für alle natürlichen Zahlen.

Peano-Axiome:

$$0 \cdot m = 0$$
$$(n+1) \cdot m = (n \cdot m) + m$$
$$n \cdot (m_1 + m_2) = n \cdot m_1 + n \cdot m_2$$