1 Grundlagen aus der Algebra

VL #1

1.1 Mengen und Abbildungen

a) Mengen

Bsp.: endliche Menge $X := \{x_1, x_2, \dots, x_n\}$

Definition ↗ ↖ Elemente

- $x_i \in X$: „x_i ist Element von X." $(i = 1, \dots, n)$
- $\{1, 2, 3\} = \{2, 1, 3\}$ usw. — keine Reihenfolge
- $\{x, x, x\} = \{x\}$ — Mehrfachnennung

Def.: Eine Menge ist eine Sammlung wohlunterscheidbarer Objekte zu einem Ganzen.
Die leere Menge $\emptyset$ enthält kein Element.
Eine Menge Y heißt Teilmenge von X $(Y \subset X)$, falls für jedes $y \in Y$ auch $y \in X$ gilt.[1] Zwei Mengen X und Y sind genau dann gleich, wenn $X \subset Y$ und $Y \subset X$ gilt.
Kurznotation: $X = Y \Leftrightarrow X \subset Y$ und $Y \subset X$

[1] Gleichheit ist erlaubt: $X \subset X$

Bsp.: unendliche Mengen

- natürliche Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$, $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$
- ganze Zahlen $\mathbb{Z} = \{0, -1, +1, -2, +2, \dots\}$
- rationale Zahlen $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z},\ q \neq 0\}$
- reelle Zahlen $\mathbb{R}$ = äquivalente Cauchyfolgen in $\mathbb{Q}$

  ($\rightarrow$ Analysis)
- Komplexe Zahlen $\mathbb{C} = \{z = a + ib \mid a, b \in \mathbb{R}\}$

Die Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ sind abzählbar, $\mathbb{R}$ und $\mathbb{C}$ nicht.

Es gilt $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

Def.: Mengenoperationen

Vereinigung: $A \cup B = \{x \mid x \in A \text{ oder } x \in B\}$

$$\bigcup_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ für ein } i = 1, \dots, n\}$$

Durchschnitt: $A \cap B = \{x \mid x \in A \text{ und } x \in B\}$

$$\bigcap_{i=1}^{n} A_i = \{x \mid x \in A_i \text{ für alle } i = 1, \dots, n\}$$

Differenz: $A \setminus B = \{x \mid x \in A \text{ und } x \notin B\}$

Komplement bzgl. einer Grundmenge $X \supset A$:

$$A^c = X \setminus A \quad \text{(auch: } \bar{A},\ C_X A,\ CA\text{)}$$

kartesisches Produkt: $A \times B = \{(a, b) \mid a \in A, b \in B\}$

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) \mid a_i \in A_i\}$$

geordnete Tupel

Bsp.: i) $\{1\} \cap \{1,2\} = \{1\}$

ii) $\mathbb{N} \setminus \text{Primzahlen} = \{1,4,6,8,9,\dots\}$

iii) sei $A_i = \{n \geq i\} \subset \mathbb{N}$ für $i \in \mathbb{N}$. Für $i \leq j$ ist $A_i \subset A_j$.
Dann ist $\bigcup_{i\in\mathbb{N}} A_i = \mathbb{N}$ und $\bigcap_{i\in\mathbb{N}} A_i = \emptyset$. $\bigcap_{i=1}^{n} A_i = A_n$

iv) $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R} = \{(x,y) \mid x,y\in\mathbb{R}\}$

Def.: Zwei Mengen A und B heißen disjunkt, falls $A\cap B = \emptyset$. Eine Familie von Mengen $(A_i)_{i\in I}$ heißt paarweise disjunkt, falls $A_i \cap A_j = \emptyset$ für alle $i \neq j$ mit $i,j\in I$.

Bsp.: Sei $A_i = \{-i, i\}$ für $i\in\mathbb{N}_0$. Dann ist (A_i) paarweise disjunkt und $\dot{\bigcup}_{i\in\mathbb{N}} A_i = \mathbb{Z}$.
disjunkte Vereinigung

b) Aussagenlogik

<u>Def.:</u> Eine Aussage p ist entweder wahr oder falsch.
Die Verneinung von p heißt Negation $\neg p$ oder $\bar{p}$.
Verknüpfungen von Aussagen:

- Konjunktion: $p \wedge q$ ist genau dann wahr, wenn p und q beide wahr sind.
- Disjunktion: $p \vee q$ ist genau dann wahr, wenn p oder q (oder beide) wahr sind.
- Implikation: $p \Rightarrow q$ „wenn p, dann q"
- Äquivalenz: $p \Leftrightarrow q$ „q gilt genau dann, wenn p gilt"

<u>Bsp.:</u> „es regnet" $\Rightarrow$ „die Straße ist naß" (Umkehrung ist falsch!)

<u>Bem.:</u> die Implikation $p \Rightarrow q$ ist äquivalent zu:

- q folgt aus p
- p ist hinreichende Bedingung für q
- q ist notwendige Bedingung für p
- Umkehrschluß: $\neg q \Rightarrow \neg p$

  ($\nearrow$ Beweis durch Widerspruch)

Es gilt die Wahrheitstabelle: (Übung)

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
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

Satz: (de Morgansche Regeln)

Für zwei Aussagen p, q gelten die Negationsregeln:

$$\overline{p \wedge q} = \overline{p} \vee \overline{q} \quad \text{und} \quad \overline{p \vee q} = \overline{p} \wedge \overline{q}.$$

Analog gilt für zwei Mengen A, B: $\quad \overline{A} = X \setminus A$

$$\overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{und} \quad \overline{A \cup B} = \overline{A} \cap \overline{B}.$$

Beweis: Wahrheitstabelle für alle 4 Möglichkeiten für (p, q) wahr/falsch zu sein. (Übung)

Mengen: $\overline{A \cap B} = X \setminus (A \cap B) = \{x \in X \mid x \notin A \cap B\}$

$$\begin{aligned} x \notin A \cap B &\Leftrightarrow \neg(x \in A \text{ und } x \in B) \\ &\Leftrightarrow x \notin A \text{ oder } x \notin B \\ &\Leftrightarrow x \in \overline{A} \text{ oder } x \in \overline{B} \Leftrightarrow x \in \overline{A} \cup \overline{B}. \end{aligned}$$

$\square$

c) Prinzip der vollständigen Induktion

Es soll eine Aussage $p(n)$ für alle $n \geq m$, $n, m \in \mathbb{N}$ bewiesen werden. Dazu genügt es zu zeigen, daß

i) $p(m)$ gilt, — Induktionsanfang

ii) aus $p(n)$ folgt $p(n+1)$ für alle $n \geq m$. — Induktionsschritt

<u>Bsp. 1:</u> Sei $M \subset \mathbb{N}_0$ eine Menge mit den Eigenschaften

i) $0 \in M$, und

ii) $n \in M \Rightarrow n+1 \in M$.

Dann ist $M = \mathbb{N}_0$.

<u>Bem.:</u> Summenzeichen: $\sum_{k=1}^{4} k^2 = 1^2 + 2^2 + 3^2 + 4^2$

<u>Bsp. 2:</u> Zu zeigen: $\sum_{k=1}^{n} (2k-1) = n^2$, $n \in \mathbb{N}$

i) $n=1$: $2 \cdot 1 - 1 = 1$ ✓

ii) die Formel gelte für $n \geq 1$. Dann ist

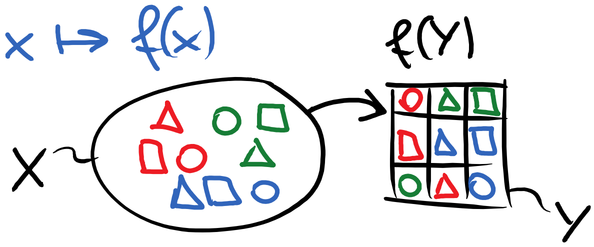
$$\sum_{k=1}^{n+1} (2k-1) = \sum_{k=1}^{n} (2k-1) + [2(n+1)-1]$$
$$= n^2 + 2n + 1 = (n+1)^2$$

$\square$

d) Abbildungen

<u>Def.:</u> Sind X und Y Mengen, so versteht man unter einer **Abbildung** f von X nach Y eine Vorschrift, die jedem $x \in X$ eindeutig ein $f(x) \in Y$ zuordnet.

Schreibweise: $f: X \to Y \;,\; x \mapsto f(x)$



<u>Bemerkungen:</u>

(1) Zuordnung oft explizit durch eine Formel, z.B. $f: \mathbb{R} \to \mathbb{R} \;,\; f(x) = 3x + 2$

(2) X heißt **Definitionsbereich**, Y heißt **Bildbereich** von f

(3) $f, g: X \to Y$ heißen **gleich**, wenn $f(x) = g(x) \quad \forall x \in X$ $\qquad \forall$ für alle

(4) ist $M \subset X$, so bezeichnet $f|_M$ die **Restriktion** von f auf M, d.h. die Abbildung $f|_M : M \to Y$, $x \mapsto f(x)$

(5) Transport von Teilmengen:

Seien $f: X \to Y$ und $M \subset X$, $N \subset Y$. Dann heißt

$f(M) = \{f(x) \mid x \in M\}$ das **Bild** von M unter f.

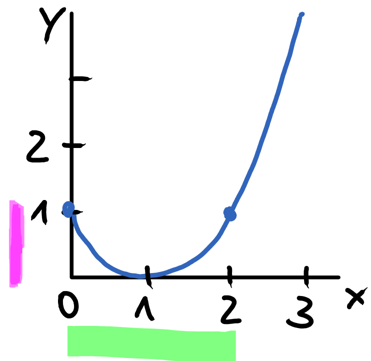
$= \{y \in Y \mid \exists x \in M \text{ mit } f(x) = y\}$ $\qquad \exists$ es existiert

(6) Sei $N \subset Y$. Wir nennen

$f^{-1}(N) = \{x \in X \mid f(x) \in N\}$

das **Urbild** von N unter f.

Bsp.: $X = [0, \infty)$, $f : X \to \mathbb{R}$, $f(x) = (x-1)^2$



$f(X) = [0, \infty) \subset \mathbb{R}$

$f^{-1}([0,1]) = [0,2]$

$f^{-1}(\{1\}) = \{0,2\}$

Def.: Eine Abbildung $f : X \to Y$ heißt injektiv, wenn $f(x) = f(x') \Rightarrow x = x'$ für alle $x, x' \in X$. Sie heißt surjektiv, wenn $f(X) = Y$, d.h. zu jedem $y \in Y$ gibt es ein $x \in X$ mit $y = f(x)$. Eine Abbildung heißt bijektiv, wenn sie injektiv und bijektiv ist.

Bem.:

(1) Durch Änderung von X und Y läßt sich jede Abbildung bijektiv machen

Bsp.: $f : \mathbb{R} \to \mathbb{R}$, $f(x) = \sin(x)$ ist nicht injektiv und nicht surjektiv.

Aber $f : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$ ist bijektiv.

(2) Ist f bijektiv, so gibt es zu jedem $y \in Y$ genau ein $x \in X$ mit $y = f(x)$. Urbilder: $f^{-1}(\{y\}) = \{x\}$.

Dies erlaubt die Definition der Umkehrabbildung:

$f^{-1} : Y \to X$, $y = f(x) \mapsto x$

Satz: Sei X eine endliche Menge und $f: X \to X$ eine Abbildung. Dann ist folgendes äquivalent:

i) f ist injektiv,
ii) f ist surjektiv,
iii) f ist bijektiv.

Bew.: Sei $X = \{x_1, \dots, x_n\}$ mit $x_i \neq x_j$ für $i \neq j$.

i) $\Rightarrow$ ii) (Beweis durch Widerspruch) Gegenannahme

Sei f nicht surjektiv, also $f(X) \neq X$. Dann besteht $f(X)$ aus $m < n$ Elementen. Wenn n Objekte (x_i) auf $m < n$ Schubladen $(f(x_i))$ verteilt werden, so befinden sich in einer Schublade mindestens zwei Objekte. (Schubfachprinzip)

Also kann f nicht injektiv sein. $\lightning$ Widerspruch zur Voraussetzung

ii) $\Rightarrow$ i) Sei f nicht injektiv, so gibt es $x_i \neq x_j$ mit $f(x_i) = f(x_j)$. Dann enthält $f(X)$ höchstens $n-1$ Elemente, also ist f nicht surjektiv. $\lightning$

Wegen i) $\Leftrightarrow$ ii) folgt ii) $\Rightarrow$ iii) und i) $\Rightarrow$ iii). Die Umkehrungen iii) $\Rightarrow$ i), ii) sind klar. $\square$

Def.: Sind X, Y, Z Mengen und $f: X \to Y$ und $g: Y \to Z$ Abbildungen, so heißt die Abbildung

$$g \circ f : X \to Z, \quad x \mapsto g(f(x)) =: (g \circ f)(x)$$

die Komposition (Hintereinanderschaltung) von f und g.

Diagramm: $X \xrightarrow{f} Y \xrightarrow{g} Z$

Satz: Sei $f: X \to Y$ eine Abbildung und X, Y nicht leer. Außerdem bezeichne id_X die identische Abbildung:

$id_X : X \to X, \quad x \mapsto x$. Dann gilt:

1) f injektiv $\Leftrightarrow$ $\exists g: Y \to X$, so daß $g \circ f = id_X$
2) f surjektiv $\Leftrightarrow$ $\exists g: Y \to X$, so daß $f \circ g = id_Y$
3) f bijektiv $\Leftrightarrow$ $\exists g: Y \to X$, so daß $g \circ f = id_X$ und $f \circ g = id_Y$. In diesem Fall ist $g = f^{-1}$.

Bew.: 1) Sei f injektiv. Dann ist $h: X \to f(X)$, $x \mapsto f(x)$ bijektiv und wir setzen $g(y) = h^{-1}(y)$ für $y \in f(X)$. Für $y \in Y \setminus f(X)$ definieren wir $g(y) = x_0$ für ein beliebiges, aber festes $x_0 \in X$. Dann ist $g: Y \to X$ eine Abbildung mit $g \circ f = id_X$.

Umkehrung: Sei $g: Y \to X$ mit $g \circ f \overset{1}{=} id_X$ gegeben. Für $x, x' \overset{2}{\in} X$ mit $f(x) \overset{3}{=} f(x')$ gilt:

$$x \overset{2}{=} id_X(x) \overset{1}{=} g(f(x)) \overset{3}{=} g(f(x')) \overset{1}{=} id_X(x') \overset{2}{=} x' \Rightarrow f \text{ injektiv.}$$

2) Sei f surjektiv. Zu jedem $y \in Y$ wählen wir ein $x \in X$ mit $y = f(x)$ und setzen $g(y) := x$. Die Abbildung $g: Y \to X$ erfüllt dann $f \circ g = \mathrm{id}_Y$.
Umkehrung: Sei $f \circ g = \mathrm{id}_Y$. Für jedes $y \in Y$ gilt $y = f(g(y)) \in f(X)$. Also $Y = f(X)$ und f surjektiv.

3) Ist f bijektiv, so erfüllt $g = f^{-1}$ beide Gleichungen. Ist umgekehrt $g: Y \to X$ mit $g \circ f = \mathrm{id}_X$ und $f \circ g = \mathrm{id}_Y$ gegeben, so ist f nach 1) und 2) bijektiv, und $g = f^{-1}$.

$\square$

Def.: Zwei Mengen X und Y heißen gleichmächtig, wenn es eine bijektive Abbildung $f: X \to Y$ gibt.
Eine Menge X heißt abzählbar, wenn sie gleichmächtig wie $\mathbb{N}$ ist, d.h. wenn sich die Elemente von X durchnumerieren lassen.

Satz: Die Mengen $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ sind abzählbar.