Mathematik 1

Skript zum Modul Mathematik 1 für inf, swt und msv

Simon König

Inhaltsverzeichnis

1 Grundlagen **3**
- 1.1 Logik . . . 3
  - 1.1.1 Logische Junktoren . . . 3
- 1.2 Prädikatenlogik und Quantoren . . . 3
- 1.3 Beweise . . . 4
  - 1.3.1 Direkter Beweis . . . 4
  - 1.3.2 Indirekter Beweis . . . 4
  - 1.3.3 Widerspruchsbeweis . . . 4

2 Mengen, Relationen und Abbildungen **5**
- 2.1 Abbildungen . . . 6
- 2.2 Mächtigkeit von Mengen . . . 7
- 2.3 Zahlenmengen . . . 7
- 2.4 Summen- und Produktzeichen . . . 8
- 2.5 Teilbarkeit und Primzahlen . . . 8

3 Komplexe Zahlen **10**
- 3.1 Polarkoordinaten-Darstellung . . . 11

4 Gruppen, Ringe und Körper **12**

5 Lineare Algebra **14**
- 5.1 Vektorräume . . . 14

1: Grundlagen

1.1: Logik

Definition 1.1: Aussage

Eine Aussage ist ein Satz, von dem es Sinn macht, zu fragen, ob er wahr oder falsch ist.

1.1.1: Logische Junktoren

Wir verknüpfen mehrere Aussagen zu größeren aussagelogischen Formeln mithilfe von logischen Junktoren:

Negation: $\neg A$ **Konjuktion:** $A \land B$ **Disjunktion:** $A \lor B$

Durch verwenden dieser grundlegenden Junkoren kann man alle Verknüpfungen darstellen. Um Schreibarbeit zu sparen gibt es verkürzende Schreibweisen

Implikation: $A \Rightarrow B \equiv \neg(A \land \neg B)$

Äquivalenz: $A \Leftrightarrow B \equiv (A \land B) \lor (\neg A \land \neg B)$

1.2: Prädikatenlogik und Quantoren

Ein Prädikat ist ein Ausdruck, der die Form einer Aussage hat, aber Variablen enthält.
$P(m) :=$„m ist eine gerade Zahl. “
Eine Aussage wird daraus erst, wenn wir angeben, für welche m das Prädikat gelten soll.
Sei M eine Menge und $P(m)$ für jedes $m \in M$ eine Aussage. Wir beschreiben die Aussage mit dem *Allquantor*:

$$\forall m \in M : P(m)$$

d.h. $P(m)$ soll für *jedes* $m \in M$ gelten.
Mit dem *Existenzquantor* bekommt das Prädikat eine andere Bedeutung:

$$\exists m \in M : P(m)$$

d.h. es soll mindestens ein $m \in M$ existieren, für das $P(m)$ gilt.

Beispiel $M = \mathbb{N}, P(m)$: „m ist eine gerade Zahl.“
$(\forall m \in M : P(m))$ ist falsch. $(\exists m \in M : P(m))$ ist jedoch wahr.

Bemerkung:

- Verneinung von quantifizieren Prädikat-Aussagen: „Prädikat verneinen und Quantoren tauschen.“

$$\neg(\forall m \in M : P(m)) \equiv \exists m \in M : \neg P(m)$$

- Bei Quantoren kommt es auf die Reihenfolge an:

$$\begin{array}{lll} \forall n \in \mathbb{N} & \exists m \in \mathbb{N} : m \geq n & \text{ist wahr} \\ \exists n \in \mathbb{N} & \forall m \in \mathbb{N} : m \geq n & \text{ist falsch} \end{array}$$

1.3: Beweise

1.3.1: Direkter Beweis

1.3.2: Indirekter Beweis

1.3.3: Widerspruchsbeweis

2: Mengen, Relationen und Abbildungen

Eine Menge ist eine wohldefinierte Gesamtheit von Objekten, den Elementen der Menge.

z.B. $\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p \in \mathbb{Z}, q \in \mathbb{N} \right\}$

Definition 2.1: Teilmenge

Eine Menge M_1 ist *Teilmenge* von M, wenn

$$\forall x \in M_1 : x \in M$$
$$\Rightarrow M_1 \subseteq M$$

Für jede Menge M gilt $\varnothing \subseteq M$ und $M \subseteq M$.
Gilt $M_1 \subseteq M$ und $M_1 \neq M$ ist M_1 eine *echte Teilmenge* von M, d.h. $M_1 \subset M$ oder $M_1 \subsetneq M$

Potenzmenge

$\mathcal{P}(M) = \mathrm{Pot}(M)$ ist die Menge aller Teilmengen von M.

Schnittmenge

$$M_s = M_1 \cap M_2; \quad M_s \coloneqq \{m \in M_1 \,|\, m \in M_2\}$$

Zwei Mengen M_1 und M_2 heißen *disjunkt*, falls $M_1 \cap M_2 = \varnothing$

Vereinigung

$$M_v = M_1 \cup M_2; \quad M_v \coloneqq \{m \,|\, m \in M_2 \vee m \in M_2\}$$

Differenz

$$M_1 \setminus M_2 \coloneqq \{m \in M_1 \,|\, m \notin M_2\}$$

Kartesisches Produkt

$$M_1 \times M_2 \coloneqq \{(m_1, m_2) \,|\, m_1 \in M_1 \wedge m_2 \in M_2\}$$

Definition 2.2: Relation

Eine Relation zwischen zwei Mengen M und N ist eine Teilmenge von $M \times N$.

$$R \subseteq M_1 \times M_2$$

ist $(x, y) \in R$, steht x mit y in Relation $\to x \sim y$.
$R \subseteq M \times M$ heißt

reflexiv , falls $\forall x \in M : (x,x) \in R$

symmetrisch , falls $\forall x, y \in M : (x,y) \in M \Rightarrow (y,x) \in R$

antisymmetrisch , falls $\forall x, y \in R : (x,y) \in M \wedge (y,x) \in R \Rightarrow x = y$

transitiv , falls $\forall x, y, z \in M : (x,y) \in R \wedge (y,z) \in R \Rightarrow (x,z) \in R$

Definition 2.3: Äquivalenzrelation

Eine Relation heißt Äquivalenzrelation, wenn sie reflexiv, symmetrisch und transitiv ist.

Definition 2.4: Ordnungsrelation

Eine Relation heißt Ordnungsrelation, wenn sie reflexiv, antisymmetrisch und transitiv ist.

2.1: Abbildungen

Definition 2.5: Abbildung

Seien M und N zwei Mengen. Eine Zuordnungsvorschift, die jedem Element $x \in M$ ein Element $f(x) \in N$ zuweist, heißt Abbildung oder Funktion von M nach N.

$$f : M \to N, x \mapsto f(x)$$

M: Definitionsbereich, N: Wertebereich

Definition 2.6:

Sei $f : M \mapsto N$ eine Abbildung. Wir definieren

- für $x \in M$ heißt $f(x) \in N$ das *Bild* von x
- für eine Teilmenge $A \subseteq M$ heißt $f(A) = \{f(x) \,|\, x \in A\}$ das *Bild der Teilmenge* A
- für eine Teilmenge $B \subseteq N$ heißt $f^{-1}(B) = \{x \in M \,|\, f(x) \in B\}$ das *Urbild* von B

Definition 2.7: Abbildungseigenschaften

Sei $f : M \to N$ eine Abbildung. Dann heißt f:

injektiv , wenn jedes Element $y \in N$ *höchstens ein Urbild* hat.

surjektiv , wenn jedes Element $y \in N$ *mindestens ein Urbild* hat. $\forall y \in N \; \exists x \in M : f(x) = y$

bijektiv , wenn jedes Element $y \in N$ *genau ein Urbild* hat. $\forall y \in N \; \exists! x \in M : f(x) = y$

Bemerkung:

1. Bijektivität gilt genau dann, wenn es eine Umkehrabbildung f^{-1} gibt:

$$\begin{aligned} f : M \to N & \qquad & f^{-1} : N \to M \\ f\left(f^{-1}(x)\right) \quad \text{mit } x \in N & \qquad & f^{-1}\left(f(x)\right) = x \quad \text{mit } x \in M \end{aligned}$$

2. Man kann jede Abbildung surjektiv machen, indem man den Wertebereich durch das Bild von f ersetzt: $N := f(M)$

2.2: Mächtigkeit von Mengen

Die Mächtigkeit einer Menge ist die Anzahl ihrer Elemente. Man schreibt $|M|$ für die Mächtigkeit von M.
Zwei Mengen A und B sind gleich mächtig, wenn es eine bijektive Abbildung $f : A \to B$ gibt.
Eine Menge heißt *abzählbar unendlich*, falls $|A| = |\mathbb{N}|$ d.h. falls es eine bijektive Abbildung $f : A \to \mathbb{N}$ gibt.
Sie heißt *überabzählbar unendlich*, falls $|A| > |\mathbb{N}|$.
Es gilt immer auch für unendliche Mengen, dass $|M| < |\mathrm{Pot}(M)|$.
Für endliche Mengen gilt $|\mathrm{Pot}(M)| = 2^{|M|}$

2.3: Zahlenmengen

Definition 2.8: Natürliche Zahlen

Die natürlichen Zahlen sind eine Menge $\mathbb{N}$, auf der eine Abbildung $f : \mathbb{N} \to \mathbb{N}$ erklärt ist, die folgende Eigenschaften hat, wobei $f(n)$ der *Nachfolger* von n heißt.

$\mathbb{N}1$ Es gibt genau ein Element in $\mathbb{N}$, das nicht Nachfolger eines anderen Elements ist.

$\mathbb{N}2$ f ist injektiv

$\mathbb{N}3$ Ist $M \subseteq \mathbb{N}$ eine Teilmenge, die folgende Eigenschaften hat:

1. $1 \in M$
2. Falls $m \in M$ und $f(m) \in M$

Dann gilt: $M = \mathbb{N}$

D.h. $M \subseteq \mathbb{N} : 1 \in M \wedge (m \in M \Rightarrow f(m) \in M) \Rightarrow M = \mathbb{N}$

Man kann zeigen, dass die natürlichen Zahlen durch diese Eigenschaften (die Peano-Axiome) gekennzeichnet sind. Das heißt, dass es im wesentlichen nur eine solche Menge mit einer solchen Abbildung f gibt, nämlich $\mathbb{N}$.
Das Axiom $\mathbb{N}3$ heißt auch Induktionsaxiom. Aus ihm folgt:

Satz 2.1: Vollständige Induktion

Sei $A(n)$ für jede natürliche Zahl $n \in \mathbb{N}$ eine Aussage, für die gilt:

- $A(1)$ ist wahr
- $\forall n \in \mathbb{N} : A(n) \Rightarrow A(n+1)$

dann ist $A(n)$ für alle $n \in \mathbb{N}$ wahr.

Definition 2.9: Graph einer Abbildung

Sei $f : M \to N$ eine Abbildung. Der Graph von f ist eine Teilmenge $\{(x, f(x)) \mid x \in M\} \subseteq M \times N$. Für Funktionen $f : \mathbb{R} \to \mathbb{R}$ ist der Graph eine Teilmenge der Ebene $\mathbb{R}^2$.
Fasst man eine Funktion als eine Relation auf, so ist der Graph das selbe wie R. $\mathrm{Graph}(f) = R \subseteq \mathbb{R} \times \mathbb{R}$

Definition 2.10: Verkettung

Seien $f : M \to N$ und $g : N \to P$ Abbildungen. Dann ist die Verkettung:

$$g \circ f : M \to P$$
$$g \circ f(x) \coloneqq g(f(x))$$

Definition 2.11: Identität

Für jede Menge M ist

$$\mathrm{id}_M : M \to M, x \mapsto x$$

die identische Abbildung auf M.

2.4: Summen- und Produktzeichen

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

Bei der Summe ist k der Summationsindex, m die untere und n die obere Summationsgrenze

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

Bemerkung:

- Ist die obere Summationsgrenze kleiner als die untere, so handelt es sich um eine *leere Summe*, ihr Wert ist 0.
- Entsprechend ist der Wert des *leeren Produkts* 1.

2.5: Teilbarkeit und Primzahlen

Definition 2.12: Teilbarkeit

Seien $n \in \mathbb{Z}, m \in \mathbb{N}$. Die Zahl m heißt *ein Teiler* von n, in Zeichen $k \cdot m = n$, wenn es ein $k \in \mathbb{Z}$ gibt, so dass $k \cdot m = n$. In diesem Fall heißt n auch teilbar durch m. Die Zahl 0 ist durch alle $m \in \mathbb{Z}$ teilbar.
Falls $m|n_1$ und $m|n_2$, dann folgt $m|n_1 + n_2$.

Definition 2.13: Größter gemeinsamer Teiler

Sei $a \in \mathbb{Z}$, die Menge aller Teiler von a ist $\mathcal{D}(a) := \{d \in \mathbb{N} \mid d|a\}$.
Die Menge aller gemeinsamer Teiler von a und b mit $a, b \in \mathbb{Z} \setminus \{0\}$ ist $\mathcal{D}(a, b) = \mathcal{D}(a) \cap \mathcal{D}(b)$.
Die Zahl $\mathrm{ggT}(a, b) = \max(\mathcal{D}(a, b))$ heißt größter gemeinsamer Teiler von a und b. Da eine ganze Zahl (außer der 0) nur endlich viele Teiler hat, existiert $ggT(a, b)$.

Definition 2.14: Primzahl

Eine natürliche Zahl heißt *Primzahl*, wenn sie genau zwei Teiler besitzt, nämlich 1 und die Zahl selbst.

$$p \in \mathbb{N} \text{ mit } |\mathcal{D}(p)| = 2$$

Satz 2.2:

Jede natürliche Zahl $n \in \mathbb{N} \wedge n \geq 2$ ist ein Produkt aus Primzahlen (1 ist das leeren Produkt).

Beweis:

$A(n)$: „Jede natürliche Zahl kleiner oder gleich n ist das Produkt von Primzahlen.“

IA $A(2)$ ist wahr, denn 2 ist selbst eine Primzahl.

IS Fallunterscheidung:

1. $n + 1$ ist prim. Dann ist $A(n + 1)$ wahr.
2. $n + 1$ ist nicht prim. Dann gibt es natürliche Zahlen 1 und m, sodass $n + 1 = l \cdot m$, wobei $l, m < n + 1$.

Nach Induktionsvoraussetzung sind somit l und m Produkte von Primzahlen, somit auch $n + 1$.

3: KOMPLEXE ZAHLEN

Definition 3.1: Komplexe Zahlen

Wir definieren $\mathbb{C}$ als Menge $\mathbb{C} := \mathbb{R} \times \mathbb{R}$, d.h. wir definieren die komplexen Zahlen als zusammengesetzte Zahlen, also als die Menge der geordneten Paare von reellen Zahlen. Wobei wir folgende Abbildungen mit $\mathbb{C} \times \mathbb{C} \to \mathbb{C}$ auf $\mathbb{C}$ festlegen:

ADDITION

$$(a, b) + (c, d) := (a + b, c + d)$$

MULTIPLIKATION

$$(a, b) \cdot (c, d) := (ac - bd, ad + bc)$$

Bemerkung:

Die Menge der reellen Zahlen kann als Teilmenge von $\mathbb{C}$ aufgefasst werden. $\mathbb{R} \subset \mathbb{C}$ indem man die injektive Abbildung $\mathbb{R} \to \mathbb{C}, a \mapsto (a, 0)$ benutzt. Die oben definierten Verknüpfungen schränken sich dann auf die Verknüpfungen in $\mathbb{R}$ ein:

- $(a, 0) + (b, 0) = (a + b, 0)$
- $(a, 0) \cdot (b, 0) = (a \cdot b - 0, a \cdot 0 + b \cdot 0) = (a \cdot b, 0)$

In diesem Sinne ist $\mathbb{C}$ eine *Erweiterung* des Körpers $\mathbb{R}$.

Definition 3.2: Imaginäre Einheit

Wir führen die imaginäre Einheit ein. $\mathfrak{i} := (0, 1)$ damit gilt:

$$(0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 0 \cdot 1) = (-1, 0) = \mathfrak{i}^2 = -1$$

Es gilt also $\mathfrak{i}^2 = -1$, daher schreibt man auch $\mathfrak{i} = \sqrt{-1}$. Die Zahlen $(0, y) = y \cdot \mathfrak{i}, y \in \mathbb{R}$ heißten imaginäre Zahlen. Wir können uns wegen $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ komplexe Zahlen als Punkte bzw. Vektoren in der *Gauß'schen Zahlenebene* vorstellen.

Satz 3.1:

Für jede komplexe Zahl $(a, b) \in \mathbb{C}$ gilt:

$$(a, b) = a + b\mathfrak{i}$$

Beweis:

durch ausrechnen der rechten Seite:

$$\begin{aligned} a + b\mathrm{i} &= (a, 0) + (b, 0) \cdot (0, 1) \\ &= (a, 0) + (b \cdot 0 - 0 \cdot 1, b \cdot 1 + 0 \cdot 0) \\ &= (a, 0) + (0, b) = (a, b) \end{aligned} \qquad \square$$

Bemerkung:

Wie man leicht nachrechnet, gelten wie in $\mathbb{R}$ die Kommutativ-, Assoziativ- und Distributivgesetze.

Definition 3.3: Konjugiert komplexe Zahl

Sei $z = a + b\mathrm{i} \in \mathbb{C}$. Dann heißt $\overline{z}$ die konjugiert komplexe Zahl $\overline{z} = a - b\mathrm{i}$ von z.

Satz 3.2: Eigenschaften der konjugiert komplexen Zahl

Seien $z, w \in \mathbb{C}$ dann gilt:

1. $\overline{z + w} = \overline{z} + \overline{w}$
2. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$
3. $\frac{1}{2}(z + \overline{z}) = \mathfrak{Re}(z)$
4. $\frac{1}{2}(z - \overline{z}) = \mathfrak{Im}(z)$
5. $z \cdot \overline{z} > 0 \in \mathbb{R}$ falls $z \neq 0$

Definition 3.4: Betrag einer komplexen Zahl

Mit der komplexen Zahl $z = a + b\mathrm{i}$ und $a, b \in \mathbb{R}$ gilt für den Betrag von z:

$$|z| = \sqrt{z \cdot \overline{z}} = \sqrt{a^2 + b^2}$$
$$|z| = |\overline{z}|$$

Insbesondere lässt sich das multiplikative Inverse wie folgt ausdrücken:

$$z^{-1} = \frac{1}{z} = \frac{\overline{z}}{z \cdot \overline{z}} = \frac{a - b\mathrm{i}}{a^2 + b^2}$$

3.1: Polarkoordinaten-Darstellung

4: Gruppen, Ringe und Körper

Definition 4.1: Verknüpfung

Sei M eine Menge. Eine Abbildung $M \times M \to M, (a,b) \mapsto a \star b$ nennt man Verknüpfung.

1. Eine Verknüpfung heißt kommutativ, falls $a \star b = b \star a \quad \forall a,b \in M$ gilt.
2. Sie heißt assoziativ, falls $a \star (b \star c) = (a \star b) \star c = \quad \forall a,b,c \in M$ gilt.
   Man kann auch $a \star b \star c$ schreiben.
3. Ein Element $e \in M$ heißt neutrales Element bezüglich der Verknüpfung $\star$,
   falls $a \star e = e \star a = a \quad \forall a \in M$ gilt.

Definition 4.2: Invertierbarkeit

Sei M eine Menge mit einer Verknüpfung $\star$, die ein neutrales Element e besitzt, ein Element $a \in M$ heißt invertierbar, falls es ein Element $a^{-1} \in M$ gibt, so dass gilt:

$$a \star a^{-1} = a^{-1} \star a = e$$

Definition 4.3: Gruppe

Eine Menge G mit einer Verknüpfung $\star$ heißt *Gruppe*, falls

G1 Die Verknüpfung assoziativ ist,

G2 ein neutrales Element besitzt,

G3 jedes Element invertierbar ist.

Falls die Verknüpfung zusätzlich kommutativ ist, nennt man die Gruppe eine *abel'sche Gruppe* oder auch kommutative Gruppe.

Definition 4.4: Ring

Sei M eine Menge mit zwei Verknüpfungen $(+, \cdot)$ und den folgenden Eigenschaften:

R1 $(M,+)$ ist eine abel'sche Gruppe mit neutralem Element 0.

R2 die Verknüpfung $\cdot$ ist assoziativ mit neutralem Element 1.

R3 es gelten die Distributivgesetze:

$$(a+b) \cdot c = ac + bc$$
$$c \cdot (a+b) = ca + cb$$

R4 $0 \neq 1$

Dan heißt M ein *Ring* (genauer ein Ring mit Eins - unitärer Ring).

Ist zusätzlich auch die Multiplikation $\cdot$ kommutativ und ist $M \setminus \{0\}$ eine Gruppe bezüglich $\cdot$ (d.h. besitzt jedes Element ein Inverses bzgl. $\cdot$) so heißt M *Körper*.

Satz 4.1: Eindeutigkeit der neutralen Elemente

In einer Gruppe ist das neutrale Element stats eindeutig, d.h. ist e ein neutrales Element und gibt es ein Element:

$$a \in G, \forall g \in G : a \star g = g \star a = g$$

Dann ist $a = e$!

Beweis:

Gelte $a \star g = g$ für ein $g \in G$. Dann folgt:

$$(a \star g) \star g^{-1} = g \star g^{-1}$$

Mit **G1** und **G3** gilt:

$$a \star (g \star g^{-1}) = e$$

Dann folgt mit **G3**:

$$a \star e = e \text{ und damit } a = e$$ □

Bemerkung:

Ähnlich dazu der Beweis, dass inverse Elemente eindeutig bestimmt sind.

Definition 4.5: Homomorphismus

Seien $(G, \star)$ und $(H, *)$ Gruppen. Eine Abbildung $f : G \to H$ heißt (Gruppen-)Homomorphismus, falls gilt:

$$f(a \star b) = f(a) * f(b) \quad \forall a, b \in G$$

Lemma 4.1:

Ein Gruppenhomomorphismus $f : G \to H$ bildet stets das neutrale Element in G auf das neutrale Element in H ab.

Beweis:

Sei e das neutrale Element in G, dann folgt:

$$f(e) * f(g) = f(e \star g) = f(g)$$

Es folgt dann, dass $f(e)$ das neutrale Element in H ist.

Definition 4.6:

Sei G eine Gruppe mit Verknüpfung $\star$ und neutralem Element e.
Eine nichtleere Teilmenge $U \subseteq G$ heißt *Untergruppe* von G, falls gilt:

UG 1 $\forall a, b \in U : a \star b \in U$ (Abgeschlossenheit)

UG 2 $\forall a \in U : a^{-1} \in U$

Immer gilt, dass der Kern eines Homomorphismus $f : G \to H$ d.h. $\mathrm{Kern}(f) = f^{-1}(\{e\})$ eine Untergruppe von G ist.

5: Lineare Algebra

5.1: Vektorräume

Beispiel

$$\begin{aligned}
\mathbb{R}^2 &= \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x, y \in \mathbb{R}\} \\
\mathbb{R}^3 &= \{(x, y, z) \mid x, y, z \in \mathbb{R}\} \\
&\vdots \\
\mathbb{R}^n &= \{(x_1, x_2, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}
\end{aligned}$$

Wir schreiben die Elemente von $\mathbb{R}^n$ auch als sogenannte Spaltenvektoren:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \text{ anstatt von } (x_1, x_2, \ldots, x_n)$$

Mit der komponentenweisen Addition, der Vektoraddition:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix}$$

wird $\mathbb{R}^n$ zu einer abel'schen Gruppe mit dem Nullvektor als neutrales Element und dem negierten Vektor als inverses Element bezüglich der Addition.
In der Vektorrechnung nennt man Zahlen (z.B. Elemente aus $\mathbb{R}, \mathbb{C}, \mathbb{Q}$) *Skalare*, um Zahlen und Vektoren deutlich zu unterscheiden.
Sei $x :- \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}$ und $\lambda \in \mathbb{R}$. Dann ist die *skalare Multiplikation* $x \cdot \lambda$ definiert durch $x \cdot \lambda := \begin{pmatrix} \lambda \cdot x_1 \\ \vdots \\ \lambda \cdot x_n \end{pmatrix}$
Die beiden Operationen Vektoraddition und skalare Multiplikation sind kennzeichnend für einen Vektorraum.

Definition 5.1: Vektorraum

Sei K ein Körper, dessen neutrales Element bezüglich der Multiplikation mit 1_K bezeichnet wird. Sei V eine Menge mit einer Verknüpfung $+$, so dass $(V, +)$ eine abel'sche Gruppe bildet.
Sei weiter eine Abbildung, genannt *skalare Multiplikation* $K \times V \to V$ gegeben, so dass folgende Bedingungen $\forall \alpha, \beta \in K; x, y \in V$ gelten:

V 1 $(\alpha \cdot \beta) \cdot x = \alpha \cdot (\beta \cdot x)$ (assoziativ)

V 2 $1_K \cdot x = x$ (neutrales Element des Körpers ist das neutrale bzgl $\cdot$)

V 3 $(\alpha + \beta) \cdot x = \alpha \cdot x + \beta \cdot x$ (distributiv 1)

V 4 $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$ (distributiv 2)

Dann ist V ein *Vektorraum* über dem Körper K. Kurz auch K-Vektorraum. Die Verknüpfung $+$ wird Vektoraddition genannt. Für $K = \mathbb{R}$ bzw. $K = \mathbb{C}$ spricht man auch von einem reellen, bzw. komplexen Vektorraum.
Elemente von V nennt man Vektoren.

Beispiele

- $\mathbb{R}^2, \mathbb{R}^3, \ldots$
- $\mathbb{C}^2$
- $\{0\}$ ist ein Vektorraum für jeden Körper K.
- Sei $V = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$ die Menge der reellen Funktionen in einer Variable. Durch die punktweise Addition

  $(f + g)(x) = f(x) + g(x)$

  und die punktweise skalare Multiplikation

  $(\lambda f)(x) = \lambda \cdot f(x)$

  wird V zu einem Vektorraum.

Definition 5.2: Untervektorraum

Sei V ein K-Vektorraum. Eine nichtleere Teilmenge $U \subseteq V$ heißt Untervektorraum bzw. Teilvektorraum, falls gilt:

UV 1 Abschluss unter Vektoraddition:

$$\forall u, v : u, v \in U \Rightarrow u + v \in U$$

UV 2 Abschluss unter skalarer Multiplikation:

$$\forall u \in U, \lambda \in K : \lambda \cdot u \in U$$

Beispiele Die folgenden sind Untervektorräume von $\mathbb{R}^2$:

- $U_1 := \left\{ \begin{pmatrix} x \\ 0 \end{pmatrix} \middle| \, x \in \mathbb{R} \right\}$ (die x-Achse)
- $U_2 := \left\{ \begin{pmatrix} x \\ x \end{pmatrix} \middle| \, x \in \mathbb{R} \right\}$ (die Winkelhalbierende des 1. und 3. Quadranten)

Lemma 5.1:

Für alle $\lambda \in K, v \in V$ wobei V ein K-Vektorraum ist, gilt:

1. $0_K \cdot v = 0_V$
2. $(-\lambda) \cdot v = -(\lambda \cdot v)$

Beweis:

1. Es gilt:

$$0 \cdot v = (0 + 0) \cdot v \underset{\textbf{(V 3)}}{=} 0 \cdot v + 0 \cdot v$$

$$0 \cdot v + (-(0 \cdot v)) = (0 \cdot v + 0 \cdot v) + (-(0 \cdot v)) \underset{\textbf{(V 1)}}{=} 0 \cdot v + (0 \cdot v + (-0 \cdot v))$$

$$0 = 0 \cdot v + 0 = 0 \cdot v$$

Definition 5.3: Linearkombination

Seien $v_1, v_2, \ldots, v_k$ Vektoren aus dem K-Vektorraum V und seien $\lambda_1, \lambda_2, \ldots, \lambda_k \in K$. Dann heißt der Vektor

$$u = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k = \sum_{j=1}^{k} \lambda_j v_j$$

Linearkombination von den Vektoren $v_1, v_2, \ldots, v_k$. Die Skalare $\lambda_1, \lambda_2, \ldots, \lambda_k$ heißen *Koeffizienten* der Linearkombination.
Sind in der Linearkombination alle Koeffizienten gleich Null, handelt es sich um die *triviale Linearkombination*. Gibt es hingegen mindestens einen Koeffizienten $\lambda_j \neq 0$, handelt es sich um einee *nichttriviale Linearkombination*.

Definition 5.4:

Sei V ein K-Vektorraum, $M \subseteq V$ eine Teilmenge. Dann heißt die Menge aller Linearkombinationen

$$\{\lambda_1 v_1 + \ldots + \lambda_k v_k \,|\, v_1, v_2, \ldots, v_k \in M, \lambda_1, \lambda_2, \ldots, \lambda_k \in K\}$$

der *Spann* oder die lineare Hülle von M.

$$\operatorname{Span}(M) := \left\{ \sum_{j=1}^{k} \lambda_j v_j \;\middle|\; \lambda_j \in K, v_j \in M \right\}$$

Beispiele

- $v = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ in $\mathbb{R}^3 \rightsquigarrow \operatorname{Span}(\{v\}) = \left\{ \begin{pmatrix} \lambda \\ \lambda \\ 0 \end{pmatrix} \;\middle|\; \lambda \in \mathbb{R} \right\}$
- $\operatorname{Span}\left(\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}\right) = \left\{ \begin{pmatrix} x_1 \\ x_2 \\ 0 \end{pmatrix} \;\middle|\; x_1, x_2 \in \mathbb{R} \right\}$ (x_1, x_2-Ebene)

Satz 5.1:

Sei V ein K-Vektorraum und $M \subseteq V$. Dann ist $\operatorname{Span}(M)$ ein Untervektorraum von V.

Beweis:

1. $\operatorname{Span}(M)$ ist nicht leer, da der Nullvektor als leere Linearkombination mindestens enthalten ist.
2. Abschluss unter skalarer Multiplikation, sei $\lambda \in K, v \in \operatorname{Span}(M)$:

$$\begin{aligned} v &= \lambda_1 v_1 + \ldots + \lambda_k v_k \quad \text{wobei } v_1, \ldots, v_k \in M \\ \lambda v &= \lambda(\lambda_1 v_1 + \ldots + \lambda_k v_k) \\ &= \lambda(\lambda_1 v_1) + \ldots + \lambda(\lambda_k v_k) \\ &= (\lambda\lambda_1) v_1 + \ldots + (\lambda\lambda_k) v_k \end{aligned}$$

3. Abschluss unter Addition:

Definition 5.5: Erzeugendensystem

Gilt $V = \mathrm{Span}(M)$ für einen K-Vektorraum V und eine Teilmenge $M \subseteq V$, so sagt man M ist ein *Erzeugendensystem* von V.
Interessant ist die minimale Anzahl an Vektoren in einem Erzeugendensystem, bzw. ein *minimales Erzeugendensystem*.

Definition 5.6: Lineare Abhängigkeit

Eine Menge von Vektoren $M \subseteq V$ heißt *linear abhängig*, wenn es eine nichttriviale Linearkombination gibt, die den Nullvektor ergibt. Andernfalls heißt M *linear unabhängig*!

Satz 5.2:

Eine Menge von Vektoren ist genau dann linear abhängig, wenn einen Vektor $v \in M$ gibt, der sich als Linearkombination mit Vektoren aus $M \setminus \{v\}$ darstellen lässt.

„⇒“ Angenommen, M ist linear abhängig. Dann gibt es Vektoren $v_1, \ldots, v_n$ und Koeffizienten $\lambda_1, \ldots, \lambda_n \in K$, so dass die Linearkombination *nichttrivial* den Nullvektor ergibt. Dann folgt:

$$\begin{aligned} \lambda_j v_j &= -\lambda_1 v_1 - \lambda_2 v_2 - \ldots - \lambda_{j-1} v_{j-1} - \lambda_{j+1} v_{j+1} - \ldots - \lambda_n v_n \quad |\lambda_j \neq 0 \\ v_j &= \frac{1}{\lambda_j} \cdot (-\lambda_1 v_1 - \lambda_2 v_2 - \ldots - \lambda_{j-1} v_{j-1} - \lambda_{j+1} v_{j+1} - \ldots - \lambda_n v_n) \end{aligned}$$

Damit ist v_j als nichttriviale Linearkombination von Vektoren aus $M \setminus \{v_j\}$ dargestellt.

„⇐“ Angenommen, es gibt einen Vektor $v \in M$ sowie Vektoren $v_1, \ldots, v_n \in M \setminus \{v\}$ und Koeffizienten $\lambda_1, \ldots, \lambda_n \in K$, so dass gilt:

$$\begin{aligned} v &= \lambda_1 v_1 + \ldots + \lambda_n v_n \\ 0 &= \lambda_1 v_1 + \ldots + \lambda_n v_n - 1 \cdot v \end{aligned}$$

Dies ist eine nichttriviale Linearkombination mit Vektoren aus M, die 0 ergibt.

Definition 5.7: Basis

Eine Teilmenge B eines Vektorraums V heißt *Basis* von V falls B ein linear unabhängiges Erzeugendensystem ist.

Beispiele