I. Grundlagen

1. Logik und Beweistechniken

1.1 Def.: (”logische Aussage”, ”Wahrheitswert”)

Eine **logische Aussage** (bezeichnet mit A, B, C, . . .) ist ein Satz, der entweder wahr oder falsch ist. Als **Wahrheitswert** $w(A)$ einer Aussage A definiert man:

$$w(A) := \begin{cases} 0, & \text{wenn } A \text{ falsch ist,} \\ 1, & \text{wenn } A \text{ wahr ist.} \end{cases}$$

Man spricht von **zweiwertiger Aussagenlogik** im Gegensatz zu ”fuzzy logic” (fuzzy = unscharf) mit z.B. $w(A) = 0.43$.

Beispiele: logische Aussagen sind:

- A = ”$3^2 > 2^3$”, $w(A) = 1$
- B = ”4 ist Primzahl”, $w(B) = 0$
- C = ”Die Zahl x hat die Eigenschaft $x > 0$”, $w(C) = 0$ für $x \leq 0$, sonst $w(C) = 1$

Verknüpfungen von Aussagen

Name	**symbolisch**	**gesprochen**
Negation	$\neg A$	nicht A
Konjunktion	$A \wedge B$	A und B
Alternative	$A \vee B$	A oder B
Implikation	$A \Rightarrow B$	aus A folgt B
Äquivalenz	$A \Leftrightarrow B$	A ist äquivalent zu B

1.2 Def.: ("Wahrheitstafel" der Verknüpfungen $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$)

Die Wahrheitswerte der Verknüpfungen werden in Abhängigkeit der Wahrheitswerte von A und B definiert (1 = wahr, 0 = falsch).

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
1	0	0	0	1	0	0
1	1	0	1	1	1	1
0	0	1	0	0	1	1
0	1	1	0	1	1	0

1.3 Tautologien

- durch Kombination von Verknüpfungen kann man kompliziertere Aussagen bilden, z.B.

$$T := (A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$$

- Eine Aussage heisst "**Tautologie**", wenn sie stets wahr ist. T ist eine Tautologie (Beweis über Wahrheitstafel).
- weitere Beispiele für Tautologien:
  - Regel von de Morgan : $[\neg(A \wedge B)] \Leftrightarrow [(\neg A) \vee (\neg B)]$
  - indirekter Schluss : $[(A \Rightarrow B) \wedge (\neg B)] \Rightarrow (\neg A)$
  - Kettenschluss : $[(A \Rightarrow B) \wedge (B \Rightarrow C)] \Rightarrow (A \Rightarrow C)$

    (Beweis über Wahrh.'tafel mit 8 Zeilen)
  - Äquivalenz von A und B : $[A \Leftrightarrow B] \Leftrightarrow [(A \Rightarrow B) \wedge (B \Rightarrow A)]$

1.4 Existenz- und All-Aussagen

- sei $A(x)$ eine **Aussage**, die von einem **Parameter** x abhängt
- **"Existenz-Operator"** $\exists$:

  $\boxed{\exists\, x :\; A(x)}$ bedeutet: "**Es existiert** ein x, so dass $A(x)$ wahr ist."

- **"All-Operator"** $\forall$:

  $\boxed{\forall\, x :\; A(x)}$ bedeutet: "**Für alle** x gilt, dass $A(x)$ wahr ist."

  manchmal schreibt man auch:

  $\boxed{A(x)\;\forall\, x}$ bedeutet: "Es gilt $A(x)$ **für alle** x."

- oft wird der Gültigkeitsbereich auf eine Menge M eingeschränkt :

  $\boxed{\exists\, x \in M :\; A(x)}$ oder $\boxed{\forall\, x \in M :\; A(x)}$

  z.B. "$\exists\, k \in \mathbb{N} :\; k^2 = 4$" oder "$\forall\, x \in \mathbb{R} :\; x^2 \geq 0$"

1.5 Beweistechniken (1)

Ziel:
Herleiten neuer wahrer Aussagen (Satz, Lemma (= Hilfssatz), Folgerung) aus bereits bekannten wahren Aussagen (z.B. **Axiomen**)

- **logische Struktur** von Satz, Lemma oder Folgerung :

  $\boxed{A \Rightarrow B}$, wobei A = **Voraussetzung** und B = **Behauptung**

- **direkter Beweis:** $\boxed{A \Rightarrow \underbrace{H_1 \Rightarrow H_2 \Rightarrow \ldots \Rightarrow H_n}_{\text{Hilfsaussagen}} \Rightarrow B}$

  Man setzt A voraus und zeigt durch eine **Kette von Implikationen** Hilfsaussagen $H_1, \ldots, H_n$, aus denen dann die Behauptung B folgt.

1.5 Beweistechniken (2)

- **indirekter Beweis:** $$\boxed{\left[A \wedge (\underbrace{\neg B}_{\text{Annahme}} \Rightarrow C) \wedge (\neg \underbrace{(C \wedge A)}_{\text{Widerspruch}}) \right] \Rightarrow B}$$
  - man setzt A voraus **und** macht die **Annahme**: "Es gilt $\neg B$."
  - aus der Annahme schlussfolgert man eine Aussage C **und**
  - die Aussage $(C \wedge A)$ stellt einen Widerspruch dar (**ist falsch**)
  - $\Rightarrow$ die **Annahme** $\neg B$ **ist falsch** $\Rightarrow B$

- **Beweis einer Äquivalenz:** $$\boxed{[(A \Rightarrow B) \wedge (B \Rightarrow A)] \Leftrightarrow [A \Leftrightarrow B]}$$
  - man beweist $(A \Rightarrow B)$ **und** $(B \Rightarrow A)$
  - dies ist **notwendig und hinreichend** für $(A \Leftrightarrow B)$

2. Mengen

Mengenbegriff nach Georg Cantor (1895)

”Eine **Menge** ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte unserer Anschauung oder unseres Denkens - welche die **Elemente** der Menge genannt werden - zu einem Ganzen.”

Schreibweisen:

symbolisch	**Erklärung**
$x \in M$	x ist ein Element von M
$x \notin M$	x ist nicht Element von M
$\emptyset$	die leere Menge (die kein Element enthält)
$M_1 \subset M_2$	jedes Element von M_1 ist auch Element von M_2
$M_1 = M_2$	$M_1 \subset M_2$ und $M_2 \subset M_1$

Definitionsmöglichkeiten für Mengen

Schreibweise: $\boxed{\text{[linke Seite]} := \text{[rechte Seite]}}$

bedeutet, dass die Bezeichnung auf der linken Seite durch den Ausdruck auf der rechten Seite definiert wird

- **aufzählende Form:** $\boxed{M := \{x_1, x_2, \ldots, x_n\}}$

  Beispiele:
  - $\mathbb{N} := \{1, 2, 3, 4, \ldots\}$ **natürliche Zahlen**
  - $\mathbb{N}_0 := \{0, 1, 2, 3, \ldots\}$ $\mathbb{N}$ **mit** 0
  - $\mathbb{Z} := \{0, -1, +1, -2, +2, -3, +3, \ldots\}$ **ganze Zahlen**

- **beschreibende Form:** $\boxed{M := \{x \mid x \text{ hat die Eigenschaft } E\}}$

  Beispiele:
  - $\mathbb{Z} := \{m \mid m \in \mathbb{N} \text{ oder } -m \in \mathbb{N} \text{ oder } m = 0\}$
  - $\mathbb{Q} := \{\frac{z}{n} \mid z \in \mathbb{Z} \text{ und } n \in \mathbb{N}\}$ **gebrochene Zahlen** (Quotienten)

Mengenverknüpfungen

2.1 Def.: ("Verknüpfungen von Mengen" $\cap, \cup, \setminus, \times$)

Zu gegebenen Mengen P und Q wird definiert:

- **Durchschnitt**

  $$P \cap Q := \{x |\ x \in P \text{ und } x \in Q\} \qquad \text{(und = } \wedge\text{)}$$

- **Vereinigung**

  $$P \cup Q := \{x |\ x \in P \text{ oder } x \in Q\} \qquad \text{(oder = } \vee\text{)}$$

- **Differenz**

  $$P \setminus Q := \{x |\ x \in P \text{ und } x \notin Q\}$$

- **kartesisches Produkt**

  $$P \times Q := \{(x, y) |\ x \in P \text{ und } y \in Q\} \qquad \text{Menge von Paaren}$$

Gilt $P \cap Q = \emptyset$, so heissen P und Q **"disjunkt"**.

3. Körperaxiome der reellen Zahlen

- **Axiome** = Grundannahmen, die nicht beweisbar sind
- wir **nehmen an**, dass uns die **Menge** $\mathbb{R}$ **der reellen Zahlen** zur Verfüfung steht und ihre Elemente einer Reihe von Axiomen genügen
- alle weiteren Eigenschaften folgen aus diesen Axiomen

Körperaxiome von $\mathbb{R}$**:** (siehe Algebra)

Auf $\mathbb{R}$ gibt es zwei Verknüpfungen, die **Addition** "$+$" und die **Multiplikation** "$\cdot$", so dass

$$\forall\, x, y \in \mathbb{R}: \quad x + y \in \mathbb{R} \quad \text{und} \quad x \cdot y \in \mathbb{R}$$

und die folgenden Regeln (für beliebige beteiligte Elemente $x, y, z \in \mathbb{R}$) gelten:

Körperaxiome von $\mathbb{R}$ (Fortsetzung)

(A1) $(x+y)+z = x+(y+z)$ (Assoziativgesetz)

(A2) $x+y = y+x$ (Kommutativgesetz)

(A3) $x+0 = x$ ($0 \in \mathbb{R}$ ist neutrales Element der Addition)

(A4) Für beliebig gegebene $a, b \in \mathbb{R}$ hat die Gleichung $\boxed{a+x=b}$ genau eine Lösung $x \in \mathbb{R}$ bezeichnet mit $x = b-a$. Statt $0-a$ schreibt man $-a$.

(M1) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (Assoziativgesetz)

(M2) $x \cdot y = y \cdot x$ (Kommutativgesetz)

(M3) $x \cdot 1 = x$ ($1 \in \mathbb{R}$ ist neutrales Element der Multiplikation)

(M4) Zu jedem $b \in \mathbb{R}$ hat die Gleichung $\boxed{a \cdot x = b}$ für jedes $0 \neq a \in \mathbb{R}$ genau eine Lösung $x \in \mathbb{R}$ bezeichnet mit $x = b/a$ oder $x = \frac{b}{a}$.

(D) $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$

Beispiel für das Folgern weiterer Eigenschaften

3.1 Folgerung:

Seien $a, b \in \mathbb{R}$. Dann gilt

(a) $a \cdot 0 = 0$

(b) Aus $a \cdot b = 0$ folgt $a = 0$ oder $b = 0$.

(c) $(-a) \cdot (-a) = a \cdot a$

3.2 Bemerkung:

Eine Menge $\mathbb{K}$ zusammen mit zwei Verknüpfungen "$+, \cdot$", die den Axiomen (A1)-(A4), (M1)-(M4) und (D) genügen, heisst **Körper**. Die Folgerung 3.1 gilt dann in jedem Körper.

Beispiele:

- Körper sind: $\mathbb{R}$, $\mathbb{Q}$ und $\mathbb{C}$ (komplexe Zahlen, kommt später)
- keine Körper sind: $\mathbb{N}$ und $\mathbb{Z}$

4. Anordnungsaxiome und Ungleichungen

- in $\mathbb{R}$ gibt es eine **Ordnungsrelation** "$<$"
- **Schreibweisen:** Seien $a, b \in \mathbb{R}$.
  - $a < b$ bedeutet "a ist **kleiner als** b"
  - $a > b$ bedeutet "a ist **größer als** b" $\Leftrightarrow$ $b < a$
  - $a \leq b$ bedeutet "$a < b$ oder $a = b$"
  - $a \geq b$ bedeutet "$a > b$ oder $a = b$"
- **Anordnungsaxiome:**

(O1) Für jedes Paar $x, y \in \mathbb{R}$ gilt **genau eine** der Beziehungen

$$x < y, \quad x = y, \quad x > y \qquad \text{(Trichotomie)}$$

(O2) $x < y$ und $y < z \Rightarrow x < z$ (Transitivität)

(O3) $x < y \Rightarrow x + z < y + z \quad \forall\, z \in \mathbb{R}$

(O4) $x < y \Rightarrow x \cdot z < y \cdot z \quad \forall\, z > 0,\ z \in \mathbb{R}$

- $x \in \mathbb{R}$ heißt **positiv**, wenn $x > 0$, und **negativ**, wenn $x < 0$
- für "$\leq$" gelten die Eigenschaften (O2) - (O4) analog

abgeleitete Aussagen zu Ungleichungen

4.1 Folgerung:

Seien $x, y, z \in \mathbb{R}$. Dann gilt

(a) $"x > 0 \quad \Rightarrow \quad -x < 0"$ und $"x < 0 \quad \Rightarrow \quad -x > 0"$

(b) $x \neq 0 \quad \Rightarrow \quad x^2 > 0$

(c) $"x > 0 \quad \Rightarrow \quad \frac{1}{x} > 0"$ und $"x < 0 \quad \Rightarrow \quad \frac{1}{x} < 0"$

(d) $x < y \quad \Rightarrow \quad x \cdot z > y \cdot z \qquad \forall\, z < 0,\ z \in \mathbb{R}$

Schreibweise: $"a < b < c"$ bedeutet $"a < b$ **und** $b < c"$

4.2 Satz:

Seien $a, b, c, d \in \mathbb{R}$. Dann gilt

(a) $0 < a < b \quad \Rightarrow \quad \frac{1}{a} > \frac{1}{b} > 0$

(b) $"a \leq b$ und $c \leq d" \quad \Rightarrow \quad a + c \leq b + d$

(c) $"0 \leq a \leq b$ und $0 \leq c \leq d" \quad \Rightarrow \quad a \cdot c \leq b \cdot d$

Der Betrag einer rellen Zahl

4.3 Def.: ("Betrag $|\cdot|$")

Unter dem **Betrag einer rellen Zahl** x versteht man die Zahl

$$|x| := \begin{cases} x, & \text{falls} \quad x \geq 0, \\ -x, & \text{falls} \quad x < 0. \end{cases}$$

Es gilt: $\quad |x| \geq 0, \qquad |-x| = |x|, \qquad |x|^2 = x^2, \qquad -|x| \leq x \leq |x|.$

4.4 Satz:

Für $x, y \in \mathbb{R}$ gilt:

(a) $\quad |x \cdot y| = |x| \cdot |y| \quad$ und $\quad \left|\dfrac{x}{y}\right| = \dfrac{|x|}{|y|}$, falls $y \neq 0$.

(b) $\quad |x + y| \leq |x| + |y| \qquad$ (Dreiecksungleichung)

(c) $\quad |x - y| \geq \big||x| - |y|\big|$

5. Vollständige Induktion

5.1 Satz:

Jede **nichtleere Menge** natürlicher Zahlen $M \subset \mathbb{N}$ hat ein **kleinstes Element** m, d.h.

$$\exists\, m \in M : \quad m \leq a \quad \forall\, a \in M.$$

5.2 Satz: (Prinzip der vollständigen Induktion)

Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Es gelten:

(a) **Induktionsanfang:** $A(1)$ ist richtig.

(b) **Induktionsschritt:** $\forall\, n \in \mathbb{N} : \quad "A(n) \;\Rightarrow\; A(n+1)"$

Dann ist $A(n)$ für alle $n \in \mathbb{N}$ richtig.

Beispiel:

$A(n) :=$ "Es gilt $\boxed{1 + 3 + 5 + \cdots + (2n-1) = n^2}$."

Vollständige Induktion (2)

Bem.: (Start der vollständigen Induktion mit $n_0 \in \mathbb{N}$)

Für jedes $n \in \mathbb{N}$ sei $A(n)$ eine Aussage. Es gelten:

(a) **Induktionsanfang:** $A(n_0)$ ist richtig.

(b) **Induktionsschritt:** $\forall\, n \in \mathbb{N},\, n \geq n_0 :$ "$A(n) \;\Rightarrow\; A(n+1)$"

Dann ist $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq n_0$ richtig.

Summen, Produkte, Fakultät, Potenz

Summen- u. Produktzeichen:

Seien m ein **Anfangsindex** und n ein **Endindex** mit $m, n \in \mathbb{Z}$ und $m \leq n$. Dann wird folgende Schreibweise vereinbart:

$$\sum_{k=m}^{n} a_k := a_m + a_{m+1} + \cdots + a_n$$

soie

$$\prod_{k=m}^{n} a_k := a_m \cdot a_{m+1} \cdot \ \ldots \ \cdot a_n$$

n **Fakultät :** $\quad n! := \prod_{k=1}^{n} k = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n, \qquad 0! := 1$

n-te **Potenz :** $\quad a^n := \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ Faktoren}}, \qquad a^0 := 1 \quad \forall\, a \in \mathbb{R} \quad (\Rightarrow \ 0^0 := 1)$

Potenzgesetze, Bernoulli'sche Ungleichung

Potenzgesetze : Seien $m, n \in \mathbb{N}_0$ und $a, b \in \mathbb{R}$. Dann gilt:

$$a^m \cdot a^n = a^{m+n}, \qquad (a \cdot b)^n = a^n \cdot b^n, \qquad (a^m)^n = a^{m \cdot n}.$$

5.3 Satz: (Bernoulli'sche Ungleichung)

Für $n \in \mathbb{N}$ und $x \in \mathbb{R}$ mit $x \geq -1$ gilt:

$$(1+x)^n \geq 1 + nx.$$

Binomialkoeffizient, Binomischer Lehrsatz

Binomialkoeffizient : seien $n, k \in \mathbb{N}_0$ mit $k \leq n$

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} \qquad (\text{"}n \text{ über } k\text{"})$$

5.4 Lemma: (Pascal'sches Dreieck)

Für $n, k \in \mathbb{N}$ mit $1 \leq k \leq n$ gilt:

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}.$$

5.5 Satz: (Binomischer Lehrsatz)

Für $n \in \mathbb{N}$ und $x, y \in \mathbb{R}$ gilt:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Intervall-Schreibweisen

Seien $a, b \in \mathbb{R}$ mit $a < b$ gegebene **Intervallgrenzen.** Dann definiert man folgende Intervalle:

- **offene Intervalle:**
  - $(a, b) := \{x \in \mathbb{R} | \; a < x < b\}$
  - $(a, \infty) := \{x \in \mathbb{R} | \; a < x\}$
  - $(-\infty, a) := \{x \in \mathbb{R} | \; x < a\}$
- **abgeschlossene Intervalle:**
  - $[a, b] := \{x \in \mathbb{R} | \; a \leq x \leq b\}$
  - $[a, \infty) := \{x \in \mathbb{R} | \; a \leq x\}$
  - $(-\infty, a] := \{x \in \mathbb{R} | \; x \leq a\}$
- **halboffene Intervalle:**
  - $[a, b) := \{x \in \mathbb{R} | \; a \leq x < b\}$
  - $(a, b] := \{x \in \mathbb{R} | \; a < x \leq b\}$