

KAPITEL 0

Motivation

1. Zahlbereiche

$\mathbb{N} := \{0, 1, 2, \dots\}$ = Menge der *natürlichen Zahlen* mit Addition “+”, Multiplikation “·” und Anordnung “<”.

$\mathbb{Z} := \mathbb{N} \cup (-\mathbb{N})$ = Menge der *ganzen Zahlen*. Gleichungen der Art $a + x = b$ können in \mathbb{Z} für beliebige $a, b \in \mathbb{N}$ (oder auch $a, b \in \mathbb{Z}$) gelöst werden.

$\mathbb{Q} := \{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$ = Menge der *rationalen Zahlen* \rightarrow . Gleichungen der Art $ax + b = c$ können in \mathbb{Q} für beliebige $a, b, c \in \mathbb{Z}$ mit $a \neq 0$ gelöst werden (bzw. $a, b, c \in \mathbb{Q}$).

\mathbb{R} = Menge der *reellen Zahlen*, entsteht aus \mathbb{Q} durch Vervollständigung (\uparrow Analysis).

\mathbb{C} = Menge der *komplexen Zahlen* (\uparrow Analysis). Gleichungen der Art $ax^2 + bx + c = d$ können gelöst werden für beliebige $a, b, c, d \in \mathbb{R}$ (bzw. \mathbb{C}) mit $(a, b) \neq (0, 0)$.

Es gilt:

$$\begin{array}{c} \text{Körper} \\ \underbrace{\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \mathbb{R} \subsetneq \mathbb{C}} \\ \text{Ringe} \end{array}$$

2. Vektorrechnung in \mathbb{R}^d (bzw. \mathbb{C}^d)

motiviert z.B. durch die Physik

—BILD—

Addition “+” Subtraktion von *Vektoren*, Skalarmultiplikation.

3. Vektorräume

- ▷ mathematische Konzeption zur Grundlegung der “Vektorrechnung”
- ▷ zwei Abstraktionsrichtungen
 - ◇ beliebig viele Dimensionen, nicht nur 1, 2, 3; sogar ∞ -dimensional
 - ◇ *beliebige Körper* als Koordinatenbereiche (wichtig z.B. für Kryptographie).

4. Skalarprodukte und Determinanten

- ▷ Zusätzlich zur Vektorrechnung *Winkel* zwischen Vektoren und *Vektorlängen*
- ▷ dadurch: Grundlegung der Elementargeometrie.

5. Lineare Gleichungssysteme

—BILD—

Gesucht: Menge aller Lösungen (x, y) für das lineare Gleichungssystem:

$$\begin{cases} 2y = x + 2 \\ 2y = 4 - x \end{cases}$$

Eliminiere y :

$$4 - x = x + 2 \Leftrightarrow 2 = 2x \Leftrightarrow 1 = x.$$

Setze x ein:

$$2y = 1 + 2 = 3 \Leftrightarrow y = \frac{3}{2}.$$

6. Symmetriebegriffe

—BILD—

Grundlagen

1. Aussagenlogik und Quantoren

1.1. Aussagen. Die (Aussagen-) Logik handelt von mathematischen *Aussagen*, die nach gewissen Regeln aus einer gewissen Menge von Symbolen gebildet werden. Eine wohlgeformte Aussage hat entweder den *Wahrheitswert* "wahr" oder "falsch".

BEISPIEL 1.1. Aussagen:

- ▷ "0 ∈ ℤ", bzw. "0 ist eine ganze Zahl"
- ▷ "2 + 2 = 5"
- ▷ "a + a = 2 · a gilt für alle natürlichen Zahlen a"

BEMERKUNG 1.2. Ob eine Aussage wahr oder falsch ist, hängt vom axiomatischen Kontext ab.

Aus bereits vorhandenen Aussagen A und B lassen sich wie folgt neue Aussagen bilden:

- ▷ *Negation*: $\neg A$ ist wahr genau dann, wenn A falsch ist; lies als: "nicht A "
- ▷ *Konjunktion*: $A \& B$ ist wahr genau dann, wenn A und B beide wahr sind; lies als: " A und B ". Manchmal schreibt man auch " $A \wedge B$ ".
- ▷ *Disjunktion*: $A \vee B$ ist wahr genau dann, wenn mindestens A oder B wahr sind; lies als: " A oder B "
- ▷ *Subjunktion*: $A \Rightarrow B$ ist definiert als $(\neg A) \vee B$; lies als: "aus A folgt B "
- ▷ *Äquivalenz*: $A \Leftrightarrow B$ ist wahr genau dann, wenn die Wahrheitswerte von A und B gleich sind (d.h. beide wahr oder beide falsch); lies als: " A ist äquivalent zu B "

1.2. Wahrheitstabeln. Diese Konstruktionen neuer Aussagen aus bestehenden lassen sich durch die folgende *Wahrheitstafel* zusammenfassen:

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

Durch Inspektion aller möglichen Wahrheitswertbelegungen lassen sich zum Beispiel folgende *Sätze der Aussagenlogik (Tautologien)* beweisen:

- (1) $A \vee (\neg A)$ *Tertium non datur*
- (2) $\neg(A \vee B) \Leftrightarrow (\neg A) \& (\neg B)$ und $\neg(A \& B) \Leftrightarrow (\neg A) \vee (\neg B)$ *De Morganschen Regeln*
- (3) $\left. \begin{array}{l} (A \& B) \Leftrightarrow (B \& A) \\ (A \vee B) \Leftrightarrow (B \vee A) \end{array} \right\} \text{Kommutativität}$
- (4) $\left. \begin{array}{l} (A \& B) \& C \Leftrightarrow A \& (B \& C) \\ (A \vee B) \vee C \Leftrightarrow A \vee (B \vee C) \end{array} \right\} \text{Assoziativität}$
- (5) $\left. \begin{array}{l} A \& (B \vee C) \Leftrightarrow (A \& B) \vee (A \& C) \\ A \vee (B \& C) \Leftrightarrow (A \vee B) \& (A \vee C) \end{array} \right\} \text{Distributivgesetze}$

Zusätzlich gelten die folgenden *Regeln des logischen Schließens*, die man ebenfalls durch Inspektion der Wahrheitstafel verifizieren kann:

SATZ 1.3 (Direkter Schluss). $[A \& (A \Rightarrow B)] \Rightarrow B$

SATZ 1.4 (Indirekter Schluss). $[(\neg B) \& (A \Rightarrow B)] \Rightarrow \neg A$

BEWEIS.

A	B	$\neg B$	$A \Rightarrow B$	$(\neg B) \& (A \Rightarrow B)$	$\neg A$	$[(\neg B) \& (A \Rightarrow B)] \Rightarrow \neg A$
w	w	f	w	f	f	w
w	f	w	f	f	f	w
f	w	f	w	f	w	w
f	f	w	w	w	w	w

□

SATZ 1.5 (Kontraposition). $(A \Rightarrow B) \Rightarrow (\neg B \Rightarrow \neg A)$

Der folgende Satz dient dazu, eine andere Beweismethode als durch Wahrheitstafeln zu demonstrieren.

BEISPIEL 1.6. Es gilt $[A \Rightarrow (B \vee C)] \Leftrightarrow [(A \& \neg B) \Rightarrow C]$.

BEWEIS.

$$\begin{aligned}
 & [A \Rightarrow (B \vee C)] \\
 & \Leftrightarrow [\neg A \vee (B \vee C)] \Leftrightarrow [(\neg A \vee B) \vee C] \\
 & \Leftrightarrow [\neg(\neg A \vee B) \Rightarrow C] \Leftrightarrow [(A \& \neg B) \Rightarrow C]
 \end{aligned}$$

□

BEISPIEL 1.7. Die folgende Aussage gilt z.B. über \mathbb{Q} :

$$\underbrace{\lambda\mu = 0}_A \Rightarrow \underbrace{\lambda = 0}_B \quad \text{oder} \quad \underbrace{\mu = 0}_C$$

Dies ist gleichwertig zu:

$$\underbrace{\lambda\mu = 0}_A \quad \text{und} \quad \underbrace{\lambda \neq 0}_{\neg B} \Rightarrow \underbrace{\mu = 0}_C$$

1.3. Quantoren. Sei I eine Menge und $(A_i)_{i \in I}$ eine Familie von Aussagen.

DEFINITION 1.8 (Allquantor). “ $\forall i \in I : A_i$ ” ist eine Aussage, die wahr ist genau dann, wenn die Aussage A_i wahr ist für jedes $i \in I$; lies als: “für alle $i \in I \dots$ ”.

DEFINITION 1.9 (Existenzquantor). “ $\exists i \in I : A_i$ ” ist eine Aussage, die wahr ist genau dann, wenn es (mindestens) ein $i \in I$ gibt, so dass A_i wahr ist; lies als: “es existiert ein $i \in I \dots$ ”.

DEFINITION 1.10 (Quantor zur eindeutigen Existenz). “ $\exists! i \in I : A_i$ ” ist eine Aussage, die wahr ist genau dann, wenn es genau ein $i \in I$ gibt, so dass A_i wahr ist (d.h. für alle anderen $j \in I \setminus \{i\}$ ist A_j falsch).

BEISPIEL 1.11. $[\exists n \in \mathbb{N} : n^2 = 5]$ ist falsch.

BEISPIEL 1.12. $[\forall q \in \mathbb{Q} : \exists r \in \mathbb{Q} : 2r = q]$ ist wahr.

2. Mengenlehre

Hier wird nur ein naiver Zugang zur Mengenlehre angeboten.

DEFINITION 2.1. (1) Eine *Menge* ist eine Zusammenfassung bestimmter, wohlunterscheidbarer Objekte zu einem ganzen. Die Objekte heißen *Elemente* der Menge.

(2) *Extensionalität*: $A = B \Leftrightarrow (\forall x : x \in A \Leftrightarrow x \in B)$

(3) *leere Menge*: $\emptyset := \{x : x \neq x\}$

(4) $A \subseteq B \Leftrightarrow (\forall x : x \in A \Rightarrow x \in B)$

(5) $A \subsetneq B \Leftrightarrow (A \subseteq B) \& (A \neq B)$.

(6) *Potenzmenge* $\mathcal{P}(A) := \{x : x \subseteq A\}$

BEMERKUNG 2.2. Ungehemmte naive Mengenbildung führt zu Widersprüchen; z.B. (Russell): Es sei $R := \{x : x \notin x\}$. Die naive Frage: ‘Gilt “ $R \in R$ ” oder “ $R \notin R$ ”?’ führt auf einen Widerspruch. Die *axiomatische Mengenlehre* löst dieses Problem, indem sie solche Fragen als *syntaktisch unzulässig* ausschließt.

Ähnlich wie man Aussagen miteinander verknüpfen kann, kann man auch Mengen miteinander verknüpfen. Es seien im Folgenden A und B Mengen.

DEFINITION 2.3. (1) $A \setminus B := \{x : x \in A \text{ und } x \notin B\}$ *Differenzmenge*

(2) $A \cap B := \{x : x \in A \text{ und } x \in B\}$ *Schnittmenge*

(3) $A \cup B := \{x : x \in A \text{ oder } x \in B\}$ *Vereinigungsmenge*

SATZ 2.4. *Es gilt:*

(1) $A \cap B = B \cap A$

(2) $A \cup B = B \cup A$

(3) $A \cap (B \cap C) = (A \cap B) \cap C$

(4) $A \cup (B \cup C) = (A \cup B) \cup C$

(5) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

(6) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Vergleichen Sie mit den in Abschnitt 1.2 aufgeführten Sätzen der Aussagenlogik.

3. Relationen und Funktionen

DEFINITION 3.1 (Geordnetes Paar). $(x, y) := \{\{x, y\}, \{x\}\}$

SATZ 3.2. $(x, y) = (x', y') \Leftrightarrow x = x' \text{ und } y = y'$.

BEWEIS. Sei $(x, y) = (x', y')$. Dann folgt $(\{x, y\} = \{x', y'\} \text{ und } \{x\} = \{x'\})$ oder $(\{x, y\} = \{x'\} \text{ und } \{x\} = \{x', y'\})$. Wir unterscheiden zwei Fälle.

Fall 1: $x = y$. Dann ist $\{x\} = \{x', y'\}$ und damit $x = x' = y'$

Fall 2: $x \neq y$. Dann ist $\{x, y\} \neq \{x'\}$ und damit $\{x, y\} = \{x', y'\}$. Außerdem gilt $\{x\} = \{x'\}$, also $x = x'$ und dann auch $y = y'$.

Die umgekehrte Inklusion folgt direkt. □

DEFINITION 3.3. Zu zwei Mengen X, Y heißt

$$x \times y := \{(x, y) : x \in X \text{ und } y \in Y\}$$

das *kartesische Produkt* von X und Y .

DEFINITION 3.4. Eine (*binäre*) *Relation* auf zwei Mengen X und Y ist eine beliebige Teilmenge von $X \times Y$. Falls $R \subseteq X \times Y$, so setzen wir

$$xRy \Leftrightarrow (x, y) \in R.$$

DEFINITION 3.5. Sei R eine Relation auf M

(1) R heißt *reflexiv*, falls

$$\forall x \in M : xRx$$

(2) R heißt *symmetrisch*, falls

$$\forall x, y \in M : xRy \Leftrightarrow yRx$$

(3) R heißt *antisymmetrisch*, falls

$$\forall x, y \in M : xRy \& yRx \Rightarrow x = y$$

(4) R heißt *transitiv*, falls

$$\forall x, y, z \in M : xRy \& yRz \Rightarrow xRz.$$

DEFINITION 3.6. \triangleright Eine *Äquivalenzrelation* ist reflexiv, symmetrisch und transitiv.

\triangleright Eine *Ordnungsrelation* ist reflexiv, antisymmetrisch und transitiv.

DEFINITION 3.7. Sei M eine Menge und $P \subseteq \mathcal{P}(M)$. Dann heißt P *Partition* von M , falls die folgenden Bedingungen erfüllt sind:

$\triangleright \forall m \in P : m \neq \emptyset$

$\triangleright \forall m, m' \in P : m \neq m' \Rightarrow m \cap m' = \emptyset$

$\triangleright \bigcup \{m : m \in P\} = M$

Sei \sim eine Äquivalenzrelation auf eine Menge M . Zu $x \in M$ setze

$$[x]_{\sim} := \{y \in M : x \sim y\} \text{ Äquivalenzklasse}$$

SATZ 3.8. Die Äquivalenzklassen $\{[x]_{\sim} : x \in M\}$ einer beliebigen Äquivalenzrelation \sim partitionieren M . Umgekehrt definiert jede Partition eine Äquivalenzrelation.

BEWEIS. Übung. □

BEISPIEL 3.9. Betrachte die Menge der ganzen Zahlen \mathbb{Z} , und wähle $m \in \mathbb{Z}$.

$$x \equiv_m y \Leftrightarrow \exists k \in \mathbb{Z} : km = x - y$$

Die Relation \equiv_m wird als “kongruent mod m ” gelesen. Die Kongruenzrelation ist eine Äquivalenzrelation, denn:

$\triangleright \equiv_m$ ist reflexiv:

$$\text{Sei } x \in \mathbb{Z} \Rightarrow 0 \cdot m = x - x \Rightarrow x \equiv_m x.$$

$\triangleright \equiv_m$ ist symmetrisch:

$$\text{Seien } x, y \in \mathbb{Z} \text{ mit } x \equiv_m y \Rightarrow ex \cdot k \in \mathbb{Z}:$$

$$km = x - y \Rightarrow (-k)m = y - x \Rightarrow y \equiv_m x.$$

$\triangleright \equiv_m$ ist transitiv:

$$\text{Seien } x, y, z \in \mathbb{Z} \text{ mit } x \equiv_m y \text{ und } y \equiv_m z \Rightarrow ex \cdot k, l \in \mathbb{Z}, \text{ so dass } km = x - y \text{ und } lm = y - z \Rightarrow (k+l)m = x - z \Rightarrow x \equiv_m z.$$

\triangleright Die resultierenden Partitionen sehen so aus:

$$\mathbb{Z} = \{0, 2, -2, 4, -4, \dots\} \cup \{1, -1, 3, -3, \dots\} \text{ für } m = 2$$

und

$$\mathbb{Z} = \{0, 3, -3, 6, -6, \dots\} \cup \{1, -2, 4, -5, 7, -8, \dots\} \cup \{2, -1, 5, -4, 8, -7, \dots\} \text{ für } m = 3$$

\triangleright Äquivalenzklassen:

$$[x]_{\equiv_m} = \{x, x \pm m, x \pm 2m, \dots\} = x + m\mathbb{Z}.$$

DEFINITION 3.10. Eine Relation $R \subseteq X \times Y$ heißt *Funktion* von X nach Y , falls gilt

$$\forall x \in X : \exists y \in Y : xRy$$

und

$$\forall x \in X : \forall y \in Y : \forall y' \in Y : xRy \& xRy' \Rightarrow y = y'.$$

Man spricht von *Rechtseindeutigkeit*. Notation: " $R : X \rightarrow Y$ ".

Die vorherige Definition verlangt, dass eine Funktion jedem Element des *Definitionsreichs* X ein Element des *Wertebereichs* Y zuordnet. Lässt man diese Bedingung weg, redet man von einer *partiellen Funktion*.

DEFINITION 3.11. (1) Eine Funktion $f : X \rightarrow Y$ heißt *injektiv*, falls

$$\forall x, x' \in X : f(x) = f(x') \Rightarrow x = x'$$

(2) Eine Funktion $f : X \rightarrow Y$ heißt *surjektiv*, falls

$$\forall y \in Y : \exists x \in X : f(x) = y.$$

(3) Eine Funktion $f : X \rightarrow Y$ heißt *bijektiv*, falls f injektiv und surjektiv ist.

(4) Zu $Y' \subseteq Y$ ist

$$f^{-1}(Y') := \{x \in X : f(x) \in Y'\}$$

das (*volle*) *Urbild* von Y' unter f .

DEFINITION 3.12. Seien A, B, C Mengen und $f : B \rightarrow C$ und $g : A \rightarrow B$ Abbildungen. Die Abbildung

$$f \circ g : A \rightarrow C : a \mapsto f(g(a))$$

heißt *Verkettung* von f und g . [hier auch als "erst g , dann f "].

Seien A, B, C, D Mengen und $f : C \rightarrow D$, $g : B \rightarrow C$, $h : A \rightarrow B$ Abbildungen.

SATZ 3.13.

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

BEWEIS. Sei $a \in A$. Dann gilt

$$\begin{aligned} [f \circ (g \circ h)](a) &= f((g \circ h)(a)) = f(g(h(a))) \\ &= (f \circ g)(h(a)) = [(f \circ g) \circ h](a) \end{aligned}$$

□

4. Gruppen, Ringe, Körper

DEFINITION 4.1. Eine (binäre) *Verknüpfung* auf einer Menge M ist eine Abbildung

$$* : M \times M \rightarrow M : (m, m') \mapsto m * m'$$

BEMERKUNG 4.2. Je nach Verknüpfung sind teils sehr unterschiedliche Notationen üblich.

BEISPIEL 4.3. (1) $M = \mathbb{Z}$, $* = + \leftarrow$ Addition

(2) $M = \mathbb{R}$, $* = \cdot \leftarrow$ Multiplikation

(3) M beliebig, \cup und \cap Verknüpfungen auf $\mathcal{P}(M)$.

DEFINITION 4.4. Seien A, B Mengen. Dann bezeichnet

$$A^B := \{f : B \rightarrow A\}$$

die Menge aller Abbildungen von B nach A .