Mathematik für Wirtschaftsinformatik Vorlesungsnotizen

Matthias Keller

Inhaltsverzeichnis

Vorbemerkung

Vorwissen

Die natürlichen Zahlen hat der liebe Gott gemacht,
alles andere ist Menschenwerk. Leopold Kronecker.

Für diese Vorlesung werden wir die Kenntnis der natürlichen Zahlen einschließlich der damit verbundenen Ordnung, Addition und Multiplikation voraussetzen. Wir bezeichnen die Menge der natürlichen Zahlen $1, 2, 3, \ldots$ mit $\mathbb{N}$.

Eine Rechnung

Der Kurs wird mit 6 Leistungspunkten (LP) gewertet. Jeder Leistungspunkt entspricht 30h Arbeit. Damit geht es um

$$180 \text{ h Arbeit}$$

Davon gehen ab:

$$\begin{aligned} -60h &\quad (4 \text{ h Vorlesung und Übung in 15 Wochen}) \\ -40h &\quad (1 \text{ Woche Prüfungsvorbereitung}). \end{aligned}$$

Damit verbleiben noch

$$80\text{h Arbeit.}$$

Auf 15 Wochen verteilt bedeutet dies ca.

$$5 \text{ h und } 20 \text{ min Arbeit/ Woche}$$

also

$$1 \text{ h Arbeit / Wochentag.}$$

Folgerung

Es muss gearbeitet werden!

KAPITEL 1

Grundlagen: Logik und Mengenlehre

1. Vorrede

Es gibt einen Unterschied zwischen "gesundem Menschenverstand" und "logischem Denken".

"Gesunder Menschenverstand":

- Baut auf meinen Erfahrungen auf:

  > *"Der gesunde Menschenverstand ist die Summe aller Vorurteile, die sich bis zum 18. Lebensjahr im Bewusstsein festgesetzt haben."* Albert Einstein

- Effektiv, schnell aber manchmal falsch ("Bauchgefühl")
- Super um vor einem Mammut wegzulaufen

"Logisches Denken":

- Baut auf meinen abstrakten Überlegungen auf:

  > *"Durch bloßes logisches Denken vermögen wir keinerlei Wissen über die Erfahrungswelt zu erlangen; alles Wissen über die Wirklichkeit geht von der Erfahrung aus und mündet in ihr."* Albert Einstein

- Immer richtig aber manchmal langsam und manchmal irrelevant ("Kopf")
- Super um etwas auf den Mond zu schießen

Mathematik ist "logisches Denken"; für ihre Interpretation braucht man "gesunden Menschenverstand".

> *"Man sollte alles so einfach wie möglich sehen - aber auch nicht einfacher."* Albert Einstein

2. Aussagenlogik

Definition (Aussage; Aristoteles 384-322 v. Chr.). Eine *Aussage* ist ein sprachliches Gebilde, von dem es sinnvoll ist zu sagen, ob es wahr sei oder falsch.

Bemerkung. Ein wichtiges Kriterium, ob es sich bei einem Satz um eine Aussage handelt oder nicht, ist ob er *objektiv* verständlich ist.

Bemerkung. Es ist nicht erforderlich zu wissen, ob das Gebilde wahr oder falsch ist.

Beispiel. Interessantes:

- In Berlin gibt es mehr Dönerläden als in Istanbul. (Aussage – wahr)
- Der Mietspiegel in Berlin ist im Schnitt niedriger als in Potsdam. (Aussage – falsch)
- Potsdam ist klein. Berlin ist groß. (keine Aussagen)

Lebensnahes:

- Mathematik ist großartig. (keine Aussage)
- Sie werden die Prüfung nur bestehen, wenn Sie mir während Vorlesung konzentriert zu hören. (Aussage)

Philosophisches:

- Es gibt keine absolute Wahrheit. (Aussage - falsch)

Mathematisches:

- 1+1 (keine Aussage)
- 1+1=3 (Aussage – falsch)

Aus zwei gegebenen Aussagen kann man ganz viele weitere Aussagen konstruieren.

DEFINITION. Seien A und B Aussagen.

- $A \wedge B$ (sprich "A und B") ist die Aussage, die genau dann wahr ist, wenn beide Aussagen wahr sind. ("Konjunktion")
- $A \vee B$ (sprich "A oder B") ist die Aussage, die genau dann falsch ist, wenn beide Aussagen falsch sind. ("Disjunktion")
- $A \Longrightarrow B$ (sprich "Aus A folgt B" oder "Wenn A dann B") ist die Aussage, die genau dann falsch ist, wenn A wahr und B falsch ist. ("Implikation")
- $A \Longleftrightarrow B$ (sprich "A genau dann wenn B") ist die Aussage, die genau dann wahr ist, wenn A und B entweder beide wahr oder beide falsch sind. ("Äquivalenz")
- $\neg A$ (sprich "nicht A) ist die Aussage, die genau dann wahr ist, wenn A falsch ist. ("Negation")

Die obigen Aussagen heißen *Aussageverbindungen.*

BEISPIEL. Sei

- A: In Berlin gibt es mehr Schwaben als Berliner in Schwaben.
- B: Der Mietspiegeln in Berlin ist im Schnitt niedriger als in Potsdam.

Dann gilt

- A wahr
- B falsch
- $A \wedge B$ ist falsch
- $A \vee B$ ist wahr
- $A \Longrightarrow B$ ist falsch
- $B \Longrightarrow A$ ist wahr
- $A \Longleftrightarrow B$ ist falsch

- $\neg A$ ist falsch
- $\neg B$ ist wahr

Eine nützliche Methode zur Bestimmung vom Wahrheitswert einer Aussage sind *Wahrheitswerttafeln*:
Seien A und B Aussagen.

A	B	$A \wedge B$	$A \vee B$	$A \Longrightarrow B$	$A \Longleftrightarrow B$	$\neg A$
w	w	w	w	w	w	f
w	f	f	w	f	f	f
f	w	f	w	w	f	w
f	f	f	f	w	w	w

Beispiel (Modus ponuns). Seien A und B Aussagen. Betrachte die Aussage

$$(A \wedge (A \Longrightarrow B)) \Longrightarrow B$$

Diese Schlussregel wird auch *modus ponens* genannt. In Worten: Wenn A wahr ist und B aus A folgt, so ist B wahr. Mittels einer Wahrheitswerttabelle lässt sich zeigen, dass sie unabhängig von den Wahrheitswerten von A und B wahr ist.

A	B	$A \Longrightarrow B$	$A \wedge (A \Longrightarrow B)$	$(A \wedge (A \Longrightarrow B)) \Longrightarrow B$
w	w	w	w	w
w	f	f	f	w
f	w	w	f	w
f	f	w	f	w

Beispiel. Seien

A : Es regnet.
B : Die Straße ist nass.

D.h. es regnet und wann immer es regnet ist auch die Straße nass, also ist die Straße nass.

Ein weiteres Beispiel für modus ponens.

Beispiel. Seien

A : $2 < 3$.
B : $4 < 9$.

A ist wahr, $A \Longrightarrow B$ ist wahr (quadrieren).

Definition (Tautologie). Eine Aussageverbindung die unabhängig von den Wahrheitswerten ihrer Bestandteile wahr ist, heißt *Tautologie*.

Beispiel.
- Modus ponens ist eine Tautologie.
- *Indirekter Schluss*: $(A \wedge (\neg B \Longrightarrow \neg A)) \Longrightarrow B$.
  Wenn A wahr ist und $\neg A$ aus $\neg B$ folgt, so ist B wahr. (Übung)
  Ein Beispiel
  A : $23 < 25$; $\neg A$: $23 \geq 25$

$B : \sqrt{23} < 5$; $\neg B$: $\sqrt{23} \geq 5$
A ist wahr, $(\neg B \Longrightarrow \neg A)$ ist wahr (quadrieren). D.h. B ist wahr.

- *Kontraposition*: $(A \Longrightarrow B) \Longleftrightarrow (\neg B \Longrightarrow \neg A)$
  Wenn B aus A folgt, so folgt $\neg A$ aus $\neg B$.

Definition (Variable). Ein sprachliches Zeichen, für das beliebige Ausdrücke einer bestimmten Art eingesetzt werden können, heißt *Variable*. Die Menge der Ausdrücke die für eine Variable eingesetzt werden können heißt ihr *Grundbereich*.

Bemerkung. Variablen habe keine selbständige Bedeutung und sind bedeutungsleere Zeichen, die nur dazu dienen, die Stellen anzuzeigen, an denen die bedeutungsvollen Konstanten einzusetzen sind.

Bemerkung. Beachte, dass Variablen nicht nur für Zahlenwerte stehen können, sondern für alles mögliche wie Mengen, Funktionen und Obstsorten.

Man kann Variablen feste Werte zuweisen. Sei x_0 ein Element aus einem Grundbereich. Soll die Variable x den festen Wert x_0 annehmen so schreiben wir

$$x := x_0.$$

Die Variable x trägt ab jetzt bis auf Widerruf den Wert 42. "Bis auf Widerruf" heißt i.d.R. bis zum Ende der Umgebung in der sie auftritt (wie etwa des Beispieles, des Beweises, des Abschnitts oder der Vorlesung) oder bis sie neu definiert wird.

Beispiel. Sei n eine Variable über $\mathbb{N}$. Schreiben wir $n := 42$, so hat n innerhalb dieses Beispiels den festen Wert 42.

3. Mengen

Emmy Noether berichtete zu den Anfängen der Entwickling der Mengenlehre folgende Anekdote:

> *"Dedekind äußerte sich, hinsichtlich des Begriffs der Menger: er stelle sich eine Menge vor wie einen geschlossenen Sack, der ganz bestimmte Dinge enthalte, die man aber nicht sehe, und von denen man nichts wisse, außer dass sie vorhanden und bestimmt seien. Einige Zeit später gab Cantor seine Vorstellung einer Menge zu erkennen: Er richtete seine kolossale Figur auf, beschrieb mit erhobenem Arm eine großartige Geste und sagte mit einem unbestimmten Blick: 'Eine Menge stelle ich mir vor wie einen Abgrund'."*

Wir gehen hier von einem naiven Mengenbegriff aus.

Definition (Menge, Georg Cantor, 1895). Unter einer *Menge* verstehen wir jede Zusammenfassung von bestimmten wohl unterscheidbaren Objekten unserer Anschauung oder unseres Denkens zu einem Ganzen.

Bemerkung. Wir werden später kurz diskutieren, inwiefern diese Definition in sich widersprüchliche Objekte zulässt. Das auf Zermelo-Fraenkel zurückgehende Axiomensystem der Mengenlehre schließt solche Widersprüche aus. In dieser Vorlesung werden wir jedoch nicht im Detail darauf eingehen.

Bemerkung. Um sprachlichen Verwirrungen vorzubeugen, beachte, dass eine *Menge* und die *Anzahl* der in ihr enthaltenen Elemente, NICHT das gleiche sind.

Definition (Leere Menge). Wir nennen die Menge, die kein Element enthält, die *leere Menge* und bezeichnen sie mit $\emptyset$.

Notation (Element und Teilmenge). Ist X eine Menge so schreiben wir $x \in X$ (lies: x *Element* von X) falls x zu X gehört. Gehört x nicht zu X, so schreibt man $x \notin X$.
Seien X und Y Mengen. Dann bedeutet $Y \subseteq X$ (lies: Y *Teilmenge* von X), dass jedes Element von Y auch zu X gehört. Falls $Y \subseteq X$ und $X \subseteq Y$ gilt, so schreiben wir $X = Y$ und sagen die Mengen sind gleich. Falls $Y \subseteq X$ aber $Y \neq X$, so heißt Y eine *echte Teilmenge* von X und wir schreiben $Y \subsetneq X$ oder $Y \subset X$.

Definition. Sei E eine Eigenschaft. Wir bezeichnen mit

$$\{x \mid x \text{ hat die Eigenschaft } E\}$$

die Menge der Elemente die die Eigenschaft E haben.

Bemerkung. In der obigen Definition ist x eine Variable. Das Zeichen x kann beliebig ausgetauscht werden.

$$\begin{aligned}\{x \mid x \text{ hat } E\} &= \{y \mid y \text{ hat } E\}\\ &= \{N \mid N \text{ hat } E\}\\ &= \{\Omega \mid \Omega \text{ hat } E\}\end{aligned}$$

Bemerkung. Mengen mit endlichen vielen Elementen werden meist durch Aufzählungen innerhalb der Mengenklammern notiert. So ist die Menge der Zahlen 1, 2 und 3 etwa gegeben durch

$$\{1, 2, 3\}.$$

Die definierende Eigenschaft E ist hier gerade eine der Zahlen 1, 2 oder 3 zu sein.

Beispiel.

- $\mathbb{N} = \{n \mid n \in \mathbb{N}\} = \{n \mid n \text{ ist natürliche Zahl}\}$
- $2\mathbb{N} := \{n \in \mathbb{N} \mid \text{ es existiert } k \in \mathbb{N} \text{ mit } n = 2k\} = \{n \in \mathbb{N} \mid n \text{ ist gerade Zahl}\}$

- $2\mathbb{N}+1 := \{n \in \mathbb{N} \mid n = 1$ oder es existiert $k \in \mathbb{N}$ mit $n = 2k+1\} = \{n \in \mathbb{N} \mid n$ ist ungerade Zahl$\}$
- $P = \{p \in \mathbb{N} \mid p \geq 2$und p ist nur durch 1 und sich selbst teilbar$\}$ Primzahlen
- $\{1, \ldots, 42\} = \{n \in \mathbb{N} \mid n \leq 42\}$.

Es gilt $2\mathbb{N}, 2\mathbb{N}+1, P \subsetneq \mathbb{N}$.

Bemerkung. Man kann auch Mengen von Mengen definieren. Sei z.B. X eine Menge so bezeichnet $\{X\}$ die Menge, die nur die Menge X enthält. Beachte $\mathbb{N} \neq \{\mathbb{N}\}$, denn $\mathbb{N}$ enthält unendlich viele natürliche Zahlen während $\{\mathbb{N}\}$ nur ein Element enthält nämlich $\mathbb{N}$.
Hier ist allerdings Vorsicht geboten. Ein Axiom der Mengenlehre besagt, dass eine Menge sich nicht selbst enthalten darf. Das führt sonst auf Widersprüche.
Z.B. ist die Menge der Mengen, die sich nicht selbst enthalten ein in sich widersprüchliches Objekt: Sei X diese Menge. Es stellt sich nun die Frage, X sich selbst enthält. Falls X selbst in X enthalten wäre, denn dann enthält X mit X eine Menge die sich selbst enthält. Widerspruch. Falls X nicht in X enthalten ist, dann müsste X ein Element von X sein, da sie eine Menge ist die sich nicht selbst enthält. Widerspruch. Diese Paradoxie geht auf Bertrand Russell zurück.
Eine Umformulierung der Russellschen Paradoxie lautet wie folgt: "Der Barbier ist der Mann im Dorf der alle die Männer rasiert, die sich nicht selbst rasieren".

Beispiel. Sei A die Menge der Äpfel, B die Menge der Birnen, C die Menge der Clementinen, ... Dann ist die Menge $\mathcal{F}$ der Fruchtsorten gerade

$$\mathcal{F} = \{A, B, C, \ldots\}$$

Beachte ein einzelner Apfel ist keine Fruchtsorte: Sei a ein Apfel, dann gilt $a \in A$ aber $a \notin \mathcal{F}$.

Definition (Potenzmenge). Die *Potenzmenge* $\mathcal{P}(X)$ einer Menge X ist die Menge aller Teilmengen von X, d.h. $\mathcal{P}(X) = \{A \mid A \subseteq X\}$.

Beispiel.
- $\mathcal{P}(\emptyset) = \{\emptyset\}$.
- Sei $X = \{x\}$. Dann ist $\mathcal{P}(X) = \{\emptyset, \{x\}\}$.
- Sei $X = \{x, y\}$. Dann ist $\mathcal{P}(X) = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$.

Durch folgende Operationen lassen sich aus gegebenen Mengen weitere Mengen konstruieren.

Definition. Es bezeichnet $X \setminus Y$ (lies: X ohne Y) die Menge der Elemente von X, die nicht zu Y gehören, d.h.

$$X \setminus Y := \{z \mid z \in X \text{ und } z \notin Y\}.$$

Der *Durchschnitt* $X \cap Y$ der Mengen X und Y ist gegeben durch

$$X \cap Y := \{z \mid z \in X \text{ und } z \in Y\}.$$

Die *Vereinigung* der Mengen X und Y ist gegeben durch

$$X \cup Y := \{z \mid z \in X \text{ oder } z \in Y\}.$$

Beispiel.

$$\begin{aligned} \mathbb{N} \setminus (2\mathbb{N}) &= 2\mathbb{N} + 1, \\ \mathbb{N} \setminus (2\mathbb{N} + 1) &= 2\mathbb{N}, \\ (2\mathbb{N}) \cup (2\mathbb{N} + 1) &= \mathbb{N}, \\ (2\mathbb{N}) \cap (2\mathbb{N} + 1) &= \emptyset. \end{aligned}$$

Notation. $\mathbb{N}_0 := \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\}$.

Diese Operationen $\setminus$, $\cap$ und $\cup$ können durch sogenannte Venn-Diagramme dargestellt werden.
Bilder

Bemerkung. Eine alternative Darstellung sind sogenannte Euler-Diagramme. Bei diesen werden nur die tatsächlichen Überschneidungen zwischen den Mengen dargestellt. Im Gegensatz dazu werden in Venn-Diagrammen alle möglichen Überlappungen der Flächen dargestellt (auch wenn diese leer sind). Als Beispiel betrachte man die drei Mengen $A = \{1, 2\}$, $B = \{2, 3\}$ und $C = \{4\}$. S.h. http://blog.stevemould.com/venn-vs-euler-diagrams/.

Definition. Ist A eine nicht leere Menge und zu jedem $\alpha \in A$ eine Menge X_α gegeben, so nennt man X_α, $\alpha \in A$, eine *Familie von Mengen*. Für eine Familie X_α, $\alpha \in A$, von Mengen definiert man

$$\bigcup_{\alpha \in A} X_\alpha := \{z \mid z \text{ gehört zu (mindestens) einer der Mengen } X_\alpha\}$$

sowie

$$\bigcap_{\alpha \in A} X_\alpha := \{z \mid z \text{ gehört zu allen Mengen } X_\alpha\}.$$

Beispiel. Sei $A = \mathbb{N}$ und $X_n = \{1, \ldots, n\}$ für $n \in \mathbb{N}$. Dann gilt

$$\bigcup_{n \in \mathbb{N}} X_n = \mathbb{N}, \quad \bigcap_{n \in \mathbb{N}} X_n = \{1\}.$$

Beispiel. Sei A das deutsche Alphabet. Sei

$$X_\alpha = \{\text{Tiere die mit dem Buchstaben } \alpha \text{ beginnen}\}$$

für $\alpha \in A$. Dann gilt

$$\bigcup_{\alpha \in A} X_\alpha = \{\text{Tiere}\}, \quad \bigcap_{\alpha \in A} X_\alpha = \emptyset.$$

Lemma (DeMorgansche Gesetze). *Ist X_α, $\alpha \in A$, eine Familie von Mengen und X eine Menge, so gilt*

(a) $X \setminus \bigcup_{\alpha \in A} X_\alpha = \bigcap_{\alpha \in A} X \setminus X_\alpha$.

(b) $X \setminus \bigcap\limits_{\alpha \in A} X_\alpha = \bigcup\limits_{\alpha \in A} X \setminus X_\alpha$.

Beweis. (a) "$\subseteq$": Sei $x \in X \setminus \bigcup_{\alpha \in A} X_\alpha$. Wäre $x \in X_\alpha$ für ein $\alpha \in A$, dann $x \in \bigcup_{\alpha \in A} X_\alpha$. Widerspruch. Also $x \in X \setminus X_\alpha$ für alle $\alpha \in A$ und somit $x \in \bigcap_{\alpha \in A} X \setminus X_\alpha$.
"$\supseteq$": Sei $x \in \bigcap_{\alpha \in A} X \setminus X_\alpha$. Wäre $x \in \bigcup_{\alpha \in A} X_\alpha$, dann gäbe es $\alpha \in A$ mit $x \in X_\alpha$. Widerspruch. Also $x \in X \setminus \bigcup_{\alpha \in A} X_\alpha$.
(b) Übung. □

Definition (Kartesisches Produkt). Aus zwei Objekten a, b bilden wir das *geordnete Paar* (a, b). Damit können wir aus zwei Mengen X, Y das *kartesische Produkt*

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

bilden.

Bemerkung. Beachte $(1, 42) \neq (42, 1)$, aber $\{1, 42\} = \{42, 1\}$.

4. Relationen

Definition. Eine *Relation auf* einer Menge X ist eine Teilmenge R von $X \times X$.

Notation. Statt $(x, y) \in R$ schreibt man oft auch $x \overset{R}{\sim} y$ oder $x \sim y$.

Definition (Äquivalenzrelation). Eine Relation auf X heißt

- *reflexiv*, wenn gilt: $x \sim x$ für alle $x \in X$,
- *symmetrisch*, wenn gilt $x \sim y \Longrightarrow y \sim x$,
- *transitiv*, wenn gilt: $x \sim y$ und $y \sim z \Longrightarrow x \sim z$.

Eine *Äquivalenzrelation* ist eine reflexive, symmetrische, transitive Relation.

Beispiel. Sei X die Menge derStudierenden in Potsdam und

$$R_1 = \{(x, y) \mid x \text{ und } y \text{ haben am selben Tag Geburtstag}\}$$
$$R_2 = \{(x, y) \mid x \text{ und } y \text{ kennen sich}\}$$
$$R_3 = \{(x, y) \mid x \text{ kennt } y\ \}$$

Dann ist R_1 eine Äquivalenzrelation. R_2 ist reflexiv und symmetrisch aber nicht transitiv. Die Relation R_3 is reflexiv aber nicht symmetrisch und transitiv.

Definition (Äquivalenzklassen). Sei X eine Menge mit einer Äquivalenzrelation $\sim$ gegeben. Für jedes x definieren wir die Menge

$$[x] := \{y \in X \mid x \sim y\}$$

welche die *Äquivalenzklasse* von x genannt wird. Ein Element von $[x]$ wird Repräsentant genannt.

BEISPIEL. Sei $k \in \mathbb{N}$. Definiere auf $\mathbb{N}$ die Relation

$$n \sim m \quad :\Longleftrightarrow n \text{ und } m \text{ haben bei Division durch } k \text{ den gleichen Rest.}$$

Dann ist $\sim$ eine Äquivalenzrelation, denn es ist offensichtlich reflexiv, symmetrisch und transitiv. Für Äquivalenzklasse $[n]$ schreiben wir auch

$$n \bmod k := [n]$$

und wir bezeichnen die Menge der Äquivalenzklassen mit

$$\mathbb{Z}_k := \{[n] \mid n \in \mathbb{N}\} = \{n \bmod k \mid n \in \mathbb{N}\}.$$

Es gibt genau k Äquivalenzklassen, denn bei Division durch k kann der Rest nur eine von den Zahlen $0, 1, \ldots, k-1$ sein. Weiterhin ist der Rest innerhalb einer Äquivalenzklasse gerade ihr kleinster Repräsentant. Weiterhin lässt sich auf $\mathbb{Z}_k$ eine Addition und eine Multiplikation definieren via

$$\begin{aligned}(n \bmod k) + (m \bmod k) &:= (n+m) \bmod k\\ (n \bmod k) \cdot (n \bmod k) &:= (n \cdot m) \bmod k.\end{aligned}$$

Diese Operationen sind *wohl definiert*, dass heißt sie hängen nicht von der Wahl der Repräsentanten ab:
Beweis. Seien $n, m \in \mathbb{N}$. Dann gibt es natürliche Zahlen $0 \leq r_n, r_m < k$ und $N, M \in \mathbb{N}_0$ mit

$$n = N \cdot k + r_n \quad m = M \cdot k + r_m.$$

Seien $x, x' \in [n]$ und $y, y' \in [m]$. Dann existieren natürliche Zahlen $X, X', Y, Y' \in \mathbb{N}$ mit

$$\begin{aligned} x &= X \cdot k + r_n & y &= Y \cdot k + r_m\\ x' &= X' \cdot k + r_n & y' &= Y' \cdot k + r_m \end{aligned}$$

Somit gilt

$$\begin{aligned} x + y &= X \cdot k + r_n + Y \cdot k + r_m = (X+Y) \cdot k + (r_n + r_m)\\ x' + y' &= X' \cdot k + r_n + Y' \cdot k + r_m = (X'+Y') \cdot k + (r_n + r_m). \end{aligned}$$

Somit haben $x+y$ und $x'+y'$ bei Division durch k den gleichen Rest, nämlich $(r_n + r_m)$ falls $r_n + r_m < k$ und $(r_n + r_m - k)$ falls $r_n + r_m \geq k$. Analog gilt

$$\begin{aligned} x \cdot y &= (X \cdot k + r_n) \cdot (Y \cdot k + r_m)\\ &= X \cdot Y \cdot k^2 + (X \cdot r_m + Y \cdot r_n) \cdot k + r_n \cdot m\\ &= (X+Y) \cdot k + (r_n + r_m)\\ x' \cdot y' &= (X' \cdot k + r_n) \cdot (Y' \cdot k + r_m)\\ &= X' \cdot Y' \cdot k^2 + (X \cdot r_m + Y \cdot r_n) \cdot k + r_n \cdot r_m \end{aligned}$$

Da die ersten beiden Terme auf der rechten Seite durch k teilbar sind bleibt nur noch jeweils $r_n \cdot r_m$ übrig. $\square$

Für $k = 2$ gilt z.B.

$$\begin{aligned}
[0] + [0] &= (1 + 0) \bmod 2 = 0 \bmod 2 = [0] \\
[1] + [0] &= (1 + 0) \bmod 2 = 1 \bmod 2 = [1] \\
[1] + [1] &= (1 + 1) \bmod 2 = 2 \bmod 2 = 0 \bmod 2 = [0]
\end{aligned}$$

Definition (Ordnungsrelation). Eine *Ordnungsrelation* oder *Ordnung* auf einer Menge X ist eine Relation R, die reflexiv, transitiv und antisymmetrisch ist. Dabei heißt *antisymmetrisch*, dass

$$x \sim_R y \text{ und } y \sim_R x \Longrightarrow x = y.$$

Ist R eine Ordnungsrelation auf X, so heißt das Paar (X, R) eine *geordnete Menge*. Eine geordnete Menge heißt *total geordnet*, wenn für alle $x, y \in X$ immer $x \sim_R y$ oder $y \sim_R x$ gilt.

Notation. Für eine Ordnungsrelation R schreibt man oft das Symbol $\leq$, d.h. falls $x \sim_R y$ so schreibt man $x \leq y$.

Beispiel.
- $(\mathbb{N}, \leq)$ ist eine total geordnete Menge.
- Sei X eine Menge, dann ist $(\mathcal{P}(X), \subseteq)$ eine geordnete aber nicht total geordnete Menge.

5. Funktionen

Eine *Relation zwischen* zwei Mengen X und Y ist eine Teilmenge R von $X \times Y$.
Eine wichtige Klasse von Relationen zwischen zwei Mengen sind Funktionen.

Definition (Funktion). Eine *Abbildung* oder *Funktion* von einer Menge X in die Menge Y ist eine Relation f zwischen X und Y (d.h. $f \subseteq X \times Y$), so dass für alle $x \in X$ existiert genau ein $y \in Y$ mit $(x, y) \in f$. D.h. f ordnet jedem Element von X genau ein Element von Y zu.
Wir schreiben

$$f : X \longrightarrow Y \quad \text{oder} \quad X \longrightarrow Y, x \mapsto f(x).$$

Es heißt dann X der *Definitionsbereich* von f, sowie Y der *Wertebereich* von f und $\mathrm{Bild}(f) := \{f(x) \mid x \in X\} \subseteq Y$ das *Bild* von f. Ist $f : X \longrightarrow Y$ eine Funktion und $A \subseteq Y$, so heißt

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

das *Urbild* von A unter f.

Bemerkung. Wir unterscheiden zwischen einer Funktion f und ihren Werten $f(x)$. Insbesondere ist eine Funktion $f : X \to Y$ ein Element von $X \times Y$ und $f(x)$ ein Element von Y.

BEISPIEL (Identität). Sei X eine beliebige Menge. Dann ist $\mathrm{id}_X : X \longrightarrow X$ die Abbildung, die $x \in X$ auf x abbildet. Dann ist X der Definitions- und Wertebereich, sowie

$$\mathrm{Bild}(\mathrm{id}_X) = X \quad \mathrm{id}_X^{-1}(A) = A, \quad A \subseteq X.$$

Etwa: $X = \{1,2,3\} \longrightarrow \{1,2,3\}, 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 3$.

BEISPIEL (Konstante Funktion). Seien X, Y beliebige Mengen und $c \in Y$. Dann wird die Abbildung $f : X \longrightarrow Y, x \mapsto c$, die jedes $x \in X$ auf c abbildet, die *konstante Funktion* mit Wert c genannt und wir schreiben $g \equiv c$. Dann ist X der Definitionsbereich, Y der Wertebereich, sowie

$$\begin{aligned} \mathrm{Bild}(f) &= \{c\} \\ f^{-1}(A) &= \begin{cases} X & : c \in A \\ \emptyset & : c \notin A \end{cases}, \quad A \subseteq X. \end{aligned}$$

Etwa: $f : \mathbb{N} \longrightarrow \mathbb{N}, n \mapsto 1$, dann ist $f(n) = 1$ für alle $n \in \mathbb{N}$.

BEISPIEL. Sei $k \in \mathbb{N}$ und

$$f : \mathbb{N} \to \mathbb{Z}_k,\ n \mapsto n \bmod k$$

Dann ist

$$\mathrm{Bild}(f) = \mathbb{Z}_k.$$

Sei r_n der Rest von allen $x \in n \bmod k$ bei Division durch k. Dann ist

$$f^{-1}(\{n \bmod k\}) = \{k \cdot m + r_n \mid m \in \mathbb{N}_0\}$$

LEMMA. *Seien X und Y Mengen und $f : X \to Y$ eine Abbildung. Für die Urbilder der Mengen $A, B \subseteq Y$ gilt*

$$\begin{aligned} f^{-1}(A \cup B) &= f^{-1}(A) \cup f^{-1}(B) \\ f^{-1}(A \cap B) &= f^{-1}(A) \cap f^{-1}(B) \\ f^{-1}(A \setminus B) &= f^{-1}(A) \setminus f^{-1}(B) \end{aligned}$$

Beweis. Übung. □

DEFINITION (Komposition). Seien X, Y, Z Mengen. Die *Komposition* $g \circ f$ der Abbildungen $f : X \longrightarrow Y$, $g : Y \longrightarrow Z$ ist gegeben durch

$$g \circ f : X \longrightarrow Z, x \mapsto g(f(x)).$$

Komposition ist assoziativ, d.h. es gilt

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

(Denn $(g \circ (f \circ h))(x) = g((f \circ h)(x)) = g(f(h(x))) = (g \circ f)(h(x)) = ((g \circ f) \circ h)(x)$.) Damit können wir also die Klammern weglassen.

BEISPIEL. Für jede Abbildung $g : X \to Y$ gilt

$$g \circ \mathrm{id}_X = g = \mathrm{id}_Y \circ g.$$

Beispiel. Für $k \in \mathbb{N}$ seien die Vielfachen von k gerade gegeben durch

$$k\mathbb{N} := \{kn \mid n \in \mathbb{N}\}$$

Sei

$$f : \mathbb{N} \longrightarrow 10\mathbb{N}, \quad n \mapsto 10n$$
$$g : 10\mathbb{N} \longrightarrow \mathbb{N}, m \mapsto m/2.$$

Dann ist die Komposition $g \circ f$ gerade Multiplikation mit 5.

Beispiel. Sei $k \in \mathbb{N}$ und für $n \in \mathbb{N}$ sei r_n der Rest von allen x in $n \bmod k$ bei Division durch k, d.h. für alle $x \in n \bmod k$ gilt $x = X \cdot k + r_n$ für ein gewisses X. Seien

$$f : \mathbb{N} \longrightarrow \mathbb{Z}_k, \quad n \mapsto n \bmod k$$
$$g : \mathbb{Z}_k \longrightarrow \{0, \dots, k-1\}, n \bmod k \mapsto r_n.$$

Dann gibt die Komposition $g \circ f$ gerade den Rest der Division durch k an.

Definition (Injektiv, surjektiv und bijektiv). Eine Abbildung $f : X \longrightarrow Y$ heißt *surjektiv*, wenn zu jedem $y \in Y$ ein $x \in X$ existiert mit $y = f(x)$ (d.h. $Bild(f) = Y$).
Eine Abbildung $f : X \longrightarrow Y$ heißt *injektiv*, wenn aus $x \neq z$ folgt $f(x) \neq f(z)$.
Ist $f : X \longrightarrow Y$ injektiv und surjektiv, so heißt es *bijektiv*.

Bemerkung. Bijektivität ist eine strukturelle Art fest zu stellen, ob zwei endliche Mengen die gleiche Anzahl von Elementen haben. Seien z.B. P die Menge Personen in einer Vorlesung und S die vorhandenen Sitzplätze. Wenn man zu faul zum zählen ist und feststellen möchte ob es gleich viel Personen wie Sitzplätze gibt, kann man die Personen bitten Platz zu nehmen. Dies wird dann durch eine Abbildung

$$f : P \longrightarrow S$$

gegeben wobei $f(p)$ der Sitzplatz ist, auf dem sich die Person p niederlässt. Nun gilt

- Die Abbildung f ist surjektiv, falls alle Sitzplätze besetzt sind. (In diesem Fall ist die Anzahl der Sitzplätze auf jeden Fall kleiner gleich als die Anzahl der Personen.)
- Die Abbildung f ist injektiv, falls auf jedem Sitzplatz höchstens eine Person sitzt. (In diesem Fall ist die Anzahl der Sitzplätze auf jeden Fall größer gleich als die Anzahl der Personen.)
- Falls auf jedem Platz genau eine Person sitzt, ist die Abbildung bijektiv. (In diesem Fall ist die Anzahl der Sitzplätze gleich der Anzahl der Person.)

Beispiel. Sei X eine Menge. Die Identität $\mathrm{id}_X : X \to X, x \mapsto x$ ist injektiv und surjektiv und somit bijektiv.

BEISPIEL. Seien X, Y Mengen und $c \in Y$. Die konstante Funktion $X \to Y, x \mapsto c$ ist genau dann injektiv und surjektiv (und somit bijektiv) wenn Y nur aus dem Element c besteht.

BEISPIEL. Die Abbildung

$$\mathbb{N} \to \mathbb{N}, n \mapsto 2n$$

ist injektiv aber nicht surjektiv. Hingegen ist die Abbildung

$$\mathbb{N} \to 2\mathbb{N}, n \mapsto 2n$$

injektiv und surjektiv und somit bijektiv.

BEISPIEL. Sei $k \in \mathbb{N}$. Die Abbildung

$$\mathbb{N} \mapsto \mathbb{Z}_k,\ n \mapsto n \bmod k$$

ist surjektiv aber nicht injektiv. Hingegen ist die Abbildung

$$\{1, \ldots, k\} \to \mathbb{Z}_k, n \mapsto n \bmod k$$

surjektiv und injektiv und somit bijektiv.

PROPOSITION. *Sei $f : X \longrightarrow Y$ gegeben. Dann sind äquivalent:*

(i) *f bijektiv.*
(ii) *Es gibt ein $g : Y \longrightarrow X$ mit $f \circ g = id_Y$ und $g \circ f = id_X$.*

In diesem Fall, ist die Funktion g aus (ii) *eindeutig bestimmt.*

Beweis. (i) $\Longrightarrow$ (ii): Sei f bijektiv. Da f bijektiv ist existiert für jedes y genau ein $x_y \in X$ mit $f(x_y) = y$. Definiere

$$g : Y \to X,\ y \mapsto x_y.$$

Damit gilt für alle $y \in X$

$$(f \circ g)(y) = f(g(y)) = f(x_y) = y$$

und alle $x \in X$

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

(ii) $\Longrightarrow$ (i): Sei g eine Funktion wie angenommen und angenommen f ist nicht bijektiv, d.h. entweder ist f nicht injektiv oder nicht surjektiv. Ist f nicht injektiv, so gibt es $y \in Y$ und $x \neq x'$ in X mit $y = f(x) = f(x')$. Dann ist $x \neq g(y)$ oder $x' \neq g(y)$. O.E. $x \neq g(y)$. Dann gilt

$$(g \circ f)(x) = g(f(x)) = g(y) \neq x$$

Also $g \circ f \neq \mathrm{id}_X$. Widerspruch.
Ist f nicht surjektiv, dann gibt es ein $y \in Y$ so dass $f(x) \neq y$ für alle $x \in X$. Also insbesondere gilt für $x_y = g(y)$, dass $f(x_y) \neq y$ und somit

$$f \circ g(y) = f(g(y)) = f(x_y) \neq y.$$

Also $f \circ g \neq \mathrm{id}_Y$. Widerspruch.

Nun noch zur Eindeutigkeit. Seien g und g' zwei Abbildungen wie in (ii). Dann gilt mit $\mathrm{id}_Y = f \circ g'$ und $\mathrm{id}_X = g \circ f$

$$g = g \circ \mathrm{id}_Y = g \circ (f \circ g') = (g \circ f) \circ g' = \mathrm{id}_X \circ g' = g'.$$

□

Die Funktion g wird *Umkehrfunktion* von f genannt und (oft) mit f^{-1} bezeichnet. (Nicht zu verwechseln mit dem Urbild!)
Mit dem Begriff der Bijektion können wir nun "Unendlichkeit" definieren.

Definition. Eine Menge X heißt *unendlich* wenn es eine bijektive Abbildung $f : X \to Y$ auf eine echte Teilmenge Y von X gibt.

Schließlich brauchen wir manchmal noch Einschränkungen von Funktionen: Sei $f : X \longrightarrow Y$ gegeben und A eine Teilmenge von X. Dann bezeichnen wir mit f_A oder $f|_A$ die *Einschränkung* von f auf A gegeben durch

$$f|_A : A \longrightarrow Y, x \mapsto f(x).$$

6. Verknüpfungen

Eine Abbildung $* : X \times X \longrightarrow X$ heißt *Verknüpfung* auf X. Man schreibt oft $x * y$ statt $*(x, y)$. Die Verknüpfung $* : X \times X \longrightarrow X$ heißt

- *kommutativ*, wenn gilt $x * y = y * x$ für alle $x, y \in X$
- *assoziativ*, wenn gilt $x * (x * z) = (x * y) * z$ für alle $x, y, z \in X$.

Ist die Verknüpfung assoziativ, so kann man die Klammern auch weglassen.

Beispiel.
- Die Addition und Multiplikation auf $\mathbb{N}$ ist eine assoziative Verknüpfung.
- Die Addition und Multiplikation auf $\mathbb{Z}_k$ ist eine assoziative Verknüpfung.
- Sei X eine Menge und $F(X)$ die Menge der Funktionen $X \to X$. Dann ist die Komposition $\circ$ eine assoziative Verknüpfung.

KAPITEL 2

Arithmetik: Gruppen, Körper und Zahlen

In diesem Kapitel lernen wir die Strukturen kennen, die den Grundrechenarten zugrunde liegen.

1. Gruppen

Definition (Monoid, (Halb-)Gruppe). Eine *Halbgruppe* ist eine Menge G mit einer Verknüpfung $*$ für die gilt:

(G1) $*$ ist assoziativ.

Eine *Monoid* ist eine Halbgruppe für die zusätzlich gilt:

(G2) Es existiert $e \in G$ so dass $e * g = g * e = g$, für alle $g \in G$ welches das *neutrale Element* genannt wird.

Weiterhin ist G eine *Gruppe* falls zusätzlich gilt

(G3) Für alle $g \in G$ existiert $h \in G$, so dass $g*h = h*g = e$, welches das *inverse Element* zu g genannt und oft mit g^{-1} bezeichnet wird.

Definition. Ein Monoid bzw. eine (Halb-)Gruppe heißt *abelsch* falls die Verknüpfung kommutativ ist.

Beispiel.
- $\mathbb{N}$ ist eine abelsche Halbgruppe bzgl. der Addition und ein abelscher Monoid bzgl. der Multiplikation. Dabei ist das neutrale Element gerade 1.
- $\mathbb{N}_0$ ist eine abelscher Monoid bzgl. der Addition und Multiplikation. Dabei ist das neutrale Element gerade 0 bzw. 1.
- $\mathbb{Z}_k$ ist eine abelsche Gruppe bezüglich der Addition. Das neutrale Element bzgl. Addition ist $0 \bmod k$. Das *inverse Element* der Addition zu $n \bmod k$ ist gerade $(n \bmod k)^{-1} = (k-n) \bmod k$ denn

$$n \bmod k + (k-n) \bmod k = k \bmod k = 0 \bmod k.$$

  $(\mathbb{Z}_k, +)$ wird auch zyklische Gruppe genannt.
- Sei X eine Menge. Dann ist die Menge $F(X)$ der Funktionen $X \to X$ ein Monoid bzgl. der Komposition. Das neutrale Element ist id_X. Die Gruppe $(F(X), \circ)$ ist im Allgemeinen nicht abelsch: Sei $c \in X$, sei f eine Funktion mit $f(c) \neq c$ und sei

$g \equiv c$ die konstante Funktion mit Wert c. Dann gilt

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

Lemma. *Sei $(G, *)$ eine Gruppe. Dann ist das neutrale und inverse Element eindeutig bestimmt.*

Beweis. Angenommen e und e' sind neutrale Elemente. Dann gilt

$$e = e * e' = e'.$$

Sei $g \in G$ und $h, h' \in G$ inverse Elemente zu g. Dann gilt

$$h = h * e = h * (g * h') = (h * g) * h' = e * h' = h'.$$

□

2. Körper

Definition. Ein Körper ist eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$, so dass

(K1) $(K, +)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 0 bezeichnet und das inverse Element zu $k \in K$ mit $-k$. (Addition)

(K2) $(K \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe. Das neutrale Element wird mit 1 bezeichnet und das inverse Element zu $k \in K \setminus \{0\}$ mit k^{-1}. (Multiplikation)

(K3) Für alle $a, b, c \in K$ gilt

$$(a + b) \cdot c = a \cdot c + b \cdot, \quad \text{(Distributivgesetz).}$$

Beispiel (Kleinster (nichtrivialer) Körper). $\mathbb{Z}_2$ mit oben eingeführter Addition und Multiplikation ist ein Körper. Für die inversen Elemente der Addition und Multiplikation gilt:

k	$-k$	k^{-1}
0	0	-
1	1	1

Beispiel (Zweitkleinster Körper). $\mathbb{Z}_3$ mit oben eingeführter Addition und Multiplikation ist ein Körper. Für die inversen Elemente der Addition und Multiplikation gilt:

k	$-k$	k^{-1}
0	0	-
1	2	1
2	1	2

Die beiden Beispiele oben sind Beispiele endlicher Körper. Diese spielen eine wichtige Rolle in Anwendungen wie etwa der Codierungstheorie. Die entsprechende Theorie geht auf Evariste Galois zurück. In der Tat lässt charakterisieren, wann $\mathbb{Z}_k$ ein Körper ist.

THEOREM. *$\mathbb{Z}_k$ ist genau dann ein Körper wenn k eine Primzahl ist.*

Zum Beweis brauchen wir etwas Vorbereitung. Zuerst zeigen wir, dass Multiplikation mit 0 erwartungsgemäß immer 0 liefert.

LEMMA. *In einem Körper K gilt für alle $k \in K$*

$$k \cdot 0 = 0 \cdot k = 0$$

Beweis.

$$\begin{aligned}
0 \cdot k &= (0 \cdot k) + \Big((0 \cdot k) - (0 \cdot k)\Big) && \text{Inverses Element der Addition} \\
&= \Big((0 \cdot k) + (0 \cdot k)\Big) - (0 \cdot k) && \text{Assoziativität der Addition} \\
&= ((0 + 0) \cdot k) - (0 \cdot k) && \text{Distributivgesetz} \\
&= (0 \cdot k) - (0 \cdot k) && \text{0 neutrales Element der Addition} \\
&= 0 && \text{Inverses Element der Addition}
\end{aligned}$$

□

Aus dem obigen Lemma folgen wir folgende wichtige Eigenschaft eines Körpers, die sogenannte Nullteilerfreiheit. Diese besagt, dass falls eine Multiplikation 0 ergibt, dann schon eine der beiden Faktoren 0 sein muss.

LEMMA (Nullteilerfreiheit). *In einem Körper K gilt für alle $a, b \in K$ mit $a \cdot b = 0$, dass $a = 0$ oder $b = 0$.*

Beweis. Angenommen $a \neq 0$. Dann existiert das inverse Element a^{-1}

$$\begin{aligned}
b &= 1 \cdot b && \text{neutrales Element der Multiplikation} \\
&= a^{-1} \cdot a \cdot b && a^{-1} \cdot a = 1 \\
&= a^{-1} \cdot 0 && \text{Annahme} \\
&= 0 && \text{nach obigem Lemma}
\end{aligned}$$

□

Nun kommen wir zum Beweis des Theorems, dass $\mathbb{Z}_k$ genau dann ein Körper ist wenn k eine Primzahl ist.

Beweis. [Beweis des Theorems] Falls k keine Primzahl ist, dann existiert ein $1 < n < k$ welches k teilt, d.h. es existiert $1 < m < k$ mit $n \cdot m = k$ und somit

$$(n \cdot m) \bmod k = k \bmod k = 0 \bmod k$$

Damit existiert ein Nullteiler welches nach obigem Lemma in einem Körper unmöglich ist.

Es bleibt zu zeigen, dass $\mathbb{Z}_p$ für jede Primzahl p ein Körper ist. (K1) und (K3) sind klar. Für (K2) ist die Existenz von inversen Elementen zu zeigen.

Dazu brauchen wir einen Satz von Euklid über den größten gemeinsamen Teiler $\mathrm{ggT}(a, n)$ von zwei Zahlen $a, n \in \mathbb{N}$. Dieser besagt, dass es ganze Zahlen s und t gibt mit

$$\mathrm{ggT}(a, n) = s \cdot a + t \cdot n$$

Sei nun $a \bmod p \in \mathbb{Z}_p$ mit $a \neq 0$ und $n = p$. Da p eine Primzahl ist, so ist $\mathrm{ggT}(a, p) = 1$. Also

$$s \cdot a = 1 - t \cdot p \quad \text{and} \quad - s \cdot a = t \cdot p - 1$$

Es gibt zwei Fälle:
Fall $s > 0$: Dann ist $t < 0$ und $-t \cdot p > 0$. Dann ist $(a \bmod p)^{-1} = s \bmod p$ denn

$$(s \bmod p) \cdot (a \bmod p) = (s \cdot a) \bmod p = (1 - t \cdot p) \bmod p = 1 \bmod p.$$

Fall $s < 0$: Dann ist $t > 0$ und $(a \bmod p)^{-1} = (-s) \bmod p$ denn

$$(-s \bmod p) \cdot (a \bmod p) = (-s \cdot a) \bmod p = (t \cdot p - 1) \bmod p = 1 \bmod p.$$

$\square$

3. Zahlen

3.1. Natürliche Zahlen und Primzahlen. Wir sind bereits mit den natürlichen Zahlen vertraut. Diese haben folgende charakteristische Eigenschaft:

- Beginnt man bei 1 und addiert sukkzesive +1, so erhält man schließlich alle natürlichen Zahlen.

Mathematisch wird diese Eigenschaft durch das Induktionsaxiom charakterisiert, durch welches sich die natürlichen Zahlen axiomatisch einführen lassen.

Axiom (Axiom der vollständigen Induktion). Sei für jede natürliche Zahl $n \in \mathbb{N}$ eine Aussage $A(n)$ gegeben. Falls $A(1)$ wahr ist und für alle n die Aussage $A(n+1)$ aus der Aussage $A(n)$ folgt so gilt $A(n)$ für alle $n \in \mathbb{N}$.

Notation. Seien $a_1, \ldots, a_n$ Zahlen, dann schreiben wir für die Summe

$$\sum_{k=1}^{n} a_k := a_1 + \ldots + a_n.$$

Diese Notation ist präziser als die ... da sie genau angibt was für jeden Summanden zwischen dem 1. und dem n-ten zu tun ist.

Theorem. *Für alle $n \in \mathbb{N}$ gilt*

$$\sum_{k=1}^{n} k = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

(Beachte die der Zähler auf der rechten Seite ist immer eine gerade Zahl.)

Beweis. Sei $A(n)$ die Aussage des Satzes für $n \in \mathbb{N}$. Dann gilt $A(1)$ denn

$$\frac{1(1+1)}{2} = 1.$$

Angenommen $A(n)$ ist wahr. Berechnen nun die linke Seite von $A(n+1)$ in dem wir $A(n)$ nutzen

$$\begin{aligned} 1 + 2 + \ldots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\left(\frac{n}{2} + 1\right) \\ &= (n+1)\frac{(n+2)}{2}. \end{aligned}$$

□

Bemerkung. Beachte, dass die Gültigkeit der Aussage $A(n) \Longrightarrow A(n+1)$ "weniger" ist als die Gültigkeit der Ausage $A(n+1)$. Sei z.B. für $n \in \mathbb{N}$

$A(n)$ ich habe im Jahr $2015 + n$ mindestens n Millionen Euro auf meinem Konto

und es gelte $A(n) \Longrightarrow A(n+1)$, d.h. wenn man n Millionen Euro hat, dann kann man innerhalb eines Jahres eine zweite Million dazugewinnen. Leider ist aber $A(1)$ nicht wahr.

Beispiel. Alle Menschen haben die gleiche Haarfarbe.
Beweis. $n = 1$: klar.
$n \Longrightarrow n+1$: Sei eine Gruppe von $n+1$ Menschen gegeben. Wir schicken nun eine Person von diesen $n+1$ aus dem Raum. Es verbleiben n Personen, die nach Induktionsvoraussetzung die gleiche Haarfarbe haben. Nun bitten wir die Person, die den Raum verlassen hat, den Raum wieder zu betreten und schicken eine andere Person hinaus. Nach Induktionsvoraussetzung haben alle in dieser Gruppe von n Personen die gleiche Haarfarbe. Insbesondere hat die Person die als erstes den Raum verlassen hat, die gleiche Haarfarbe wie alle anderen ...
Wo liegt der logische Fehler?

Eine wichtige Klasse von natürlichen Zahlen sind Primzahlen.

Definition. Eine natürliche Zahl $n \geq 2$ heißt *Primzahl* wenn sie nur durch 1 und sich selbst teilbar ist.

Ein wichtiger Satz den wir hier nicht beweisen werden ist die Grundlage für die Bedeutung der Primzahlen in Anwendungen wie der Kodierungstheorie.

Theorem (Eindeutigkeit der Zerlegung in Primzahlen). *Für jede natürliche Zahl $n \geq 2$ existiert ein $k \leq n$ und Primzahlen $p_1 \leq p_2 \leq \ldots \leq p_k$,* *so dass*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k.$$

Weiterhin gibt es unendlich viele Primzahlen. Dieser Satz geht auf Euklid zurück.

THEOREM. *Es gibt unendlich viele Primzahlen.*

Beweis. Angenommen es gibt nur endlich viele Primzahlen. Wir bezeichnen sie mit $p_1, \ldots, p_n$. Sei

$$m = p_1 \cdot p_2 \cdot \ldots \cdot p_n.$$

Betrachte nun $m+1$. Da $p_1, \ldots, p_n < m+1$ kann $m+1$ keine Primzahl sein. Damit ist $m+1$ also durch eine Primzahl q teilbar und da $q \in \{p_1, \ldots, p_n\}$ teilt q auch m d.h. es gibt natürliche Zahlen k und l, so dass

$$m + 1 = q \cdot k \quad m = q \cdot l.$$

Somit gilt

$$1 = (m + 1) - m = q \cdot k - q \cdot l = q(k - l).$$

D.h. q teilt auch 1. Das ist aber ein Widerspruch, da 1 keine Primteiler hat. $\square$

3.2. Die ganzen Zahlen. Die Addition zweier natürlicher Zahlen liefert immer eine natürliche Zahlen. Allerdings kann man nicht zwei beliebige natürliche Zahlen von einander subtrahieren ohne die natürlichen Zahlen zu verlassen. Das gleiche gilt für $\mathbb{N}_0$.
Präzise ausgedrückt hat die Gleichung für gegebenes n und k in $\mathbb{N}_0$

$$k + x = n$$

genau dann eine Lösung $x \in \mathbb{N}_0$ wenn $k \leq n$. Z.B. hat die Gleichung

$$42 + x = 0$$

keine Lösung in $\mathbb{N}_0$.
Wir fügen also alle Lösungen x von Gleichungen der Form $k + x = n$ hinzu und bezeichnen sie mit $n - k := x$. Nun sagen wir $(n - k)$ ist äquivalent zu $(n' - k')$ falls l existiert so dass $n + l = n'$ und $k + l = k'$ oder $n = n' + l$ und $k = k' + l$. Die Äquivalenzklasse von $[n - 0]$ bezeichnen wir mit n und die Äquivalenzklasse von $[0 - n]$ mit $-n$.
Anders ausgedrückt ist $\mathbb{N}_0$ nur ein Monoid bezüglich der Addition und keine Gruppe. D.h. außer 0 hat kein $n \in \mathbb{N}$ ein inverses Element.
Fügen wir zu jedem $n \in \mathbb{N}$ ein inverses Element hinzu, dass wir mit $-n$ bezeichnen erhalten wir die ganzen Zahlen, d.h.

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2 \ldots\} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}.$$

Man kann sich leicht überzeugen, dass $\mathbb{Z}$ eine Gruppe bezüglich der Addition ist.

3.3. Die rationalen Zahlen. Allerdings ist $\mathbb{Z}\setminus\{0\}$ auch nur ein Monoid bzgl. der Multiplikation, d.h. für gegebene $p, q \in \mathbb{Z}\setminus\{0\}$ hat die Gleichung

$$p \cdot x = q$$

nur dann eine Lösung wenn q ein Vielfaches von q ist. Anders ausgedrückt.
Wir bezeichnen die Lösung von $p \cdot x = q$ mit

$$\frac{p}{q} := x.$$

Wir bilden wieder Äquivalenzklassen unter der Äquivalenzrelation

$$\frac{p}{q} \sim \frac{p'}{q'} :\Longleftrightarrow p \cdot q' = p' \cdot q.$$

und bezeichnen die Menge der Äquivalenzklassen mit $\mathbb{Q}$ und nennen sie die *rationalen Zahlen.* Die ganzen Zahlen lassen sich offensichtlich als Untermenge auffassen. Das bedeutet z.B.

$$\left[\frac{2}{3}\right] = \left[\frac{4}{6}\right] = \ldots = \left[\frac{28}{42}\right] = \ldots = \left[\frac{42}{63}\right] = \ldots.$$

Der Einfachheit halber lässt man die Äquivalenzklammern weg.
Auf $\mathbb{Q}$ hat man folgende Addition und Multiplikation

$$\frac{p}{q} + \frac{r}{s} = \frac{p \cdot s + r \cdot q}{qs} \quad \text{und} \quad \frac{p}{q} \cdot \frac{r}{s} = \frac{p \cdot r}{q \cdot s}.$$

Mit diesen Operationen ist $\mathbb{Q}$ ein Körper.

Bemerkung. Beide Operationen sind wohldefiniert, d.h. sie hängen nicht von der Wahl der Repräsentanten ab. Z.B. ist

$$\frac{1}{2} + \frac{1}{2} = 1 = \frac{21}{42} + \frac{42}{84}.$$

Die “falsche Addition”

$$\frac{p}{q} + \frac{r}{s} = \frac{p + r}{q + s}$$

hingegen ist nicht wohldefiniert

$$\frac{1}{2} + \frac{1}{3} = \frac{1+1}{2+3} = \frac{2}{5}$$
$$\frac{1}{2} + \frac{2}{6} = \frac{1+2}{2+6} = \frac{3}{8}.$$

Wir können jede rationale Zahl quadrieren und erhalten wieder eine rationale Zahl. Allerdings zeigt das nächste Theorem, dass die Umkehrung – das Wurzelziehen – selbst für natürliche Zahlen nicht immer rationale Lösungen hat.

Theorem ($\sqrt{2}$ ist irrational). *Die Gleichung*

$$x^2 = 2$$

hat keine Lösung in $\mathbb{Q}$.

Beweis. Angenommen es gäbe eine Lösung $\frac{p}{q} \in \mathbb{Q}$ und nehmen wir an p und q sind teilerfremd. D.h.

$$\frac{p^2}{q^2} = 2$$

Damit folgt aber

$$p^2 = 2 \cdot q^2$$

Also ist p^2 gerade und somit auch p, d.h. es existiert $r \in \mathbb{N}$ mit

$$p = 2r$$

und somit

$$(2r)^2 = 2 \cdot q^2$$

bzw. nach Division durch 2

$$2 \cdot r^2 = q^2$$

Wir schließen wie oben dass q gerade ist. Das ist aber ein Widerspruch zur Teilerfremdheit von p und q. □

3.4. Die algebraischen Zahlen. Wenn wir nun alle Lösungen x von sogenannten Polynomgleichungen

$$q_n x^n + \ldots + q_1 x + q_0 = p$$

mit $q_0, \ldots, q_n, p \in \mathbb{Q}$ erhalten wir die Menge der *algebraischen Zahlen.* Die Menge der algebraischen Zahlen beinhaltet insbesondere die geometrischen Verhältnisse die man mit Zirkel und Lineal aus der Einheitsstrecke konstruieren kann.
Eine klassische Frage der Griechen war die Frage nach der Quadratur des Kreises, d.h. ob man ein Quadrat mit Zirkel und Lineal konstruieren kann welches den gleichen Flächeninhalt hat wie ein Kreis. Bezeichnen wir den Flächeninhalt des Kreises mit π. Die Frage ist also ob sich eine Strecke der Länge $\sqrt{\pi}$ konstruieren lässt (das Quadrat mit Seitenlänge $\sqrt{\pi}$ hätte gerade den Flächeninhalt π). Da sich Wurzeln konstruieren lassen, ist diese Frage also äquivalent dazu, ob sich eine Strecke mit Länge π konstruieren lässt. Wie oben diskutiert lassen sich alle konstruierbaren Strecken durch Lösungen von Polynomgleichungen, d.h. algebraische Zahlen, beschreiben. Die Frage nach der Quadratur des Kreises übersetzt lässt sich also in die Frage verallgemeinern ob π eine algebraische Zahl ist.

Theorem (Lindemann 1882). *π ist keine algebraische Zahl.*

3.5. Die reellen Zahlen. D.h. die bisherige Strategie der Erweiterung der Zahlen durch Lösungen von Gleichungen führt uns also hier nicht weiter.
Wir nutzen zur Vervollständigung von $\mathbb{Q}$ stattdessen die Ordnungsstruktur. In der Tat, können wir auf $\mathbb{Q}$ folgende Ordnungsrelation einführen

$$\frac{p}{q} \leq \frac{r}{s} \quad :\Longleftrightarrow \quad ps \leq qr.$$

Diese Ordnungsrelation ist wohldefiniert (Übung) und stimmt offensichtlich mit der Ordnung auf $\mathbb{N}$ überein.
Wir haben gesehen, dass $x^2 = 2$ in $\mathbb{Q}$ keine Lösung hat. Insbesondere hat die Menge

$$D_{\sqrt{2}} := \{x \in \mathbb{Q} \mid x < 0 \vee x^2 < 2\}$$

zwar von oben beschränkt aber hat keine kleinste obere Schranke in $\mathbb{Q}$.
Wir betrachten also alle Mengen $\delta \subseteq \mathbb{Q}$ mit den Eigenschaften:

- δ ist von oben beschränkt hat aber keine kleinste obere Schranke, d.h. es existiert $s \in \mathbb{Q}$ mit $d \leq s$ für alle $d \in \mathbb{Q}$ aber für alle $d \in \delta$ existiert $d' \in \delta$ mit $d < d'$,
- für alle $d \in \delta$ und $d' \leq d$ folgt $d' \in \delta$.

Solche Mengen sind als *Dedekindsche Schnitte* bekannt.
Man kann jede rationale Zahl mit genau einem Schnitt identifizieren nämlich

$$\delta_q := \{x \in \mathbb{Q} \mid x < q\}, \quad q \in \mathbb{Q}$$

und auch z.B. $\sqrt{2}$, via $\delta_{\sqrt{2}}$.
Wir können auf diesen Schnitten eine Ordnung einführen via

$$\delta \leq \delta' \quad :\Longleftrightarrow \quad \text{für alle } d \in \delta \text{ existiert } d' \in \delta' \text{ mit } d \leq d'.$$

Wir können nun auf diesen Schnitten eine Addition und eine Multiplikation einführen via

$$\delta + \delta' = \{d + d' \mid d \in \delta, d' \in \delta'\}$$

und für $\delta, \delta' \geq \delta_0 (= 0)$

$$\delta \cdot \delta' = \{p \in \mathbb{Q} \mid d, d' \geq 0, d \in D, d' \in D', p \leq d \cdot d'\}.$$

und geeigneter Fortsetzung für negative δ.
Die Menge dieser Schnitte zusammen mit der Addition und Multiplikation liefert einen Körper der mit der obigen Ordnung total geordnet ist.
Wir nennen diesen Körper die reellen Zahlen und bezeichnen ihn mit $\mathbb{R}$.

3.6. Die komplexen Zahlen. Wie oben diskutiert lassen sich innerhalb der reellen Zahlen alle Gleichungen der Art

$$x^2 \leq r$$

für $r \in \mathbb{R}$ mit $r \geq 0$ lösen.
Allerdings hat die Gleichung

$$x^2 = -1$$

keine Lösung in $\mathbb{R}$. Wir fügen jetzt ein Element zu $\mathbb{R}$ hinzu welches wir als eindeutige Lösung der Gleichung definieren und mit i bzw. $\sqrt{-1}$ bezeichen und die *imaginäre Einheit* nennen.
Für dieses Element gilt also

$$i^2 = -1.$$

Weiterhin definieren wir die Multiplikation von i mit einer reellen Zahl v als das Produkt $v \cdot i$ und die Addition dieser Produkte mit einer reellen Zahl u als $u + v \cdot i$. Die Menge dieser Objekte nennen wir die komplexen Zahlen und bezeichen sie mit

$$\mathbb{C} := \{u + v \cdot i \mid u, v \in \mathbb{R}\}.$$

Für eine komplexe Zahl $z = u + i \cdot v$ nennen wir $\operatorname{Re} z := u$ den *Realteil* und $\operatorname{Im} v$ den *Imaginärteil.*
Wir führen auf $\mathbb{C}$ folgende Addition und Multiplikation ein

$$(u + i \cdot v) + (u' + i \cdot v') := (u + u') + i \cdot (v + v')$$
$$(u + i \cdot v) \cdot (u' + i \cdot v') := (u \cdot u' - v \cdot v') + i \cdot (u \cdot v' + u' \cdot v)$$

Diese Operationen sind mit den oben diskutierten Operationen konsistent.
Es lässt sich leicht (aber mühsam) überprüfen, dass $\mathbb{C}$ mit dieser Addition und Multiplikation ein Körper ist.
Offensichtlich lässt sich $\mathbb{C}$ mit $\mathbb{R}^2 := \mathbb{R} \times \mathbb{R}$ identifizieren via

$$\mathbb{C} \to \mathbb{R}^2,\ u + i \cdot v \mapsto (u, v).$$

Hinter dieser Identifikation verbirgt sich eine wichtige geometrische Interpretation. Diese Darstellung der komplexen Zahlen wird die Gaußsche Zahlenebene genannt.
In der Gaußschen Zahlen Ebene ist die Addition von zwei komplexen Zahlen gerade die wohlbekannte Addition von zwei Vektoren aus $\mathbb{R}^2$.
Beispiel Bild
Auch die Multiplikation hat eine geometrische Interpretation. Dafür brauchen wir aber die Darstellung von Vektoren in $\mathbb{R}^2$ durch Polarkoordinaten. Jeder Vektor $(u, v) \in \mathbb{R}^2$ lässt auch durch seine Länge und seinen Winkel zur ersten Koordinatenachse eindeutig bestimmen. (**Bild**)

Sei r die Länge und φ das Argument für eine komplexe Zahl $z = u+i\cdot v$, (d.h. $r = \sqrt{u^2 + v^2}$ und $\cos\varphi = v/r$ und $\sin\varphi = u/r$).
Dann hat das Produkt z und z' die Länge $r \cdot r'$ und das Argument $\varphi + \varphi'$ (**Bild**).

KAPITEL 3

Lineare Algebra

In diesem Kapitel geht es um Geometrie in Vektorräumen.

1. Lineare Gleichungssysteme

Eine wichtige Motivation kommt aus dem Lösen von lineare Gleichungssystemen.

Definition (Lineares Gleichungssystem). Seien $n, m \in \mathbb{N}$, $a_{i,j}, b_i \in \mathbb{R}$, $i = 1, \dots, n$, $j = 1, \dots, m$. Dann heißt

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n &= b_2 \\ \vdots \qquad & \qquad \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

ein *(lineares) Gleichungssystem* in den Unbekannten $x_1, \dots, x_m$. Die Menge der Tupel $(x_1, \dots, x_m)$ für die die Gleichungen gelten heißt die *Lösungsmenge* des Gleichungssystems und jedes dieser Tupel heißt *Lösung*.

Bemerkung. Eine Anwendung wo lineare Gleichungssystem auftreten ist die Produktion. Seien $P_1, \dots, P_m$ Produkte und $b_1, \dots, b_m$ die zu produzierende Anzahl von $P_1, \dots, P_m$. Seien $T_1, \dots, T_n$ die Typen von Teile die zur Produktion von $P_1, \dots, P_m$ benötigt werden. Dann geben $a_{1,1}, \dots, a_{1,n}$ wieviele Teile $T_1, \dots, T_n$ zur Produktion von P_1 benötigt werden, $a_{2,1}, \dots, a_{2,n}$ wieviele Teile $T_1, \dots, T_n$ zur Produktion von P_2, usw. Die Lösung $(x_1, \dots, x_n)$ des Gleichungssystems gibt also an wieviele Teile man insgesamt braucht um $b_1, \dots, b_m$ Produkte vom Typ $P_1, \dots, P_m$ herzustellen.

Bemerkung. Ein Gleichungssystem kann eine, keine oder unendlich viele Lösungen haben.

- Das Gleichunssystem

$$\begin{aligned} x_1 + x_2 &= 1 \\ x_2 &= 1 \end{aligned}$$

hat nur die Lösung $(x_1, x_2) = (0, 1)$.

- Das Gleichunssystem

$$\begin{aligned} x_1 + x_2 &= 1 \\ x_1 \quad &= 42 \\ x_2 &= 1 \end{aligned}$$

  hat keine Lösung, denn $42 + 1 \neq 1$.

  Das Gleichunssystem

$$\begin{aligned} x_1 + x_2 &= 1 \\ 42x_1 + 42x_2 &= 42 \end{aligned}$$

  hat unendlich viele Lösungen. Es ist nämlich $(x_1, x_2) = (1, 1 - r)$ für jedes $r \in \mathbb{R}$ eine Lösung.

Der Grund warum wir die ersten beiden Beispiele "auf einen Blick" lösen konnten, liegt darin, dass das Gleichungssystem in der sogenannten Stufenform ist. Wir diskutieren hier den Gaußschen Algoritmus der angibt wie sich jedes Gleichungssystem auf Stufenform bringen lässt. Das bedeutet wie sich für ein Gleichungssystem

$$\begin{aligned} a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3 + \cdots + a_{1,n}x_n &= b_1 \\ a_{2,1}x_1 + a_{2,2}x_2 + a_{2,3}x_3 + \cdots + a_{2,n}x_n &= b_2 \\ a_{3,1}x_1 + a_{3,2}x_2 + a_{3,3}x_3 + \cdots + a_{3,n}x_n &= b_m \\ \vdots \qquad &\quad \vdots \\ a_{m,1}x_1 + a_{m,2}x_2 + a_{m,3}x_3 + \cdots + a_{m,n}x_n &= b_m \end{aligned}$$

reelle Zahlen $\tilde{a}_{i,j}, \tilde{b}_i$ finden lassen, so dass das Gleichungssystem

$$\begin{aligned} \tilde{a}_{1,1}x_1 + \tilde{a}_{1,2}x_2 + \tilde{a}_{1,3}x_3 + \cdots + \tilde{a}_{1,n}x_n &= \tilde{b}_1 \\ \tilde{a}_{2,2}x_2 + \tilde{a}_{2,3}x_3 + \cdots + \tilde{a}_{2,n}x_n &= \tilde{b}_2 \\ \tilde{a}_{3,3}x_3 + \cdots + \tilde{a}_{3,n}x_n &= \tilde{b}_3 \\ \vdots \qquad &\quad \vdots \end{aligned}$$

dieselbe Lösungsmenge besitzt.
Dies geschieht in $2m$ Schritten:

- In m "Vorwärtsschritten" durch geschicktes Multiplizieren und Subtrahieren der Zeilen voneinander.
- In m "Rückwärtsschritten" durch Einsetzen.

Wir demonstrieren dies an Beispielen.

Beispiel. Sei

$$\begin{array}{lll} 2x_1 & 3x_2 & = 2 \\ x_1 & 2x_2 & = 1 \qquad | \cdot (-2) \end{array}$$

Addieren erste und zweite Zeile nachdem wir die zweite mit (-2) multipliziert haben

$$\begin{array}{lll} 2x_1 & 3x_2 & = 2 \\ & -x_2 & = 1 \qquad | \cdot (-2) \end{array}$$

Lesen x_2 an der letzten Zeile ab

$$x_2 = -1$$

und setzen $x_2 = -1$ in erste Zeile ein und lösen nach x_1 auf

$$2x_1 + 3 \cdot (-1) = 2 \quad \Longrightarrow \quad x_1 = \frac{5}{2}$$

Damit haben wir eine Lösung.

Beispiel. Gegeben sei das Gleichungssystem

$$\begin{array}{lllll} 2x_1 & +2x_2 & +4x_3 & = 5 & \\ x_1 & -x_2 & +x_3 & = 3 & | \cdot (-2) \\ -x_1 & -2x_2 & -x_3 & = -1 & | \cdot 2 \end{array}$$

Addieren das (-2)-fache von der zweiten Zeile zur ersten und das 2-fache der dritten zur ersten:

$$\begin{array}{lllll} 2x_1 & +2x_2 & +4x_3 & = 5 & \\ & 4x_2 & +2x_3 & = -1 & \\ & -2x_2 & +2x_3 & = 3 & | \cdot 2 \end{array}$$

Addieren das 2-fache der dritten Zeile zur zweiten

$$\begin{array}{llll} 2x_1 & +2x_2 & +4x_3 & = 5 \\ & 4x_2 & +2x_3 & = -1 \\ & & +6x_3 & = 3 \end{array}$$

Lesen den Wert für x_3 ab

$$x_3 = \frac{1}{2}$$

und setzen $x_3 = 1/2$ in die zweite Zeile ein und erhalten

$$4x_2 + 2 \cdot \frac{1}{2} = -1 \quad \Longrightarrow \quad x_2 = -\frac{1}{2}.$$

Setzen $x_3 = 1/2$ und $x_2 = -1/2$ in die erste Zeile ein und erhalten

$$2x_1 + 2 \cdot \frac{1}{2} + 4 \cdot \left(-\frac{1}{2}\right) = 5 \quad \Longrightarrow \quad 2x_1 - 1 = 5 \quad \Longrightarrow \quad x_1 = 3.$$

Damit ist $(x_1, x_2, x_3) = (3, -1/2, 1/2)$ die Lösung des Gleichungssystems.

Das zweite Beispiel mit leerer Lösungsmenge ist schon auf Stufenform. Wir sehen, dass der dritte Rückwärtsschritt auf einen Widerpsruch führt. Das dritte Beispiel oben hat die Stufenform

$$\begin{aligned} x_1 + x_2 &= 1 \\ 0 &= 0 \end{aligned}$$

D.h. wir haben einen Freiheitsgrad in der Wahl von x_1 oder x_2.
Es ist effizienter in Theorie und Anwendung ein lineares Gleichungssystem in Matrixschreibweise zu notieren.

$$A = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}, \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

wobei A eine $m \times n$ Matrix ist, b ein m-dimensionaler Vektor und suchen einen n

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

so, dass

$$\begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

oder kurz

$$A \cdot x = b.$$

Dabei ist die Multiplikation $A \cdot x$ gerade so definiert, dass sie auf obiges Gleichungssystem führt: Für die j-te Komponente auf der rechten Seite nehmen wir die j-Zeile der Matrix auf linken Seite und multiplizieren die i-te Komponente mit der i-ten Komponente des Vektors x und bilden die Summe.
Wir illustrieren die Matrixmultiplikation an einigen Beispielen.

Beispiel. $n = m = 2$

$$\begin{pmatrix} 1 & 2 \\ 0 & 42 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 2 + 2 \cdot 1 \\ 0 \cdot 2 + 42 \cdot 1 \end{pmatrix} = \begin{pmatrix} 3 \\ 42 \end{pmatrix}$$

$n = 3$, $m = 2$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 1 \cdot 7 + 2 \cdot 8 + 3 \cdot 9 \\ 4 \cdot 7 + 5 \cdot 8 + 6 \cdot 9 \end{pmatrix} = \begin{pmatrix} 50 \\ 131 \end{pmatrix}$$

$n = 2$, $m = 3$

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 7 \\ 8 \end{pmatrix} = \begin{pmatrix} 1 \cdot 7 + 2 \cdot 8 \\ 3 \cdot 7 + 4 \cdot 8 \\ 5 \cdot 7 + 6 \cdot 8 \end{pmatrix} = \begin{pmatrix} 23 \\ 53 \\ 83 \end{pmatrix}$$

$n = m = 3$

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \cdot 3 + 2 \cdot 2 + 3 \cdot 1 \\ 4 \cdot 3 + 5 \cdot 2 + 6 \cdot 1 \\ 7 \cdot 3 + 8 \cdot 2 + 9 \cdot 1 \end{pmatrix} = \begin{pmatrix} 10 \\ 28 \\ 46 \end{pmatrix}$$

Wir bezeichnen den Raum der n-Tupel von reellen Zahlen mit $\mathbb{R}^n$, d.h.

$$\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$$

In diesem Sinne ist eine $m \times n$ Matrix A eine Abbildung

$$A : \mathbb{R}^n \to \mathbb{R}^m$$

Für die Frage ob sich die Gleichung

$$A \cdot x = b$$

eindeutig lösen lässt, lässt sich so nun so umformulieren

- Existenz einer Lösung $\iff$ A surjektiv
- Eindeutigkeit der Lösung $\iff$ A injektiv

Im folgenden werden wir eine Theorie aufzubauen, die die Lösbarkeit von linearen Gleichungssystem systematisch untersucht.

2. Vektorräume und Dimension

Definition. Eine Menge V mit einer Addition $+ : V \times V \to V$ und einer skalaren Multiplikation $\cdot : \mathbb{R} \times V \to V$ heißt (reeller) Vektorraum, falls

(V1) $(V, +)$ ist eine abelsche Gruppe. (Wir bezeichnen das neutrale Element mit 0)
(V2) $(r + s) \cdot v = r \cdot v + s \cdot v$ für alle $v \in V$, $r, s \in \mathbb{R}$
(V3) $r \cdot (v + w) = r \cdot v + r \cdot w$ für alle $v, w \in V$, $r \in \mathbb{R}$
(V4) $(r \cdot s) \cdot v = r \cdot (s \cdot v)$ für alle $v \in V$, $r \in \mathbb{R}$
(V5) $1 \cdot v = v$ für alle $v \in V$.

Beispiel. Sei $\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_1, \ldots, x_n \in \mathbb{R}\}$ mit der Addition

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$

und der skalaren Multiplikation

$$r \cdot (x_1, \ldots, x_n) := (r \cdot x_1, \ldots, \cdot x_n)$$

ist ein Vektorraum.

Bild für $\mathbb{R}^2$

Vektorräume können auch sehr "unanschaulich" sein, wie das folgende Beispiel zeigt.

Beispiel. Sei $F(\mathbb{R})$ die Menge der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Mit der Addition $f + g$ und skalaren Multiplikation $r \cdot f$ gegeben durch

$$(f + g)(x) := f(x), \quad (r \cdot f)(x) := r \cdot f(x), \qquad x \in \mathbb{R}$$

für $f, g \in F(X)$, $r \in \mathbb{R}$ ist $F(\mathbb{R})$ ein Vektorraum.

Dieser Vektorraum ist allerdings für die meisten praktischen wie theoretischen Zwecke zu "groß". Ein "kleinerer" und nützlicher Raum ist der Vektorraum der Polynome: Sei $n \in \mathbb{N}$. Wir bezeichnen mit $P_n(\mathbb{R})$ die Menge aller *Polynome vom Grad kleiner gleich* n, d.h. von Funktionen $p : \mathbb{R} \to \mathbb{R}$ für die $p_0, p_1, p_2 \dots, p_n \in \mathbb{R}$ existieren, so dass

$$p(x) = p_0 + p_1 x + p_2 x^2 + \dots + p_n x^n.$$

Die Zahlen $p_0, \dots, p_n$ heißen *Koeffizienten.*
Offensichtlich ist $P_n(\mathbb{R}) \subseteq F(X)$. Man kann zeigen, dass mit der oben definierten Addition und Multiplikation $P_n(\mathbb{R})$ ein Vektorraum ist. (Hier ist zu beweisen, dass $p + q \in P_n(\mathbb{R})$ und $r \cdot p \in P_n(V)$ für $p, q \in P_n(\mathbb{R})$ und $r \in \mathbb{R}$ s.h. Übung).

Definition (Unterraum). Eine Teilmenge U eines Vektorraums V heißt *Unterraum*, falls U mit der Addition und skalaren Multiplikation von V wieder ein Vektorraum ist. Für eine endliche Teilmenge $W = \{v_1, \dots, v_n\}$ bezeichnen wir mit

$$\mathrm{span} W = \{r_1 v_1 + \dots + r_n v_n \mid r_1, \dots, r_n \in \mathbb{R}\}$$

den von W *aufgespannten Unterraum.*

Beispiel. $\{(0, x) \mid x \in \mathbb{R}\}$, $\{(x, 0) \mid x \in \mathbb{R}\}$, $\{(x, x) \mid x \in \mathbb{R}\}$, $\{(x, -x) \mid x \in \mathbb{R}\}$ sind Unterräume von $\mathbb{R}^2$, (**Bild**). Sie werden z.B. von den Vektoren $(0, 1)$, $(1, 0)$, $(1, 1)$, $(1, -1)$ aufgespannt.

Beispiel. $\{(x, y, 0) \mid x, y \in \mathbb{R}\}$, $\{(x, 0, z) \mid x, z \in \mathbb{R}\}$, $\{(0, y, z) \mid y, z \in \mathbb{R}\}$, sind Unterräume von $\mathbb{R}^3$, (**Bild**). Sie werden z.B. von den Vektoren $(1, 1, 0)$, $(1, 0, 1)$, $(0, 1, 1)$ aufgespannt.

Definition (Lineare Abhängigkeit). Sei V ein Vektorraum. Die Vektoren $v_1, \dots, v_n \in V$ heißen *linear abhängig* falls $r_1, \dots, r_n \in \mathbb{R}$

$$r_1 \cdot v_1 + \dots + r_n \cdot v_n = 0.$$

Falls solche $r_1, \dots, r_n$ nicht existieren heißen $v_1, \dots, v_n$ *linear unabhängig.*

Beispiel. Sei $V = \mathbb{R}^2$.

- $(1, 0)$ und $(2, 0)$ sind linear abhängig: Wähle $r_1 = -2$ und $r_2 = 1$.
- $(1, 0)$ und $(0, 1)$ sind linear unabhängig: Angenommen $r_1 \cdot (1, 0) + r_2(0, 1) = 0$, dann folgt $r_1 = r_2 = 0$.
- $(1, 1)$ und $w = (1, -1)$ sind linear unabhängig: Denn $r_1 + r_2 = 0$ und $r_1 - r_2 = 0$ haben nur die Lösung $r_1 = r_2 = 0$.
- $(1, 0)$, $(0, 1)$ und $(1, 1)$ sind linear unabhängig: Wähle $r_1 = r_2 = 1$ und $r_3 = -1$.

Beispiel. Sei $V = \mathbb{R}^3$.

- $(1, 0, 0)$, $(0, 1, 0)$ und $(0, 0, 1)$ sind linear unabhängig.

- $(1,1,1)$, $(1,1,-1)$ und $(1,-1,-1)$ sind linear unabhängig. Für gegebene r_1, r_2, r_3 habe wir also folgendes Gleichungssystem zu lösen

$$\begin{array}{llll} r_1 & +r_2 & +r_3 & = 0 \\ r_1 & +r_2 & -r_3 & = 0 \qquad | \cdot (-1) \\ r_1 & -r_2 & -r_3 & = 0 \qquad | \cdot (-1) \end{array}$$

Subtrahieren zweite und dritte Gleichung von der ersten und erhalten

$$\begin{array}{llll} r_1 & +r_2 & +r_3 & = 0 \\ & & +2r_3 & = 0 \qquad | \cdot (-1) \\ & +2r_2 & +2r_3 & = 0 \qquad | \cdot (-1) \end{array}$$

Aus zweiten Gleichung folgt nun $r_3 = 0$. Einsetzen in dritte Gleichung liefert $r_2 = 0$. Einsetzen in erste Gleichung liefert $r_1 = 0$.

Definition (Basis). Sei V ein Vektorraum. Eine Menge von linear unabhängigen Vektoren $v_1, \dots, v_n$ heißt eine *Basis* von V falls

$$\operatorname{span}\{v_1, \dots, v_n\} = V.$$

Beispiel. Sei $V = \mathbb{R}^2$.

- Die Vektoren $e = (1,0)$, $f = (0,1)$ bilden eine Basis. Offensichtlich kann jeder Vektor (x_1, x_2) via $x_1(1,0) + x_2(0,1)$ dargestellt werden.
- Die Vektoren $v = (1,1)$ und $w = (1,-1)$ bilden eine Basis. Da v und w linear unabhängig sind und gilt

$$e = \frac{1}{2}(v+w) \quad \text{und} \quad f = \frac{1}{2}(v-w).$$

Wir haben bereits gesehen, dass sich jeder Vektor mittels e und f darstellen lässt.

Lemma. *Sei V ein Vektorraum und $v_1, \dots, v_n$ eine Basis. Dann existieren für jeden Vektor $x \in V$ eindeutige reelle Zahlen $x_1, \dots, x_n \in \mathbb{R}$, so dass*

$$x = x_1 \cdot v_1 + \ldots + x_n \cdot v_n.$$

Beweis. (Übung) □

Definition. Die im Lemma präsentierte Darstellung heißt *Entwicklung in der Basis $v_1, \dots, v_n$.*

Bemerkung. Wenn wir in einem Vektorraum V eine Basis $v_1, \dots, v_n$ gewählt haben können wir jeden Vektor $x = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$ mit einem Vektor $(x_1, \dots, x_n)$ in $\mathbb{R}^n$ identifizieren.

LEMMA. *Sei V ein Vektorraum und und $\{v_1,\dots,v_n\}$ eine Basis. Für alle $w \in V$ sind die Vektoren $w, v_1,\dots,v_n$ linear abhängig.*

Beweis. Da $w \in V = \mathrm{span}\{v_1,\dots,v_n\}$ gilt $w = r_1 v_1 + \ldots + r_n v_n$ für gewisse $r_1,\dots,r_n \in \mathbb{R}$. Somit folgt für $r_{n+1} = -1$

$$r_1 v_1 + \ldots + r_n v_n - w = 0.$$

□

Das Lemma hat folgende Konsequenz.

THEOREM. *Sei V ein Vektorraum und $B_1 = \{v_1,\dots,v_n\}$ und $B_2 = \{w_1,\dots,w_m\}$ Basen. Dann gilt $m = n$.*

Beweis. Angenommen $n \neq m$ und o. E. $n < m$. Da $\mathrm{span} B_1 = V$ gibt es für jedes $j = 1,\dots,n$ Zahlen $r_1^{(j)},\dots,r_n^{(j)}$, so dass

$$\begin{aligned} w_1 &= r_1^{(1)} v_1 + \ldots + r_m^{(1)} v_m \\ \vdots &= \quad \vdots \\ w_n &= r_1^{(n)} v_1 + \ldots + r_m^{(n)} v_m \end{aligned}$$

Nach dem Gaußschen Algorithmus können wir die Gleichungen so umstellen, dass wir Zahlen $s_1^{(j)},\dots,s_n^{(j)} \in \mathbb{R}$, $j = 1,\dots,n$ erhalten, so dass

$$\begin{aligned} v_1 &= s_1^{(1)} w_1 + \ldots + s_m^{(1)} w_n \\ \vdots &= \quad \vdots \\ v_n &= s_1^{(n)} w_1 + \ldots + s_m^{(n)} w_n \end{aligned}$$

Nach dem vorherigen Lemma die Vektoren $w_{n+1}, v_1,\dots,v_n$ linear abhängig, d.h. es gibt $r_1^{(n+1)},\dots,r_{n+1}^{(n+1)} \in \mathbb{R}$, so dass

$$r_1^{(n+1)} v_1 + \ldots + r_n^{(n+1)} v_n + r_{n+1}^{(n+1)} w_{n+1} = 0.$$

Da $v_1,\dots,v_n$ linear unabhängig sind gilt $r_{n+1}^{(n+1)} \neq 0$. Einsetzen der n Gleichungen liefert in die letzte liefert nach umsortieren

$$\begin{aligned} 0 =& r_1^{(m+1)} \left(s_1^{(1)} w_1 + \ldots + s_n^{(1)} w_n \right) + \ldots + r_n^{(n+1)} \left(r_1^{(n)} w_1 + \ldots + r_n^{(n)} w_n \right) \\ &+ r_{n+1}^{(n+1)} w_{n+1} \\ =& r_1 w_1 + \ldots + r_n w_n + r_{n+1}^{(n+1)} w_{n+1} \end{aligned}$$

wobei $r_j = r_1^{(n+1)} s_j^{(1)} + \ldots + r_n^{(n+1)} s_j^{(n)}$, $j = 1,\dots,n$ und $r_{n+1} = r_{n+1}^{(n+1)}$. Daraus folgt, dass $w_1,\dots,w_{n+1}$ linear abhängig sind. Das ist ein Widerspruch dazu, dass B_2 eine Basis ist. □

DEFINITION. Sei V ein Vektorraum und $\{v_1,\dots,v_n\}$ eine Basis. Dann bezeichnet $\dim V := n$ die *Dimension* des Vektorraums und wir nennen V einen endlich dimensionalen Vektorraum.

Beispiel. Sei $V = \mathbb{R}^n$. Die Vektoren $e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, 0, \ldots, 0)$, $\ldots$, $e_n = (0, \ldots, 0, 1)$ bilden eine Basis, die auch die *Standardbasis* genannt wird. Damit ist

$$\dim \mathbb{R}^n = n.$$

Beispiel. Sei X eine Menge. Dann ist der Raum $F(X)$ der Funktionen von $X \to \mathbb{R}$ genau dann ein endlich dimensionaler Vektorraum falls X endlich ist. (Übung)

3. Lineare Abbildungen

Definition. Seien V, W Vektorräume. Eine Abbildung $L : V \to W$ heißt *linear* oder *Homorphismus* falls

$$L(r \cdot v + s \cdot w) = r \cdot L(v) + s \cdot L(w)$$

für alle $v, w \in V$ und $r, s \in \mathbb{R}$. Ein bijektiver Homomorphismus heißt *Isomorphismus*.

Beispiel. Sei $V = W = \mathbb{R}^n$ und $a \in \mathbb{R}$. Dann ist

$$f : \mathbb{R}^n \to \mathbb{R}^n,\ f(x) = ax$$

linear. (**Bild** $n = 1$, $n = 2$).

Beispiel. Sei $V = \mathbb{R}^n$, $W = \mathbb{R}^m$ mit $m \leq n$. Dann sind

$$\begin{aligned} p &: \mathbb{R}^n \to \mathbb{R}^m,\ (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_m) \\ i &: \mathbb{R}^m \to \mathbb{R}^n,\ (x_1, \ldots, x_m) \mapsto (x_1, \ldots, x_n, 0, \ldots, 0) \end{aligned}$$

linear. (**Bild** $n = 2$, $m = 1$).

Beispiel. Sei $V = \mathbb{R}^n$, $W = \mathbb{R}^m$. Dann ist für jede $m \times n$ Matrix A die Abbildung

$$\mathbb{R}^n \to \mathbb{R}^m, \quad x \mapsto A \cdot x$$

linear. Weiter unten werden wir sehen, dass sich jede lineare Abbildung als Matrix darstellen lässt.

Beispiel. Die Abbildung

$$L : P_n(\mathbb{R}) \to \mathbb{R}^{n+1}, \quad p \mapsto (p_0, p_1, \ldots, p_n)$$

ist linear. Die Abbildung ist bijektiv. D.h. es existiert eine Umkehrabbildung $L^{-1} : \mathbb{R}^{n+1} \to P_n(\mathbb{R})$, die einem Vektor $(a_1, a_2, \ldots, a_n, a_{n+1})$ das Polynom mit den Koeffizienten $p_0) = a_1, p_1 = a_2, \ldots, p_n = a_{n+1}$ zuordnet. D.h. anstelle im Vektorraum der Polynome zu rechnen, können wir auch zunächst L anwenden, dann im "vertrauten" $\mathbb{R}^{n+1}$ rechnen, um dann das Ergebnis mit L^{-1} nach $P_n(\mathbb{R})$ zurück zu überführen.

Dass sich im obigen Beispiel, die Betrachtungen von $P_n(\mathbb{R})$ auf $\mathbb{R}^{n+1}$ zurückführen lassen, ist kein Zufall, sondern dem liegt ein struktureller Satz zugrunde nämlich, dass zwei Vektorräume genau dann isomorph sind wenn sie die gleiche Dimension haben. Das hat insbesondere Konsequenz, dass alle n-dimensionalen Vektorräume bis auf Isomorphie gleich $\mathbb{R}^n$ sind.
Um diesen Satz zu beweisen brauchen wir noch etwas Vorbereitung.

Definition. Seien V, W Vektorräume und $L : V \to W$ linear. Dann heißt

$$\begin{aligned} \operatorname{Ker} L &:= \{v \in V \mid Lv = 0\} && \textit{Kern} \text{ von } L. \\ \operatorname{Bild} L &:= \{Lv \in W \mid v \in V\} && \textit{Bild} \text{ von } L. \end{aligned}$$

Theorem. *Seien V, W Vektorräume und $L : V \to W$ linear. Dann sind $\operatorname{Ker} L \subseteq V$ und $\operatorname{Bild} L \subseteq W$ Unterräume.*

Beweis. Wir haben zu zeigen, dass falls $v, v' \in \operatorname{Ker} L$ und $w, w' \in \operatorname{Bild} L$, so auch $r \cdot v + r' \cdot v' \in \operatorname{Ker} L$ und $r \cdot w + r' \cdot w' \in \operatorname{Bild} L$ für alle $r, r' \in \mathbb{R}$. Aufgrund der Linearität von L folgt

$$L(r \cdot v + r' \cdot v') = r \cdot Lv + r' \cdot Lv' = 0.$$

D.h. $(r \cdot v + r' \cdot v') \in \operatorname{Ker} L$.
Seien $w, w' \in \operatorname{Bild} L$ und $v, v' \in V$ mit $w = Lv$ und $w' = Lv'$. Dann gilt

$$r \cdot w + r' \cdot w' = r \cdot Lv + r' \cdot Lv' = L(r \cdot v + r' \cdot v').$$

□

Lemma. *Seien V, W Vektorräume und $L : V \to W$ linear. Dann ist L injektiv genau dann wenn $\operatorname{Ker} L = \{0\}$.*

Beweis. Angenommen $\operatorname{Ker} L \neq \{0\}$. Sei $v \in \operatorname{Ker} L$, $v \neq 0$. Dann gilt

$$L(-v) = -Lv = 0.$$

D.h. L ist nicht injektiv. Angenommen L ist nicht injektiv. Dann existieren $v_1 \neq v_2$ mit $Lv_1 = Lv_2$. Dann gilt

$$L(v_1 - v_2) = Lv_1 - Lv_2 = 0$$

Also $v_1 - v_2 \in \operatorname{Ker} L$ und somit $\operatorname{Ker} L \neq \{0\}$. □

Theorem. *Seien V, W endlich dimensionale Vektorräume und $L : V \to W$ linear. Dann gilt*

$$\dim V = \dim \operatorname{Bild} L + \dim \operatorname{Ker} L$$

Beweis. Angenommen $\dim W = n$ und $\dim \operatorname{Ker} L = k \leq n$. Sei $v_1, \ldots, v_k$ eine Basis von $\operatorname{Ker} L$ und wir ergänzen diese Basis mit $v_{k+1}, \ldots, v_n$ zu einer Basis von V. Dann gilt

$$\underbrace{\operatorname{span}\{v_1, \ldots, v_k\}}_{= \operatorname{Ker} L} \cap \operatorname{span}\{v_{k+1}, \ldots, v_n\} = \{0\}.$$

Dann gilt aufgrund der Linearität von L

$$\operatorname{span}\{Lv_{k+1}, \ldots, Lv_n\} = \operatorname{Bild} L$$

da für $x = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$ gilt

$$\begin{aligned} Lx &= L(\underbrace{x_1 \cdot v_1 + \ldots + x_k \cdot v_k}_{\in \operatorname{Ker} L}) + L(x_1 \cdot v_{k+1} + \ldots + x_n \cdot v_n) \\ &= 0 + L(x_1 \cdot v_{k+1} + \ldots + x_n \cdot v_n) \end{aligned}$$

Außerdem sind $Lv_{k+1}, \ldots, Lv_n$ linear unabhängig: Seien $r_{k+1}, \ldots, r_n \in \mathbb{R}$, so dass

$$0 = r_{k+1} \cdot Lv_{k+1} + \ldots + r_n \cdot Lv_n = L(r_{k+1} \cdot v_{k+1} + \ldots + r_n \cdot v_n)$$

d.h. $r_{k+1} \cdot v_{k+1} + \ldots + r_n \cdot v_n \in \operatorname{Ker} L$. Aus obiger Betrachtung folgt $r_{k+1} \cdot v_{k+1} + \ldots + r_n \cdot v_n = 0$ und da $v_{k+1}, \ldots, v_n$ linear unabhängig folgt $r_{k+1} = \ldots = r_n = 0$. Es folgt, dass $Lv_{k+1}, \ldots, Lv_n$ eine Basis von $\operatorname{Bild} L$ ist und somit $\dim \operatorname{Bild} L = n - k$. Es folgt also

$$\dim \operatorname{Ker} L + \dim \operatorname{Bild} L = k + (n - k) = n = \dim V.$$

□

Theorem. *Seien V, W Vektorräume. Dann gilt*

(a) *Es existiert ein injektiver Homomorphismus $L : V \to W$ genau dann wenn $\dim V \leq \dim W$.*
(b) *Es existiert ein surjektiver Homomorphismus $L : V \to W$ genau dann wenn $\dim V \geq \dim W$.*

Insbesondere existiert ein Isomorphismus $L : V \to W$ genau dann wenn $\dim V = \dim W$.

Beweis. (a) $\Longrightarrow$: Für einen injektiven Homomorphismus $L : V \to W$ gilt $\operatorname{Ker} L = \{0\}$. Also folgt nach dem Theorem oben

$$\dim V = \dim V - \underbrace{\dim \operatorname{Ker} L}_{=0} = \dim \operatorname{Bild} L \leq \dim W$$

da $\operatorname{Bild} L$ ein Unterraum von W ist.
(b) $\Longrightarrow$: Für einen injektiven Homomorphismus $L : V \to W$ gilt $\operatorname{Bild} L = W$. Also folgt

$$\dim V \geq \dim V - \dim \operatorname{Ker} L = \dim \operatorname{Bild} L = \dim W.$$

Angenommen .

Für die Rückrichtungen seien $v_1, \dots, v_n$ bzw. $w_1, \dots, w_m$ Basen von V bzw. W. Für einen Vektor $x \in V$ sei

$$x = x_1 \cdot v_1 + \ldots + x_n \cdot v_n$$

die Entwicklung in der Basis $v_1, \dots, v_n$. Wir definieren eine lineare Abbildung $L : V \to W$ via

$$L(x) = x_1 \cdot w_1 + \ldots + x_n \cdot w_n.$$

(a) $\Longleftarrow$: Sei $n = \dim V \geq \dim W = m$. Dann ist L injektiv, da die Entwicklung in einer Basis eindeutig ist.
(b) $\Longleftarrow$: Sei $n = \dim V \leq \dim W = m$. Dann ist L surjektiv, da $w_1, \dots, w_n$ eine Basis ist.
Das "insbesondere" folgt nun direkt aus (a) und (b). $\square$

Korollar 1. *Seien V, W endlich dimensionale Vektorräume,* $\dim V = \dim W$ *und $L : V \to W$ linear. Dann ist L ein Isomorphismus genau dann wenn* $\operatorname{Ker} L = \{0\}$.

Beweis. Sei nun L ein Isomorphismus. Dann ist L injektiv und nach Lemma oben also $\operatorname{Ker}\{0\} = 0$.
Sei $\operatorname{Ker} L = \{0\}$. Nach dem Lemma oben ist L injektiv. Außerdem folgt aus der Formel Nach dem Lemma oben gilt

$$\dim W = \dim V = \dim \operatorname{Ker} L + \dim \operatorname{Bild} L = \dim \operatorname{Bild} L.$$

Da $\operatorname{Bild} L \subseteq W$ folgt $\operatorname{Bild} L = W$ und somit ist L surjektiv. Also ist L ein bijektiver Homomorphismus. $\square$

Bemerkung. Für $L : V \to W$ mit $\operatorname{Ker} L = \{0\}$ gilt, dass L auf $\operatorname{Bild} L$ umkehrbar ist.

4. Skalarprodukte und Matrizen

Wir haben bereits gesehen, dass sich sobald wir in einem n-dimensionalen Vektorraum eine Basis gewählt haben, sich jeder Vektor als ein Vektor in $\mathbb{R}^n$ darstellen lässt.
In diesem Abschnitt werden wir zeigen, sich jede linearen Abbildung als Matrix darstellen lässt, sobald in den Vektorräumen Basen gewählt wurden.
Dafür ist der Begriff des Skalarprodukts nützlich.

Definition (Skalarprodukt). Sei V ein reeller Vektorraum. Eine Abbildung

$$V \times V \to \mathbb{R}, \quad (v, w) \mapsto \langle v, w \rangle$$

heißt Skalarprodukt,

(S1) $\langle u, r \cdot v + s \cdot w \rangle = r\langle u, v \rangle + s\langle u, w \rangle$ für alle $u, v, w \in V$ und $r, s \in \mathbb{R}$ (*bilinear*)
(S2) $\langle u, v \rangle = \langle v, u \rangle$ für alle $u, v \in V$ (*symmetrisch*)

(S3) $\langle v, v\rangle \geq 0$ und $\langle v, v\rangle = 0$ dann und nur dann wenn $v = 0$. (*positiv definit*)

Wir bezeichnen mit

$$|v| := \sqrt{\langle v, v\rangle}$$

die zu dem Skalarprodukt gehörige *Norm*.

Beispiel. Auf $\mathbb{R}^n$ ist das *Euklidische Skalarprodukt* gegeben durch

$$\langle u, v\rangle_n = u_1v_1 + u_2v_2 + \ldots + u_nv_n.$$

Mit diesem Skalarprodukt können Längen und Winkel beschrieben werden (**Bild Winkel**.
Sei $n = 1$. Dann ist $\langle v, u\rangle = u \cdot v$, $u, v \in \mathbb{R}$ und $|u| = \sqrt{u^2} = \begin{cases} u & : u \geq 0 \\ -u & : u < 0 \end{cases}$
Sei $n = 2$. Sei $v \in \mathbb{R}^2$, dann stellen wir fest, dass

$$|v| = \sqrt{\langle v, v\rangle_2} = \sqrt{v_1^2 + v_2^2}$$

gerade die Euklidische Länge des Vektors v darstellt.
Weiterhin seien $u, v \in \mathbb{R}^2$ mit $u, v \neq 0$

$$\begin{aligned} \langle u, v\rangle_2 &= u_1v_1 + u_2v_2 \\ &= \sqrt{u_1^2 + u_2^2}\sqrt{v_1^2 + v_2^2}\frac{u_1v_1 + u_2v_2}{\sqrt{u_1^2 + u_2^2}\sqrt{v_1^2 + v_2^2}} \\ &= |u||v| \cos \alpha(u, v) \end{aligned}$$

wobei $\alpha(u, v)$ gerade "der" Winkel zwischen u und v ist.
Für Vektoren in $\mathbb{R}^n$ gelten analoge Betrachtungen, so definiert $|v|$ ebenso die Euklidische Länge und $\langle u, v\rangle$ wird "der" Winkel beschrieben, den u und v in der von ihnen aufgespannten Ebene beschrieben.
Insbesondere stellen wir fest, wenn u und v senkrecht aufeinander stehen, d.h. ihr Winkel gerade $\pi/2$ ist (bzw. $3\pi/2$), dann ist $\langle u, b\rangle = 0$.

Bemerkung. Sei V ein Vektorraum mit Skalarprodukt und $v \in V$. Dann ist die Abbildung

$$V \to \mathbb{R},\ w \mapsto \langle v, w\rangle$$

linear.

Definition. Seien V, W endlich dimensionale Vektorräume, $v_1, \ldots, v_n$ eine Basis von V und $L : V \to W$ eine lineare Abbildung. Dann heißen die Vektoren $Lv_1, \ldots, Lv_n$ die *Zeilenvektoren* von L bzgl. $v_1, \ldots, v_n$.

Definition. Seien V, W endlich dimensionale Vektorraum, $v_1, \ldots, v_n$ bzw. $w_1, \ldots, w_m$ Basen in V bzw. W. Seien

$$\begin{aligned} &P : \mathbb{R}^n \to V,\ (x_1, \ldots, x_n) \mapsto x_1 \cdot v_1 + \ldots + x_n \cdot v_n \\ &Q : W \to \mathbb{R}^{mn},\ x_1 \cdot w_1 + \ldots + x_m \cdot w_m \mapsto (x_1, \ldots, x_m) \end{aligned}$$

und seien $e_1, \dots, e_n$ und $f_1, \dots, f_m$ die Standardbasen von $\mathbb{R}^n$ und $\mathbb{R}^m$ und sei $\langle \cdot, \cdot \rangle_m$ das Euklidische Skalarprodukt in $\mathbb{R}^m$. Für eine lineare Abbildung $L : V \to W$ ist

$$A_L := \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}$$

mit

$$a_{i,j} = \langle f_i, QLPe_j \rangle, \quad i = 1, \dots, m, \ j = 1, \dots, n,$$

die Matrixdarstellung von L bzgl. der Basen $v_1, \dots, v_n$ bzw. $w_1, \dots, w_m$ und $\langle \cdot, \cdot \rangle$. Wir identifizieren A_L mit der Abbildung

$$\mathbb{R}^n \to \mathbb{R}^m, x \mapsto A_L$$

Theorem. *In der Situation wie in der Definition oben gilt*

$$L = Q^{-1} \circ A_L \circ P^{-1}.$$

(Bild kommutatives Diagramm)

Definition. Für eine Matrix

$$A := \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix}$$

bezeichnen wir mit

$$a_1 = (a_{1,1}, \dots, a_{1,n}), \dots, a_m = (a_{m,1}, \dots a_{m,n})$$

die *Zeilenvektoren* von A und

$$a^{(1)} = \begin{pmatrix} a_{1,1} \\ \vdots \\ a_{m,1} \end{pmatrix}, \dots, a^{(n)} = \begin{pmatrix} a_{1,n} \\ \vdots \\ a_{m,n} \end{pmatrix}$$

die *Spaltenvektoren* von A.

Theorem. *Sei A ein $m \times n$ Matrix.*

(a) *A ist injektiv genau dann wenn die Spaltenvektoren linear unabhängig sind.*
(b) *A ist surjektiv genau dann wenn die Spaltenvektoren linear unabhängig sind.*
(c) *A ist bijektiv genau dann wenn $m = n$ und die Spalten- oder die Zeilenvektoren linear unabhängig sind.*

5. Eigenwerte und Eigenvektoren

DEFINITION (Eigenwerte und Eigenvektoren). Sei V ein Vektorraum und $L : V \to V$ linear. Ein Vektor $v \in V \setminus \{0\}$, heißt *Eigenvektor* zu einem *Eigenwert* $\lambda \in \mathbb{R}$ falls

$$Lv = \lambda v.$$

BEISPIEL. Für eine $n \times n$ Diagonalmatrix

$$\begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$$

sind die Eigenfunktionen gerade die Standardbasis $e_1, \ldots, e_n$ des $\mathbb{R}^n$ mit den zugehörigen Eigenwerten $d_1, \ldots, d_n$. Z.B. hat die Matrix

$$\begin{pmatrix} 1 & & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 42 \end{pmatrix}$$

gerade die Eigenwerte $1, 0, 42$.

BEMERKUNG. Ist v ein Eigenvektor einer Matrix zum Eigenwert λ, so ist auch jedes $\alpha \cdot v$, $\alpha \neq 0$, ein Eigenvektor. Sind weiterhin $v_1, \ldots, v_k$ Eigenvektoren zum gleichen Eigenwert λ so ist auch jeder Vektor aus $\operatorname{span}\{v_1, \ldots, v_k\} \setminus \{0\}$ ein Eigenvektor.

Die Eigenwerte für allgemeine Matrizen zu berechnen ist aufwendiger: Im Allgemeinen erhält man die Eigenwerte in dem man die Nullstellen des charakteristischen Polynoms der Matrix bestimmt. Nach Ermitteln der Eigenwerte läuft die Bestimmung der zugehörigen Eigenvektoren über die Lösung eines linearen Gleichungssystem.
Für den 2×2 kann man die Eigenwerte explizit ausrechnen.

LEMMA. *Eine* 2×2 *Matrix*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

hat zwei Eigenwerte λ_+ *und* λ_-

$$\lambda_\pm = \frac{a+d}{2} \pm \sqrt{\frac{(a+d)^2}{4} - (ad - bc)}$$

Beweis. Nachrechnen, dass für diese beiden Werte, die für die Eigenwertgleichung $Av = \lambda v$ eine Lösung $v \neq 0$ haben. □

BEISPIEL.

$$\begin{pmatrix} 1 & 5 \\ 1 & 1 \end{pmatrix}$$

hat die Eigenwerte $\lambda_\pm = 1 \pm \sqrt{5}$.

Folgendes Lemma liefert eine

DEFINITION. Eine $n \times n$ Matrix heißt *symmetrisch*, falls für ihre Matrixelemente $a_{k,l} = a_{l,k},\ k,l = 1,\dots,n$ gilt.

Allgemeiner gilt folgender Satz für symmetrische Matrizen.

THEOREM. *Sei L eine symmetrische $n \times n$ Matrix. Dann hat L genau n reelle Eigenwerte und die zugehörigen Eigenvektoren bilden eine Basis. Außerdem existiert eine bijektive Matirx U deren Spaltenvektoren Eigenvektoren sind, so dass*

$$L = U\Lambda U^{-1}.$$

wobei

$$\Lambda = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

die Diagonalmatrix aus den Eigenvektoren ist.

BEMERKUNG. Das Produkt AB zweier $n \times n$ Matrizen A und B bezeichnet gerade die Matrix die durch die Hintereinanderausführung beschreibt, d.h. $(AB)v = A(Bv)$. Man beachte, dass die Hintereinanderausführung im Allgemeinen nicht kommutativ ist.

BEMERKUNG. Die Multiplikation eines Vektors mit U aus obigem Theorem entspricht einem Basiswechsel von der Standardbasis in die Basis der Eigenvektoren. Damit gilt das L in der Basis der Eigenvektoren nichts anderes als Multiplikation mit einer Diagonalmatrix ist.

KAPITEL 4

Graphentheorie

Definition (Graph). Ein Graph G ist ein Paar (V, E) bestehend aus einer Menge V, deren Elemente die Vertizes (oder *Ecken* oder *Knoten*) genannt werden, und einer Menge E von zweielementigen Teilmengen von V, d.h.

$$E \subseteq \{\{v, w\} \mid v, w \in V, v \neq w\},$$

deren Elemente *Kanten* genannt werden.

Beispiel. Sei $V = \{1, 2, 3\}$ und $E = \{\{1, 2\}, \{2, 3\}, \{3, 1\}\}$. Bild.

Beispiel. Sei $V = \{1, 2, 3, 4, 5\}$ und $E = \{\{1, 3\}, \{3, 5\}, \{5, 2\}, \{2, 4\}, \{4, 1\}\}$. Bild.

Definition. Zwei Vertizes $v, w \in V$ heißen adjazent falls eine Kante $\{v, w\} \in E$ existiert. Man schreibt $v \sim w$.

Bemerkung. Die Adjazenzrelation ist symmetrisch. Sie ist anti-reflexiv, d.h. ein Vertex ist nie adjazent zu sich selbst. In der Regel ist sie nicht transitiv. Die einzige Ausnahme sind sogenannte vollständige Graphen wo jeder Vertex mit jedem durch eine Kante verbunden ist, d.h. $E \subseteq \{\{v, w\} \mid v, w \in V, v \neq w\}$. Ein Graph heißt endlich falls $\#V < \infty$.

Definition (Vertexgrad). Sei $G = (V, E)$ ein Graph. Dann heißt die Funktion $d : V \to \mathbb{N}$

$$d(v) = \#\{w \in V \mid \{v, w\} \in E\}$$

der *Vertexgrad* von v.

Lemma (Handschlag-Lemma). *Sei $G = (V, E)$ ein Graph mit $V = \{v_1, \ldots, v_n\}$. Dann gilt*

$$\sum_{k=1}^{n} d(v_k) = 2\#E$$

Beweis. Die Zahl $d(v)$ gibt gerade an wieviele Kanten von $v \in V$ ausgehen. Beim Summieren von $d(v)$ über die Vertizes wird jede Kante $\{v, w\} \in E$ genau zweimal gezählt, einmal als Kante die von v ausgeht und einmal als Kante die von w ausgeht. $\square$

Definition (Adjazenzmatrix). Sei $G = (V, E)$ ein Graph, so dass $V = \{v_1, \ldots, v_n\}$. Die Adjazenzmatrix des Graphen ist die $n \times n$ Matrix A mit den Elementen

$$A(k,l) = \begin{cases} 1 & : \{v_k, v_l\} \in E \\ 0 & : \text{sonst} \end{cases}$$

Bemerkung. Die Adjazenzmatrix ist eine symmetrische Matrix.

Bemerkung. Aus der Adjazenzmatrix lässt sich der Graph rekonstruieren.

Beispiel. Sei $V = \{1, 2, 3\}$ und $E = \{\{1, 2\}, \{2, 3\}, \{3, 1\}\}$.

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$$

Beispiel. Sei $V = \{1, 2, 3, 4, 5\}$ und $E = \{\{1, 3\}, \{3, 5\}, \{5, 2\}, \{2, 4\}, \{4, 1\}\}$.

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{pmatrix}$$

Eine weitere wichtige Matrix ist die sogenannte Laplacematrix.

Definition (Laplacematrix). Sei $G = (V, E)$ ein Graph, so dass $V = \{v_1, \ldots, v_n\}$. Die Laplacematrix des Graphen ist die $n \times n$ Matrix Δ mit den Elementen

$$\Delta(k,l) = \begin{cases} -1 & : \{v_k, v_l\} \in E \\ d(v_k) & : k = l \\ 0 & : \text{sonst} \end{cases}$$

Bemerkung. Bezeichnet D die Diagonalmatrix die als Einträge gerade die Vertexgrade hat, so gilt

$$\Delta = D - A.$$

Um zu berechnen wie die Adjazenz- und Laplacematrizen auf einen Graphen wirken ist folgende Konvention nützlich.

Notation. Sei $G = (V, E)$ ein Graph mit $V = \{v_1, \ldots, v_n\}$ und $x \in \mathbb{R}^n$. Die Summe über alle Komponenten x_k von x für die der Vertex v_k zu einem festen Vertex v_i adjazent ist bezeichnen wir mit

$$\sum_{k: v_k \sim v_i} x_k.$$

LEMMA. *Sei $G = (V, E)$ ein Graph mit $V = \{v_1, \dots, v_n\}$ und $x \in \mathbb{R}^n$. Dann gilt*

$$(Ax)_i = \sum_{k: v_k \sim v_i} x_k$$
$$(\Delta x)_i = d(v_i)x_i - \sum_{k: v_k \sim v_i} x_k = \sum_{k: v_k \sim v_i} (x_i - x_k).$$

DEFINITION. Zwei Graphen $G = (V, E)$ und $G' = (V', E')$ heißen *isomorph* wenn es eine bijektive Abbildung $F : V \to V'$ gibt, so dass $\{F(v), F(w)\} \in E'$ falls $\{v, w\} \in E$.

THEOREM. *Die Adjazenzmatrizen zweier isomorpher Graphen haben die gleichen Eigenwerte.*

Beweis. Zwei isomorphe Graphen haben bis auf umnummerieren der Komponenten die gleichen Adjazenzmatrizen. Eine entsprechende Umnummerierung der Eigenvektoren liefert gerade die gewünschte Gleichheit der Eigenwerte. □

BEMERKUNG. Die Aussage gilt ebenso für die Laplacematrizen zweier isomorpher Graphen.

BEMERKUNG. Eine wichtige Frage war ob man an der Gleichheit der Eigenwerte auch erkennt ob zwei Graphen isomorph sind. Dies ist nicht der Fall wie durch folgende Beispiele von Graphen nachgerechnet werden kann.

DEFINITION (Pfade und Zusammenhangskomponenten). . Sei $G = (V, E)$ ein Graph. Ein Tupel von Vertizes $(v_1, \dots, v_n)$ heißt ein Pfad von v nach w, falls $v = v_1$, $w = v_n$ und $\{v_1, v_2\}, \{v_2, v_3\}, \dots, \{v_{n-1}, v_n\} \in E$. Eine Teilmenge $W \subseteq V$ heißt *Zusammenhangskomponente*, wenn für alle Vertizes $v, w \in W$ ein Pfad von v nach w existiert und für alle Vertizes $v \in W$ und $w' \in V \setminus W$ kein Pfad existiert.

THEOREM. *Sei Δ die Adjazenzmatrix eines Graphen $G = (V, E)$ mit $\#V = n$. Dann gilt*

$$\dim\{x \in \mathbb{R}^n \mid \Delta x = 0\} = \#\{\textit{Zusammenhangskomponenten von } G\}.$$

Beweis. $\geq$: Sei $W \subseteq V$ eine Zusammenhangskomponente. Dann ist der Vektor $x \in \mathbb{R}^n$

$$x_i = \begin{cases} 1 & v_i \in W \\ 0 & v_i \in V \setminus W \end{cases}, \quad i = 1, \dots, n,$$

ein Eigenvektor zum Eigenwert 1. Denn

$$(\Delta x)_i = d(v_i)x_i - \sum_{k: v_k \sim v_i} x_k = \begin{cases} d(v_i) - d(v_i) = 0 & v_i \in W \\ 0 - 0 & v_i \in V \setminus W \end{cases}$$

Damit liefert jede Zusammenhangskomponente einen Vektor. Es ist leicht zu sehen, dass diese Vektoren unabhängig sind, da auf der Komponente jedes Vertizes genau eine den Wert 1 hat und alle anderen 0. Damit folgt, dass sie einen Unterraum von der Anzahl der Zusammenhangskomponenten aufspannen.
$\leq$: Dafür brauchen wir das Skalarprodukt auf $\mathbb{R}^n$. Sei $x \in \mathbb{R}^n$ mit $\Delta x = 0$. Dann gilt

$$\begin{aligned}
0 &= \sum_{i=1}^{n} (\Delta x)_i x_i \\
&= \sum_{i=1}^{n} (d(v_i) x_i - \sum_{k: v_k \sim v_i} x_k) x_i \\
&= \sum_{i=1}^{n} \sum_{k: v_k \sim v_i} (x_i - x_k) x_i \\
&= \frac{1}{2} \sum_{i=1}^{n} \sum_{k: v_k \sim v_i} (x_i - x_k) x_i + \frac{1}{2} \sum_{k=1}^{n} \sum_{i: v_i \sim v_k} (x_k - x_i) x_k \\
&= \frac{1}{2} \sum_{i=1}^{n} \sum_{k: v_k \sim v_i} (x_i - x_k)^2
\end{aligned}$$

Da Quadrate immer positiv sind, müssen die Differenzen auf der rechten Seite immer 0 sein. D.h. $x_i = x_k$ falls $v_i \sim v_k$. Das bedeutet aber gerade, dass x auf einer Zusammenhangskomponente konstant ist.

$\square$

KAPITEL 5

Analysis

Analysis ist die Kunst Grenzwerte zu bilden. Elliott Lieb.

In diesem Kapitel beschäftigen wir uns mit Grenzwerten von Reihen und Folgen.

1. Grenzwerte von Folgen

DEFINITION (Folge). Eine Abbildung $\mathbb{N} \to \mathbb{R}, n \mapsto x_n$ heißt *Folge*. Wir bezeichnen die Folge mit (x_n) oder $(x_n)_{n\in\mathbb{N}}$.

BEISPIEL.
- Sei $c \in \mathbb{R}$. Dann heißt die Folge (x_n) mit $x_n = c$, $n \in \mathbb{N}$ *konstante Folge*.
- Sei $x_n = (-1)^n$ Dann ist $x_n = 1$ für $n \in 2\mathbb{N}$ und $x_n = -1$ für $n \in 2\mathbb{N} + 1$ und (x_n) heißt *alternierende Folge*.
- $x_n = n$, $n \in \mathbb{N}$.
- $x_n = p_n$ wobei p_n die n-te Primpzahl ist, $n \in \mathbb{N}$.
- $x_n = \frac{1}{n}$, $n \in \mathbb{N}$.
- Sei $a \geq 0$ und $x_n = a^n$, $n \in \mathbb{N}$.
- Sei $a \in \mathbb{R}$ und $x_n = (1 + a/n)^n$.

Bilder: Folge als Funktion,

DEFINITION (Konvergenz). Eine Folge (x_n) heißt *konvergent* gegen $x \in \mathbb{R}$ falls für alle $\varepsilon > 0$ ein $N \in \mathbb{N}$ existiert, so dass $|x - x_n| < \varepsilon$ für alle $n \in \mathbb{N}$. In diesem Fall heißt x der *Grenzwert* der Folge und wir schreiben

$$\lim_{n\to\infty} x_n = x \quad \text{oder} \quad x_n \to x,\, n \to \infty.$$

Ist eine Folge nicht konvergent, so heißt sie *divergent*.

BEMERKUNG. Anschaulich bedeutet Konvergenz einer Folge (x_n) gegen x, dass sie x beliebig nahe kommt, wenn man nur n groß genug wählt.

Bilder: Schlauch, Falle

BEISPIEL.
- Die konstante Folge $x_n = c$, $n \in \mathbb{N}$ ist konvergent mit Grenzwert c.
  Beweis. Sei $\varepsilon > 0$. Dann gilt für $N = 1$, dass $|x_n - c| = 0 < \varepsilon$ für $n \geq 1$. □

- Die alternierende Folge $x_n = (-1)^n$, $n \in \mathbb{N}$ ist divergent.
  Beweis. Sei $x \in \mathbb{R}$ beliebig und $\varepsilon = 1$. Sei $n \in 2\mathbb{N}$. Dann ist $|x_n - x| = |1-x| \geq 1 = \varepsilon$ falls $x \leq 0$ oder $|x_{n+1} - x| = |x-1| \geq 1 = \varepsilon$ falls $x > 0$. □

- $x_n = n$, $n \in \mathbb{N}$ ist divergent.
  Beweis. Sei $x \in \mathbb{R}$ beliebig und $\varepsilon = 1$. Für alle $n \geq x + 1$ gilt $|x_n - x| = |n - x| \geq 1 = \varepsilon$. □

- $x_n = n$-te Primzahl, $n \in \mathbb{N}$ ist divergent.
  Beweis. Analog wie $x_n = n$, $n \in \mathbb{N}$. □

- $x_n = \frac{1}{n}$, $n \in \mathbb{N}$ ist konvergent gegen $x = 0$.
  Beweis. Sei $\varepsilon > 0$. Wähle $N \in \mathbb{N}$ mit $N > 1/\varepsilon$. Dann gilt $|x_n - 0| = 1/n < \varepsilon$, $n \geq N$. □

Bemerkung. Anschaulich machen die Beispiele deutlich, dass es zwei Gründe geben kann warum eine Folge nicht konvergiert:

1. Die Folge nähert sich keinem Wert, z.B. $x_n = n$.
2. Die Folge nähert sich zu vielen Werten, z.B. $x_n = (-1)^n$.

Wir fassen einen Spezialfall des ersten Falls in einer eigenen Definition.

Definition. Eine Folge (x_n) heißt *bestimmt divergent* gegen ∞ (bzw. $-\infty$) falls für alle $C \in \mathbb{R}$ ein N existiert mit $x_n \geq C$ (bzw. $x_n \leq C$) für alle $n \geq N$. In diesem Fall schreiben wir

$$\lim_{n\to\infty} x_n = \infty \quad \text{oder} \quad x_n \to \infty,\, n \to \infty,$$
$$(\text{bzw. } \lim_{n\to\infty} x_n = -\infty \quad \text{oder} \quad x_n \to -\infty,\, n \to \infty).$$

Beispiel. Die Folgen $x_n = n$ bzw. $y_n = -n$ sind bestimmt divergent gegen ∞ bzw. $-\infty$. Die Folge $z_n = (-1)^n n$ hingegen ist nicht bestimmt divergent.

Bemerkung. Konvergenz ist eine Eigenschaft, die erst "weit draußen" entschieden wird. D.h. die ersten Folgeglieder sind für die Betrachtungen irrelevant. Z.B. haben zwei Folgen die sich nur an endlich vielen Stellen unterscheiden die gleichen Konvergenzeigenschaften.

Um die Konvergenz weiterer Folgen zu untersuchen, beweisen wir nun einen Satz.

Theorem (Sandwich-Theorem). *Seien (y_n) und (z_n) gegen x konvergente Folgen. Sei (x_n) eine Folge für die ein n_0 existiert mit*

$$y_n \leq x_n \leq z_n, \quad n \geq N.$$

Dann ist (x_n) konvergent und es gilt

$$\lim_{n\to\infty} x_n = x.$$

Beweis. Sei $\varepsilon > 0$. Da $y_n \to x$ und $z_n \to x$ existiert $N \geq 0$ so dass

$$|y_n - x| < \varepsilon \quad \text{und} \quad |z_n - x| < \varepsilon, \qquad n \geq N$$

und insbesondere

$$y_n - x > -\varepsilon \quad \text{und} \quad z_n - x < \varepsilon, \qquad n \geq N.$$

Ohne Einschränkung sei $N \geq n_0$. Dann folgt

$$-\varepsilon < y_n - x \leq x_n - x \leq z_n - x < \varepsilon, \qquad n \geq N.$$

und somit

$$|x_n - x| < \varepsilon, \qquad n \geq N.$$

□

Bemerkung. Das Theorem wird angewendet in dem man eine komplizierte Folge (x_n) nach oben und unten durch Folgen (y_n) und (z_n) abschätzt, für die man die Konvergenzeigenschaften kennt.

Für bestimmt divergente Folgen gibt es eine Variante des Sandwich-Theorems.

Theorem (Variante Sandwich-Theorem).

(a) *Sei (y_n) bestimmt gegen ∞ divergiert und sei (x_n) eine Folge für die ein $N \geq 0$ existiert, so dass $x_n \geq y_n$ für $n \geq N$. Zeigen Sie, dass (x_n) bestimmt gegen ∞ divergiert.*

(b) *Sei (z_n) bestimmt gegen $-\infty$ divergiert und sei (x_n) eine Folge für die ein $N \geq 0$ existiert, so dass $x_n \leq z_n$ für $n \geq N$. Zeigen Sie, dass (x_n) bestimmt gegen ∞ divergiert.*

Beweis. Übung. □

Beispiel. $x_n = a^n$, $n \in \mathbb{N}$, konvergiert für $0 < a < 1$ gegen 0, für $a = 1$ gegen 1 und divergiert bestimmt gegen ∞ für $a > 1$.

Beweis. Die Aussage für $a = 1$ ist klar, da $x_n = 1^n = 1$.
Für den Beweis von $a > 1$ verwenden wir die Bernoulli-Ungleichung, die sich leicht mit vollständiger Induktion beweisen lässt: Für $r \geq -1$ gilt

$$(1 + r)^n \geq 1 + nr.$$

Damit folgt für $a > 1$, dass

$$x_n = a^n = (1 - (a + 1))^n \geq 1 + n(a + 1) =: z_n$$

Da (z_n) bestimmt gegen ∞ divergiert so auch (x_n). Für den Fall $0 < a < 1$ betrachten wir $b := 1/a > 1$ und die Folge $1/x_n = b^n$. Aus den Betrachtungen gerade eben folgt, dass $(1/x_n)$ bestimmt divergiert. Somit konvergiert $(x_n) = (1/(1/x_n))$ gegen 0. □

Beispiel. Sei $n! = 1 \cdot \ldots \cdot n$ und betrachte $x_n = 2^n/n!$, $n \geq 1$. Dann konvergiert (x_n) gegen 0.
Beweis. Offensichtlich $x_n \geq 0$. Setze also $y_n = 0$. Weiterhin gilt

$$x_n = \frac{2}{1} \cdot \frac{2}{2} \cdot \frac{2}{3} \cdot \ldots \cdot \frac{2}{n-1} \cdot \frac{2}{n} \leq 4\frac{1}{n} =: z_n$$

Von z_n wissen wir $z_n \to 0$. □

Wir kommen nun zu einem nächsten Konvergenzkriterium. Dafür brauchen wir die Begriffe der Monotonie und Beschränktheit von Folgen.

Definition (Beschränktheit). Eine Folge (x_n) heißt *beschränkt*, falls ein $C \geq 0$ existiert, so dass

$$-C \leq x_n \leq C, \quad n \in \mathbb{N}.$$

Beispiel. Die konstante und alternierende Folge sind beschränkt, (wähle $C = c$ bzw. $C = 1$.) ebenso $(1/n)$. Die Folge $x_n = n$ ist unbeschränkt und ebenso $x_n = (-1)^n$.

Definition (Monotonie). Eine Folge (x_n) heißt *monoton fallend* (bzw. *monoton wachsend*) falls

$$x_n \geq x_{n+1} \quad (\text{bzw. } x_n \leq x_{n+1}) \quad n \in \mathbb{N}.$$

Beispiel. Die konstante Folge ist sowohl monoton fallend und monoton wachsend. Die alternierende Folge ist nicht monoton. Die Folge $(1/n)$ ist monoton fallend. Die Folge $x_n = n$ ist monoton wachsend.

Theorem. *Sei (x_n) eine beschränkte, monoton fallende (bzw. monoton wachsende) Folge. Dann ist (x_n) konvergent.*

Beweis. Angenommen (x_n) ist beschränkt und monoton wachsend. Wir bezeichnen die kleinste obere Schranke der Menge

$$M := \{x_n \mid n \in \mathbb{N}\}$$

mit s. Da (x_n) beschränkt ist, gilt $s < \infty$. Angenommen es existiert ein $\varepsilon > 0$, so dass für alle $n \geq 0$

$$s - x_n = |s - x_n| \geq \varepsilon$$

Dann gilt

$$s - \varepsilon \geq x_n$$

Damit ist $s - \varepsilon$ eine kleinere obere Schranke an M. Das ist ein Widerspruch dazu, dass s die kleinste obere Schranke ist.
Der Beweis für monoton fallende Folgen ist analog mittels der größten unteren Schranke der Menge M. □

Bemerkung. Der Beweis des obigen Satzes stützt sich auf die Existenz von kleinste oberen Schranken von beschränkten Mengen in $\mathbb{R}$. Das ist in der Tat eine charakteristische Eigenschaft der reellen Zahlen.

Bemerkung. Der Satz ist auch in sofern bemerkenswert, da er eine bloße Existenzaussage eines Grenzwertes ist. Im Gegensatz zum Sandwich-Theorem liefert er keine direkte Möglichkeit den Grenzwert zu berechnen.

Beispiel (Einfache Beispiele). Der Satz ist z.B. auf die Folge

$$x_n = \frac{1}{\sqrt{n}}$$

anwendbar, da die Folge (x_n) ist monoton fallend und von unten durch 0 und von oben durch 1 beschränkt.
Der Satz ist nicht anwendbar auf die Folge

$$x_n = (-1)^n, \quad n \in \mathbb{N},$$

da die Folge zwar beschränkt ist aber nicht monoton.
Der Satz ist nicht anwendbar auf die Folge

$$x_n = n, \quad n \in \mathbb{N},$$

da die Folge zwar monoton wachsend ist aber nicht beschränkt.

Beispiel. Der Umfang von regelmäßigen in den Kreis mit Radius 1 einbeschriebenen Polygonen konvergiert gegen 2π. Diese Approximation von π geht auf Archimedes zurück. (**Bild**)

Beispiel (Koch-Kurve). Die Länge der Koch-Kurve ist unendlich. Zwar ist die Folge (L_n) der approximierenden Längen monoton wachsend, allerdings ist die Folge nicht beschränkt da der Streckenzug bei jedem Iterationsschritt um den Faktor 4/3 länger wird, d.h.

$$L_{n+1} = \frac{4}{3} L_n = \left(\frac{4}{3}\right)^{n+1}.$$

Der Flächenhalt ist hingegen endlich. Das werden wir später zeigen.

Beispiel (Goldene Schnitt). Der Goldene Schnitt bezeichnet ein Verhältnis Φ von zwei Zahlen a und b für welches gilt

$$\frac{a+b}{a} = \frac{a}{b} =: \Phi.$$

Er beschreibt das ein Teilungsverhältnis von zwei Strecken bei dem das Verhältnis des Ganzen zu seinem größeren Teil a dem Verhältnis des größeren zum kleineren Teil b entspricht. Umstellen der Gleichung

$$\frac{a}{b} - 1 - \frac{b}{a} = 0$$

beziehungsweise mit $\frac{a}{b} = \Phi$ wie folgt:

$$\Phi - 1 - \frac{1}{\Phi} = 0\,.$$

Multiplikation mit Φ ergibt die quadratische Gleichung

$$\Phi^2 - \Phi - 1 = 0$$

mit den beiden Lösungen $\frac{1\pm\sqrt{5}}{2}$ von denen die positive gerade Φ ist.
Es besteht ein Zusammenhang zwischen Φ und der Folge (f_n) der Fibonacci-Zahlen

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots$$

die gerade durch die Rekursionsformel

$$f_1 = 1,\ f_2 = 1 \qquad f_{n+2} = f_{n+1} + f_n,\ n \geq 1$$

geben ist: Die Rekursionsformel liefert gerade

$$\varphi_n := \frac{f_{n+2}}{f_{n+1}} = \frac{f_{n+1} + f_n}{f_{n+1}} = 1 + \frac{f_n}{f_{n+1}} = 1 + \frac{1}{\varphi_{n-1}} = 1 + \frac{1}{1 + \frac{1}{\varphi_{n-2}}}.$$

Diese Folge (φ_{2n}) ist monoton wachsend (!) und (φ_{2n+1}) ist monoton fallend (!). Beide Folgen sind durch 0 und 2 von unten und oben beschränkt. Damit existieren Grenzwerte

$$\Phi_1 := \lim_{n\to\infty} \varphi_{2n}, \qquad \Phi_2 := \lim_{n\to\infty} \varphi_{2n+1}.$$

Da beide die obige Gleichung

$$\Phi = 1 + \frac{1}{1 + \frac{1}{\Phi}} \quad \Leftrightarrow \quad \Phi - 1 - \frac{1}{\Phi} = 0.$$

erfüllen. Somit folgt $\Phi = \Phi_1 = \Phi_2$.

Wir betrachten jetzt eine wichtige Funktion, die über den Grenzwert von Folgen definiert wird.
Die Zahl e spielt bei kontinuierlichen Wachstumsvorgängen eine Rolle, z.B. stetige Verzinsung: Kapital A Zinsatz 100 Prozent. Dann hat man nach einem Jahr bei

- 0 mal (äquidistant) Abheben und Einzahlen : $A(1 + 1)$
- 1 mal (äquidistant) Abheben und Einzahlen: $A(1 + 1/2)(1 + 1/2)$
- 2 mal (äquidistant) Abheben und Einzahlen: $A(1 + 1/3)(1 + 1/3)(1 + 1/3)$
- etc.

Dieser Prozess wird durch die Exponentialfunktion beschrieben.

Theorem (Exponentialfunktion). *Sei $x \in \mathbb{R}$. Die Folge $((1 + x/n)^n)$ konvergiert und wir bezeichnen*

$$e^x := \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n.$$

Es gilt

$$\begin{aligned} e^0 &= 1 \\ e^{x+y} &= e^x e^y, \quad , x, y \in \mathbb{R}, \\ e^{-x} &= \frac{1}{e^x}. \end{aligned}$$

Bemerkung. Beachte. $1+\frac{1}{n}\to 1$, aber $a^n\to\infty$ für $a>1$. Die Frage ist also, welcher Effekt sich durchsetzt.

Für den Beweis brauchen wir noch etwas Vorbereitung. Dafür beweisen wir drei Lemmas, die alle auch unabhängig von der Definition der Exponentialfunktion an vielen Stellen der Mathematik auftauchen und eine große Rolle spielen.
Das erste Hilfslemma ist die Bernoullische Ungleichung.

Lemma (Bernoulli Ungleichung). *Für $x\geq -1$ und $n\in\mathbb{N}$ gilt*

$$(1+x)^n\geq 1+nx.$$

Beweis. Induktion nach n.
$n=1$: $1+x=1+x$.
$n\Longrightarrow n+1$:

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n\\ (\text{Induktionsannahme, } 1+x\geq 0) &\geq (1+x)(1+nx)\\ &= 1+(n+1)x+x(nx)\\ &\geq 1+(n+1)x. \end{aligned}$$

□

Das zweite Hilfslemma ist der Binomische Satz. Um diesen zu formulieren brauchen wir noch zwei neue Notationen. Die erste ist das Summenzeichen.

Notation (Summe). Seien $x_1,\dots,x_n$ Zahlen so bezeichnen wir die Summe dieser Zahlen mit

$$\sum_{i=1}^{n} x_i := x_1+x_2+\ldots+x_n.$$

Die zweite ist der Binominialkoeffizient.

Notation. Für ganze Zahlen $0\leq k\leq\leq n$ bezeichnet

$$\left(\begin{array}{c} n\\ k\end{array}\right) := \frac{n!}{(n-k)!k!}.$$

den Binominialkoeffizienten und wir sprechen "n über k".

Bemerkung. Man kann leicht mit vollständiger Induktion zeigen, dass $\left(\begin{array}{c} n\\ k\end{array}\right)$ gerade die Anzahl der Möglichkeiten ist um k Elemente aus einer n-elementigen Menge auszuwählen. Inbesondere gilt die Rekursionsformel:

$$\binom{n}{k}+\binom{n}{k-1}=\binom{n+1}{k}.$$

Diese Rekursionsformel folgt direkt: Sei eine $n+1$ elementige Menge gegeben. Sei ein Element p aus dieser Menge fixiert. Dann gibt es $\binom{n}{k-1}$

k-elementige Teilmengen die p enthalten und $\binom{n}{k}$ k-elementige Teilmengen, die p nicht enthalten. (Zeichnung: n weiße Kugeln und eine schwarze Kugel ....)

Lemma (Binomische Satz). *Sei $n \in \mathbb{N}$ und $x, y \in \mathbb{R}$. Dann gilt*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Beweis. Wir beweisen die Aussage mit Induktion:
$n = 1$: Klar.

$n \Longrightarrow (n+1)$: Direkte Rechnung liefert

$$(x+y)^{n+1} \quad = (x+y)(x+y)^n = (x+y) \textstyle\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

(Dabei folgt die letzte Gleichung aus der Induktionsannahme für n.) Damit können wir weiter rechnen

$$\begin{aligned}
\ldots \quad &= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1} \\
(k \rightsquigarrow k-1) \quad &= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n-k+1} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1} \\
(\text{Rekursion}) \quad &= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^k y^{n-k+1} + y^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}.
\end{aligned}$$

Damit ist der Beweis abgeschlossen. □

Als letztes benötigen wir noch die geometrische Summenformel.

Lemma (Geometrische Summenformel). *Seien $x, y \in \mathbb{R}$ mit $x \neq y$. Dann gilt für jedes $n \in \mathbb{N}$*

$$\frac{x^n - y^n}{x - y} = \sum_{k=0}^{n-1} x^k y^{(n-1)-k} = \sum_{k=0}^{n-1} y^k x^{(n-1)-k}.$$

Insbesondere gilt für $q \neq 1$ und $n \in \mathbb{N}_0$ die Formel

$$\sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}.$$

Beweis. Wir rechnen

$$\begin{aligned}(x-y)\sum_{k=0}^{n-1}x^k y^{(n-1)-k} &= \sum_{k=0}^{n-1}x^{k+1}y^{(n-1)-k}-\sum_{k=0}^{n-1}x^k y^{n-k}\\ \text{(Teleskopsumme)} &= \sum_{k=1}^{n}x^k y^{n-k}-\sum_{k=0}^{n-1}x^k y^{n-k}\\ &= x^n-y^n.\end{aligned}$$

Die zweite Gleichheit folgt durch Vertauschen von x und y. Das 'Inbesondere' folgt mit $x=1$ und $y=q\neq 1$. □

Wir kommen nun zum Beweis des Satzes für den Grenzwert der die Exponentialfunktion definiert
Beweis. Wir zeigen die Existenz des Grenzwertes für $x=1$. Der allgemeine Fall lässt sich mit geringfügigen Modifikation beweisen.
Sei

$$x_n=\left(1+\frac{1}{n}\right)^n$$

Wir zeigen, dass (y_n) wachsend und beschränkt ist. Die Bernoulli Ungleichung liefert

$$\left(1+\frac{1}{n}\right)^n\left(1-\frac{1}{n}\right)^n=\left(1-\frac{1}{n^2}\right)^n\geq\left(1-\frac{x}{n}\right)$$

also

$$x_n=\left(1+\frac{1}{n}\right)^n\geq\frac{\left(1-\frac{1}{n}\right)}{\left(1-\frac{1}{n}\right)^n}=\frac{1}{\left(1-\frac{1}{n}\right)^{n-1}}=\left(\frac{n}{n-1}\right)^{n-1}=\left(1+\frac{1}{n-1}\right)^{n-1}$$
$$=x_{n-1}$$

für alle $n\geq 2$. Die Folge (x_n) ist also monoton wachsend. Die Folge (x_n) ist beschränkt durch 3:

$$
\begin{aligned}
x_n &= \left(1+\frac{1}{n}\right)^n \\
\text{(Binomischer Satz)} \quad &= \sum_{k=0}^{n} \binom{n}{k} \frac{1}{n^k} \\
&= 1+\sum_{k=1}^{n} \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}\frac{1}{n^k} \\
\text{(Umsortieren)} \quad &= 1+\sum_{k=1}^{n} \frac{n(n-1)\dots(n-k+1)}{n\dots n}\frac{1}{k!} \\
&\leq 1+\sum_{k=1}^{n} \frac{1}{k!} \\
\text{(Induktion: } k! \geq 2^{k-1}) \quad &\leq 1+\sum_{k=1}^{n} \frac{1}{2^{k-1}} \\
\text{(Geometrische Summe)} \quad &\leq 1+\frac{1-(1/2)^{n+1}}{1-1/2} \leq 3.
\end{aligned}
$$

Damit damit ist $x_n = \left(1+\frac{1}{n}\right)^n$ monoton wachsend und beschränkt. Nach dem Theorem oben konvergiert (x_n) gegen einen Grenzwert. Der Fall für $x \geq 0$ und $x \neq 1$ folgt analog bis auf den vorletzten Schritt in der letzten Ungleichungskette.
Die Aussage $e^0 = 1$ ist klar, da $(1+\frac{0}{n})^n = 1$ für alle n.
Die Gleichung $e^x = 1/e^{-x}$ lässt sich wie folgt sehen

$$\left(1+\frac{x}{n}\right)^n\left(1+\frac{(-x)}{n}\right)^n = \left(1-\frac{x^2}{n^2}\right)^n = \left(1-\frac{(x^2/n)}{n}\right)^n = \dots$$

Ebenso $e^{x+y} = e^x e^y$

$$\left(1+\frac{x}{n}\right)^n\left(1+\frac{y}{n}\right)^n = \left(1+\frac{x+y}{n}+\frac{xy}{n^2}\right)^n = \left(1-\frac{(x^2/n)}{n}\right)^n = \dots$$

□

2. Reihen

Wir betrachten nun eine spezielle Form von Folgen sogenannte Reihen.

Definition (Reihe). Seien $a_n \in \mathbb{R}$, $n \in \mathbb{N}$. Wir nennen die Folge

$$x_n = \sum_{k=1}^{n} a_k = a_1 + a_2 + \ldots + a_n$$

die zu (a_n) gehörige *Reihe*. Wir sagen die Reihe konvergiert, falls (x_n) konvergiert.

Beispiel (Geometrische Reihe). Sei $q \in \mathbb{R}$. Wir haben gezeigt, dass für $q \neq 1$ und $n \in \mathbb{N}_0$ die Formel gilt

$$x_n := \sum_{k=0}^{n} q^k = \frac{1-q^{n+1}}{1-q}$$

und für $q = 1$ gilt

$$x_n := \sum_{k=0}^{n} q^k = n+1$$

Wir nennen die Folge (x_n) die geometrische Reihe und stellen fest, dass (x_n) genau dann konvergiert wenn $-1 < q < 1$.

Beispiel (Koch-Kurve). Wir haben gesehen, dass die Länge der Koch-Kurve unendlich ist. Ihr Flächenhalt ist hingegen endlich: Angenommen das Dreieck unterhalb der ersten Iteration hat den Flächeninhalt $F_1 = 1$. Bei der zweiten Iteration kommt an jeder der 4 Strecken ein Dreieck mit Flächeninhalt 1/9 hinzu, d.h. $F_2 = F_1 + 4\frac{1}{9}$, und bei der n-ten Iteration kommt ein Flächeninhalt von $4^{n-1} \cdot (1/9)^{n-1}$ hinzu, d.h.

$$\sum_{n=0}^{\infty} \left(\frac{4}{9}\right)^n = \frac{1}{1-4/9} = \frac{9}{5}.$$

Beispiel. $x_n = \sum_{k=2}^{n} \frac{1}{k(k-1)}$ konvergiert gegen 1:

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

Beispiel (Harmonische Reihe). $x_n = \sum_{k=1}^{n} 1/k$ ist divergent (**obwohl** $\frac{1}{n} \to 0$):

$$1+1/2+\underbrace{(1/3+1/4)}_{\geq\frac{1}{2}}+\underbrace{(1/5+\ldots+1/8)}_{\geq\frac{1}{2}}+\ldots+\underbrace{\left(\frac{1}{2^n+1}+\ldots+\frac{1}{2^{n+1}}\right)}_{\geq\frac{1}{2}}\ldots.$$

Theorem (Exponentialfunktion - revisited). *Für alle $x \in \mathbb{R}$ gilt*

$$e^x := \lim_{n\to\infty} \left(1+\frac{1}{n}\right)^n = \sum_{k=0}^{\infty} \frac{x^n}{n}.$$

Insbesondere konvergiert die Reihe auf der rechten Seite.