Lineare Algebra und diskrete Mathematik

Timo Scholz

February 3, 2023

Contents

1 Grundlegende Begriffe und algebraische Strukturen

1.1 Zahlen und Mengen

1.1.1 Naiver Mengen- und Zahlenbegriff

- Eine Menge ist definiert durch das, "was drin ist" (naiver Mengenbegriff
- Sie enthält unterscheidbare Objekte ohne Vielfachheit
- Die Reihenfolge der Elemente ist egal

Wichtige Mengen:

- $\mathbb{N}$: natürliche Zahlen {1, 2, 3, ...}
- $\mathbb{N}_0$: natürliche Zahlen {1, 2, 3, ...}
- $\mathbb{Z}$: ganze Zahlen {..., -2, -1, 0, 1, 2, ...}
- $\mathbb{Q}$: rationale Zahlen $\{\frac{p}{q} : p, q \in \mathbb{Z}, q \neq 0\}$
- Unter Hinzunahme von Grenzwerten ergibt sich die Menge der reellen Zahlen $\mathbb{R}$

1.1.2 Mengenlehre

Umfangsdefinition: $M = \{2, 4, 6, 8\}$
Inhaltsdefinition: $M = \{m : m \in \mathbb{N}$, m ist gerade, $m \leq 8\}$
Sei M eine Menge

- $m \in M$: M ist Element von M
- $m \neq M$: M ist nicht Element von M
- $M := \emptyset$: M ist die leere Menge {}
- $|M|$: Anzahl der Elemente von M
  (unendliche Mengen: $|M| = \infty$)

Seien A, B Mengen

- $A \subseteq B$: A ist Teilmenge von B, d.h. alle Elemente von A sind auch in B
- $A = B$: A enthält genau die gleichen Elemente wie B, d.h. $A \subseteq B$ und $B \subseteq A$
- $A \subset B$: A ist echte Teilmenge von B, d.h. $A \subseteq B$ und $A \neq B$

Falls $|A| = |B| < \infty$ und $A \subseteq B$, dann ist $A = B$

- $A \cup B := \{a : a \in A$ oder $a \in B\}$ Vereinigung von A und B

- $A \cap B := \{a : a \in A \text{ und } a \in B\}$ Schnittmenge von A und B
- $A \setminus B := \{a, a \in A \text{ aber } a \notin B\}$ Differenzmenge von A und B

Für $|A| = |B| < \infty$ gilt:
$|A \setminus B| = |A| - |A \cap B|$
$|A \cup B| = |A| + |B| - |A \cap B|$

- A und B heißen disjunkt, falls $A \cap B = \emptyset$

Für A, B disjunkt, schreibe auch $A \dot{\cup} B$ statt $A \cup B$

- Falls klar ist, welches M gemeint ist: $A^c := M \setminus A$
- Transitivität: Gilt $A \subseteq B$ und $B \subseteq C$, dann gilt auch $A \subseteq C$
- Kommutativität: $A \cup B = B \cup A$
- Assoziativität: $(A \cup B) \cup C = A \cup (B \cup C)$
  $(A \cap B) \cap C = A \cap (B \cap C)$
- Distributivität: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- De-morgansche Regeln: $(A \cap B)^c = A^c \cup B^c$
  $(A \cup B)^c = A^c \cap B^c$

Sei A eine Menge

- $\mathcal{P}(A) := \{B : B \subseteq A\}$
  z.B. $\mathcal{P}(\{1,2\}) = \{\{1\}, \{2\}, \{1,2\}\}$ $\qquad$ $\mathcal{P}$ nennt man Potenzmenge
- $|\mathcal{P}(A)| = 2^{|A|}$

1.1.3 Tupel und kartesische Produkte

Seien A und B Mengen

- Tupel: $(a, b) : a \in A, b \in B$
- Kartesisches Produkt:= $A \times B\{(a, b) : a \in A, b \in B\}$
- Analog: $A_1 \times A_2 \times A_3 ... \times A_n := \{(a_1, a_2, a_3 ... a_n) : a_i \in A_i\}$

1.2 Aussagelogik und Funktionen

1.2.1 Logische Aussagen

Eine logische Aussage ist entweder wahr oder falsch.
z.B. 4 ist durcch 2 teilbar.

Seien A, B Aussagen

- $\neg A$: Negation von A, ist genau dann wahr, wenn A falsch ist
- $A \wedge B$: Konjunktion, ist genau dann wahr, wenn A und B beide wahr sind
- $A \vee B$: Disjunktion, ist genau dann wahr, wenn A oder B oder beide wahr sind
- $A \Rightarrow B$: Implikation, aus A folgt B
- $A \Leftrightarrow B$: Äquivalenz, aus A folgt B und aus B folgt A

Für $A \Rightarrow B$ schreibt man auch

- A ist hinreichend für B
- B ist notwendig für A
- B gilt, wenn A gilt

Für $A \Leftrightarrow B$ schreibt man auch

- A = B
- A ist notwendig und hinreichend für B
- B ist notwendig und hinreichend für A
- B gilt genau dann, wenn A gilt
- A gilt genau dann, wenn B gilt

Seien A, B, C Aussagen

- Transitivität: Aus $A \Rightarrow B$ und $B \Rightarrow C$ folgt $A \Rightarrow C$
  Aus $A \Leftrightarrow B$ und $B \Leftrightarrow C$ folgt $A \Leftrightarrow C$
- Kommutativität: $A \wedge B = B \wedge A$
  $A \vee B = B \vee A$
- Assoziativität: $(A \wedge B) \wedge C = A \wedge (B \wedge C)$
  $(A \vee B) \vee C = A \vee (B \vee C)$
- Distributivität: $A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C)$
  $A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C)$
- Doppelte Negation: $\neg(\neg A) = A$
- De-morgansche Regeln:
  $\neg(A \vee B) = (\neg A) \wedge (\neg B)$
  $\neg(A \wedge B) = (\neg A) \vee (\neg B)$
- Komposition: $(A \Rightarrow B) = (\neg B \Rightarrow \neg A)$

Beweistechniken

- direkter Beweis: $V \Rightarrow A$
- indirekter Beweis: $\neg A \Rightarrow \neg V$
- indirekter Beweis mit Widerspruch: Zeige $V \wedge (\neg A) \Rightarrow B$ und B ist falsch
- Zwischenschritte: $V \Rightarrow Z_1, Z_1 \Rightarrow Z_2, ..., Z_n - 1 \Rightarrow Z_n, Z_n \Rightarrow A$
- Fallunterscheidung: $V \Rightarrow F_1 \wedge F_2, F_1 \Rightarrow A, F_2 \Rightarrow A$

1.2.2 Quantoren

Sei X eine Menge

- Allquantoren: $\forall x \in X : A(x)$ Für alle $x \in X$ gilt $A(x)$
- Existenzquantoren: $\exists x \in X : A(x)$ Es existiert ein $x \in X$ für das $A(x)$ wahr ist
  $\exists! x \in X : A(x)$ Es existiert genau ein $x \in X$ für das $A(x)$ wahr ist
- Negation von Quantoren: $\neg(\forall x \in X : A(x)) \Leftrightarrow \exists x \in X : \neg A(x)$
  $\neg(\exists x \in X : A(x)) \Leftrightarrow \forall x \in X : \neg A(x)$
- Vertauschung (Kombination) von Allquantoren:
  $$\forall x \in X : \forall y \in Y : A(x,y) \Leftrightarrow \forall y \in Y : \forall x \in X : A(x,y)$$
- Vertauschung (Kombination) von Existenzquantoren:
  $$\exists x \in X : \exists y \in Y : A(x,y) \Leftrightarrow \exists y \in Y : \exists x \in X : A(x,y)$$
  $$\exists x | in X : \forall y \in Y : A(x,y) \Rightarrow \forall y \in Y : \exists x \in X : A(x,y)$$
  Fall 1: x kann nicht von y abhängen
  Fall 2: x kann von z abhängen

Beispiel

$\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : m \geq n$	Stimmt, wähle z.B. $m = n + 1$
$\exists m \in \mathbb{N} : n \in \mathbb{N} : m \geq n$	Stimmt nicht

1.2.3 Funktionen

Seien X und Y Mengen
Eine Funktion ordnet jedem $x | in X$ genau ein $y \in Y$ zu
$$f : X \to Y, x \mapsto y : f(x)$$
X ist die Definitionsmenge, Y die Zielmenge

Statt Funktion sagt man auch Abbildung, Operator, Funktionale
$f : X \to Y$ ist:

- injektiv, falls $\forall x, x^1 \in X : x \neq x^1 \Rightarrow f(x) \neq f(x^1)$
  $\Leftrightarrow \forall x, x^1 \in X : f(x) = f(x^1) \Rightarrow x = x^1$
- surjektiv, falls $\forall y \in Y : \exists x \in X : f(x) = y$
- bijektiv, falls f injektiv und surjektiv
  $\forall y \in Y : \exists! x \in X : f(x) = y$

Für bijektive Funktionen können wir die Umkehrfunktion definieren:
$f^{-1} : Y \to X : f^{-1}(y) := x$, wo $x \in X$ erfüllt $f(x) = y$

Seien $f : X \to Y, g : Y \to Z$ zwei Funktionen zwischen Mengen X, Y, Z
$g \circ f = X \to Z, x \mapsto g \circ f(x) := g(f(x))$

Sind f, g bijektiv, dann gilt
$g \circ f$ bijektiv und $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

Sei $X' \subseteq X$ definiere
$f(X') = \{f(x) : x \in X'$

Beispiel
$f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$
$f([1, 3]) = [1, 9]$

Für $Y' \subseteq Y$ definiere
$f^{-1}(Y') := \{x \in X : f(x) \in Y\}$
(auch dann, wenn f nicht bijektiv ist, also $f^{-1} : Y \to X$ nicht existiert)

Beispiel
$f : \mathbb{R} \to \mathbb{R}, f(x) = x^2$
$f^{-1}([1, 9]) = [1, 3] \cup [-3, -1]$

Falls f bijektiv ist und $y \in Y$
$x = f^{-1}(y)$ mit $f(x) = y$
$\{x\} = f^{-1}(\{y\})$

Für $f : X \to Y$ gilt immer $|f(X)| \leq |X|$

Falls f injektiv $\Rightarrow |f(X)| = |X|$

Ist $|X| = |Y| < \infty$ dann gilt f injektiv $\Leftrightarrow |f(X)| = |X|$

Falls f surjektiv $\Rightarrow f(x) = y \Rightarrow |f(x)| = |Y|$

Falls $Y < \infty$, dann gilt f surjektiv $\Leftrightarrow |f(X)| = |Y|$

Ist $|X| = |Y| < \infty$, dann gilt f injektiv $\Leftrightarrow f$ surjektiv $\Leftrightarrow f$ bijektiv

1.3 Algebraische Strukturen

Sei A eine Menge

- Eine Verknüpfung ist eine Funktion
  $$\circ : A \times A \to A$$
  Für $\circ(a, b)$ schreibe $a \circ b$ mit $a, b \in A$

Beispiel
$\mathbb{N}$ mit $+$
$\mathbb{Z}$ mit $*$
{falsch, wahr} mit AND

Aber nicht $\mathbb{N}$ mit $-$, da das Ergebnis außerhalb von $\mathbb{N}$ liegen kann

Eine Gruppe $(G, \circ)$ ist eine Menge $G \neq \emptyset$ zusammen mit einer Verknüpfung $\circ : G \times G \to G$, für die gilt:

- (G1) Assoziativität: $(a \circ b) \circ c = a \circ (b \circ c), \forall a, b, c \in G$
- (G2) Existenz des neutralen Elements $\exists e \in G : a \circ e = e \circ a = a, \forall a \in G$
- G(3) Existenz inverser Elemente $\forall a \in G : \exists a' \in G : a \circ a' = a' \circ a = e$

(G1) - G(3) heißen auch Gruppenaxiome

Beispiele
$\mathbb{Z}$ mit $+$ ist eine Gruppe
$\mathbb{Q}$ mit $*$ ist keine Gruppe, da 0 kein inverses Element hat, aber
$\mathbb{Q} \setminus \{0\}$ ist eine Gruppe

Eine Gruppe heißt kommutativ (auch abelsch), wenn zusätzlich gilt:

- (G4) Kommutativität: $a \circ b = b \circ a, \forall a, b \in G$

Eine Menge $G \neq \emptyset$ mit Verknüpfung $\circ$ heißt Halbgruppe, wenn (G1) erfüllt ist
$(G, \circ)$ heißt kommutative Halbgruppe, falls (G1) und (G4) erfüllt sind

Ein Ring $(R, +, *)$ ist eine Menge $R \neq \emptyset$ zusammen mit zwei Verknüpfungen $+ : R \times R \to R$ und $* : R \times R \to R$, für die gilt:

- (R1) $(R, +)$ ist eine kommutative Gruppe
- (R2) $(R, *)$ ist eine Halbgruppe
- (R3) Es gelten Distributivgesetze: $\forall a, b, c \in R$ gilt
$$a * (b + c) = a * b + a * c$$
$$(a + b) * c = a * c + b * c$$

$(R, +, *)$ heißt kommutativer Ring, falls $*$ kommutativ
$(R, +, *)$ heißt Ring mit 1, falls neutrales Element bezüglich $*$ existiert

Sei X Menge, R Ring
$$F := \{f : X \to R\}$$
$$+ : F \times F \to F, (f + g)(x) = f(x) + g(x)$$
$$* : F \times F \to F, (f * g)(x) = f(x) * g(x)$$
Dann ist $(F, +, *)$ ein Ring. Ist R kommutativ, dann auch F. Besitzt R eine Eins, dann auch F

Ein Körper (engl. field) $(K, +, *)$ ist eine Menge K mit Verknüpfungen $+, *)$, für die gilt:

- (K1) $(K, +)$ ist eine kommutative Gruppe
- (K2) $(K \setminus \{0\}, *)$ ist eine kommutative Gruppe
- (K3) Es gelten die Distributivgesetze: $a * (b + c) = a * b + a * c)$
$(a + b) * c = a * c + b * c$

Beispiel
$(\mathbb{Q}, +, *)$ ist ein Körper
Rechenregeln im Körper: Für $x, y, z \in K$

- Kommutativgesetz $x + y = y + x$
$x * y = y * x$
- Assoziativgesetz $(x + y) + z = x + (y + z)$
$(x * y) * z = x * (y * z)$
- Distributivgesetz $x * (y + z) = x * y + x * z$
- Neutrale Elemente $x + 0 = x$
$x * 1 = x$
- Inverse Elemente $x + (-x) = 0$
$x * x^{-1} = 1$, für $x \neq 0$

2 Diskrete Mathematik

Die diskrete Mathematik beschäftigt sich mit endlichen Mengen $\mathbb{N}$ oder $\mathbb{Z}$

2.1 Natürliche Zahlen und vollständige Induktion

$\mathbb{N} = \{1, 2, 3, ...\}$
$\mathbb{N}$ ist die Menge, die die 1 enthält und zu jeder Zahl $n \in \mathbb{N}$ auch $n + 1$ enthält

Satz 2.1 Vollständige Induktion
Gilt eine Aussage $A(n)$ für $n = 1$ und gilt außerdem $A(n) \Rightarrow A(n+1)$, dann gilt $A(n), \forall n \in \mathbb{N}$
Beweis: Die Menge der n, für die $A(n)$ gilt, enthält 1 und für jede enthaltene Zahl ist auch +1 enthalten. Dies ist also $\mathbb{N}$