V1G3 – Lineare Algebra I

Dozent:
Prof. Dr. Jan Schröer

Mitschriften von:
Tien Nguyen Thanh

WS 2021/2022
Stand: 4. Januar 2022

Inhaltsverzeichnis

1 Grundlagen

1.1 Mengen

Wir wollen uns mit einer sehr naiven, aber für unsere Zwecke ausreichenden, Mengenbegriff beschäftigen. Was eine Menge wirklich ist, erfahren wir von den Logikern und Mengentheoretikern.

Definition 1.1 (naive Menge)**.** Eine Menge M ist eine Zusammenfassung von verschiedenen Objekten, welche dann Elemente genannt werden, zu einem Objekt.

Beispiel 1.2.

- $\mathbb{N} \coloneqq \{0, 1, 2, \ldots\}$, die Menge der *natürliche Zahlen*. In dieser Vorlesung gehört die Null dazu.
- $\mathbb{Z} \coloneqq \{\ldots, -2, -1, 0, 1, 2, \ldots\}$, die Menge der *ganze Zahlen*.
- $\mathbb{Q} \coloneqq \{a/b \mid a, b \in \mathbb{Z}, b \geq 1\}$, die Menge der *rationale Zahlen*.
- $\mathbb{R}$, die Menge der *rationalen Zahlen*.

- $\mathbb{C}$, die Menge der *komplexen Zahlen*.
- $\varnothing$, die leere Menge, die per Definition keine Elemente enthält.

Bezeichnung 1.3 (Quantoren, Mengenschreibweise, Relationen)**.** Einige häufig verwendete Symbole

- $(\dots) \coloneqq (\dots)$ definiert das, was links steht, durch das, was rechts steht.
- $\forall$ bedeutet „für alle“.
- $\exists$ bedeutet „es existiert“.
- Wenn M eine Menge ist, bezeichnet $|M|$ die Anzahl der Elemente in M (*Kardinalität*). Für die leere Menge ist $|\varnothing| = 0$.
- Eine Menge M heißt *n-elementig*, falls $|M| = n$ ($n \geq 0$).
- Allgemein notieren wir Mengen bspw. durch

$$\{21, 35\} = \{x \in \mathbb{N} \mid 5 \leq x \leq 40, 7 \mid x, x \in \{7, 14, 28\}\}.$$

  $\{\ \}$ sind Mengenklammern.

  $\mid$ steht oft für „mit der Eigenschaft“. In unserem Beispiel heißt das „alle $x \in \mathbb{N}$ mit der Eigenschaft, dass $\dots$“

  , steht oft für „und“, eine logische Verknüpfung der Bedingungen bzw. Eigenschaften.

  $\in$ steht für „ist Element von“. Hingegen ist $\notin$ „ist kein Element von“.

  $=$ steht für „gleich“, d. h. links und rechts steht das gleiche und können gegenseitig ausgetauscht werden. Analog ist $\neq$ „ungleich“.

- $\leq, <, \geq, >$ sind „kleiner gleich“, „(echt) kleiner“, „größer gleich“, „(echt) größer“.

Bemerkung 1.4. Die Reihenfolge und Vielfachheit der Elemente in der Aufzählung von Mengen ist egal. Deshalb ist $\{1, 2, 3\} = \{2, 1, 3\} = \{1, 1, 3, 2, 3\}$.

Definition 1.5 (Teilmenge)**.** Seien A und B Mengen. Dann ist

- A eine *Teilmenge* von B, falls $x \in B$ für alle $x \in A$, geschrieben $A \subseteq B$, und
- A eine *echte Teilmenge* von B, falls $A \subseteq B$, aber $A \neq B$, geschrieben $A \subset B$.

Bemerkung 1.6. Für jede Menge M gilt $\varnothing \subseteq M$, aber $\varnothing \in M$ im Allgemeinen nicht.

Weiterhin definieren wir

Definition 1.7 (Mengenoperatoren)**.** Für Mengen A und B seien

- $A \cap B \coloneqq \{x \mid x \in A, x \in B\}$ der *Durchschnitt* von A und B,
- $A \cup B \coloneqq \{x \mid x \in A \text{ oder } x \in B\}$ die *Vereinigung* von A und B,
- $A \setminus B \coloneqq \{x \mid x \in A, x \notin B\}$ die *Mengendifferenz* von A und B,
- $\mathcal{P}(A) \coloneqq \{U \mid U \subseteq A\}$ die *Potenzmenge* von A.

Definition 1.8 (Indexmenge)**.** Sei I eine *Indexmenge*, d. h. für jedes $i \in I$ ist A_i eine Menge. Dann sind

$$\bigcap_{i \in I} A_i \coloneqq \{x \mid x \in A_i \text{ für alle } i \in I\} \qquad \text{und} \qquad \bigcup_{i \in I} A_i \coloneqq \{x \mid \text{es gibt ein } i \in I \text{ mit } x \in A_i\}$$

der *Durchschnitt* bzw. *Vereinigung* der Mengen A_i über die Indexmenge I.

Beispiel 1.9.

- $\mathcal{P}(\{1, 2\}) = \{\varnothing, \{1\}, \{2\}, \{1, 2\}\}$ ist 4-elementig.

- $\{1,2,3\} \cup \{2,3\} = \{1,2,3\}$.
- $\{1,2\} \setminus \{1,3\} = \{2\}$. Die Differenzmenge $A \setminus B$ nimmt B von A weg.
- $\varnothing \cup \{1,2\} = \{1,2\} \neq \{\varnothing, 1, 2\} = \{\varnothing\} \cup \{1,2\}$. Die Vereinigung mit der leeren Menge macht nichts.
- $\{\varnothing, \{1,2,3,4\}\}$ ist 2-elementig, wohingegen $\{\varepsilon, 1, 2, 3, 4\}$ 5-elementig ist.

Definition 1.10 (Paar)**.** Ein *Paar* (oder *2-Tupel*) besteht aus der Angabe eines ersten Elements a und eines zweiten Elements b. Wir schreiben (a, b).

Bemerkung 1.11. Bei Paaren ist (im Gegensatz zu Mengen) die Reihenfolge wichtig. Es gilt $(a, b) = (b, a)$ genau dann, wenn $a = b$: *Achtung*: $(a, a) \neq \{a, a\} = \{a\}$.

Definition 1.12 (KARTESISCHES Produkt, Tupel)**.** Das *KARTESISCHE Produkt* zweier Mengen A und B ist $A \times B \coloneqq \{(a, b) \mid a \in A, b \in B\}$.

Für Mengen $A_1, A_2, \ldots, A_n$ ist das *KARTESISCHE Produkt*

$$A_1 \times \cdots \times A_n \coloneqq \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } 1 \leq i \leq n\},$$

dessen Elemente *n-Tupel* genannt werden.

Sei A eine Menge und $n \geq 1$. Dann ist

$$A^n \coloneqq \underbrace{A \times \cdots \times A}_{n \text{ mal}}$$

das *n-fache KARTESISCHE Produkt* von A.

Bemerkung 1.13. Zwei Tupel sind gleich, wenn sie gleich viele *Einträge* bzw. *Komponenten* haben und wenn an jeder Stelle die Komponenten gleich sind.

Bezeichnung 1.14. Die n-Tupel $(a_1, a_2, \ldots, a_n)$ schreiben wir oft auch senkrecht auf:

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}$$

Beispiel 1.15. Sind A, B und C Mengen, dann sind die Elemente in $A \times B \times C$ 3-Tupel der Form (a, b, c), während die Elemente in $(A \times B) \times C$ 2-Tupel der Form $((a, b), c)$.

1.2 Logik

Definition 1.16 (Implikation, Äquivalenz)**.** Seien A, B und C Aussagen. Dann bedeuten

- $A \implies B$ „A impliziert B“, „aus A folgt B“,
- $A \iff B$ „A genau dann, wenn B“, „A und B sind äquivalent“, d. h. $A \implies B$ und $B \implies A$,
- $\neg A$, „nicht A“.

Zwei Schlussregeln, die wir oft verwenden werden:

Satz 1.17 (Syllogismus, Kontraposition)**.**

- *Aus $A \implies B$ und $B \implies C$ folgt $A \implies C$ (*Syllogismus*).*
- *Es gilt $A \implies B$ genau dann, wenn $\neg B \implies \neg A$ (*Kontraposition*).*

Beispiel 1.18.

$$\underbrace{\text{„Wenn es regnet,}}_{A} \ \underbrace{\text{ist die Straße nass.“}}_{B} \qquad (A \implies B)$$

ist äquivalent zu

$$\underbrace{\text{„Wenn die Straße nicht nass ist,}}_{\neg B} \ \underbrace{\text{dann regnet es nicht.“}}_{\neg A} \qquad (\neg B \implies \neg A)$$

1.2.1 Beweis durch Induktion

Für jedes natürliche $n \geq 1$ sei $A(n)$ eine Aussage. Wenn das Ziel ist, $A(n)$ für alle $n \geq 1$ zu zeigen, dann kann *vollständige Induktion* helfen. Die Beweisstrategie:

- *Induktionsanfang*: Wir zeigen, dass $A(1)$ richtig ist.
- *Induktionsschritt*: Wir nehmen an, dass $A(n)$ richtig ist. Damit beweisen wir, dass auch $A(n+1)$ richtig ist.

Das Beweisprinzip basiert auf dem Dominoeffekt: Mit dem Induktionsanfang ist $A(1)$ wahr. Mit dem Induktionsschritt folgt aus $A(1)$ auch $A(2)$. Wieder mit dem Induktionsschritt folgt aus $A(2)$ auch $A(3)$ usw. Damit haben wir die Aussagen $A(n)$ für alle $n \geq 1$ gezeigt.

Beispiel 1.19.

- Für alle $n \geq 1$ gilt $A(n)\colon \sum_{k=1}^{n}(2k-1) = n^2$.
  - *Induktionsanfang* ($n = 1$): $2 \cdot 1 - 1 = 1^2$ ist wahr und deshalb auch $A(1)$.
  - *Induktionsschritt*: Es gilt

$$\sum_{k=1}^{n+1}(2k-1) = \left(\sum_{k=1}^{n}(2k-1)\right) + (2(n+1)-1) = n^2 + 2n + 1 = (n+1)^2.$$

    Dabei verwendeten wir für die zweite Gleichheit die Induktionsvoraussetzung. Folglich gilt $A(n+1)$.

- Ein falscher Induktionsbeweis: Wir behaupten, dass $A(n)\colon$ (7 teilt 10^n) für alle $n \geq 1$ gilt.
  - *Induktionsschritt*: Angenommen $A(n)$ ist wahr, d. h. es gilt $10^n = 7a$ für ein $a \geq 1$ in $\mathbb{N}$. Dann gilt auch $10^{n+1} = 10 \cdot 10^n = 10 \cdot 7a$. Also gilt $A(n+1)$.
  - *Induktionsanfang*: Aber $A(1)$ ist falsch!

1.2.2 Beweis durch Widerspruch

Das Beweisprinzip ist, das Gegenteil der Behauptung anzunehmen und das auf einen Widerspruch mit der Voraussetzung zu führen. Folglich war die Annahme falsch und die Behauptung richtig.

Beispiel 1.20. *Behauptung*: $\sqrt{2} \notin \mathbb{Q}$.

Beweis: Angenommen $\sqrt{2} \in \mathbb{Q}$, d. h. Es gibt $a, b \in \mathbb{Z}$, $b \geq 1$ mit $\sqrt{2} = a/b$. Wir können annehmen, dass a und b teilerfremd sind (also der Bruch vollständig gekürzt ist).

Quadrieren liefert $2 = a^2/b^2 \iff 2b^2 = a^2$. Damit sind a^2 und a durch 2 teilbar, insbesondere auch a^2 durch $2 \cdot 2 = 4$ teilbar. Somit teilt 4 auch $2b^2$, also sind b^2 und b auch durch 2 teilbar (aufgrund der Eindeutigkeit der Primfaktorzerlegung). Das bedeutet, dass a und b durch 2 teilbar sind, was im Widerpsruch zur Teilerfremdheit steht.

1.2.3 Gleichheit von Mengen

Bemerkung 1.21. Zwei Mengen sind *gleich*, wenn sie dieselben Elemente besitzen.

Seien A und B zwei Mengen. Um zu beweisen, dass $A = B$ ist, muss man zum Einen $A \subseteq B$ und zum Anderen $B \subseteq A$ zeigen. Der Beweis ist im Regelfall also zweiteilig!

1.3 Abbildungen

Die Idee hinter Abbildungen ist es, Mengen in Beziehung zu setzen.[1]

Definition 1.22 (Abbildung)**.** Seien X und Y Mengen. Eine *Abbildung* f von X nach Y ist eine Vorschrift, durch die jedem $x \in X$ genau ein $f(x) \in Y$ zugeordnet wird.[2]

[1] Eigentlich sind es die *Relationen* die das erfüllen, wovon Abbildungen eine spezielle Form sind.

[2] Die Menge X bezeichnen wir als *Definitionsmenge* und Y als *Zielmenge*. Die Elemente aus X heißen *Urbilder* oder *Argumente*, die Elemente aus Y heißen *Zielelemente*. Die tatsächlich angenommen Werte nennen wir *Bilder* oder schlicht *Werte*, und deren Menge auch *Bild* oder *Bildmenge*.

Bemerkung 1.23. Jedes x wird genau einem $f(x)$ zugeordnet. Trotzdem ist es möglich, dass verschiedene x demselben $f(x)$ zugeordnet werden.

Bemerkung 1.24. Zwei Abbildungen sind gleich, wenn sie dieselben Definitions- und Zielmengen haben sowie elementweise bzw. punktweise gleich sind (d. h. deren Vorschrift dasselbe macht).

Bezeichnung 1.25. Wir schreiben $f\colon X \to Y$, $x \mapsto f(x)$. Dabei verwenden wir $\to$ zwischen Mengen und $\mapsto$ zwischen Elementen.

Definition 1.26 (Menge aller Abbildungen)**.** Seien X und Y Mengen. Dann ist $\mathrm{Abb}(X, Y)$ die *Menge aller Abbildungen* von X nach Y.

Beispiel 1.27. Die Abbildung $f\colon \mathbb{Z} \to \mathbb{N}$, $x \mapsto x^2$ bildet jedes $x \in \mathbb{Z}$ auf $x^2 \in \mathbb{N}$ ab.

Definition 1.28 (Identität)**.** Sei X eine Menge. Als *Identität* von X bezeichnen wir die Abbildung $\mathrm{id}_X\colon X \to X$, $x \mapsto x$. Es gilt also $\mathrm{id}_X(x) = x$ für alle $x \in X$.

Definition 1.29 (Komposition von Abbildungen)**.** Seien $f\colon X \to Y$ und $g\colon Y \to Z$ Abbildungen. Dann ist

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

die *Komposition* (*Hintereinanderschaltung*, *Verkettung*) von f und g, gelesen „g verknüpft mit f“, „g komponiert mit f“, „g nach f“ oder „g Kringel f“.

Bezeichnung 1.30. Wir schreiben auch manchmal gf für $g \circ f$.

Es gilt also

$$X \xrightarrow{f} Y \xrightarrow{g} Z, \quad x \mapsto f(x) \mapsto g(f(x)).$$

Definition 1.31 (injektiv, surjektiv, bijektiv)**.** Sei $f\colon X \to Y$ eine Abbildung. Dann ist

- f *text*, falls für alle $x_1, x_2 \in \mathbb{R}$ mit $x_1 \neq x_2$ gilt: $f(x_1) \neq f(x_2)$,
- f *surjektiv*, falls für jedes $y \in Y$ ein $x \in X$ existiert, sodass $f(x) = y$ ist, und
- f *bijektiv*, falls f injektiv und surjektiv ist. Dann nennen wir f eine *Bijektion*.

Definition 1.32 (Umkehrabbildung)**.** Sei $f\colon X \to Y$ eine bijektive Abbildung. Dann ist die *Umkehrabbildung* $f^{-1}\colon Y \to X$ definiert durch $f^{-1}(f(x))\colon x$ für alle $x \in X$ bzw. $f(x) \in Y$.
Es gilt dann $f^{-1} \circ f = \mathrm{id}_X$ und $f \circ f^{-1} = \mathrm{id}_Y$.

Umkehrabbildungen kann es nur für Bijektionen geben. Da auch f^{-1} eine Abbildung sein soll und Abbildungen jedem $y \in Y$ *genau ein* $x \in X$ zuordnet, müssen wir die Injektivität von f voraussetzen. Dann sind nämlich $f^{-1}(f(x_1))$ und $f^{-1}(f(x_2))$ für $x_1, x_2 \in X$ mit $x_1 \neq x_2$ auch unterschiedlich. Da f^{-1} von Y nach X abbilden soll, muss $f^{-1}(y)$ für alle Y definiert werden, weshalb wir die Surjektivität voraussetzen müssen. Dann gibt es für jedes $y \in Y$ ein $x \in X$ mit $y = f(x)$, sodass $f^{-1}(y) = x$ wohldefiniert[3] ist.
Auch die Komposition der Abbildung und dessen Umkehrung ergibt Sinn: $f^{-1} \circ f$ bildet von X nach Y und wieder nach X ab, und $f \circ f^{-1}$ bildet von Y nach X und wieder nach Y ab.

Beispiel 1.33.

1. $f\colon \{1, 2, 3\} \to \{1, 2\}$ mit $1 \mapsto 1$, $2 \mapsto 1$ und $3 \mapsto 2$ ist surjektiv, aber nicht injektiv.
2. $f\colon \{1, 2\} \to \{1, 2, 3\}$ mit $1 \mapsto 3$ und $2 \mapsto 1$ ist injektiv, aber nicht surjektiv.
3. $f\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto x - 41$ ist injektiv und surjektiv, also bijektiv.
4. $f\colon \mathbb{Z} \to \mathbb{Z}$, $x \mapsto 2x$ ist injektiv, aber nicht surjektiv (die ungeraden Zahlen werden nicht getroffen).
5. $f\colon \mathbb{Z} \to \mathbb{Z}$ mit $2n \mapsto n$ und $2n + 1 \mapsto n$ (für $n \in \mathbb{Z}$) ist surjektiv, aber nicht injektiv.
6. Seien X und Y zwei endliche Mengen mit gleich vielen Elementen. Dann ist die Abbildung $f\colon X \to Y$ genau dann injektiv, wenn f surjektiv ist.

[3] Der Begriff *wohldefiniert* meint, dass ein Begriff eindeutig und widerspruchsfrei definiert ist, also weder unmöglich noch mehrdeutig ist.

7. Die Abbildung $f\colon \{\text{Menschen in Bonn}\} \to \mathbb{N}$ definiert durch $x \mapsto \text{Alter}(x)$ ist weder surjektiv (Menschen werden nicht beliebig alt) noch injektiv (zwei Menschen können dasselbe Alter haben).

8. Für ein fixiertes $(a, b, c, d) \in \mathbb{Q}^4$ definieren wir $f\colon \mathbb{Q}^2 \to \mathbb{Q}^2$, $(x, y) \mapsto (ax + by, cx + dy)$. Die Abbildung f ist genau dann bijektiv, wenn $ad - bc \neq 0$ gilt. Außerdem ist f genau dann injektiv, wenn f surjektiv ist. (Der Beweis dafür erfolgt später.)[4]

Ende der Vorlesung 1 am 12. Oktober 2021

Definition 1.34. Seien M und I Mengen. Dann sei

$$M^I \coloneqq \text{Abb}(I, M)$$

die *Menge aller Abbildungen* $I \to M$.

Achtung: Es sind die Abbildungen von I nach M, nicht von M nach I!

Beispiel 1.35. Für $I = \{1, \dots, n\}$ ist die Abbildung $M^I \to M^n$, $f \mapsto (f(1), \dots, f(n))$ bijektiv, wobei M^n bekanntlich das n-fache kartesische Produkt bezeichnet.

Offensichtlich haben alle $f \in M^I$ dieselben Definitions- und Zielmengen. Dann sind zwei Abbildungen genau dann gleich, wenn sie für jedes Argument denselben Wert liefern, d. h. wenn die Tupel ihrer Werte gleich sind. Andersherum definiert jedes Tupel eine Abbildung, denn es gibt alle möglichen Zuordnungen $I \to M$ an.[5]

Achtung: Die hier beschriebene Abbildung bildet *Abbildungen* f auf n-*Tupel derer Werte* ab.

Definition 1.36 (Bild, Urbild einer Menge)**.** Sei $f\colon X \to Y$ eine Abbildung. Und seien $A \subseteq X$ und $B \subseteq Y$ Teilmengen. Wir bezeichnen

$$f(A) \coloneqq \{f(x) \mid x \in A\} \qquad \text{und} \qquad f^{-1}(B) \coloneqq \{x \mid f(x) \in B\}$$

als *Bild* von A unter f bzw. *Urbild* von B unter f. Dahingegen ist $f(X)$ das *Bild* von f. Es gilt stets $f^{-1}(Y) = X$.

Warnung: Die Schreibweise $f^{-1}(B)$ impliziert nicht, dass eine Umkehrabbildung existiert.

Bemerkung 1.37. Wir beachten, dass das nicht jedes $y \in B$ ein Urbild $\in f^{-1}(B)$ haben muss, ähnlich wie eine Abbildung nicht surjektiv sein muss. Genauso kann es mehrere Urbilder $x_1, x_2 \in f^{-1}(B)$ mit $x_1 \neq x_2$ zu einem Bild y mit $f(x_1) = f(x_2) = y$ geben, ähnlich wie eine Abbildung nicht injektiv sein muss.

Definition 1.38 (Graph)**.** Der *Graph* einer Abbildung $f\colon X \to Y$ ist

$$\Gamma(f) \coloneqq \{(x, f(x)) \mid x \in X\} \subseteq X \times Y.$$

Der Graph ist also eine „Zeichnung“ der Funktion, also die Menge aller Punkte der „Ebene“, die zur Funktion „gehören“.

Bemerkung 1.39. Damit können wir den Begriff der Abbildung mengentheoretisch definieren. Seien X und Y Mengen, und sei $\Gamma \subseteq X \times Y$ (eine Relation) eine Menge von Paaren mit den folgenden Eigenschaften:

1. Für jedes $x \in X$ gibt es ein $y \in Y$ mit $(x, y) \in \Gamma$ (jedem Urbild wird ein Bild zugeordnet).

2. Falls $(x, y_1), (x, y_2) \in \Gamma$, so ist $y_1 = y_2$ (das Bild eines Urbilds ist eindeutig).

Damit definieren wir eine *Abbildung* $f_\Gamma\colon X \to Y$ durch $f_\Gamma(x) \coloneqq y$ für jedes $(x, y) \in \Gamma$. Offensichtlich gilt für den Graphen $\Gamma(f_\Gamma) = \Gamma$.

[4] Das ist das Matrix-Vektor-Produkt, wobei a, b, c, d die Einträge einer Matrix $A \in \mathbb{Q}^{2,2}$ ist und x, y die Einträge eines Vektors v. Dann ist A genau dann ein Isomorphismus, wenn A invertierbar ist, also $ad - bc \neq 0$. Genauso ist eine quadratische Matrix genau dann ein Monomorphismus, wenn sie ein Epimorphismus ist.

[5] In fortgeschrittener Sprache: Die Abbildung ist ein *Mengenisomorphismus*, also ein bijektiver Homomorphismus, der die Mengenstruktur (auch wenn sehr banal) erhält.

1.4 Übungsaufgaben

Aufgabe 1.A (B01.A1)**.** Seien X und Y Mengen. Beweisen Sie die Äquivalenz folgender Aussagen:

(i) $X \subseteq Y$,

(ii) $X \cap Y = X$,

(iii) $X \cup Y = Y$,

(iv) $X \setminus Y = \varnothing$.

Lösung. Wegen dem Syllogismus in Satz 1.17 können wir die Äquivalenz mehrerer Aussagen effizient zeigen, indem wir im „Kreis“ schlussfolgern, z. B. (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) $\Longrightarrow$ (i).

Beweis.

1. (i) $\Longrightarrow$ (ii): Wenn jedes $x \in X$ auch in Y liegt, ist die Bedingung $x \in Y$ in der Definition der Schnittmenge $X \cap Y = \{x \in X \mid x \in Y\}$ redundant. Deshalb gilt $X \cap Y = \{x \in X\} = X$.

2. (ii) $\Longrightarrow$ (iii): Nach Voraussetzung müssen wir uns die Vereinigung $(X \cap Y) \cup Y$ anschauen. Da nun nach Definition der Schnittmenge $X \cap Y \subseteq Y$ gilt, erhalten wir $(X \cap Y) \cup Y = Y$.

3. (iii) $\Longrightarrow$ (iv): Nach Voraussetzung können wir uns $X \setminus (X \cup Y)$ anschauen. Gemäß der Definition der Vereinigung gilt stets $X \in X \cup Y$, d. h. in der Mengendifferenz nehmen wir von X mindestens alle Elemente von X weg, also ist $X \setminus (X \cup Y) = \varnothing$.

4. (iv) $\Longrightarrow$ (i): Wenn nach der Differenz $X \setminus Y = \{x \in X \mid x \notin Y\}$ keine Elemente übrig bleiben, so haben alle $x \in X$ die Bedingung $x \notin Y$ nicht erfüllt, d. h. es gilt $x \in Y$ für alle $x \in X$ und damit $X \subseteq Y$. □

Eine alternative, sehr mengentheoretische, aber auch prägnante Lösung ist folgende:

Beweis.

$$
\begin{aligned}
\text{(i)} \Longrightarrow \text{(ii)}\colon \quad & X = X \cap X \subseteq X \cap Y \subseteq X, \\
\text{(ii)} \Longrightarrow \text{(iv)}\colon \quad & \varnothing \subseteq X \setminus Y = (X \cap Y) \setminus Y \subseteq Y \setminus Y = \varnothing, \\
\text{(iv)} \Longrightarrow \text{(iii)}\colon \quad & X \cup Y = \big((X \setminus Y) \cup (X \cap Y)\big) \cup Y = (X \setminus Y) \cup \big((X \cap Y) \cup Y\big) \\
& \qquad = (X \setminus Y) \cup Y = \varnothing \cup Y = Y, \\
\text{(iii)} \Longrightarrow \text{(i)}\colon \quad & X = X \cup \varnothing \subseteq X \cup Y = Y.
\end{aligned}
$$

□

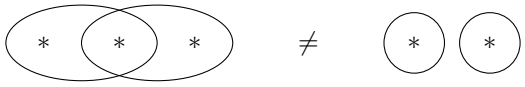
Aufgabe 1.B (B01.A2)**.** Diskutieren Sie den folgenden Induktionsbeweis:

Behauptung: Für jedes $n \geq 1$ gilt: Halten sich n Personen in einem geschlossenen Raum auf, so sind entweder alle geimpft oder alle sind ungeimpft.

Beweis mit Induktion: Der Fall $n = 1$ ist klar. Die Aussage sei nun wahr für n. Sind dann $n + 1$ Personen im Raum, so wähle eine Person aus und schicke sie hinaus. Nach Induktionsannahme haben die verbleibenden Personen denselben Impfstatus. Wir holen die ausgewählte Person wieder herein und senden eine andere Person hinaus. Die im Raum verbliebenen n haben wiederum denselben Impfstatus. Damit hat die zuerst hinaus gesandte Person denselben Impfstatus wie alle anderen im Raum befindlichen Personen. Da dies nach dem ersten Beweisschritt auch für die als zweites hinaus gesandte Person zutrifft, haben alle $n+1$ Personen denselben Impfstatus.

Lösung. Der Induktionsschritt ist eine gute Beweisstrategie, funktioniert aber nur für $n \geq 3$ und versagt bei $n = 2$.

Ein Gegenbeispiel für $n = 2$: Im Raum ist ein Geimpfter und ein Ungeimpfter. Geht eine Person raus, haben die verbleibenden Personen im Raum immer denselben Impfstatus (weil nur eine Person verbleibt). Es fehlen aber Dritte, mit denen wir zu beiden Zeitpunkten den Impfstatus der Personen, die den Raum verlassen, vergleichen können.



Aufgabe 1.C. Zeigen Sie: Für alle $n \geq 1$ gilt

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \tag{1.40}$$

Lösung. Beweis. Wir führen eine vollständige Fallunterscheidung über n durch. Dabei ist $A(n)$ (1.40).

- *Induktionsanfang*: Für $n = 1$ ist $1^2 = \frac{1}{6}(1 \cdot 2 \cdot 3)$ wahr und folglich ist auch $A(1)$ wahr.
- *Induktionsschritt*: Wenn $A(n)$ gilt, gilt auch

$$\begin{aligned}\sum_{k=1}^{n+1} k^2 = (n+1)^2 + \sum_{k=1}^{n} k^2 &\overset{A(n)}{=} (n+1)^2 + \frac{n(n+1)(2n+1)}{6} = \frac{n+1}{6}\big(6(n+1) + n(2n+1)\big) \\ &= \frac{n+1}{6}\big((4n+6) + n(2n+3)\big) = \frac{(n+1)(n+2)(2n+3)}{6},\end{aligned}$$

  also ist auch $A(n+1)$ wahr. □

Alternativ können wir das auch nicht induktiv über Teleskopsummen zeigen.

Beweis. In der Summe heben sich der Minuend k^3 des Index i mit dem Subtrahenden $-(k-1)^3$ des Index $i+1$ auf. Damit gilt

$$\begin{aligned}n^3 = \sum_{k=1}^{n}\big(k^3 - (k-1)^3\big) = 3\sum_{k=1}^{n} k^2 - 3\sum_{k=1}^{n} k + \sum_{k=1}^{n} 1 = 3\sum_{k=1}^{n} k^2 - 3\frac{n(n+1)}{2} + n \\ \iff \sum_{k=1}^{n} k^2 = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6} = \frac{n(n+1)(2n+1)}{6}.\end{aligned}$$

□

2 Körper

Auch *Rechenbereich* genannt. Körper verallgemeinern und abstrahieren die uns gewohnten rationalen oder reellen Zahlen und deren Rechenoperationen. Dennoch sollten wir uns ab sofort von den uns bekannten Beispielen lösen, da die in der (linearen) Algebra betrachteten Objekte sehr abstrakt werden und nicht unbedingt analog zu unserem Vorwissen funktionieren.

2.1 Körperaxiome

Definition 2.1 (Körper)**.** Ein *Körper* ist eine Menge K zusammen mit zwei Abbildungen

$$+\colon K \times K \to K, \quad (a,b) \mapsto a+b \qquad \text{und} \qquad \cdot\colon K \times K \to K, \quad (a,b) \mapsto a \cdot b,$$

Addition bzw. *Multiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $a + (b + c) = (a + b) + c$ für alle $a, b, c \in K$ (*Assoziativität der Addition*);

(A2) $a + b = b + a$ für alle $a, b \in K$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_K \in K$ mit $a + 0 = a$ für alle $a \in K$ (Existenz eines *Nullelements*);

(A4) Zu jedem $a \in K$ gibt es ein $-a \in K$ mit $a + (-a) = 0$ (Existenz eines *additiven Inversen*);

(M1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in K$ (*Assoziativität der Multiplikation*);

(M2) $a \cdot b = b \cdot a$ für alle $a, b \in K$ (*Kommutativität der Multiplikation*);

(M3) Es existiert ein Element $1 = 1_K \in K$ mit $1 \neq 0$ und $1 \cdot a = a$ für alle $a \in K$ (Existenz eines *Einselements*);

(M4) Zu jedem $a \in K$ mit $a \neq 0$ gibt es ein $a^{-1} \in K$ mit $a \cdot a^{-1} = 1$ (Existenz des *multiplikativen Inversen*);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ für alle $a, b, c \in K$ (*Distributivität*).

Oftmals lassen wir den Index K wie in 0_K und 1_K weg, wenn der Kontext klar ist. Manchmal schreiben wir ihn aber hinzu, um zu verdeutlichen, dass sie zum Körper K gehören.

Bemerkung 2.2. Wir setzen $1 \neq 0$ voraus, d. h. ein Körper hat mindestens zwei Elemente.[1]

Bemerkung 2.3. Dabei steht der Ausdruck $a+b$ eigentlich für $+\big((a,b)\big)$ und $a \cdot b$ für $\cdot\big((a,b)\big)$. Streng genommen müssten wir z. B. die Assoziativität der Addition (A1) als

$$a+(b+c)=(a+c)+b \quad \longrightarrow \quad +\Big(\big(a,+\big((b,c)\big)\big)\Big) = +\Big(\big(+\big((a,b)\big),c\big)\Big)$$

und die Kommutativität der Addition (A2) als

$$a+b=b+a \quad \longrightarrow \quad +\big((a,b)\big) = +\big((b,a)\big)$$

schreiben.

Bezeichnung 2.4. Neben diesen Axiomen führen wir noch einige Konventionen ein.

- Um Klammern zu sparen, gilt *Punktrechnung vor Strichrechnung*. Damit können wir z. B. das Distributivgesetz (D) umschreiben als $a \cdot c + b \cdot c$, ohne dass Verwirrung entsteht.
- Wir definieren $a - b \coloneqq a + (-b)$ und $ab \coloneqq a \cdot b$ für $a, b \in K$. Somit können wir Plusklammern und Malpunkte weglassen, wenn der Sinn dabei nicht verfälscht wird (z. B. nicht $1 \cdot 2 \neq 12$).
- Für $a, b \in K$ mit $b \neq 0$ sei
$$\frac{a}{b} \coloneqq a/b \coloneqq a \cdot b^{-1}.$$

Diese Regeln und Schreibweisen sind alles Konventionen und hängen nicht mit der Struktur oder den Eigenschaften eines Körper zusammen. Wir hätten genauso jede andere Konvention einführen können.

Bezeichnung 2.5. Wir definieren kurz $K^\times \coloneqq K \setminus \{0\}$.

Ab sofort meinen wir mit K immer einen Körper mit den Operationen $+$ und $\cdot$, falls nicht anders spezifiziert. Manchmal schreiben wir auch $(K, +, \cdot)$ für einen Körper.

2.2 Beispiele von Körpern

Beispiel 2.6. $\mathbb{Q}$ und $\mathbb{R}$ mit den üblichen Abbildungen $+$ und $\cdot$ sind Körper.

Beispiel 2.7. $\mathbb{Z}$ ist kein Körper, da (nur) (M4) nicht erfüllt wird.

Beispiel 2.8. $\mathbb{C}$, die Menge der komplexen Zahlen mit $+$ und $\cdot$ ist ein Körper.

Beispiel 2.9. Sei $K \coloneqq \{a, b\}$ mit $a \neq b$. Wir definieren die Abbildungen $+\colon K \times K \to K$ und $\cdot\colon K \times K \to K$ durch[2]

$$\begin{aligned} a+a&=a, & a+b&=b, & b+a&=b, & b+b&=a,\\ a\cdot a&=a, & a\cdot b&=a, & b\cdot a&=a, & b\cdot b&=b. \end{aligned}$$

K erfüllt alle Axiome eines Körpers, wobei das Nullelement $0_K = a$ und das Einselement $1_K = b$ ist, also $K = \mathbb{F}_2 \coloneqq \{0, 1\}$. Der Körper ist der kleinstmögliche Körper (jeder Körper muss mindestens 0 und 1 enthalten). Tatsächlich ist der Körper sogar eindeutig, was wir aber nicht beweisen werden.

Beispiel 2.10. Sei $K \coloneqq \mathbb{Q}(\sqrt{2}) \coloneqq \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$.[3] Wir definieren die Abbildungen $+\colon K \times K \to K$ und $\cdot\colon K \times K \to K$ als Einschränkung von $+\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ und $\cdot\colon \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ (d. h. die Abbildungen sind dieselben aus $\mathbb{R}$ bis auf den kleineren Definitionsbereich). Insbesondere heißt das

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) \coloneqq (a + c) + (b + d)\sqrt{2}$$

und

$$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) \coloneqq (ac + 2bd) + (ad + bc)\sqrt{2}.$$

[1] Traditionell wird in der Algebra $1 \neq 0$ definiert. Es gibt aber „esoterische“ Konzepte eines einelementigen Körpers $\mathbb{F}_1$, d. h. $1 = 0$, was aber einige Körpereigenschaften verliert.

[2] Die Abbildungen ähneln der Addition und Multiplikation modulo 2.

[3] Das ist eine sog. Körperadjunktion bzw. Körpererweiterung

Die meisten Körperaxiome sind offensichtlich erfüllt. Für (M4) stellt sich jedoch die Frage, ob $(a+b\sqrt{2})^{-1} \in K$ für alle $a + b\sqrt{2} \neq 0$ existiert. *Antwort*: Ja, denn

$$(a + b\sqrt{2})-1 \coloneqq \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

mit

$$\frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{1}{a + b\sqrt{2}}.$$

Beachte: Die Brüche sind definiert, weil $(a/b)^2 \neq 2 \iff a^2 - 2b^2 \neq 0$ wegen $\sqrt{2} \notin \mathbb{Q}$.

2.3 Rechenregeln in Körpern

Lemma 2.11 (Linksdistributivität)**.** *Es gilt $a(b + c) = ac + ac$ für alle $a, b, c \in K$.*

Beweis. Es gilt $a(b + c) \overset{(M2)}{=} (b + c)a \overset{(D)}{=} ba + ca \overset{(M2)}{=} ab + ac.$ □

Lemma 2.12 (Eindeutigkeit der Null)**.** *Es gibt nur ein Nullelement in einem Körper.*

Beweis. Seien $0'$ und $0''$ Nullelemente im Körper K. Dann gilt $0'' \overset{(A3)}{=} 0'' + 0' \overset{(A2)}{=} 0' + 0'' \overset{(A3)}{=} 0'$. Dabei haben wir für die erste Gleichheit die Eigenschaft $0' = 0_K$ und für die letzte Gleichheit $0'' = 0_K$ ausgenutzt. □

Lemma 2.13. *Für alle $a \in K$ gilt $0a = 0$.*

Beweis. Sei $a \in K$. Dann gelten

$$0a \overset{(A3)}{=} (0 + 0)a \overset{(D)}{=} 0a + 0a, \tag{2.14}$$

$$0 \overset{(A4)}{=} 0a + (-(0a)) \overset{(2.14)}{=} (0a + 0a) + (-(0a)) \overset{(A1)}{=} 0a + (0a + (-(0a))) \overset{(A4)}{=} 0a + 0 \overset{(A3)}{=} 0a.$$ □

In den Übungsaufgaben werden wir noch eine Vielzahl weiterer Regeln beweisen.

2.4 Charakteristik eines Körpers

Bezeichnung 2.15. Sei K ein Körper. Für $a \in K$ und $0 \neq m \in \mathbb{N}$ definieren wir

$$m \cdot a \coloneqq \underbrace{a + a + \cdots + a}_{m \text{ mal}}.$$

Definition 2.16 (Charakteristik)**.** Wir definieren $\operatorname{char}(K)$ als die *Charakteristik* von K als

$$\operatorname{char}(K) \coloneqq \begin{cases} 0 & \text{falls } m \cdot 1_K \neq 0_K \text{ für alle } m \in \mathbb{N} \setminus \{0\}, \\ \min\{m \in \mathbb{N} \setminus \{0\} \mid m \cdot 1_K = 0_K\} & \text{sonst.} \end{cases}$$

Lemma 2.17. *Sei K ein Körper mit $\operatorname{char}(K) = p > 0$. Dann ist p eine Primzahl.*

Beweis. Angenommen p wäre keine Primzahl, sodass es $p_1, p_2 \in \mathbb{N}$ mit $p_1, p_2 \geq 2$ und $p = p_1 p_2$ gibt. Aus der Minimalität der Charakteristik folgt $p_1 \cdot 1_K \neq 0$ und $p_2 \cdot 1_K \neq 0$. Damit gilt

$$(p_1 \cdot 1_K)(p_2 \cdot 1_K) = (p_1 p_2) \cdot 1_K = p \cdot 1_K = 0_K.$$

Aufgrund der Nullteilerfreiheit in einem Körper (s. Übungsaufgabe) gilt $p_1 \cdot 1_K = 0_K$ oder $p_2 \cdot 1_K = 0_K$, ein Widerspruch.[4] □

Ende der Vorlesung 2 am 15. Oktober 2021

[4] Die Charakteristik hat einige interessante Eigenschaften:
Aus einer positiven Charakteristik folgt sofort $a + a + \ldots a = 0$. Sie hilft und zu bestimmen, wann ein Ausdruck Null wird, was wichtig für das Rechnen im Körper ist (wir denken an $a + 0 = 0$, $0a = 0$ und, dass 0^{-1} nicht existiert). In diesem Kontext ist $\operatorname{char}(K) = 2$ besonders wichtig, denn in dem Fall ist $a + a = 0$ für alle $a \in K$, d. h. jedes Element ist sein eigenes additives Inverse. $\operatorname{char}(K) \neq 2$ garantiert uns die Existenz der $2 \coloneqq 1 + 1$.
Jeder Teilkörper eines Körpers hat dieselbe Charakteristik wie der Körper, z. B. $\operatorname{char}(\mathbb{F}_2) = \operatorname{char}(\mathbb{F}_4) = 2$. Damit haben Körper mit gleicher Charakteristik auch eine ähnliche Struktur.
Die Charakteristik ist eigentlich für Ringe (die später folgen) definiert. All diese Eigenschaften gelten auch für Ringe.

2.5 Die Ringe $\mathbb{Z}_m$

Definition 2.18 (Ring)**.** Ein *Ring* ist eine Menge R zusammen mit zwei Abbildungen

$$+\colon R \times R \to R, \quad (a,b) \mapsto a+b \qquad \text{und} \qquad \cdot\colon R \times R \to R, \quad (a,b) \mapsto a \cdot b$$

Addition bzw. *Multiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $a + (b + c) = (a + b) + c$ für alle $a, b, c \in R$ (*Assoziativität der Addition*);

(A2) $a + b = b + a$ für alle $a, b \in R$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_R \in R$ mit $a + 0 = a$ für alle $a \in R$ (Existenz eines *Nullelements*);

(A4) Zu jedem $a \in R$ gibt es ein $-a \in R$ mit $a + (-a) = 0$ (Existenz eines *additiven Inversen*);

(R1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ für alle $a, b, c \in R$ (*Assoziativität der Multiplikation*);

(R2) Es existiert ein Element $1 = 1_R \in R$ mit $1 \neq 0$ und $1 \cdot a = a$ für alle $a \in R$ (Existenz eines *Einselements*);

(D) $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$ und $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ für alle $a, b, c \in K$ (*Distributivität*).

Definition 2.19 (kommutativer Ring)**.** Ein Ring R heißt *kommutativ*, falls zusätzlich $a \cdot b = b \cdot a$ für alle $a, b \in \mathbb{R}$ gilt.

Bemerkung 2.20.

1. Im Vergleich zu einem Körper sind die Axiome der Addition identisch. Bei der Multiplikation fehlt lediglich die Kommutativität (M2) und die Existenz des Inversen (M4). Aufgrund der fehlenden Kommutativität werden in der Distributivität beide Multiplikationsreihenfolgen angeben, die wir auch beide nachweisen müssen.

2. In einem Ring wird nicht verlangt, dass $1_R \neq 0_R$. Ist aber $1_R = 0_R$, so folgt daraus $a = 1_R a = 0_R a = 0_R$ für alle $a \in R$, also $R = \{0_R\}$.

Bezeichnung 2.21 (Nullring)**.** Wir nennen $R = \{0_R\}$ den trivialen[5] *Nullring*.

Wir übernehmen für Ringe alle Schreibkonventionen in bezeichnung 2.4, die wir für Körper festlegten (bis auf Brüche).

Lemma 2.22. *Seien $a, m \in \mathbb{N}$ mit $m \geq 1$. Dann existieren eindeutig bestimmte Elemente $r, q \in \mathbb{N}$ mit $0 \leq r < m$, sodass $a = qm + r$ gilt. Setze $r_m(a) \coloneqq r$.*

Beweis. Zu jedem $a \in \mathbb{N}$ gibt es ein eindeutig bestimmtes $q \in \mathbb{N}$ mit $qm \leq a < (q+1)m$. Mit $r \coloneqq a - qm$ folgt die Behauptung. □

Definition 2.23 ($\mathbb{Z}$ modulo m)**.** Sei $m \in \mathbb{N}$ mit $m \geq 2$. Dann sei $\mathbb{Z}_m \coloneqq \{0, 1, \ldots, m-1\}$. Für $a, b \in \mathbb{Z}_m$ definieren wir noch Abbildungen $+$ und $\cdot$ durch $a + b \coloneqq r_m(a +_{\mathbb{Z}} b)$ und $a \cdot b \coloneqq r_m(a \cdot_{\mathbb{Z}} b)$. (Die Operationen in den $r_m(\ldots)$ kommen aus $\mathbb{Z}$.)

Manchmal ist es hilfreich, auch die Operatoren aus verschiedenen Mengen durch Subskripte zu unterscheiden, also $+_K$, $\cdot_R$, etc.

Lemma 2.24. *$(\mathbb{Z}_m, +, \cdot)$ ist ein kommutativer Ring.*[6]

Beweis. Übungsaufgabe. □

Lemma 2.25. *$(\mathbb{Z}_m, +, \cdot)$ ist genau dann ein Körper, wenn m eine Primzahl ist.*

[5] Als *triviale* Objekte werden oft offensichtliche oder sehr einfache Objekte sowie uninteressante Randfälle bezeichnet.
[6] Ein sog. *Restklassenring modulo m*.

Beweis. Angenommen $\mathbb{Z}_m$ ist ein Körper. Dann folgt $\operatorname{char}(\mathbb{Z}_m) = m$ aus der Definition der Addition über die Addition in $\mathbb{Z}$ (in $\mathbb{Z}$ ist $m1 = 1 + 1 + \cdots + 1 = m$). Nach Lemma 2.17 ist m eine Primzahl.

Für die Umkehrung sei nun m eine Primzahl. Zuerst zeigen wir, dass $\mathbb{Z}_m$ nullteilerfrei ist. Seien $a, b \in \mathbb{Z}_m$ mit $a \cdot b = 0 = r_m(a + b)$. Folglich wird ab von m geteilt (Rest 0). Da m eine Primzahl ist, folgt (aus dem *Lemma von* EUKLID): m teilt a oder m teilt b. Weil nun $0 \leq a, b < m$ ist, muss $a = 0$ oder $b = 0$ sein. Folglich haben wir gezeigt, dass $\mathbb{Z}_m$ nullteilerfrei ist.

Nun zeigen wir, dass jedes $a \in \mathbb{Z}_m$ mit $a \neq 0$ ein multiplikatives Inverses besitzt. Für solche a definieren wir die Abbildung $\rho_a \colon \mathbb{Z}_m \to \mathbb{Z}_m$, $x \mapsto xa$. Dann ρ_a ist injektiv: Aus $xa = \rho_a(x) = \rho_a(y) = ya \iff (x - y)a = 0$ folgt aufgrund Nullteilerfreiheit $x - y = 0 \iff x = y$. Da $\mathbb{Z}_m$ endlich ist, ist ρ_a auch surjektiv.

Aus der Bijektion folgt, dass $0a, 1a, \ldots, (m-1)a$ paarweise verschieden sind (injektiv), und diese Elemente auch jedes Element aus $\mathbb{Z}_m$ repräsentiert (surjektiv), insbesondere die 1. Es gibt also ein $x \in \mathbb{Z}_m$ mit $xa = 1$. Zu jedem $a \in \mathbb{Z}_m \setminus 0$ gibt es also ein multiplikatives Inverses $x \in \mathbb{Z}_m$, sprich a ist invertierbar, was Axiom (M4) erfüllt. Die restlichen Körperaxiome folgen aus dem kommutativen Ring. □

Vom kommutativen Ring zum Körper fehlt nur noch die Existenz des multiplikativen Inversen. Hierfür haben wir alle möglichen Kandidaten für das Inverse betrachtet, also $0a, 1a, \ldots, (m-1)a$. Wir beobachten, dass diese Menge genau $\mathbb{Z}_m$ entspricht, es also eine einfache Bijektion ρ_a geben muss, die wir auch beweisen haben. Der Trick hier war zu zeigen, dass $\mathbb{Z}_m$ nullteilerfrei ist (ein gutes Zeichen, da Nullteilerfreiheit eine Körpereigenschaft ist).

Bezeichnung 2.26 (endlicher Körper)**.** Für Primzahlen p schreiben wir auch $\mathbb{F}_p \coloneqq \mathbb{Z}_p$.

3 Vektorräume

Definition 3.1 (Vektorraum)**.** Sei K ein Körper. Ein *Vektorraum über K* oder *K-Vektorraum* ist eine Menge V zusammen mit zwei Abbildungen

$$+ \colon V \times V \to V, \quad (v_1, v_2) \mapsto v_1 + v_2 \qquad \text{und} \qquad \cdot \colon K \times V \to V, \quad (a, v) \mapsto a \cdot v,$$

Addition bzw. *Skalarmultiplikation* genannt, sodass folgende Regeln (Axiome) gelten:

(A1) $v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$ für alle $v_1, v_2, v_3 \in V$ (*Assoziativität der Addition*);

(A2) $v_1 + v_2 = v_2 + v_1$ für alle $v_1, v_2 \in V$ (*Kommutativität der Addition*);

(A3) Es existiert ein Element $0 = 0_V \in V$ mit $v + 0_V = v$ für alle $v \in V$ (Existenz eines *Nullelements*);

(A4) Zu jedem $v \in V$ gibt es ein $-v \in V$ mit $v + (-v) = 0$ (Existenz eines *additiven Inversen*);

(SM1) $(ab) \cdot v = a \cdot (b \cdot v)$ für alle $a, b \in K$ und $v \in V$;

(SM2) $1_K \cdot v = v$ für alle $v \in V$;

(SM3) $a \cdot (v_1 + v_2) = a \cdot v_1 + a \cdot v_2$ für alle $a \in K$ und $v_1, v_2 \in V$;

(SM4) $(a + b) \cdot v = (a \cdot v) + (b \cdot v)$ für alle $a, b \in K$ und $v \in V$.

Wir schreiben oft auch einfach V für den K-Vektorraum $(V, +, \cdot)$.

Bezeichnung 3.2. Um die Notation zu vereinfachen, legen wir $v_1 - v_2 \coloneqq v_1 + (-v_2)$, $av \coloneqq a \cdot v$ für alle $v_1, v_2, v \in V$ und $a \in K$ sowie *Punkt- vor Strichrechnung* fest.

Bezeichnung 3.3 (Vektor, Skalar, Nullvektor)**.** Die Elemente von V nennen wir *Vektoren*, die Elemente von K nennen wir *Skalare*. Das Nullelement 0_V heißt *Nullvektor* oder auch *die Null von V*.

Bemerkung 3.4.

1. Es ist sehr wichtig, zu wissen, welchen Grundkörper K der Vektorraum hat. Dieselbe Menge V, aber über zwei verschiedene Körper K_1 und K_2, sind zwei verschiedene Vektorräume, nämlich ein K_1- und ein K_2-Vektorraum. Im Allgemeinen ist ein Vektorraum über einen anderen Körper kein Vektorraum mehr, da er z. B. nicht mehr abgeschlossen ist.
2. Die Skalarmultiplikation multipliziert ein Skalar mit einem Vektor (wie der Name schon sagt, also kein Skalarprodukt). Wir beachten auch die Reihenfolge der Skalarmultiplikation, d. h. Skalare werden von *links* multipliziert.

Wie bei Körpern gibt es eine Vielzahl an Rechenregeln für Vektorräume, die wir in den Übungen beweisen.

3.1 Beispiele von Vektorräumen

Bezeichnung 3.5 (Nullvektorraum)**.** Sei $V \coloneqq \{0\}$ über K der (triviale) *Nullvektorraum* (oft auch einfach nur $V = 0$). Addition und Skalarmultiplikation können nur auf genau eine Weise definiert werden:

$$+\colon V \times V \to V, \qquad 0 + 0 \mapsto 0$$
$$\cdot\colon V \times V \to V, \qquad 0 \cdot 0 \mapsto 0$$

Beispiel 3.6. Sei K ein Körper. Dann ist K ein K-Vektorraum mit Addition und Skalarmultiplikation definiert als Addition und Multiplikation von K.

Definition 3.7 (Standardvektorraum)**.** Sei K ein Körper. Für $n \geq 1$ sei $V \coloneqq K^n$ das n-fache kartesische Produkt von K. Die Elemente aus K^n schreiben wir oft als Spalten

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$$

mit $a_1, \ldots, a_n \in K$. Wir definieren komponentenweise

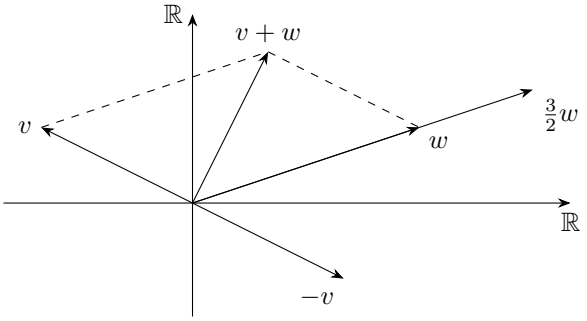
$$+\colon V \times V \to V \quad \text{durch} \quad \left(\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \right) \mapsto \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

und

$$\cdot\colon K \times V \to V \quad \text{durch} \quad \left(a, \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \right) \mapsto \begin{pmatrix} ab_1 \\ \vdots \\ ab_n \end{pmatrix}.$$

Dann ist $(V, +, \cdot)$ ein K-Vektorraum, der sog. *Standardvektorraum*. Wir legen $K^0 \coloneqq 0$ aus K fest.
Dabei stammt die komponentenweise Addition und Multiplikation aus K.

In $V = \mathbb{R}^2$ mit $K = \mathbb{R}$ können wir Addition und Skalarmultiplikation visualisieren, indem wir Vektoren als Pfeile darstellen. Addition heißt dann Aneinanderreihen von Pfeilen; Skalarmultiplikation heißt dann Strecken/Stauchen oder Änderung der Richtung von Pfeilen. Das sollte aus der Schule bekannt sein.



Ein sehr wichtiges Beispiel von Vektorräumen:

Definition 3.8 (Funktionenraum)**.** Sei K ein Körper und sei $I \neq \varnothing$ eine Menge. Wir setzen $V \coloneqq K^I \coloneqq \mathrm{Abb}(I, K)$ und definieren

$$+\colon V \times V \to V, \quad (f, g) \mapsto f + g \qquad \text{und} \qquad \cdot\colon K \times V \to V, \quad (a, f) \mapsto af,$$

punktweise durch

$$(f + g)(x) \coloneqq f(x) + g(x) \qquad \text{und} \qquad (af)(x) \coloneqq a(f(x))$$

für alle $f, g \in V$, $a \in K$, und $x \in I$.

Dann ist $(V, +, \cdot)$ ein K-Vektorraum, der sog. *(lineare) Funktionenraum*. Wir definieren $K^{\varnothing} = 0$ als Nullabbildung.

Dabei ist in den Definitionsgleichungen auf der linken Seite Addition und Skalarmultiplikation in V, sowie auf der rechten Seite Addition und Multiplikation in K.[1,2]

Ein noch wichtigeres Beispiel ist

Definition 3.9 (Menge aller Abbildungen)**.** Sei K ein Körper und sei $I \neq \varnothing$ eine Menge. Dann ist

$$K^{(I)} \coloneqq \{f \in K^I \mid f(x) \neq 0 \text{ für nur endlich viele } x \in I\}$$

ein K-Vektorraum, wobei wir Addition und Skalarmultiplikation von K^I benutzen. Wir definieren $K^{(\varnothing)} = 0$ als Nullabbildung.

Jede Abbildung $f \in K^{(I)}$ bildet also fast alle $x \in I$ (bis auf endlich viele) auf 0 ab.

Definition 3.10 (Teilkörper)**.** Sei $(L, +, \cdot)$ ein Körper und sei K eine Teilmenge von L, sodass die Eigenschaften

1. $0, 1 \in K$ (neutrale Elemente);
2. $a + b \in K$ für alle $a, b \in K$ (Abgeschlossenheit unter Addition);
3. $a \cdot b \in K$ für alle $a, b \in K$ (Abgeschlossenheit unter Multiplikation);
4. $-a \in K$ für alle $a \in K$ (additive Inverse) und
5. $a^{-1} \in K$ für alle $a \in K^\times$ (multiplikative Inverse)

erfüllt sind. Durch Einschränkung erhalten wir die Abbildungen

$$+\colon K \times K \to K \qquad \text{und} \qquad \cdot\colon K \times K \to K.$$

(Das ist aufgrund der Abgeschlossenheit von $+$ und $\cdot$ garantiert, s. Punkte 2 und 3.) Wir können leicht überprüfen, dass K einen Körper bildet, und nennen K einen *Teilkörper* von L.

Beispiel 3.11. Ist K ein Teilkörper von L, so ist L ein K-Vektorraum, wobei die Skalarmultiplikation $\cdot\colon K \times L \to L$ durch Einschränkung der Multiplikation $\vdots\ L \times L \to L$ definiert ist.

Bspw. ist der Körper $\mathbb{Q}(\sqrt{2})$ ein $\mathbb{Q}$-Vektorraum, der Körper $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum und $\mathbb{R}$ auch ein $\mathbb{Q}(\sqrt{2})$-Vektorraum.

Definition 3.12 (externe direkte Summe)**.** Seien V und W zwei K-Vektorräume. Dann ist die $V \times W$ wieder ein K-Vektorraum, wobei Addition und Skalarmultiplikation komponentenweise definiert sind durch

$$(v_1, w_1) + (v_2, w_2) \coloneqq (v_1 + v_2, w_1 + w_2) \qquad \text{und} \qquad a(v, w) \coloneqq (av, aw)$$

für alle $v, v_1, v_2 \in V$, $w, w_1, w_2 \in W$ und $a \in K$. Der K-Vektorraum $V \times W$ nennen wir die *(externe) direkte Summe* von V und W und schreiben $V \oplus W$.

Noch ein Beispiel aus der Analysis.

Beispiel 3.13. Sei $I = [a, b]$ ein abgeschlossenes Intervall in $\mathbb{R}$ und sei

$$C^0(I) \coloneqq \{\text{stetige Funktionen } I \to \mathbb{R}\}$$

eine Teilmenge von $\mathbb{R}^I$. Dann ist $C^0(I)$ ein $\mathbb{R}$-Vektorraum mit der Einschränkung von $+\colon \mathbb{R}^I \times \mathbb{R}^I \to \mathbb{R}^I$ und $\cdot\colon \mathbb{R} \times \mathbb{R}^I \to \mathbb{R}^I$ auf die neue Definitionsmenge $I \subset \mathbb{R}$.

Ende der Vorlesung 3 am 19. Oktober 2021

[1] An dieser Stelle fragt man sich vielleicht, warum der Standardvektorraum K^n und der Funktionenraum K^I identisch notiert werden. Das liegt daran, dass sie tatsächlich „identisch“ (d. h. *isomorph*) sind, weil es eine Bijektion wie in Beispiel 1.35 gibt.

[2] Für $I = \mathbb{N}$ lässt sich auch der „unendlichdimensionale“ *Folgenraum*

$$K^{\mathbb{N}} \coloneqq \{(a_1, a_2, a_3, \dots) \mid a_i \in K \text{ für alle } i \in \mathbb{N}\}$$

(wie in der Analysis) definieren.

3.2 Unterräume

Definition 3.14. Sei V ein K-Vektorraum. Eine Teilmenge U von V heißt *Unterraum* von V, falls gilt:

1. $U \neq \varnothing$;
2. $u_1 + u_2 \in U$ für alle $u_1, u_2 \in U$ und
3. $au \in U$ für alle $a \in K$ und $u \in U$.

Lemma 3.15. *Sei U ein Unterraum von V. Durch Einschränkung der Addition und Skalarmultiplikation von V erhalten wir Abbildungen $+\colon U \times U \to U$ und $\cdot\colon K \times U \to U$ (was aufgrund Punkte 2 und 3 möglich ist). Dann ist U zusammen mit beiden Einschränkungen ein K-Vektorraum.*

Beweis. Sei $u \in U$. Aus Punkt 3 folgen $0u = 0 \in U$ und $(-1)u = -u \in U$. Deshalb gelten die Vektorraumaxiome (A3) und (A4). Alle anderen Axiome folgen aus V. □

Beispiel 3.16.

1. Die Teilmengen V und $\{0\}$ (statt $\{0\}$ schreiben wir oft nur 0) sind Unterräume von V, die sog. *trivialen Unterräume*.
2. Sei $v \in V$. Dann ist
$$U_v \coloneqq Kv \coloneqq \{av \mid a \in K\}$$
der kleinste Unterraum von V, welcher v enthält.

Bezeichnung 3.17 (Gerade)**.** Ist $v \neq 0$, so nennen wir U_v die durch v verlaufende *Gerade*.

Beispiel 3.18.

1. Für jede Menge I ist $K^{(I)}$ ein Unterraum von K^I, denn nach Addition und Skalarmultiplikation hat jede Abbildung immer noch nur endlich viele Stellen ungleich 0.
2. Sei $I = [a, b]$ ein Intervall in $\mathbb{R}$. Dann ist $C^0(I)$ ein Unterraum von $\mathbb{R}^I$, weil sich die Stetigkeit unter Addition und Skalarmultiplikation nicht ändert.
3. Die Elemente des $\mathbb{R}$-Vektorraums $\mathbb{R}^{\mathbb{N}}$ sind die in der Analysis behandelten reellen Folgen. Die Teilmenge der konvergenten reellen Folgen ist ein Unterraum von $\mathbb{R}^{\mathbb{N}}$, da aufgrund der Grenzwertsätze die Folgen nach Addition und Skalarmultiplikation immer noch konvergieren.

Definition 3.19 (Durchschnitt, Summe)**.** Seien U_1 und U_2 Unterräume von V. Dann ist $U_1 \cap U_2$ der *Durchschnitt* von U_1 und U_2 sowie
$$U_1 + U_2 \coloneqq \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\}$$
ist die *Summe* von U_1 und U_2. $U_1 \cap U_2$ und $U_1 + U_2$ sind Unterräume von V.

Definition 3.20 (interne direkte Summe)**.** Seien U_1 und U_2 Unterräume von V. Ist $U_1 \cap U_2 = 0$, so nennen wir $U_1 \oplus U_2 \coloneqq U_1 + U_2$ die *(interne) direkte Summe* von U_1 und U_2.

Ende der Vorlesung 4 am 22. Oktober 2021

A Trickkiste